Download: Greenwald on the Value of Privacy

Zapproved **has published** a complimentary recap of the PREX17 keynote address by Pulitzer Prize-winning journalist Glenn Greenwald, which explores the boundary layer between law and technology in the connected society.

In the fallout of the Edward Snowden NSA leaks, he explores the reasons why monitoring and evaluating the impact of our technology are crucial and discusses in detail:

- When weighing the importance of privacy, consider all of your personal information from all of your email accounts, social profiles and medical profiles.
- Ten years ago technology was the number one way privacy was compromised. Now, technology is the number one leading tool for how privacy is protected.
- Digital surveillance has become so prevalent and consequential that the NSA's motto for their citizen surveillance programs is "Collect it all."

Download the keynote summary.

What Does Ransomware Cost Companies?

By Eric Begun
King & Fisher Law Group, PLLC

In its 10-Q filing for the quarter ended September 30, 2017, Merck & Co., Inc. stated the following:

> On June 27, 2017, the Company experienced a network cyber-attack that led to a disruption of its worldwide operations, including manufacturing, research and sales operations. … [T]he Company was unable to fulfill orders for certain other products in certain markets, which had an unfavorable effect on sales for the third quarter and first nine months of 2017 of approximately $135 million. … In addition, the Company recorded manufacturing-related expenses, … as well as expenses related to remediation efforts … , which aggregated $175 million for the third quarter and first nine months of 2017.

Worth noting, this $310 million amount likely does not include all legal fees, forensic costs, and all other costs, expenses, and losses related to the cyber-attack. Nor does it appear to include other costs, expenses, and losses that may be indirectly revealed elsewhere in Merck's business or operations. The attack in question is the NotPetya ransomware attack, which impacted countless companies worldwide on June 27 of this year.

Lost Business Resulting from Ransomware

Merck's announcement is remarkable for several reasons,

especially for those who negotiate technology contracts and agreements with data privacy and security implications. First, it's noteworthy in its relatively clear quantification of lost business resulting from the ransomware attack. That is, often it is difficult to quantify lost business, lost sales, and consequential damages when negotiating liability provisions related to data security and information security in technology agreements and other commercial contracts. This is not to say that Merck's recitation of these amounts is a new rule-of-thumb or benchmark, but it may start a conversation.

Quantifiable Losses

Second, the loss numbers reported by Merck are not small ones. It is common to discount publicly announced forecasts of ransomware impacts that are viewed as extreme – $75 billion per year, according to one recently cited resource. But the concreteness of Merck's number and the specificity of the ransomware attack merits attention.

Ransomware is Fact-Specific

Third, the Merck announcement implicitly underscores the criticality of the precise facts surrounding the NotPetya ransomware attack and the unique business and situation of Merck. Not all ransomware or malware attacks can cause the same sort or amount of losses reported by Merck, nor does the same ransomware or other malware give rise to the same quality or quantity of losses for every corporate victim. When negotiating data privacy and data security provisions in commercial technology contracts and similar agreements, it is important for all sides to consider the specific circumstances and risks related to the transaction and parties in question.

Ransomware Impacts Are Not Necessarily Per-Record

And, fourth, the Merck report sheds light on the financial repercussions of ransomware, as opposed to other malware and hacking activities. That is, there are a number of industry and other reports and surveys that speak to the financial and other impacts of data breaches and security breaches on a per-

record basis (for example, cost per record, records per breach, etc.). The 2017 Ponemon Institute Cost of a Data Breach Study, Verizon's 2017 Data Breach Investigations Report, and Gemalto's Breach Level Index Findings for the First Half of 2017 are just a few. However, in many cases the particular per-record numbers reported do not provide a clear picture of the financial effects of ransomware, which often is not the kind or scope of cyber-attack that can be assessed on a per-record basis.

Merck's 10-Q for the third quarter of 2017 is definitely not a quick-fix answer to the question of how much a ransomware attack would or could financially impact a company. However, for attorneys, contract professionals, and others who draft and negotiate technology agreements and contracts and, specifically, information and data security and privacy provisions, the Merck quarterly report is potentially meaningful.

