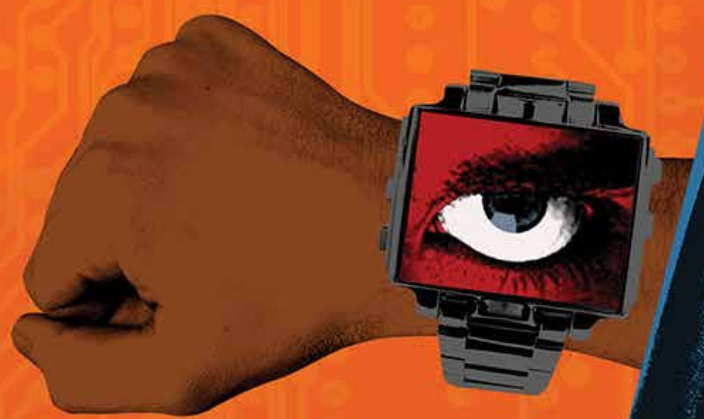
MoFo Tech

Information, Trend-Spotting, and Analysis for Science and Tech-Based Companies from **Morrison & Foerster** LLP

2014 SPRING / SUMMER

Who's Watching Whom?

FOR WEARABLE-TECH MAKERS, ATTENTION TURNS TO QUESTIONS OF PRIVACY



BERLIN
Wilkommen, Bienvenue, Start-ups

BRIBERY
Third-Party Tradeoffs

MOBILE PAYMENTS
Think Like a Regulator

Meet Our MVPs.

Michael Jacobs
Two-time *Am Law* Litigator of the Week
BTI Client Service All-Star, 2012 – 2014

Harold McElhinny
Am Law Litigator of the Year, 2014
NLJ Most Influential Lawyers, 2013

Rachel Krevans
Two-time *Am Law* Litigator of the Week
Chambers IP Woman of the Year, 2013

At Morrison & Foerster, we have many valuable players. Over the years, our team of more than 300 IP trial lawyers, high-end patent prosecutors, and licensing specialists have earned the reputation for trying — and winning — complex IP cases.

We are Morrison & Foerster — a global firm of exceptional credentials. With more than 1,000 lawyers in 17 offices in key technology and financial centers in the United States, Europe, and Asia, our clients include some of the largest financial institutions, investment banks, and Fortune 100, technology, and life science companies. We've been included on *The American Lawyer*'s A-List for 10 straight years. *Chambers Global* named MoFo its 2013 USA Law Firm of the Year, and *Chambers USA* named us 2013 Intellectual Property Firm of the Year. Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger.

MORRISON
FOERSTER

MoFo Tech™

Information, Trend-Spotting, and Analysis for Science and Tech-Based Companies from **Morrison & Foerster** LLP

Spring Summer 2014

TECH TODAY is moving more quickly than ever. Tech companies are rushing to be the first to the patent office, the first to market, the first to pivot when circumstances dictate. But while tech companies are looking to keep up with changing consumer demands, it's often the lawyers and regulators trying to keep up with the technology that's being introduced. As our cover story (page 8) demonstrates, **wearable technology**, which consumers are warming to, is rife with privacy issues, which are being sorted out. Similarly, myriad regulatory agencies are vying to make sure the emerging **mobile payments** industry (page 16) stays on track. But on the flip side, as **Chuck Duross** explains in our new Q&A column (page 14), the DOJ's growing focus on FCPA enforcement—with other countries creating similar laws—means that tech companies need to watch their steps to make sure they haven't overlooked key risks.

"Organizations have come to realize the tremendous value within their machine-generated data."

LENNY STEIN, GENERAL COUNSEL, SPLUNK INC., PAGE 10

The 411

Departments

FPO FPO FPO FPO FPO

Printed on Recycled Paper

Visit the enhanced electronic version of MoFo Tech by scanning this QR code.

The 411

LOG IN BY GARY JAMES

Laying the Groundwork for Natural Gas Vehicles

INFRASTRUCTURE AND REGULATIONS MAY DICTATE SPEED OF ADOPTION

AMERICA'S SHALE GAS revolution is making waves in transportation technology. Currently, only 1 percent of all natural-gas-fueled vehicles worldwide are running on U.S. roads, according to trade association NGVAmerica. But, in the coming years, U.S. NGV use is expected to accelerate, particularly among truck fleets. Why? Natural gas costs $1.50 to $2 less than gasoline per equivalent gallon. It's also cleaner burning, with up to 30 percent less greenhouse gas emissions.

The potential for NGVs highlights the need for additional gas pipeline and distribution infrastructure and for supportive energy regulatory policies at the federal and state levels, says Bob Fleishman, senior of counsel at Morrison & Foerster. "It's a question of making sure that, as CNG and LNG fueling stations and other new users come on line, there's an adequate supply of natural gas available."

At the national level, the Federal Energy Regulatory Commission oversees the construction of interstate pipelines and related infrastructure in a safe and environmentally sensitive manner, Fleishman says. At the state level, public utility commissions play a key role in making sure adequate mainlines and local service lines are in place to meet growing demand and, if gas utilities want to participate in NGV markets, that the competitive playing field is level for other providers.

In the U.S., transit bus systems have been early adopters of natural gas: About 20 percent of all transit buses nationwide now run on compressed natural gas or liquefied natural gas. Demand for NGVs is also growing steadily in the medium-duty and heavy-duty truck segments. UPS operates one of the largest alternative-fuel fleets in the country, with more than 2,700 hybrid, electric, and natural gas vehicles. The Atlanta-based company is investing nearly $70 million to build 13 LNG fueling stations to support its growing fleet. The increasing availability of inexpensive natural gas has created compelling new opportunities for companies such as UPS to save money and cut emissions, says Susan Mac Cormac, a partner in Morrison & Foerster's San Francisco office who works with UPS. "Natural gas is a huge step forward,," she says. "But longer-term, we'll need to come up with other creative approaches to meet our country's fueling needs." Emerging technologies such as hydrogen fuel cells hold great promise for both cars and trucks, she adds.

As commercial fleets add NGVs, the market for fueling locations grows. Leading the way is Clean Energy Fuels, which owns, operates, maintains, or supplies 445 CNG and LNG fueling stations nationwide. The company is building this network on interstate highways and in major metropolitan areas. Clean Energy is also building a new LNG production facility in Florida to supply LNG to the marine and rail industries.

"We have helped Clean Energy Fuels raise more than half a billion dollars to support their investments in new clean energy fueling infrastructure," says Steve Rowles, chair of Morrison & Foerster's San Diego Corporate Group. "Having a robust fueling network in place from coast to coast will make it easier for more fleets to make the move to LNG and CNG."

