crowell moring

# ISRAEL PRACTICE NEWSLETTER

## INSIDE THIS ISSUE




VOLUME 2 | ISSUE 4 | SUMMER 2016


## **Foreign Companies Operating in the U.S.:** Product Discounts Given Outside the U.S. Can Present Corruption Risks Under U.S. Law

*By Thomas A. Hanusik and Derek A. Hahn*

Before he was sentenced to 22 months in prison, Vincente Garcia had an important position at SAP International Inc. (SAP): Vice-President of Global and Strategic Accounts in Latin America. He used that position to orchestrate $145,000 in bribes to Panamanian officials for the award of government technology contracts.

The key to his bribery scheme: excessive discounts on sales of SAP software.

How did Garcia convert software discounts into bribes? The answer: indirect sales. In the technology sales channel suppliers sometimes sell products "indirectly" to a customer through a local partner, often a distributor or reseller. The local partner purchases the products from the supplier, then resells them to the customer at a higher price.

Technology companies routinely provide discounts to their local partners for legitimate business reasons—like beating the competition for a particular deal. The local partners are expected to pass the additional discounts on to the customer in order to lower the ultimate sale price and win the contract.

Garcia's scheme involved granting excessive discounts for certain indirect sales to the government of Panama. The local partner purchased products from the supplier at the excessively discounted price. But instead of passing the discount on the government customer, the partner used the extra margin for improper purposes: (i) to pay bribes to the Panamanian officials who awarded the contracts; and (ii) to pay kickbacks to Garcia.

Garcia's conduct eventually came to the attention of the U.S. Department of Justice (DOJ) and Securities and Exchange Commission (SEC). Garcia pled guilty to conspiring to violate the Foreign Corrupt Practices Act (FCPA) and separately settled with the SEC and paid $85,965 in disgorgement of the kickbacks he received (plus prejudgment interest). SAP International's parent company SAP SE settled with the SEC for $3,700,000 in disgorgement (plus prejudgment interest), representing the "ill-gotten gains" from

the contracts procured through the bribery scheme. While Garcia and SAP were ordered to cease and desist from future violations, neither was assessed a civil monetary penalty.

The SEC held SAP accountable even while acknowledging that Garcia (1) concealed his scheme from others at SAP, (2) falsified internal approvals for the discounts, and (3) otherwise circumvented SAP's internal controls (perhaps explaining why SAP paid no civil monetary penalty). The SEC found that SAP did not have adequate internal controls under the FCPA because: employees had "wide latitude" to approve discounts, explanations for discounts were accepted without verification, and large discounts were not subject to heightened anti-corruption scrutiny.

Takeaway: The cases against Garcia and SAP are part of a larger wave of anti-corruption enforcement by authorities across the globe. U.S. authorities continue to push the jurisdictional bounds of the FCPA, targeting not only U.S. domestic concerns and issuers, but also foreign companies and foreign nationals who engage in related conduct in the U.S. Other countries are ramping up their anti-corruption enforcement as well.

Companies in the technology sales channel can mitigate the risks of corruption by adopting appropriate internal controls. Those controls should be tailored to the company's specific business model and risk profile. For technology companies making indirect sales, the cases against Garcia and SAP demonstrate that internal controls over discounts are an important component of an effective anti-corruption compliance program.


***Thomas A. Hanusik*** *is a partner and co-chair of the firm's White Collar & Regulatory Enforcement Group. Tom's practice focuses on white-collar defense, SEC Enforcement, FINRA Enforcement and internal investigations.*

***Derek A. Hahn*** *is a counsel in the firm's Orange County, California office. His practice focuses on white-collar defense, internal investigations, complex litigation, and compliance counseling.*


## **Deal Note:** Crowell & Moring Advises GigPeak, Inc. on Underwritten Public Offering

**Washington, D.C. – June 15, 2016:** GigPeak, Inc., a leading innovator of semiconductor ICs and software solutions for high-speed connectivity and high-quality video compression over the Network and the Cloud, today announced the closing of its underwritten public offering of an aggregate of 13,194,643 newly issued shares of common stock at a price to the public of $2.00 per share. GigPeak received net proceeds to the Company of approximately $24.8 million after underwriting discounts and commissions. In addition, certain officers and directors of the Company as well as certain stockholders of the Company, as selling stockholders, sold 1,180,357 shares of previously issued shares of common stock in the underwritten public offering at a price of $2.00 per share. GigPeak received no proceeds from the sale of shares by the selling stockholders.

Crowell & Moring served as lead legal counsel to GigPeak in this transaction, and the team included Jeffrey C. Selman, Joshua Reynolds, Karen Kopel, Ilana Lubin, and Kelly Howard.

# In the News

## **Icon of IP:** Crowell & Moring's Terry Rea

*By Matthew Bultman*

*Law360, New York (June 3, 2016, 5:12 PM ET)* -- When Crowell & Moring LLP partner Teresa Stanek Rea became the deputy director of the U.S. Patent and Trademark Office in spring 2011, she knew Congress was considering landmark legislation that could overhaul the nation's patent system.

But like many others, Rea had doubts about whether anything would be passed. Lawmakers had been trying to change the patent rules for more than a decade, and previous efforts had fallen apart for one reason or another.

"I thought when they passed it, I would be a member of private practice, and I would offer input and criticism to the government," she said. "Lo and behold, it did surprise me when I got there that I would work with [former USPTO director] Dave Kappos and the entire team at the USPTO on what would turn out to be a tsunami of implementation."