Former NSC Adviser Christopher Fonzone Joins Sidley in DC

Sidley Austin LLP has announced that Christopher Fonzone, former National Security Council (NSC) legal adviser and deputy assistant and counsel to the President, has joined the firm as a partner in its Washington, D.C. office. He will be a member of Sidley's global Privacy and Cybersecurity practice.

Fonzone has years of experience advising high-level government officials on some of the most pressing national security issues of our time. Most recently, he provided counsel to the National Security Advisor, NSC staff and other White House officials on legal matters concerning cybersecurity, foreign investment issues and trade sanctions, intelligence, military and counter-terrorism operations, and international disputes. He played a pivotal role in helping to develop the Obama Administration's Executive Orders on cybersecurity and position on key legislation designed to enhance the deployment of cybersecurity defensive measures and facilitate the sharing of cyber threat information between the public and private sectors. Prior to his time at the White House, Fonzone held positions within the Department of Justice and the Department of Defense, where he advised senior officials on a wide array of domestic and international legal issues, including those involving national security, military operations and litigation.

"Chris is an extraordinarily accomplished lawyer with significant high-level policy experience and an impressive background providing counsel on complex cybersecurity issues," said Alan Raul, founder and co-leader of Sidley's global Privacy and Cybersecurity practice. "We are proud to have Chris become a key member of our practice and join a growing number of notable recent additions to our privacy and cybersecurity group. We are very excited to welcome him to the team and look forward to working with him to expand our privacy and cybersecurity work in the defense and intelligence sectors."

Sidley's Privacy and Cybersecurity practice has grown this year, and now has more than 70 lawyers worldwide focused on U.S. compliance and litigation, the EU's General Data Protection Regulation and Asia's fast-evolving privacy regimes. In addition to internal growth, the practice has recently added lawyers in the privacy and cybersecurity space

including:
• Wim Nauwelaerts, a leading EU data protection lawyer, who is a new partner in Brussels;
• Tim Muris, former Federal Trade Commission chairman, now senior counsel in Washington, D.C.;
• Anthony Gardner, former U.S. Ambassador to the EU, now senior counsel in Brussels and London; and
• Kate Heinzelman, who joined the firm's privacy, cybersecurity and healthcare practices as counsel in Washington, D.C., following her service as deputy general counsel of the Department of Health and Human Services and associate White House counsel.

Supreme Court Leaves Holes in Anti-Hacking Law

The U.S. Supreme Court declined last week to consider two cases concerning the Computer Fraud and Abuse Act (CFAA), leaving certain questions unresolved regarding liability for computer hacking and the prospect for potentially harsh criminal and civil penalties, according to a post on the website of **Androvett Legal Media & Marketing**.

"Given the current state of the law, someone could potentially be put in jail or subject to civil liability under the CFAA in

one jurisdiction and not in another for the very same act," said attorney **Shain Khoshbin** of Dallas-based **Munck Wilson Mandala**. "In fact, someone could be potentially criminally prosecuted and civilly liable simply for password sharing."

The CFAA was originally intended to criminally prosecute individuals who accessed classified information by hacking into government computers. The federal statute was later amended to allow private civil actions for violation of the act. This allowed businesses to take the offensive against hackers and those who improperly access digital assets stored in computers.

"As the definition of 'computer' continues to expand, and computer networks continue evolving to include social media platforms, cloud storage and a wide variety of subscription-based services, the CFAA will undoubtedly continue to be tested in the court system," said Khoshbin.

"The CFAA is a valuable tool for businesses to use as part of their crisis management plan for data breaches, and to seek justice from those who improperly access electronic assets. But the judiciary or Congress needs to address and resolve some important issues so the law can be applied consistently."