Photograph by **CHIP SIMONS**

THE "INTERNET OF THINGS" RISES

Refrigerators that tell you you're out of milk, cars that warn of an imminent collision, implants that know if you've taken your medicine–by tying almost anything into a wireless network, the "Internet of Things" promises to transform several industries. Yet in the eyes of regulators and lawmakers, the IoT presents new risks ranging from privacy and security breaches to catastrophic system failures.

Regulators in the U.S. and EU are particularly concerned that IoT devices could collect and disseminate personal information without users' consent–an issue they're already worried about when it comes to mobile phone apps, says Alistair Maughan, a London partner and co-chair of the Technology Transactions Group at Morrison & Foerster. Both the IoT itself and any potential regulatory frameworks are in their infancy. But tech companies may want to get ahead of the issue by monitoring public statements by regulators on the IoT, including speeches by FTC commissioners and the EU's Commission's 2013 report on the IoT. "To future-proof your design, you'll want to consider legal and regulatory ramifications very early in the process," Maughan says. "And you may want to focus on approaches that will work in the maximum number of jurisdictions possible." **RICHARD SINE**

Illustration by **KEVIN POPE**

FOCUS BY PETER HAAPANIEMI

Bitcoins, Big Headaches?

HAZARDS ABOUND FOR COMPANIES SEEKING TO ACCEPT BITCOIN

THE BITCOIN "CRYPTOCURRENCY" has gained momentum in the market, and some businesses, including Overstock.com and TigerDirect.com, now accept bitcoins as payment. Many others are wondering if Bitcoin is a good fit for them—and they should factor regulatory uncertainty into their calculations.

In the U.S., certain companies exchanging bitcoins and real currency must register with the Financial Crimes Enforcement Network and are subject to Bank Secrecy Act regulation, says Jeremy Mandell, an associate in the Financial Services Practice Group at Morrison & Foerster. Such companies may also be subject to state licensing requirements, which can be burdensome for start-ups and smaller firms.

Other concerns include the potential for illicit use and fraud—Bitcoin has been the currency of choice for some online black markets. And there have been major incidents of theft: in December, some $5 million worth of bitcoins was drained from accounts on Sheep Marketplace, one of those black markets. When such problems occur, there's little recourse for victims. "There are no consumer protections like those we see in more traditional payment mechanisms; there are limited dispute resolution rights, no deposit insurance for virtual currency holders, and account access can be restricted," says Mandell. "But the market is evolving to address these consumer exposures."

As virtual currencies become more widespread, regulators will continue to scrutinize them. The IRS ruled recently that bitcoins are property, and some states are also moving forward. The New York State Department of Financial Services announced that it will propose a virtual currency regulatory framework by late 2014. "Other states are taking about these issues too," says Mandell, "so we are likely to see more regulation of virtual currency—sooner rather than later."

CRITICAL MASS BY JEFF HEILMAN

Europe's Incubator Central

BERLIN IS BECOMING THE CONTINENT'S TOP START-UP DESTINATION

JÖRG MEISSNER, a partner in Morrison & Foerster's new Berlin office, had an eye-opening experience while visiting Silicon Valley to check out the start-up culture there.

"In Berlin, the streets and coffee shops buzz with people on their iPads pitching ideas, with start-up events happening practically every night," says Meissner, a corporate and finance lawyer who represents both founders and investors. "The scene is visible and active; it is the real deal."

Investment in young companies in Berlin is one-tenth that of Silicon Valley, Meissner notes. Yet the action is lively. Incubators are popping up throughout the sprawling city.

"Berlin is overtaking London and Tel Aviv as Europe's top start-up destination," he says. "Why? For the same reason that attracted artists here almost a decade ago: plentiful and affordable living and work space. Munich, Hamburg, and Cologne have some start-up activity, but at double the living costs, people choose Berlin."

The Berlin story began with the three Samwer brothers, who ignited the scene in 1999 by funding a German version of eBay and then selling it to eBay 100 days later for €38 million.

"Their model was to clone U.S. successes," says Meissner of the Samwers, whose empire now includes global incubator Rocket Internet; European Founders, their fund for early- and later-stage Internet businesses; and Global Founders Capital, targeting start-ups worldwide.

Players more focused on innovation have since come into prominence, but Berlin has yet to hit full stride. "For all the activity, there are simply fewer investors here, and absent a huge IPO story, U.S. interest remains lukewarm," Meissner explains. "Mindful of past bubbles, investors can be skeptical of new ideas, and the government has yet to fully get behind supporting young companies."

There are encouraging signs, however. "The government created a fund that pays business angels back 20 percent if they hold their investment for three years, subject to certain criteria," says Meissner. "Sequoia Capital recently put €18 million into a start-up here, and the €88 million round attracted by online food delivery service Delivery Hero was Berlin's largest ever. So hopes are high that Silicon Valley is coming."

There are also a growing number of corporate accelerators, Microsoft and Coca-Cola among them, providing founders with funding, mentoring, and networking support. "In 2013, leading German media company Axel Springer partnered with Plug and Play Tech Center—a leading Silicon Valley start-up investor and accelerator—to create Axel Springer Plug and Play," says Meissner who, with his team, advises Axel Springer Plug and Play on its deals. "That is the kind of direct bridge that promises well for the future."

Germany's Magic Portal

REPRESENTING ABOUT 40 MILLION TV households, Germans now receive virtually all on-demand content by Blu-ray Disc or DVD. Video-on-demand services are set to change that over the next three to five years, says Christoph Wagner, a partner in Morrison & Foerster's new Berlin office. "Look for dynamic, if not explosive interest in VoD as broadband penetration increases and major players consolidate the presently fragmented on-demand market," says Wagner, an expert in the TMT (technology, media, and telecommunications) sector, key to Germany's economy.

With the EU pushing hard for a pan-European regulatory framework around VoD, smaller players are likely out, while the big boys—U.S. Internet providers specifically—may have to pay to play. "There is a defensive wall against U.S. giants freely accessing the infrastructure," Wagner says, "although that may hinder growth."

The provider that creates what Wagner calls "the magic portal" will likely be the on-demand winner. "Germans must currently search multiple websites to find and access content," he says. "The opportunity is there for one 'magic' source. But who that will be remains to be seen." **JH**

UPDATE BY JENNIFER PILLA TAYLOR

Patent Quality: Shining Through

A NEW REVIEW PROCESS SHOWS THE IMPORTANCE OF A GOOD APPLICATION

THE NEWLY AVAILABLE procedure for challenging patent validity known as inter partes review, or IPR, is forcing patent players to raise their game—from application through litigation.

More than 800 petitions for IPR—many more than the Patent Office itself had expected—have been filed since the process became available in September 2012, according to the USPTO. And while the Patent Trial and Appeals Board issued only one final decision in the first year of IPR, there's much to be learned from its many rulings on motions so far, says Morrison & Foerster patent attorney Peter Yim.