President Barack Obama signed the America Invents Act into law in September 2011, six months into Rea's tenure at the patent office. That meant Rea, who later rose to acting director at the agency, found herself in a central role helping to implement the law.

On the outside, a lot of attention was paid to the AIA changing the method for determining the priority of patent applications from a "first-to-invent" to a "first-inventor-to-file" system. But the law did much more than that.

It was densely packed with changes, and they required rules and some form of training for patent examiners and the USPTO users, according to Rea. She had a number of duties, including leading the implementation of the Patent Trial and Appeal Board, which has emerged as a popular alternative to district courts for hearing patent validity challenges.

"It was a herculean effort that far exceed my expectations," she said. "I've never worked harder in my life."

Helping shepherd one of the world's largest intellectual property offices through its biggest shake-up in decades wasn't a position Rea planned for herself, at least not early in her career. But it was one that colleagues say she was well-equipped to handle, in part because of her background.

Rea studied pharmacy at the University of Michigan and worked as a hospital pharmacist after completing her degree. At the same time, a career in law, something she had thought about in high school, was still in the back of her mind, so she decided to pursue it, spending her nights studying law at Wayne State University in Detroit.

Her legal career started as a patent attorney for Ethyl Corp., a multinational chemical company. She made the jump to private practice when she joined Burns Doane Swecker & Mathis LLP, a boutique patent firm later acquired by Buchanan Ingersoll & Rooney PC.

Mark Supko, a partner at Crowell & Moring, was part of the team that recruited Rea to join the firm in early 2008. Supko said Rea's abilities as a lawyer stood out, but so did her background as a pharmacist and an astute business sense.

LAW360

"The combination of technical skills and business sense, I think clients find that very appealing," he said. "She is able to counsel them in a way that isn't just focused on the legal issues in front of them. She puts it into the context of their business as a whole."

Those abilities also translated well to the USPTO, which she joined in 2011, according to colleagues, who said Rea's technical background and depth of experience in the field gave her a lot of gravitas in terms of being able to pull people together and give them guidance.

"Without a doubt, everyone respected Terry for her knowledge in the field," said Margaret Focarino, a senior patent adviser at Oblon McClelland Maier & Neustadt LLP and the former commissioner for patents at the USPTO.

Rea, who has also been president of the American Intellectual Property Law Association and led other IP law associations, said she was driven to join the patent office, in part, by a desire to give back. But she admits there was also a bit of curiosity about the inner workings of the agency.

As an attorney handling patent prosecutions, she had for years observed the USPTO from the outside. But she said she wanted to get behind the curtain and see how the office interacts with other agencies, the courts and Congress.

Perhaps most surprising, she said, was what she learned from an international perspective, getting a firsthand look at how the USPTO works with patent offices in other counties. This included attending IP5 meetings, where leaders from the world's five biggest intellectual property offices — Europe, the U.S., Korea, Japan and China — discuss patent rules and how to improve the system.

Although being an international advocate for U.S. intellectual property protections might have been a new experience for Rea, colleagues raved about her diplomatic skills and said she took nicely to the role.

"She was knowledgeable about the issues, and she had the kind of personality that made her a very good representative, I think, of the U.S. and the USPTO," Focarino said.

But Rea said one of her proudest moments came in 2013, when the USPTO was ranked No. 1 in the Partnership for Public Service's annual employee survey of Best Places to Work in the Federal Government. Not only did the USPTO top more than 300 federal organizations, unusual for an agency as large as the patent office, it did so at a time when the office was transitioning through the changes required by the AIA, making the achievement all the more unlikely.

"We were ranked No. 1 by employees while the employees were inundated with huge changes, which made it amazing," said Rea, who led the USPTO as acting director for most of 2013 after Kappos' departure.

In November that same year, Rea returned to private practice as a partner at Crowell & Moring. She also became a director with C&M International Ltd., an international trade and investment consultant affiliated with the firm.

At that point, implementation of the AIA was mostly complete, and Rea had left a lasting imprint on the USPTO and the country's patent system.

"Just looking at the scope of the [AIA] regulations, it's impressive that the patent office was able to get that together as quickly and as well as they did," Supko said. "And if you look at what has happened since those were implemented, there has been a sea change in the way patent disputes are litigated."

Today, Rea focuses her practice on various intellectual property issues and disputes, including complex patent litigation, and works with clients in areas such as pharmaceuticals and health care.

She also continues to be vocal about issues surrounding innovation, including those dealing with Section 101 of the Patent Act, which is a hot-button topic in patent law as some believe recent court decisions have created uncertainty over what is eligible for a patent. For her part, Rea said she would like to see more areas of technology to be found patentable and, if possible, more clarity with Section 101.

"Businesses need clarity in order to do their work, and if we can't provide clarity, I think innovation will be diminished and less robust," she said.

Editing by Christine Chun and Patricia K. Cole.



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

# Crowell & Moring Speaks

## Cybersecurity Leadership Dinner

*Tel Aviv*

On **April 12, 2016**, Crowell & Moring hosted a program that featured Israeli and global leaders in cybersecurity. The program focused on the current U.S. corporate cybersecurity environment; current U.S. government cybersecurity environment; best practices in cybersecurity protocols and breach response; U.S. market for cybersecurity technology; and building and maintaining your U.S. presence.