Mitigating Cyber Risk: Third-

Party Service Provider Contract Considerations

Businesses are adapting to the new reality of cybersecurity threats by shoring up technology and educating employees regarding best practices and risks associated with an online presence, writes **Marc C. Tucker**, a partner in **Smith Moore Leatherwood LLP**.

"A business's electronic data is quickly becoming its most valuable asset– an asset worth protecting," he explains. "If data is trusted to a third party, the parameters of what is expected to keep your data safe should be memorialized in a contract with that service provider."

"Strategic third-party contracting practices will not eliminate all cyber risks but is an additional arrow in the quiver as you strive to protect sensitive data."

Read the article.

Join Our LinkedIn Group

You Don't Think Your Small

Business Will Get Hacked? You're Wrong.

While the majority of businesses at risk for criminal hacking are major institutions that deal with a lot of data – such as banks – the idea that small and midsize businesses aren't a target is mistaken, reports the ***Chicago Tribune***.

Reporter **Corilyn Shropshire** credits that analysis to Richard Sypniewski, CEO and managing director of Sagin, a management consulting and IT management firm.

Sypniewski said nonprofit institutions are at greater risk for criminal hacking than some other targets.

"According to [a Better Business Bureau] study, 90 percent of cyberattacks on business come from phishing emails and 90 percent of those phishing emails are ransomware, in which scammers breach a company's operating system with software designed to block access or hold data hostage until a sum of money is paid," writes Shropshire.

Read the *Chicago Tribune* article.

Join Our LinkedIn Group

Lessons Learned: Vendor Sued in Class Action Suit for Security Misses

By Eric Begun
King & Fisher

You're thinking that something about the title of this post sounds familiar, right? Information technology (IT) vendors and third party service providers have been in the spotlight for security breaches for some time (see, for example, vendor-based security lapses affecting Target, CVS, and Concentra, as just a few), and it doesn't sound surprising that an IT vendor has been sued related to a security incident. After all, whether you're an IT vendor or an IT customer, if you draft or negotiate contracts for a living, these situations are what you try to contract for, right?

Right…but…the recent federal class action suit filed in Pennsylvania against Aetna and its vendor surfaces several new privacy and security considerations for vendors and their customers. The vendor in question was not an IT vendor or service provider. Instead, the plaintiff's allegations relate to Aetna's use of a mailing vendor to send notification letters to Aetna insureds about ordering HIV medications by mail. According to the complaint, the vendor used envelopes with large transparent glassine windows – windows that did not hide the first several lines of the enclosed notification letters. The plaintiff asserts that anyone looking at any of the sealed envelopes could see the addressee's name and mailing address – and that the addressee was being notified of options for filling HIV medications. As a result, the vendor and Aetna are alleged to have violated numerous laws and legal

duties related to security and privacy.

For all vendors and service providers, but especially those that don't focus primarily on privacy and security issues, the Aetna complaint is enlightening. To these vendors and service providers, and to their customers: Do your customer-vendor contracts and contract negotiations contemplate what Aetna and its mailing vendor may not have?

- Do your contracts for non-IT and non-healthcare services fully consider the risk of privacy and security litigation? A noteworthy facet of the Aetna case is that the mailing vendor was sued for privacy and security violations that were not exclusively due to the customer's acts or omissions. That is, while the contents of the mailer certainly were key, the vendor's own conduct as a mailing services provider (not an IT or healthcare provider) was instrumental in the suit being filed against the vendor (and Aetna). Vendor services that previously didn't, or ordinarily don't, warrant privacy or security scrutiny, may, after all, need to be looked at in a new light.
- Do your contract's indemnification and limitation of liability clauses contemplate the possibility of class action litigation? Class action litigation creates a path for plaintiffs to bring litigation for claims that otherwise could not and would not be brought. Class action litigation against data custodians and owners for security breaches is the norm, and the possibility and expense of class action litigation is frequently on the minds of their attorneys and contract managers who negotiate contracts with privacy and security implications. But, for vendors and service providers providing arguably non-IT services to these customers – the idea of being subject to class action litigation is often not top-of-mind.
- Before entering into a contract, have you considered