Patent applicants should take notice of the strict limitations that the PTAB has placed on patent owners' abilities to modify their claims in response to arguments by patent challengers, says Yim. That's in sharp contrast to the practice in inter partes reexamination (the procedure supplanted by inter partes review), in which patent owners had wide berth to strengthen their patent claims through amendments. "The quality of the patent is really shining through in the results you get in these proceedings," says Yim. "It's important to get it right in the application."

Created by the federal patent reform legislation of 2011, IPR has added a new layer of strategy to patent litigation, says Morrison & Foerster patent litigator Richard Hung. Most IPR petitions are apparently related to litigation—a defendant accused of patent infringement files an IPR petition challenging the patent's validity—rather than as an attack on a patent by a competitor, he says.

Under the law, a defendant that is sued in federal district court for infringement has one year to file an IPR petition. In view of the complexity of preparing this petition, Hung notes that "one shouldn't wait until the last minute to decide whether to file one. The process would ideally begin several months out."

Once it is started, the IPR process moves rapidly because the PTAB must decide within a year. In contrast to inter partes reexamination, which was run by a patent office examiner, IPR is presided over by judges, many of them former patent litigators. Yim says a decision to keep a dispute in district court or file for IPR should hinge on the argument for invalidity. Highly technical arguments are probably best suited for a PTAB judge rather than a jury.

It's already apparent that IPR, as a kind of hybrid between patent office exams and federal court litigation, requires expertise across the patent spectrum, Hung says. "You really need to have all the members of your team, from both the patent prosecution and litigation sides, working in close collaboration."

No Billboards, Please

Companies intending to seek funding under the JOBS Act's crowdfunding provision gained a seeming advantage in September when the SEC removed its ban on the general solicitation or advertising of certain types of private placements. But this may be less promising than it sounds, says Palo Alto-based Morrison & Foerster corporate and securities partner Timothy J. Harris: "There is a strong undercurrent in Silicon Valley that companies showing their wares this way are openly admitting that they cannot raise capital by traditional means that involve the imprimatur of professional venture capital or private equity investors. This may suggest that the company is of questionable appeal or quality."

General solicitation can also be an uncertain and expensive means to obtain funding. "You can stick your billboard on the highway, but you still have the costly obligation of reasonably verifying that your investors are accredited, among other requirements," Harris says. And there are potential downsides to inviting strangers to the party and keeping them happy. Adds Harris, "Imagine having numerous high-maintenance investors bugging you for their returns." **JEFF HEILMAN**

SUPPORT BY JENNIFER GOFORTH GREGORY

When Bosses Can't Be "Friends"

NEW LAWS RESTRICT ACCESS TO EMPLOYEES' SOCIAL MEDIA ACCOUNTS

MODERN TECHNOLOGY has increasingly blurred the line between business and personal lives, thanks in large part to social media that can broadcast employees' views to friends and the public in a heartbeat. Companies are increasingly tempted to move into what may be considered "personal" domains in order to maintain their reputation or control over employees' time. And that has translated into some serious debates in courtrooms and legislatures over the limits of corporate conduct.

For example, several states have passed laws restricting access to the social media accounts of employees and job applicants. Several federal bills with similar requirements are in the works. Typically, these laws forbid employers from requesting the passwords to personal social media accounts. But some states also forbid employers from attempting to access the non-public sections of these personal accounts.

"Something as simple as asking employees to make their profiles public or a manager sending a 'friend' request to an employee may run afoul of the laws in your state," says Christine Lyon, a Morrison & Foerster partner who focuses on privacy and employment law. "Companies should consider the laws of the state where the employee is physically located."

Another prevalent question is who "owns" the followers and related materials of an employee's social media account when the employee leaves the company. Companies want to retain the loyalty of followers developed using company time and resources, while employees believe their following results from their own efforts and influence. One complicating factor: they may have used their personal devices when posting to the account. "Several lawsuits involved cases where it wasn't clear if the account was for personal or business purposes, and the employee used the account for both," says John Delaney, leader of Morrison & Foerster's Social Media practice. Delaney recommends having employees sign a social media policy and structuring it to help prevent legal disputes down the road. For example, employers should outline a process for opening new social media accounts that require sign-off from an administrator, who can influence key decisions such as the account's name.

Employers should also make sure the policy states that the company's official social media accounts—those bearing the company's name—cannot be used for personal business, he adds.

TURNING THE TIDE ON "TROLLS"

WHEN A NON-PRACTICING entity (NPE) accused 16,000 small businesses of violating its patent by merely emailing scanned documents, the New York attorney general cracked down, forcing a settlement. Then the FTC threatened to sue for deceptive trade practices–prompting the NPE to file a preemptive suit against the FTC. ¶ As NPEs (sometimes known as patent trolls) have grown more audacious, the drumbeat for action against them has grown, notes Scott Llewellyn, deputy chair of Morrison & Foerster's IP Litigation Group. There's been an onslaught of media coverage and a flurry of federal legislation, with one House bill passing by a large margin in December. In January, President Obama urged passage of a bill to reduce "needless litigation," and the White House announced further executive actions. ¶ The House bill awaits a Senate counterpart. Regardless of whether any bill reaches Obama's desk, this "sea change of opinion" could have a big impact on patent infringement cases, Llewellyn says, by "potentially changing how judges and juries look at these issues." Meanwhile, Llewellyn warns, "Be careful what you wish for, because the devil is in the details." Companies should think about the potential for unintended consequences before supporting any measure. **RICHARD SINE**

Illustration by **GREG CLARKE**

SUPPORT BY ERIC SCHOENIGER

SEC: The New Cyber-Cop

BE READY TO DISCLOSE PRIVACY BREACHES

IT SEEMS SCARCELY a week goes by without a headline blaring news of a major cybersecurity breach. And with ongoing revelations about the data-tracking activities of the National Security Agency, the public isn't growing less concerned about privacy. So it's no surprise Congress has pressed the Securities and Exchange Commission on cybersecurity.

What does that mean for corporate disclosures? "The SEC continues to hear from Congress on cybersecurity disclosures, so it will continue to focus on the issue," says David Lynn, a partner in Morrison & Foerster's Washington office and co-chair of its Corporate Finance Practice. "That means companies need to be vigilant about their disclosures."

The SEC last issued guidance on cybersecurity disclosures in 2011. Since then it has issued several dozen comment letters to companies that experienced a cybersecurity issue and failed to disclose it entirely to the SEC's liking. Even if the agency doesn't revisit its current guidance on cybersecurity disclosures, "[SEC Chair] Mary Jo White has told Congress the issue is important to the SEC," says Tony Rodriguez, a partner in Morrison & Foerster's San Francisco office whose experience includes representations in SEC matters.