## The U.S. Legal Landscape in Cybersecurity, Data Protection, and Privacy: Understanding the Law, Implementing Policies, and Responding to Crisis

*Cyber Together, Herzliya*

On **April 13, 2016**, Crowell & Moring, in conjunction with the Israeli association Cyber Together, led a program for leading Israeli cyber technology companies and executives. The program delved into U.S. and international cybersecurity and privacy legal and regulatory issues and trends;

digital risk management from policy to practice; and best practices for developing U.S. cybersecurity protocols and data breach responses. The program included C&M speakers Sam Feigin, Mark Kass and Evan Wolff.

## Assessing the Israeli Cybersecurity Experience | The Woodrow Wilson International Center for Scholars

*Washington, D.C.*

On **June 2, 2016**, Crowell & Moring partner Evan


*Dr. Eviatar Matania, Head of Israel's National Cyber Bureau*

Wolff moderated a conversation with the Head of Israel's National Cyber Bureau, Dr. Eviatar Matania. They discussed the Bureau's development, function and share key lessons learned, and the process of forging Israel's national cyber security strategy. The Honorable Jane Harman, Director, President and CEO, Wilson Center, and former U.S. Congresswoman, also participated.

## CyberWeek 2016

*Tel Aviv*

Crowell & Moring partner Evan Wolff attended Cyberweek, along with the Chief Information Security Officer of leading global professional services company Accenture and other members of the Accenture cyberteam.

*C&M's Evan Wolff*

## Fostering Innovative Digital Health Strategies Conference

*Washington, D.C.*

On **June 23, 2016**, Crowell & Moring and Accenture co-hosted a digital health technology conference, examining the intersection of business, legal, and policy issues that innovative companies face in developing and integrating successful digital health tools and platforms. Panelists included Crowell & Moring partners Jodi Daniel, John Brennan, Cheri Falvey, James Flood, and Evan Wolff, Jeff Elton, Managing Director, Global Life Sciences Management Consulting, Predictive Health Intelligence, Accenture, and other luminaries and leaders from industry (including Biogen Idec, CVS Health and Aetna) and government.

**For more Crowell & Moring events, visit our website at crowell.com/events.**

# Cybersecurity Programs – A Guide

*By Linda Lerner, Maida Lernder, Harvey Rishikof, and Jenny E. Cieplak*

Cybersecurity has been identified as the issue that keeps most corporate management and their IT, legal and compliance teams, as well as many government regulators, up at night. The time for considering whether to have a cybersecurity plan in place is long over; those plans should be in place and reviewed at least annually for their adequacy in light of current developments in federal and state governmental regulation, technology and in the types of cyberattacks being perpetrated. Companies with inadequate cybersecurity protections risk:

- Reputational harm.
- Monetary sanctions for exposing personal identifying information (PII) and personal health information (PHI) of their clients (whether retail customers or patients) and employees/applicants.
- Exposing confidential enterprise operational and business information of the company and/or its customers.
- Bringing the company's operations to a halt when ransomware infections have enabled hackers to hold the systems hostage or other types of attacks, such as Distributed Denial of Service (DDOS), impede operations. This has been particularly troublesome in the healthcare industry, where patient care may be compromised.

In addition to federal law protections and regulatory and self-regulatory rules, applicable state laws require the protection of PII and PHI. EU privacy laws govern PII transferred into the United States. Finally, a company's cybersecurity insurer may impose procedural and testing requirements as a prerequisite to underwriting that insurance.

It is critical for entities that utilize automated systems for any functionality to have a program of risk analysis and oversight for those systems to identify and minimize sources of operational risk and data loss. Companies should conduct regular, periodic and objective testing and review of automated systems to ensure their reliability, secure nature and scalability and should adopt policies and procedures that address administrative, technical and physical safeguards for the protection of customer and corporate records and information.

## What Does a Robust Cybersecurity Program Include?

### *Risk Assessment*

The company should form a Risk Analysis Committee to perform this task. Factors to be considered by the Committee include:

- Inventory of hardware with data connectivity, data transmission or data storage capability.
- Inventory of critical software and version in use.
- Policies and procedures that ensure prompt installation of software patches and upgrades.
- Inventory of types of data collected, maintained and/or disseminated, who controls it, who has access to it, and how is it transmitted and to whom.
- Internal and external threats and vulnerabilities to at-risk data, including customer and counterparty PII, corporate records and financial information.
- Threats and vulnerability of electronic infrastructure, including systems used to initiate, authorize, record, process and report financial transactions, strategic plans, key corporate documents, and risk management.
- Threats posed by third party vendors and awareness of the devices connected to their networks and network structure; threats posed by fourth party vendors (a third party vendor's vendors) are equally important.
- Understanding of the nature of the threats, including: data loss (including data at rest and interception and compromise of data in transit); loss, destruction or theft of hardware containing at-risk data; and insertion of viruses, spyware and other malware. Threats may include natural disasters, human errors and malicious attacks.
- Prioritization of threats as to possible severity, vulnerability level and past incidents. Threats identified by the firm's outside vendors (or their vendors) should also be considered.
- Deployment of protective measures.