whether the specific vendor services being provided to the particular customer in question implicate laws you hadn't considered? Vendors that operate in the information technology space – and their customers – generally are well-aware of the myriad of privacy and security laws and issues that may impact the vendors' business, including, as a very limited illustration, the EU General Data Protection Regulation, HIPAA, New York Cybersecurity Requirements, Vendors that aren't "IT" vendors (and their customers), on the other hand, may not be. For example, the Aetna mailing vendor may not have contemplated that, as alleged by the Aetna plaintiff, the vendor's provision of its services to Aetna would be subject to the state's Confidentiality of HIV-Related Information Act and Unfair Trade Practices and Consumer Protection Law.

- Have you considered which specific aspects of vendor services may directly impact potential legal liability, and have you adequately identified and addressed them in the contract? No, this is not a novel concept, but it nonetheless bears mention. A key fact to be discovered in the Aetna litigation is whether it was Aetna, or the vendor, that made the decision to use the large-window envelopes that, in effect, allegedly disclosed the sensitive and personally identifiable information. Given the current break-neck pace at which many Legal and Contract professionals must draft and negotiate contracts, however, unequivocally stating in a contract the details and descriptions of every single aspect of the services to be provided is often impractical (if not impossible). But, some contract details are still important.

Whether or not this class action suit is an outlier or is dismissed at some point, consider data security and other privacy and security issues in contracts and how vendor or service provider conduct may give rise to a security breach or

security incident.

Join Our LinkedIn Group

Equifax Breach Caused by Lone Employee's Error, Former CEO Says

The Equifax data breach happened because a single employee failed to implement software fixes, the company's former chief executive told members of Congress on Tuesday.

The New York Times reports that Richard F. Smith, who stepped down last week, repeatedly apologized to the members of the House Energy and Commerce Committee – and the American people – for the security lapse.

"Angry members of the committee tore into Mr. Smith and pressed him on how a credit bureau of Equifax's size, responsible for safeguarding billions of sensitive records on Americans' financial lives, could have allowed so much data to escape, unnoticed," write **Tara Siegel Bernard** and **Stacy Cowley**.

Read the *NYT* article.

Join Our LinkedIn Group

Hunton & Williams Partner Named Arbitrator for EU-US Privacy Shield Framework

Lisa Sotto, chair of Hunton & Williams' global privacy and cybersecurity practice and managing partner of the firm's New York office, has been selected as an arbitrator in connection with the EU-US Privacy Shield Framework Binding Arbitration Program.

The Program, developed by the U.S. Department of Commerce and European Commission, provides the terms under which Privacy Shield organizations are obligated to arbitrate claims, pursuant to the Recourse, Enforcement and Liability Principle. The binding arbitration option applies to certain "residual" claims as to data covered by the EU-US Privacy Shield. The purpose of this option is to provide a prompt, independent and fair mechanism, at the option of individuals, for resolution of claimed violations of the Principles not resolved by any of the other Privacy Shield mechanisms, if any.

In a release, the firm said Sotto has received widespread recognition for her work in the areas of privacy and cybersecurity. She chairs the US Department of Homeland Security's Data Privacy and Integrity Advisory Committee. She is regularly sought after by media outlets and industry

publications for her professional insights and appears regularly on national television and radio news programs.

Security of Information After You Install Software or Hardware

Chad King of King & Fisher in Dallas offers **some timely advice** on how companies can protect their information systems in an environment in which it is becoming increasingly difficult to stay ahead of cyber intruders.

He begins by recounting the story of how anti-virus and security company Kaspersky Lab was alleged to have been cooperating with the Russian Federal Security Service (FSB), the name of the Russian counterintelligence agency and successor of the KGB, since 2009. The U.S. federal government mandated that all software made by Kaspersky Labs be removed from government computer systems. Retailers such as Best Buy are also taking steps to remove Kaspersky Labs products from their retail offerings.