The continuing SEC scrutiny also raises concerns about potential litigation. "While we haven't necessarily seen an increase in cybersecurity cases, if a company is called out by a regulator on their disclosures, it could encourage plaintiffs to take legal action," Rodriguez observes.

What should companies do? Besides taking appropriate steps to protect data from cyberattacks and remediate breaches that do occur, make sure you have a robust process in place to communicate potential problems to corporate leaders. "Executives responsible for disclosures need to become aware of cybersecurity issues promptly so they can make appropriate disclosure decisions," Lynn advises.

Finally, approach disclosures in a thoughtful way and let the facts speak for themselves. Describe cybersecurity issues in an accurate, complete manner so as to minimize the possibility for SEC comments and potential litigation.

"Just because the last SEC guidance was issued in 2011 doesn't mean the issue has gone away," Lynn concludes. "Cybersecurity breaches will continue to happen to organizations across the board. So be vigilant about your disclosures."

ROOTING OUT CONFLICT MINERALS

IF YOUR COMPANY manufactures consumer electronics, avionics, or any product incorporating even trace amounts of gold, coltan, cassiterite, or wolframite—including their derivatives, tantalum, tin, and tungsten—you may need to ask how well you know your conflict minerals story.

Under Dodd-Frank, public companies may soon be required to report on their use of any of these minerals originating from the Democratic Republic of the Congo and nine other African nations. "The SEC adopted the rule, but it has been subject to a legal challenge to the validity of its rulemaking," says Morrison & Foerster securities partner David Lynn. "A decision was reached in April holding that the statute and the SEC rule violate the First Amendment of the Constitution. If the rule ultimately requires reporting, the practical implication is to be ready to tell your sourcing story."

Compliance could be potentially costly and complicated. Lynn suggests that companies know the country of origin; ensure that downstream suppliers (including mines, smelters, and refiners) are conflict free; review and revise sourcing policies and contracts as necessary; and raise awareness of this issue with your entire supply chain.

JEFF HEILMAN

Illustration by **CHRIS PYLE**

Worn on the

WATCHES THAT MONITOR sleep quality. Skullcaps that gauge head injury. An infant bodysuit that sends temperature and breathing updates to a mobile device. Ear buds that track your heart rate. These are just some of the innovations now emerging in the hot new field of wearable technology.

Currently estimated at $1.6 billion, the wearable device market is expected to grow to $5 billion in revenue by 2016, according to Gartner. If upcoming releases like Google Glass (scheduled for mass distribution later this year) prove as popular as smartphones and tablets—whose combined revenue topped $66 billion in 2013, according to the Consumer Electronics Association—wearable devices stand to become a major new realm in technology.

But the technology is already garnering a lot of attention from lawyers and lawmakers with concerns about how the devices—and the information they collect—can be misused. Wearable devices are just one more example of how technology gets ahead of the law, says Gabriel Meister, a New York-based partner in Morrison & Foerster's Technology Transactions Group. "Often, the legislative response to perceived risks is very blunt, until we figure out exactly what the risks are."

Close to the Vest

One of the first attempts to address privacy-related legal issues—an 1890 *Harvard Law Review* article written by attorneys Louis Brandeis and Samuel Warren—sprung from concerns about the newly introduced handheld camera. People were afraid a newspaper could photograph them in a private space and publish it the next day, according to Andrew Serwin, a Morrison & Foerster Global Privacy and Data Security Practice Group partner.

"They felt the technology was extremely invasive," Serwin says. "What happened was the volume of data and its velocity increased. Wearable technology is the same issue—just at a much faster velocity, with much more volume and permanency."

Smartphones let users quickly shoot and share images. Google Glass wearers can snap a photo by speaking a phrase. With each new device, consumers are receiving and transmitting more information that can be stored indefinitely and potentially retrieved, shared, or even sold by people unknown to the original user, especially if they are stored or shared on a centralized server.

Fitness enthusiasts, for example, wouldn't necessarily want their health insurance provider—which may base premiums on health status—to access their blood pressure readings. They presumably would want to know whether a fitness tech provider reserved the right to share information with a third party, Meister says.

"There are a lot of really attractive services a consumer can get through wearable technology," says Peter McLaughlin, of counsel in Morrison & Foerster's Global Privacy and Data Security Practice Group in New York. "But how are the folks offering the technology managing the [privacy] expectations of people who are actually using it? And who's seeing the data?"

Medical devices, another transportable tech trend, can present even greater privacy risks. "Portable insulin pumps are smaller than an iPhone, regularly record insulin levels, and can transmit the information electronically to a website a patient and doctor use," McLaughlin says. "That information is a bit more sensitive than workout stats."

In some cases, the Health Insurance Portability and Accountability Act—which is meant to assure the privacy and security of medical data—may apply. In any case, consumers will want assurance that their personal data is protected from hackers. "Wearable technology developers ought to start thinking about the security of the data in the device and the security of data transmission sooner rather than later in the development process," McLaughlin says.

Is This Thing On?

Wearable devices aren't just compact—they're discreet. They operate, present, and collect data with more subtlety than their predecessors. And that feature has raised fears that these devices could be presenting new and unforeseen risks to safety, privacy, or intellectual property. Just two examples:

In October 2013, Google Glass enthusiast Cecilia Abadie was pulled over for speeding on a San Diego highway. She was also cited for distracted driving due

Consumers love wearable devices because they're discreet and powerful. And that's exactly why regulators and privacy advocates worry about them.

BY ERIN BRERETON

e Sleeve

to the Google Glass she was wearing. The citation was later thrown out of traffic court because of a lack of evidence that Abadie was distracted by—or even using—the device.

In January, a man sporting Google Glass was removed from an Ohio movie theater and questioned by Homeland Security agents for two hours about potential copyright infringement. "Reportedly he was only wearing the glasses because he had his prescription lenses in them," Meister says. "He was ultimately able to get them to connect his Glass to a PC via USB and have a look, to prove he wasn't recording the movie."

Because Google Glass is still new, many people do not understand how it works. Over time, society may become more accepting of wearable technology, as it has with smartphones.

A fitness club is a good example of a place where many people would not like strangers to take—or share—their pictures. Many gyms warn against photos and recordings. But now that many consumers keep their camera-equipped smartphones on them at all times—including when working out, to listen to music—preventing all camera use can be challenging.

"If we become aware that inappropriate photos have been taken and we can identify the photographer, we revoke the person's membership," says a legal professional for a fitness chain. "But banning phones is just not going to work practically."