- Physical access restrictions.
- User authentication (complex, frequently changing passwords, multiple authentication modes).
- Systems access controls (least necessary).
- Use of network segmentation.
- Use of secure development practices for internally developed software.
- Selection of storage media.
- Use of and timely patching of anti-virus and firewall technology and other software.
- Use of approved software; prohibition against using unsupported software (whitelists and blacklists).
- Web filtering to block access to inappropriate or malicious websites.
- Testing, including: controls testing; enterprise technology risk assessment; vulnerability testing; penetration testing; security incident response plan testing; and enterprise risk technology testing.
- Regular system and data backup for disaster recovery.
- Documentation of threat detection measures, such as network monitoring software, monitoring for physical intrusions.
- Secure disposal of data and hardware on which data is stored.
- Due diligence on vendors and employees.
- Joining organizations to share threat information, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), the US Computer Emergency Readiness Team, Department of Homeland Security's Cyber Information Sharing and Collaboration Program, FBI's Infraguard, and the Department of Energy's Cybersecurity Risk Information Sharing Program.
- Encryption of data at rest and in transit.
- Ensuring that mobile devices are equally protected.
- Establishing relations with law enforcement and government officials.

## *Incident Response Plan*

Every company can expect to experience a cybersecurity incident. When that incident arises, a response plan should already be in place; the time of the incident is not the time to plan the response. The incident response plan should cover, at a minimum, roles and responsibilities for individuals tasked with responding to and mitigating the incident, the restoration of software and hardware, paths of communication with stakeholders and regulatory authorities, and a review of the cybersecurity plan in light of the incident. The details are critical – who will restore software and hardware, are alternates available, does the company have an alternate, independent warm or hot site, how long will it take to get up and running in various scenarios, which attorney to call and should outside counsel be engaged, should an independent forensic consultant be engaged, should an outside PR firm be engaged, and in each case, that entity and its contact person and information identified. All of these issues should be decided in advance and reviewed periodically. Tabletop exercises are especially helpful in ensuring that the responsible individuals understand the escalation process and that processes set out in an incident response plan flow smoothly.

## *Employee Training and Background Checks*

Employee training is a key component of an adequate cybersecurity plan. Some in the field believe that a substantial cause of incidents is due to human carelessness – whether it is opening a phishing email, neglecting to immediately terminate system access of a terminated employee, failure to install a patch or many other simple human errors. Vendors with effective, user-friendly educational tools attend or sponsor many cybersecurity conferences.

Cyber incidents may be caused not by employee error but by employees acting with malicious intent. Thus, it is important to conduct background checks where permitted, to ensure that access is terminated when an employee no longer needs such access, and that two-factor authentication is used so that employees cannot share login credentials.

## *Contractual Relations with Vendors*

Cybersecurity requirements for vendors should be set forth in each contract with any vendor that will be providing

information systems or that will otherwise have access to sensitive information. Those contracts should include a provision requiring the third party vendor to impose the same requirements on its service providers that the company imposes on its third party vendor. A firm's cybersecurity implementation procedures should provide a way to verify compliance by third and fourth party vendors, whether through access to testing results or audit rights.

## Stakeholders to Be Involved in Developing and Reviewing the Cybersecurity Plan

Senior management must be involved in and approve each aspect of the company's cybersecurity plan so that cybersecurity is recognized company-wide as a priority governance issue and because management ultimately must approve the budget for what can become a significant expense. A company should designate a knowledgeable individual as the Chief Information Security Officer (CISO), senior management should be included in the initial meeting and in at least the final meeting to approve the overall cybersecurity plan. Other parties that are critical to this process are IT, the affected business units, back office, risk management, internal audit, HR, compliance and legal. Finally, the involvement of the company's board of directors is very important; a lack of board involvement may be viewed as a breach of the board's fiduciary duty. As a best practice, the firm's management (whether a designated Risk Management Committee or group that has been delegated this task) should report to the board no less than annually, and preferably quarterly.

## Independent Testing

It is important to conduct independent testing so that the company's board and executive management, as well as the Chief Information Security Officer, the head of IT and/or any other staff managing the process may receive independent perspectives. Vulnerability testing, external and internal penetration testing, controls testing, incident response plan testing and enterprise technology risk assessment should be conducted by persons who are not responsible for development or operation of the systems or capabilities being tested, but that person may be internal or external, depending on the severity of the risk, applicable regulatory requirements and industry best practices. The frequency of such testing should be guided by those same factors. The board of directors and senior management should receive and review reports setting forth the results of all testing and assessment.

## Resources

- The National Institute of Standards and Technology (NIST) has published a Framework for Improving Critical Infrastructure Cybersecurity. The Framework recommends testing detection processes and procedures as well as response and recovery plans.
- The Financial Industry Regulatory Authority (FINRA), which regulates securities broker-dealers, published a Report on Cybersecurity Practices in February 2015. It contains a robust framework for drafting procedures and has a list of standards and best practices reference materials.
- On May 23, 2016, FINRA published a Checklist for Cybersecurity based on the NIST Framework that is a very useful tool for ensuring that necessary areas are covered.
- The Federal Information Security Management Act (FISMA) requires governmental agencies to evaluate and test systems annually.
- The Council for Cybersecurity's Critical Security Controls for Effective Cyber Defense recommends tabletop exercises and penetration testing, as well as continuous scanning for vulnerabilities.
- The Federal Financial Institutions Examination Council (FFIEC) stresses the importance of independent testing—i.e., testing independent of the person controlling the function being tested.
- Most of these resources are also reviewed in a recent CFTC Rule Proposal published in the Federal Register on December 23, 2015 (Vol. 80, No. 246 at page 80114).
- SANS Institute's Critical Security Controls for Effective Cyber Defense and an Effective IT Security Plan: http://www.sans.org.
- Open Web Application Security Project's guidance: http://www.owasp.org.
- ISACA Control Objectives for Information and Related Technology: http://www.isaca.org.

- The FCC's Small Biz Cyber Planning Guide is broad-ranging and very useful.