The widespread use of smartphones may have helped consumers accept their use in gyms as well, the professional says. "There was a lot of fear eight to 10 years ago when camera phones started coming out. They're here to stay; people just have to be courteous."

Promising Potential

In reality, it's almost impossible to completely eliminate all privacy-related portable technology risks, although that hasn't stopped some businesses from trying. "Some of the pre-emptive reactions to Google Glass, for example, involve certain states' gaming commissions telling casinos in certain states to go ahead and ban similar devices," Meister says. "There are also legislators, in Delaware, West Virginia, New Jersey, and Illinois at least, introducing legislation prohibiting Glass use while driving."

Society—and the legal system—may need more time to determine all the potential concerns associated with new wearable devices. New laws will emerge, just as some states and municipalities forbid texting while driving. "We're in the phase where we are trying to apply old laws to new technology," Meister says. "But at some point, when devices like this become essential, you see new laws being tailored to the technology, and not vice versa."

Although it caused a mild privacy panic in the late 19th century, society eventually made its peace with the handheld camera. Google Glass—and the wearable technology items yet to come—may very well experience the same trajectory. "What ends up happening is technologies either become ubiquitous and people get used to the invasion of privacy, or they go away," Serwin says. "You have to look at the issue with the perspective of time."

first mover
SPLUNK

Just What the Data Ordered

FOR SPLUNK, SWIFT GROWTH LED TO NEW POLICY AND PROCEDURAL REQUIREMENTS—AND NEW LEGAL CONSIDERATIONS BY ERIN BRERETON

San Francisco-based software provider Splunk's data collection and analysis product, Splunk Enterprise, was an almost instant hit upon its debut in 2006. The software, which collects and analyzes machine data generated by websites, applications, networks, and RFID assets, can identify traits like user transaction patterns and performance issues, making it useful for everyone from pizza companies to disaster relief agencies.

Companies can use Splunk Enterprise to identify fraudulent wire transfers while they're happening, route telecommunication carrier calls more efficiently, understand order delivery delays, and improve dozens of other operations.

In its first five years, Splunk's customer base swelled from 150 clients to more than 3,000. But it still relied exclusively on outside counsel to handle legal needs—until Splunk CEO Godfrey Sullivan met Lenny Stein. The former chief legal officer at winemaker Jackson Family Enterprises was introduced to Sullivan by mutual friends. Sullivan wasn't looking for a GC, Stein says. But the two got along well, and within three weeks, Stein had joined Splunk.

"The company was at an early stage and still growing rapidly," Stein says. "Its legal needs were finally getting some much-needed focus."

Stein—who has worked as GC for both start-ups and multibillion-dollar corporations—began to institute the procedures required for Splunk to eventually go public. "I did a systematic assessment of the legal needs across all functions and aspects of the business," he says. "From that, I knew what was in good shape and what required more attention."

For example, the company needed to ensure it had the proper export control policies in place. Splunk's software was able to help because it is able to detect users' geographic location by IP address when they attempt to download the product. By correlating user data with a third-party database, Splunk has been able to reject access for U.S. trade- and transaction-prohibited countries and persons and also to document its compliance with export controls.

Splunk's federal government contract work also necessitated internal compliance checks. In recent years, the customer base has expanded to include security operational centers within companies, universities, and government agencies.

While the government can be a good customer, federal contractor agreements can present concerns involving intellectual property development and pricing and billing terms, notes Rick Vacura, who co-chairs Morrison & Foerster's Government Contracts Practice and who has worked with Splunk on government compliance matters. "You have to have certain compliance policies and procedures—Lenny understood that message loud and clear. When Splunk's government market started to grow, he wanted to put into place what compliance, infrastructure, and experienced personnel were needed so he could sleep better at night and the business could grow with minimum compliance risk."

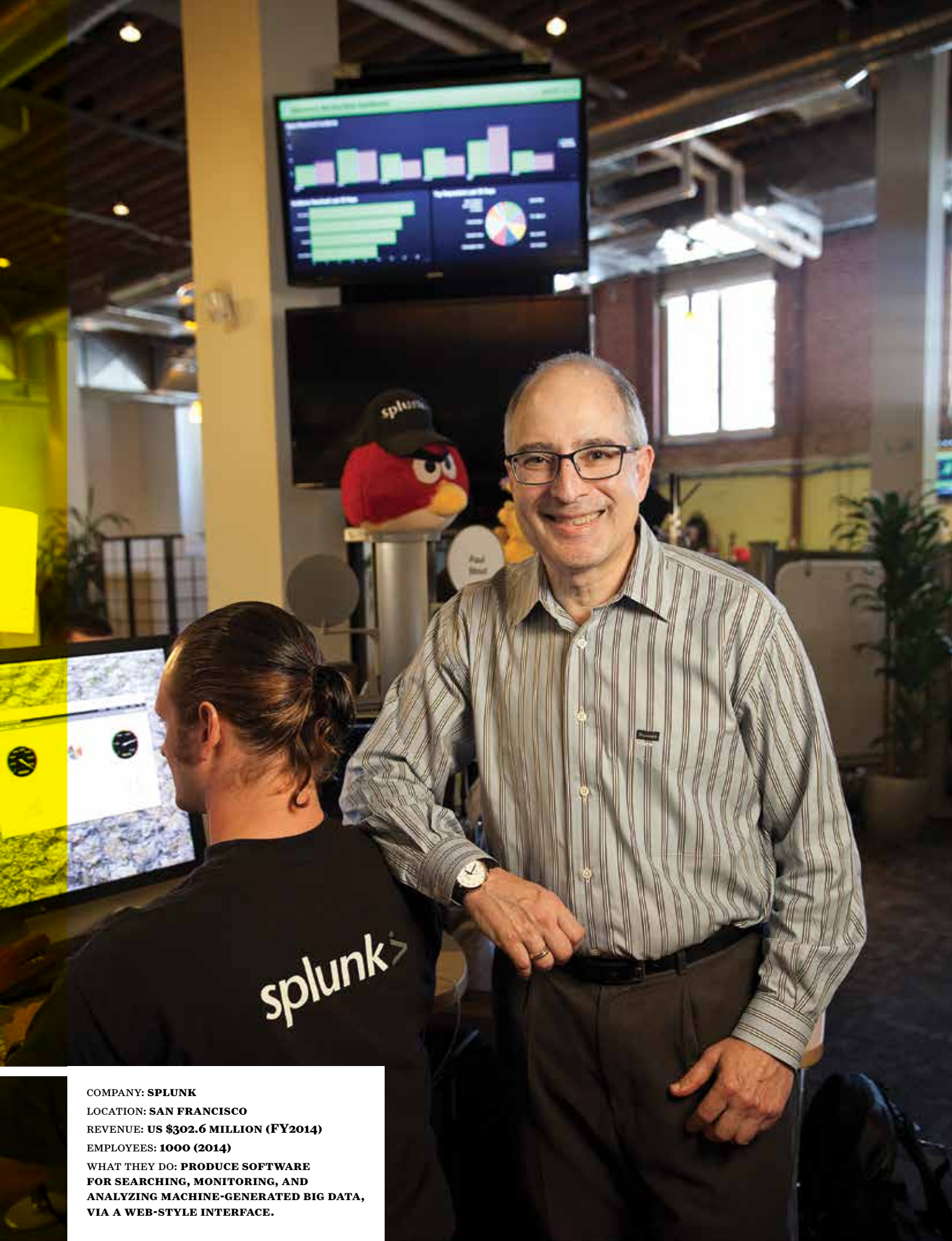
Requirements vary based on the type of contract, but contractors are generally subject to audits requiring them to substantiate any charges billed to the government. Splunk had to ensure it was carefully tracking expenses, expenditures, and other project details. "It's not unusual to have government auditors request access to a contractor's books and records regarding invoices that were submitted to—and paid by—the government three or more years prior to the audit," Vacura says. Having those records available is important because companies that can't prove compliance face stiff penalties. "If the company doesn't deliver what it promised and lacks adequate books and records, it can quickly turn into a civil or criminal false claims case," he says.

As Splunk's compliance needs grew, its legal department expanded from one person—Stein—to 17 in-house professionals. The company's client base has also increased to more than 7,000. Splunk hosts a robust online community where customers share tips for implementing Splunk products. Splunk's developers generate new offerings, but many of Splunk's new use cases actually come from its customers, Stein says.

"Organizations have come to recognize the tremendous value within their machine-generated data, now that Splunk has provided a platform to gain insight from that data in real time," Stein says. "Our customers have really led the way for our product's growth."

"The company was at an early stage and still growing rapidly. Its legal needs were finally getting some much-needed focus." **LENNY STEIN**

Photograph by **CRAIG LEE**



COMPANY: **SPLUNK**

LOCATION: **SAN FRANCISCO**

REVENUE: **US $302.6 MILLION (FY2014)**

EMPLOYEES: **1000 (2014)**

WHAT THEY DO: **PRODUCE SOFTWARE FOR SEARCHING, MONITORING, AND ANALYZING MACHINE-GENERATED BIG DATA, VIA A WEB-STYLE INTERFACE.**

DATAGRAM

Government 2.0

WITH IT SPENDING UP, FEDERAL AGENCIES ARE FINDING THEY NEED TO LOOK OUTSIDE THEIR WALLS FOR QUALIFIED TALENT. THIS IS PRESENTING NEW PUBLIC SECTOR OPPORTUNITIES FOR PRIVATE SECTOR TECH COMPANIES

BY JENNIFER GOFORTH GREGORY

THE U.S. FEDERAL government collects massive amounts of data. Everything from citizens' health care information, details about nuclear power plants, and data on the U.S. electrical grid are gathered every day. With most agencies migrating to a cloud-based solution, securing the data and breaking it into manageable units has become a high federal government priority.

As a result, the 2014 Federal Budget allocates $75.9 billion to IT spending, and many federal agencies are continuing to turn to private companies for additional support to meet the demand. This presents private companies with a tremendous opportunity to gain new clients and contracts within various federal agencies.

"This is an area of the government that has been as affected by sequestration and reduced spending as other areas," says Brad Wine, a partner in the Washington D.C. office of Morrison & Foerster. "Once a company is able to get its first government contract, especially with Homeland Security or one of the other three letter agencies and overcome barriers to entry in the federal sector, IT contracts generally and cybersecurity projects for the government in particular become a very lucrative area."

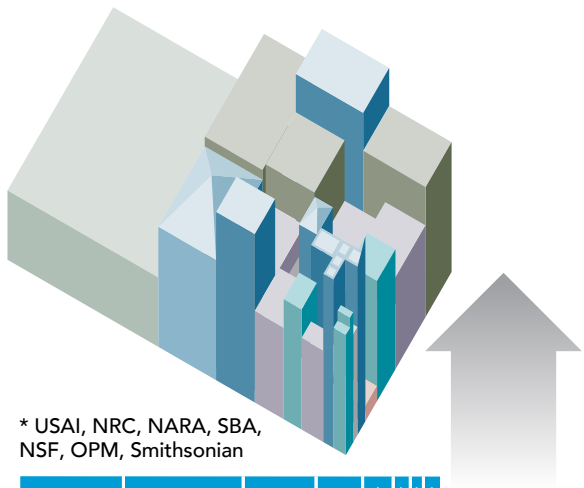
Previously, IT companies felt that they had to service either the private sector or the government. However, many companies now have a product or service that is marketable in both arenas, says Morrison & Foerster partner Greg Giammittorio. One of the trends he has noticed through his work with AlphaTech, a Morrison & Foerster initiative that focuses on peer-to-peer networking among CEOs of private technology companies and leaders of federal agencies, is federal agencies hiring companies that provide solutions to their problems. "Instead of simply wanting to spend money or hire a certain number of people, agencies are looking for companies that characterize themselves as solution-oriented providers and achieve results," Giammittorio says.

Funding for IT Projects

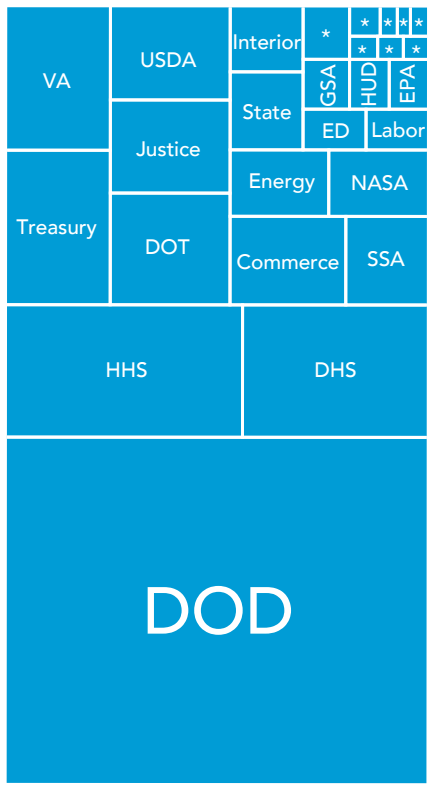
Not surprisingly, the largest funding for IT projects is available through the Department of Defense, which accounts for 44.9% of the total IT budget. But even an agency such as the Department of Education, which comprises only 11.8% of the budget, still has $622.5 million to spend on IT projects. "Since almost every agency collects data and every piece of data needs security, opportunities also exist in agencies that you might not immediately think of. Companies should be sure to not overlook those projects since fewer companies may be bidding for those agencies' dollars," says Wine.