***Linda Lerner** is a partner in the Corporate, Financial Services, and White Collar & Regulatory Enforcement groups in the firm's New York office.*

***Maida Lerner** is a senior counsel and a part of the firm's Environment & Natural Resources and Government Contracts groups.*

***Harvey Rishikof** is a senior counsel in the firm's Privacy & Cybersecurity and Government Contracts groups.*

***Jenny E. Cieplak** is a counsel in the firm's Corporate Group.*

## In Case You Missed It ... Five Key Takeaways in Developing Digital Health Platforms

*By Jodi G. Daniel and Marisa E. Adelson*

Crowell & Moring and Accenture co-hosted the Fostering Innovative Digital Health Strategies Conference in Crowell's D.C. office. The goal of the conference was to take a comprehensive look at all of the business and legal issues that need to be addressed as health care organizations and technology companies are considering innovative strategies using digital health technologies. The conference covered a wide array of digital health topics, including trends in the healthcare Internet of Things, setting up digital health platforms, legislative activity regarding health IT and telehealth, privacy, cybersecurity, and use of digital health technology to support new payment models.

Session 2, "Setting up a Platform for Digital Health," featured panelists Jodi Daniel (Partner, Crowell & Moring), Bakul Patel (Associate Director for Digital Health, Center for Devices and Radiological Health, FDA), Anna Shimanek (Senior Legal Counsel, CVS Health), Paul L. Uhrig (EVP, Chief Administrative, Legal, & Privacy Officer, Surescripts) and Ronan Wisdom (Managing Director, Accenture Digital). Key takeaways include:

- New partnerships are emerging. There is a broad movement among a variety of stakeholders – providers, payors, consumers, technology companies, and the government – toward using digital health to improve communicating with providers and patients' understanding of their own health. This leads to new opportunities to partner with other organizations and require strategies for doing so effectively from a legal and business perspective.

- Policy and innovation is not always aligned. Policy is trying to keep up with innovation, but there are gaps and regular updates to address the fast pace of innovation. The federal government, including the FDA and FCC, is working to set the right temperatures, conditions, and structures for digital health platforms. Yet, there are currently varying regulatory requirements (e.g., for apps or mobile platforms) with a lot of grey in terms of what is permitted (or not). The policy and legal structures need to be in place, and there also needs to be coordination among participating organizations to address governance beyond federal policy.

- Growing availability of data poses challenges about use of that data. Digital health is moving healthcare from episodic data to the availability of constant streams of data through things like wearables and mobile health tools. The question is how providers (with the help of technology companies) will translate this tremendous new volume of data into practical applications and benefits, particularly for health prevention and population health management. In addition, companies face difficult new logistics in dealing with digital health devices and other products.

- Governance is critically important. Companies need appropriate governance around the transfer of information and proper stakeholder engagement to make digital health work.

- The digital health legal landscape can be murky. The laws are not always caught up with the technology, and it may

not be clear how laws, regulations, and guidance apply to a particular product. At the same time, agencies are reacting and providing updated information all the time. Experienced legal counsel is critical to the success of any player in navigating the digital health space.

***Jodi G. Daniel*** *is partner in the firm's Health Care Group.*

***Marisa E. Adelson*** *is an associate in the firm's Health Care Group.*

# **International Trade Implication of Brexit:** What Companies Should Do Now

*By Charles De Jager, Dj Wolff, Gordon McAllister, and Jeffrey Snyder*

The ramifications of the United Kingdom's decision to leave the European Union will be significant, but as of today nothing has changed in practical terms. What does this mean for trade – imports, exports, sanctions, antidumping, and other daily trade issues for global business? Not very much immediately, but now is time to plan and develop a strategy for the weeks and months ahead. Isolate your U.K. operations in the supply chain, gather data, and identify options. You will then be ready to act when the time comes.

## Legal Background

The U.K. remains a member of the EU, at least for now. The European Communities Act 1972 remains in force throughout the U.K., and the U.K. remains subject to its obligations under the EU Treaties. Article 50 of the Treaty on European Union provides a two-year period from a Member State notifying its intention to leave the EU to that state's withdrawal, although this period can be extended by agreement with the European Council. It is not currently clear when the U.K. will formally submit its notification under Article 50. Until a clear picture of the post-Brexit world emerges, there may only be limited change to contend with in the short term. However, even at this early stage one thing is for sure: the consequences of the Brexit vote will be wide-reaching, and cannot be ignored by those doing business in or with the U.K.

## Trade Background

Over the years, the EU has come to assume exclusive competence over international trade in a broad sense, including the promotion of trade liberalization and the negotiation of trade agreements, the establishment of tariff rates and the imposition of trade remedies, as well as aspects of export policy and foreign direct investment. As a Member State, the U.K. has thus ceded much of its competence to the EU in the negotiation and implementation of international trade rules. Upon the U.K.'s departure from the EU, it will regain exclusive competence in the areas enumerated above. However, much will ultimately depend on the trade arrangement the U.K. will be able to agree to with the EU.

## Import Duties

Absent a customs union between the parties once the U.K. leaves the EU, the U.K. will have to issue its own tariff schedule to remain a Member of the World Trade Organization. All other WTO Members will have to approve this schedule, which could lead to the burdensome renegotiation of tariff commitments between the U.K. and key trading partners.

In the European context, not much is likely to change regarding trade between the U.K. and the EU if the U.K. obtains preferential access to the EU market equivalent to that enjoyed by Norway and Switzerland. However, a number of restrictions on trade could still apply with respect to rules of origin, trade remedies, and trade in services. Short of a preferential access arrangement, the parties may otherwise negotiate a trading arrangement based on the principle of Most-Favored Nation (MFN), the implications of which would vary much more considerably by sector.

Therefore, companies will have to follow closely and analyze carefully the negotiation of the new EU-U.K. trade arrangement and related developments at the multilateral level. The effects of the resulting changes may have a significant impact on companies' duty planning and supply

chain management activities, including the location of new production facilities or the relocation of existing ones.

## Trade Agreements

As a result of leaving the EU, the U.K. will no longer be a party to the trade agreements between the EU and third countries. It will also forego the considerable weight of the EU in trade negotiations. Although it may thus enjoy greater autonomy in setting its negotiating objectives and positions (e.g., with respect to market access in services), the U.K. may be forced to make greater concessions to trading partners enjoying equal or greater bargaining power over it alone.

In practice, the U.K. may also be required to agree to terms fairly similar to those between a particular trading partner and the EU, as countries may seek to achieve a degree of uniformity across multiple trade agreements. Therefore, the likelihood U.K. independence over its trade policy would lead to more favorable outcomes for the U.K. in its negotiation of trade agreements with third countries is unclear.

## Special Measures

The EU and U.K. could initiate trade defense proceedings and impose additional duties against unfairly traded imports from one another once the U.K. leaves the EU, whether their trade relations are governed by a preferential access or MFN-based arrangement. Although the EU currently has the administrative capability to conduct trade defense investigations, the U.K. does not. Thus, it will have to develop such a capability and related rules to conduct independent trade defense investigations to protect British domestic industries from unfair foreign competition in the future.

As these industries are currently protected by EU trade defense orders imposed on the basis of EU-wide conditions and analyses, the U.K. cannot automatically maintain these measures once it leaves the EU without exposing itself to significant challenge under the WTO rules by the trading partners whose industries are affected. Considerable time and effort will be required for the U.K. to afford WTO-consistent protection to the full range of its industries affected by unfairly traded imports.

By virtue of limiting its analyses to its own territory in this context, the U.K. might be able to more easily impose trade defense measures in certain cases. However, in others, in which its domestic industry may currently be enjoying protection as part of the EU-wide affected industry, it may be difficult for the U.K. to find injury within its own territory and impose measures. The ultimate outcome will thus once again be mixed.

## Export Controls

The U.K. itself is currently a member of all the relevant international agreements in the context of export controls (i.e., the Wassenaar Arrangement, the Missile Technology Control Regime, the Nuclear Suppliers Group, and the Australia Group). These memberships are not contingent on the U.K.'s EU membership and the U.K. Secretary of State has the statutory power to elaborate and impose export controls under domestic U.K. legislation. Therefore, the U.K. will most certainly maintain its own export control regime upon leaving the EU and there will likely be little change in the manner in which the U.K. will continue issuing licenses for exports to third countries.

A rare strong proponent and enforcer of export controls within the EU, the U.K. after its departure from the EU will no longer participate in EU-wide efforts to ensure greater harmonization in the interpretation and application of export control rules by EU Member States' authorities. This will constitute a loss to the EU and may lead allies like the U.S. to view the EU export control regime to be weaker than when it included the U.K. The grant of authorizations to EU Member States remaining within the EU may thus be affected.

The extent to which U.K. export control authorities may continue to coordinate with certain of their counterparts remaining in the EU will also have to be monitored closely. The U.K. will likely provide for preferential treatment of exports to more trusted Member States with a view to preserving existing collaboration with those Member States' authorities. However, given persistent concerns regarding the integrity and uniformity of export control enforcement in certain other Member States, the U.K. will likely impose stricter controls over exports to such Member States. Upon the U.K.'s departure from the EU, transfers of dual-use items from the U.K. to the remaining 27 EU Member States will officially become exports the licensing of which will have to be reviewed carefully for compliance purposes.

## Economic Sanctions

Similar to the other areas of international trade compliance, the U.K.'s departure from the EU will lead to an increasingly complicated economic sanctions compliance landscape. It may take years for all of the effects to be understood fully, but the following represent a few initial thoughts.

Nothing will change immediately. The U.K. will continue to implement all United Nations (as a permanent member on the United Nations Security Council), EU, and national sanctions until Brexit is fully implemented. Yet, even if these negotiations take months or years, the referendum outcome will have an impact, not least in the marginalized influence of the U.K. in ongoing EU discussions. For example, the EU's sectoral sanctions against Russia may be the first victim. Despite strong pressure from Russia and substantial question from Eastern European countries, the EU was successfully able to extend its sectoral sanctions for six months last week, in part as a result of strong U.K. advocacy. Without the U.K., will the EU have the political will to overcome the internal and external opposition to extend them? If it does not, it will create a transatlantic regulatory divide with which compliance officials will need to grapple.

These impacts will only grow more acute once the Article 50 process has been completed. Yet, even then the impacts will be difficult to determine. Given the U.K.'s strong support for economic sanctions, as well as its role (at least currently) as the global center of international finance, it seems likely that the U.K. will continue to rely heavily upon economic sanctions as a tool of foreign policy. Without the limitations imposed by a 28-country consensus-based negotiation, the U.K. will be free to pursue the strong sanctions for which it often advocates. While it will likely, for pragmatic reasons, closely follow EU sanctions, it will now be free to react more quickly, and more aggressively, if it chooses.