Who Gets What?

Percentage of funding allocated per agency



* USAI, NRC, NARA, SBA, NSF, OPM, Smithsonian



Launching a Program

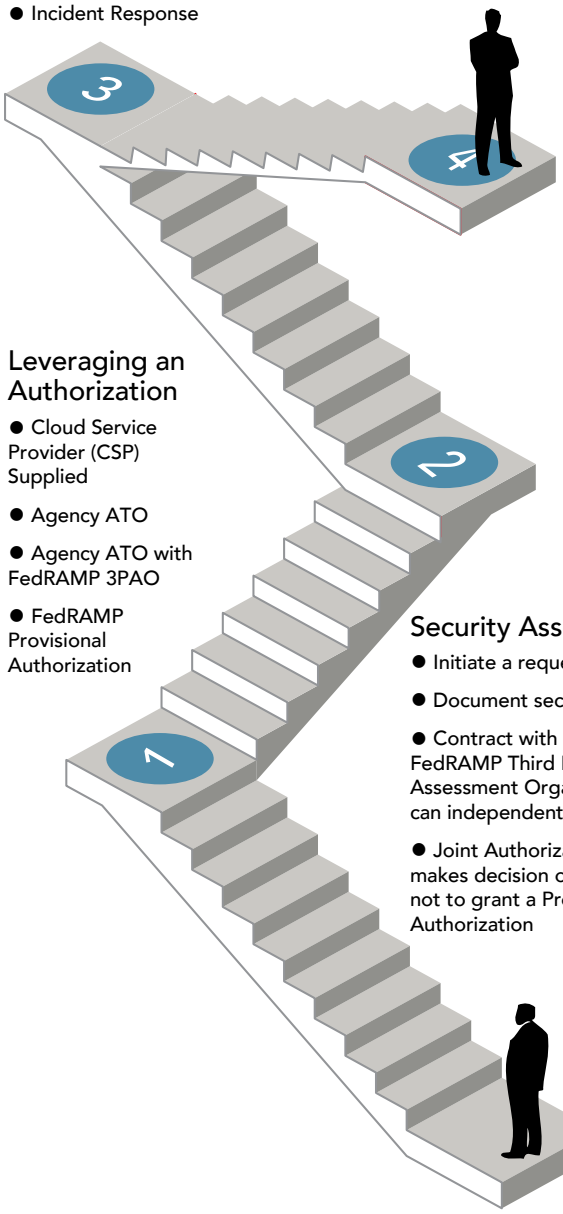
To help streamline and accelerate the process of acquiring all the certifications and clearances necessary for cybersecurity and cloud computing experts, the federal government has launched the FedRAMP program. FedRAMP is intended to ensure consistent quality among the companies that will provide cloud service to the government agencies that need them. Rather than requiring a company to become certified by each agency with which it will work, businesses can be certified to work with multiple agencies by simply following a process through which the FedRAMP Joint Authorization Board reviews all security assessments.

Ongoing Assessment and Authorization

The following is monitored:

- Operational Visibility
- Change Control Process
- Incident Response

Certified to work with multiple agencies



Leveraging an Authorization

- Cloud Service Provider (CSP) Supplied
- Agency ATO
- Agency ATO with FedRAMP 3PAO
- FedRAMP Provisional Authorization

Security Assessment

- Initiate a request
- Document security controls
- Contract with accredited FedRAMP Third Party Assessment Organization so they can independently test security
- Joint Authorization Board makes decision on whether or not to grant a Provisional Authorization

Key Cyber Investments

The 2014 President's Budget allocates more than $13B to cyber-related programs and activities.

Key priorities are:

SECURITY FEDERAL NETWORKS
$300 million

is included in new funding for DHS to support continuous monitoring of federal networks and better prevent computer intrusions

SHAPING THE FUTURE CYBER ENVIRONMENT
$85 million

for the Department of Commerce to support trusted identities in cyberspace and accelerate research and standards work on current and future information technologies

IMPROVING INCIDENT RESPONSE
$79 million

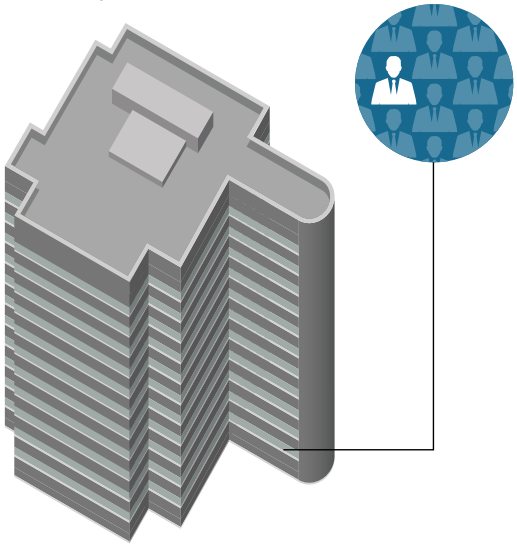
in new funding for DHS, DOJ, and DOD to help agencies and the private sector "connect the dots" in identifying and responding to cyber incidents

PROTECTING CRITICAL INFRASTRUCTURE
$5 million

in new funding is provided to DHS to assist critical infrastructure owners and operators as they secure their command and control systems

Getting in on the Ground Floor

Since it is often easier to get started with an agency when a project is just being launched, companies should keep informed about new government initiatives within their areas of expertise. Wine notes that a very effective way for a company to do business with the federal government is to start out as a sub-contractor to a larger company or a disadvantaged business already working in the space. "This allows the company to overcome the typical barriers to entry and develop a track record with the government that will increase their odds of earning future opportunities on their own," says Wine.



Q+A CHARLES DUROSS

Bribery, Twice Removed

FORMER U.S. ANTI-BRIBERY CHIEF—AND NEW MOFO PARTNER—ON THE RISKS COMPANIES OVERLOOK

Charles Duross is the head of Morrison & Foerster's Global Anti-Corruption Practice. He is the former head of the Department of Justice's Foreign Corrupt Practices Act unit, where he took a leading role in developing and implementing the government's anti-bribery enforcement strategy. Here, he discusses how tech companies can avoid violating the FCPA.

WE HAVE BEEN HEARING ABOUT MORE COMPANIES RUNNING INTO PROBLEMS RELATED TO THE FCPA. IS THIS AN INCREASING RISK?