This could include closer alignment with the U.S., a path that may be facilitated by the U.K.'s recent creation of an Office of Financial Sanctions Implementation (OFSI) modeled, in part, on the U.S.'s Office of Foreign Assets Control (OFAC). Nevertheless, despite the easy impulse to assume stronger U.K.-U.S. alignment, their approaches to certain foreign policy matters remain fundamentally divergent. For example, the U.K. has been actively encouraging its businesses to pursue business in Iran, while the U.S. has retained virtually all current primary sanctions on Iran, pursuant to the recent Joint Comprehensive Plan of Action (JCPOA).

From the perspective of economic sanctions, the real victim of Brexit may be the global centrality of the EU's sanctions regime. To date, the U.K. has been one of the strongest proponents of economic sanctions within the trading bloc. With its departure, it remains to be seen whether the other Member States will have the political will, or interest, to enact strong economic sanctions that will, inevitably, impose disproportionate costs on at least one of the EU's Member States. France remains a permanent member of the UN Security Council and Germany a strong proponent of tailored sanctions, but it only takes one EU Member State's disagreement to disrupt consensus and bring down an entire regime.

## Compliance Management Challenges Ahead

Until the U.K. officially exits the EU, current laws remain applicable without any gaps. Nonetheless, the Brexit vote and the ongoing negotiations will no doubt have an impact on Commission decisions implementing EU trade laws in many ways. For example, how will decisions on trade defense cases be affected? Might the maintenance of sanctions against Russia or the implementation of sanctions relief for Iran be altered? These questions form only the beginning of what will no doubt be a new art form: predicting the extent and nature of the gap between London and Brussels as the daily work of government collides with the Article 50 negotiations.


***Jeffrey Snyder*** *is a partner and chair of the firm's International Trade Group.*

***Charles De Jager*** *is a counsel in the firm's Brussels office. He has more than 15 years of experience as an attorney in international trade, dispute resolution, regulatory law, and government affairs.*

## DoD Proposes Significant Amendments to the DFARS Data Rights Scheme

*By John E. McCarthy Jr., Jonathan M. Baker, and Joelle Sires*

On June 16, 2016, DoD issued a proposed rule to amend the DFARS to implement section 815 of the

National Defense Authorization Act for FY 2012, which made significant changes to the data rights scheme for DoD contracts. Among other things, the proposed rule permits the release of "segregation and reintegration" technical data and computer software outside of the government (subject to restrictions), even when the item, component, or process to which that data pertains or the computer software was developed exclusively at private expense; expands DoD's ability to order technical data and computer software post-award; doubles the time period in which DoD may challenge asserted data rights restrictions; and expressly imposes no time limit on DoD's right to challenge fraudulently asserted restrictions.

***John E. McCarthy Jr.** is a partner and member of the Steering Committee for the firm's Government Contracts Group.*

***Jonathan M. Baker** is a counsel in the firm's Government Contracts Group.*

***Joelle Sires** is an associate in the firm's Government Contracts Group.*

## The DAO Hack Provides Lessons for Companies Using Blockchain and Distributed Ledger Technology

*By Evan Wolff, Jenny Cieplak, Matthew Welling, and Tyler O'Connor*

The Decentralized Autonomous Organization (the DAO), an anonymous, crowd-sourced investment vehicle using the digital currency Ether, was recently hacked in a heist that saw investors lose 3.6 million Ether coins valued at $55 million. Prior to the hack, the DAO was notable as one of the first investment funds operating on the Ethereum blockchain, a distributed ledger technology supporting "Ether" digital currency. Some news media have gone so far as to predict the end of virtual currencies in the wake of this incident. However, the incident can be taken instead for the important lessons it provides, and to inform cybersecurity readiness for safer deployment and adoption of blockchain and distributed ledger technologies.

By way of background, Ether is a digital currency similar to Bitcoin, and is traded through the Ethereum blockchain. Unlike Bitcoin, Ethereum supports "smart contracts"—automated computer programs that execute the terms of a negotiated contract.

The DAO operated using smart contracts built on the Ethereum blockchain. When investors transferred their Ether to the DAO pool, the DAO smart contract enabled these investors to vote on how the pool would be invested. The smart contract also contained an automated mechanism to enable investors to exit from the DAO that, when executed, told the DAO where to distribute their Ether. Unknown hackers exploited a weakness in the code of DAO's smart contract, enabling them to withdraw not only the Ether hackers placed in the DAO, but also the Ether of other investors.

Importantly, the DAO hack was not caused by any inherent weakness in blockchain or distributed ledger technologies; it was specific to DAO. However, the incident demonstrates the importance of cybersecurity readiness, including timely threat assessment and organizational response. The DAO hack was perpetrated by exploiting a flaw in DAO's smart contract

code—a vulnerability that was publicly identified in May, well ahead of the attack.

Traditional investment vehicles such as mutual funds and commodity pools are incentivized by the threat of civil liability and regulatory penalties to continuously test their systems. Regulators have made it clear that financial intermediaries such as fund managers, commodity pool operators and investment advisers must take care to ensure that their clients' assets and information are protected. The Securities Exchange Commission's (SEC's) February 2015 Cybersecurity Alert is one example, and the National Futures Association's August 2015 Guidance is another. Regulators have also made it clear that investment activities involving virtual currencies can have real-world repercussions. The Commodity Futures Trading Commission has asserted jurisdiction over virtual currencies as commodities, most recently in an order requiring Bitcoin exchange Bitfinex to register as a Futures Commission Merchant, and the SEC has made it clear that regardless of whether a securities investment is paid for in virtual or fiat currency, it is still subject to the agency's jurisdiction.

Unlike traditional financial intermediaries, the DAO does not appear to fall into any category of regulated entity. As its name implies, the DAO is autonomous—it is self-executing computer code. And although one or more individuals created the DAO's code, it is not clear whether those individuals will ever be identified or will continue their involvement. Thus, there may be no investment adviser, commodity pool operator or other regulated entity to take responsibility for maintaining the DAO's security. The DAO's code is open source, and therefore open to the public to identify and fix vulnerabilities and to make other changes. However, simply because the code is open source does not mean that anyone will necessarily take on the responsibility to identify and fix vulnerabilities much less take on liability for failing to fix known flaws. Given the anonymous and distributed nature of the DAO, there is little, if any, incentive to undertake the cybersecurity measure typically implemented by more traditional financial intermediaries.

As the DAO hack demonstrates, all firms using distributed ledger technologies or virtual currencies need to ensure that their own applications, as well as those they engage with, employ best practices for cybersecurity. Not only should firms prepare for incident response and crisis management in advance, but also proactively review their policies and procedures, system controls, and vendor management practices. Cyber risk review—including accessing threat intelligence and participating in Information Sharing and Analysis Organizations (ISAOs), as appropriate—and timely organizational response should be ongoing activities.

Cybersecurity has become one of the most important issues for companies and a critical consideration for managing risk, especially when incorporating new technologies. Crowell & Moring's depth of experience enables us to inform clients about emerging cybersecurity and privacy issues and risks and provide proactive counseling in assimilating new cyber/privacy requirements and new technologies like blockchain into existing business frameworks.

***Evan D. Wolff*** *is co-chair of the firm's Privacy & Cybersecurity Group, and former adviser to the senior leadership at the Department of Homeland Security (DHS). His practice focuses on homeland security, privacy, and data security including chemical security regulatory compliance, SAFETY Act, corporate internal investigations, corporate compliance and governance, congressional investigations, cyber security, and environmental audits.*

***Jenny E. Cieplak*** *is a counsel in the firm's Corporate Group.*

## **Privacy Shield Formally Adopted:** Self-Certifications Start August 1, 2016

*By Jeffrey Poston, Emmanuel Plasschaert, Jeane Thomas, and Evan Wolff*

The European Commission, alongside the U.S. Department of Commerce, on July 12 announced the final adoption of the EU-U.S. Privacy Shield (Privacy Shield), the legal framework that replaces the previously invalidated U.S.-EU Safe Harbor (Safe Harbor) framework for transatlantic data transfers.

Companies will be able to self-certify under the new regime starting August 1, 2016.

## History of the Negotiation

The European Parliament, as well as a committee of representatives of the EU Member States and their data protection authorities (Article 29 Working Party) initially criticized the Privacy Shield documents and principles first released on February 29, 2016. As a result of the criticism, the European Commission in close cooperation with the U.S. authorities, clarified and improved the initial Privacy Shield documents. On July 8, 2016, the European Union (EU) Member States in their function as the Article 31 Committee approved this amended version of the Privacy Shield.

The amendments include more explicit declarations of the European Commission regarding obligations of companies in relation to limits on personal data retention and onward transfers. The U.S. authorities in turn provided additional clarifications regarding the bulk collection of data, and have strengthened the Ombudsperson mechanism within the U.S. Department of State (a newly formed position created to address EU citizens' concerns regarding the collection of data for national security purposes).

## Future Legal Challenges

Throughout the negotiations, critics have warned of a legal challenge to the Privacy Shield. That criticism continues. Privacy activist Max Schrems as well as EU Member of Parliament Jan-Philipp Albrecht are already on record criticizing the new framework. However, the European Commission leadership stood by their final adequacy finding on July 12 with robust statements supporting their belief in the new framework's ability to reflect the requirements laid out in the European Court of Justice's October 2015 judgment ruling Safe Harbor invalid.

The EU data protection authorities are set to meet and discuss the final Privacy Shield documents on July 25, 2016. A resolution of the European Parliament on the Privacy Shield is planned for September 2016. The outcome of both processes may influence future policy or European Court of Justice decisions, but neither body is able to invalidate the European Commission's Privacy Shield adequacy finding. Though there may be political or legal challenges to the Privacy Shield, the European Court of Justice in its October 2015 judgment made clear that it alone has the authority to invalidate adequacy findings like the one Privacy Shield just received.

## Timeline for Implementation

The U.S. Department of Commerce is set to begin accepting applications for self-certification under the Privacy Shield starting August 1, 2016. Until then, companies that want to transfer personal data from the EU to the U.S. must continue using other data transfer mechanisms, such as approved Binding Corporate Rules (BCRs) or EU Standard Contractual Clauses.

Companies that wish to adhere to the new Privacy Shield data transfer framework, whether or not they were previously Safe Harbor certified, should begin to review the Privacy Shield and seek legal advice to discuss changes needed to ensure compliance with the requirements of the new framework.


***Jeffrey L. Poston** is a partner in the firm's Commercial Litigation Group.*

***Emmanuel Plasschaert** is a partner in the firm's Brussels office.*

***Jeane A. Thomas** is a counsel in the firm's Corporate Group.*

***Evan D. Wolff** is co-chair of the firm's Privacy & Cybersecurity Group*

## 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 U.S.-Israel Business.

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