I don't think bribery per se is increasing, but the risk of getting caught if you're paying bribes is. The Department of Justice has been strengthening its FCPA enforcement for years. But at the same time, many countries are now part of the OECD [Organisation for Economic Co-operation and Development] Anti-Bribery Convention, and have created their own laws that are very much like the FCPA. Forty countries have signed on, the most recent one being Russia. The OECD's Working Group on Bribery actively monitors enforcement of these laws, and there is a great deal of cooperation among countries about corruption cases. So enforcement is increasing—and not just by the U.S. government.

WHAT ARE SOME AREAS WHERE TECHNOLOGY COMPANIES RUN INTO TROUBLE?

Generally, businesses understand that they're not supposed to hand a cash bribe to a foreign official. But there are potential problems in areas that might be less obvious. One of the biggest comes from working through third parties. For example, if a company is bidding on a government project in a foreign country, it might retain a local consultant to assist, which is fine. However, if that consultant is using part of that fee to pay off a government official to obtain or retain business, that can get you in trouble. Indeed, the FCPA has a "willful blindness" provision, which means you can't avoid criminal liability by simply remaining deliberately ignorant about what your agent is doing.

SO IT'S IMPORTANT TO UNDERSTAND WHAT CONSULTANTS ARE DOING ON YOUR BEHALF IN THEIR DEALINGS WITH FOREIGN GOVERNMENTS.

Yes. But technology companies are also at risk from the distribution model that's often used in the industry. Many companies sell their products to channel partners, which add some value to the product or service—such as other hardware, software, an installation, or a service plan—and then resell it at a higher price. That's an entirely appropriate business model. But as with any third party, companies need to appreciate the potential risk if, for example, the distributor is simply reselling at a higher price without adding any legitimate value and using that profit as a slush fund to funnel bribes to government officials. It may seem to the company that it is not violating the FCPA. It has simply sold its product to another company. But if a company's employees are aware that the distributor is paying (or just offering) bribes to government officials to help sell the product, the company and its employees could be criminally liable as conspirators and aiders and abettors.

WHAT SHOULD TECH COMPANIES BE DOING TO AVOID THESE ISSUES?

One thing is to know the third parties they're doing business with. It is also fundamental to understand the business reason for working with third parties. One of the first questions asked during a DOJ or SEC investigation will often be, "What was the business purpose behind working with X?" Having a clear answer will earn credibility with regulators and underscore the company's commitment to compliance.

Also, making sure employees—and third parties—understand company policies, are properly trained, execute FCPA certifications, and are subject to appropriate ongoing reviews can prevent violations and mitigate (or avoid altogether) penalties if a problem does occur. That is just good business. Corruption tends to occur at companies with loose control environments. While I was at DOJ, we routinely saw loose control environments leading to embezzlement, self-dealing, fraud, and even antitrust violations. When a company doesn't know where its money is going, that's bad business and negatively impacts shareholder value. When companies invest in a compliance program, they are investing in the health of the business.

"I don't necessarily think bribery per se is increasing, but the risk of getting caught if you're paying bribes is certainly increasing."

Photograph by **ADAM AUEL**

Blurred Lines

TECH COMPANIES INVOLVED WITH MOBILE PAYMENTS MAY BE REGULATED LIKE BANKS **BY PETER HAAPANIEMI**

Mobile payments are taking off, and by 2017, consumers worldwide are likely to be using the technology to spend $700 billion or more annually, according to Forrester Research. But as technology companies look for ways to participate in that growth, they may find risks that they haven't anticipated.

"This is an evolving field, and there is currently no new mobile-specific regulatory framework addressing mobile payments," says Obrea Poindexter, a partner at Morrison & Foerster who leads the firm's Mobile Payments Group. Instead, mobile payments in the U.S. fall under a variety of regulators, such as the Treasury Department, the Consumer Financial Protection Bureau, and the Federal Trade Commission, which can make compliance complicated. At the same time, the mobile payments infrastructure typically involves an ecosystem of partners, such as financial institutions, payment card networks, merchants, and technology companies. This web of partnerships can blur the lines between companies, which in turn can lead to increased exposure for technology companies.

Mobile payment providers could fall under regulations that typically apply to banks. "When non-banks such as mobile payment providers are involved in things like money transmission or currency exchange, they can be classified as 'Money Services Businesses' and be subject to the Bank Secrecy Act or state money transmission laws," says Poindexter. In that case, the company may need to register with the Treasury Department's Financial Crimes Enforcement Network, file reports on suspicious financial activity, and have anti-money laundering programs in place. "That can be quite an obstacle for tech companies, especially new entrants," she says.

"U.S. regulators are sensitive to the idea that too many new laws and restrictions could impede innovation in mobile payments."

OBREA POINDEXTER

To help avoid such issues, contracts need to clearly delineate responsibilities. "It's key to define who is actually offering the product or service, and who is in charge of X, Y, and Z in the payments process," says Poindexter. It is not always easy to capture this up front, but "the regulators will look at how these relationships and products are structured to determine what regulations apply and who is responsible for compliance."

In general, Poindexter says, "U.S. regulators are sensitive to the idea that too many new laws and restrictions could impede innovation in mobile payments." But as mobile payments evolve, she says, regulators "are going to want transparent disclosure about the terms and conditions and any costs or liabilities associated with mobile payments." And with an infrastructure that can involve several technologies and partners, "they will want it to be clear who is actually responsible for the product, so that consumers know whom to contact when there are problems."

In sum, Poindexter says, companies that shape agreements with partners in the mobile payments arena should learn to "think like a regulator."

MoFo Tech IS A CUSTOM PUBLICATION PRODUCED FOR MORRISON & FOERSTER LLP BY LEVERAGE MEDIA LLC, HASTINGS-ON-HUDSON, NY.
EDITORIAL DIRECTOR: Michael Winkleman EDITOR: Richard Sine ART DIRECTOR: Patrick Mitchell, Modus Operandi Design
PRODUCTION DIRECTOR: Rosemary P. Sullivan COPY EDITOR: Sue Khodarahmi COVER ILLUSTRATION: John Ritter MORRISON & FOERSTER: Dave Harvey

Illustration by **GREG MABLY**

TELECOM POWERHOUSE

"They were just clearly and decisively head and shoulders above everyone else."

— Michael Rynowecer
President
BTI Consulting

Morrison & Foerster lawyers are dedicated to providing clients with best-in-class service. That commitment is reflected in our performance on the BTI Consulting Group's *Client Relationship Scorecard* for 2014, which recognized MoFo as the sole Powerhouse Firm in the telecommunications sector. BTI's Michael Rynowecer noted that MoFo lawyers are "clearly and decisively head and shoulders above everyone else."

Interviews with general counsel and other decision makers at more than 500 leading companies also earned MoFo top marks in high tech, banking and financial services, industrial manufacturing, professional services, and electric utilities. We stand apart as a go-to firm that clients entrust with their most vital and strategic matters.