“Although it’s unlikely we will ever have a definitive answer about whether Kaspersky Labs is gathering data for the Russian FSB, this incident highlights a growing concern that foreign governments might be collaborating with software and hardware

companies to spy on other governments, corporate enterprises, and consumers. How can companies protect themselves in this environment?

His article offers five points to consider to deal with the threat.

Read the article.

Join Our LinkedIn Group

Equifax Execs Sold Shares Before the Hack Was Announced – But Was It Insider Trading?

Los Angeles Times reporter James Rufus Koren **examines** the question: Did three Equifax executives, including the chief financial officer, engage in insider trading when they sold thousands of shares in the days after the company discovered a massive security breach?

"The credit bureau has publicly stated the executives were unaware of the hack at the time of the sales, but the size of breach and timing of the trades has nonetheless stirred

suspicion," writes **Koren**.

SEC filings show that three days after the company discovered a massive hack had stolen information of up to 143 million consumers in Equifax's files, the CFO and the president of a business unit sold more than 10,000 shares. The next day, the president of another business sold some shares. All shares sold for about $146 each.

When Equifax announced the hack weeks later, the stock closed down about 16% from the time the executives sold stock, Koren writes. The company has said the executives did not know about the hack at the time of the sales.

Read the *LA Times* article.

Join Our LinkedIn Group

Sidley Welcomes Privacy and Cybersecurity Partner Wim Nauwelaerts in Brussels

Sidley Austin LLP announces that Wim Nauwelaerts has joined the firm as a partner in its Brussels office. He will be a member of Sidley's global Privacy and Cybersecurity practice.

In a release, the firm says Nauwelaerts has almost 20 years of experience in privacy and data protection matters.

The release continues:

He advises companies on all aspects of EU and international data protection and privacy compliance, including preparation for the EU General Data Protection Regulation (GDPR), data transfer strategies, data security and breach requirements, and compliance training. He also assists clients with contract negotiations and represents them before supervisory authorities. While Mr. Nauwelaerts counsels clients in a variety of sectors, he has particular experience with life sciences, technology and new media clients.

"We have seen tremendous growth in our European data protection practice, which will continue as companies prepare for, and thereafter comply with, the GDPR," said Alan Raul, founder and co-leader of Sidley's global Privacy and Cybersecurity practice. "Adding Wim to our outstanding team of privacy practitioners in Europe, led by John Casanova and William Long, is a logical next step in ensuring we continue to provide clients with the highest level of service in developing and implementing privacy, data protection and cybersecurity programs around the world."

Join Our LinkedIn Group

Legal Ops Survey Results: AI, InfoSec, and the Cloud

OpenText Discovery (formerly Recommind) has published a report titled "Corporate Legal Ops Service Results 2017," which is available for complimentary **downloading**.

Starting in 2015, OpenText Discovery has commissioned Ari Kaplan Advisors to interview premier corporate legal ops professionals to identify new trends and eDiscovery issues. This report details the latest 2017 findings, such as:

- **AI and Analytics:** Is cost still an issue to adopting discovery analytics?
- **ECM & Discovery processes**: Are legal ops professionals consolidating their approach?
- **Cloud readiness:** Has the cloud reached a tipping point?
- **InfoSec:** Have data security concerns increased?

Download the report.

Are You Prepared for GDPR?

Take the Survey

The General Data Protection Regulation (GDPR) will become law in all EU jurisdictions on May 25, 2018 and will impact organizations that handle EU citizen data for any number of reasons, from employment to customer relations to marketing. Just because a company is not based in or even operating in the EU doesn't mean GDPR won't apply.

It is a broad and wide-ranging regulation that is posing significant challenges for the types of clients Yerra serves, namely global corporations in highly-regulated industries such as banking, consumer goods and pharmaceuticals.

To gauge readiness for GDPR across industries and global regions, Yerra has launched an **industry survey** to help benchmark where global corporations are in their preparations. The GDPR Reality Check survey is being run in collaboration with the Blickstein Group and will be open for submissions through the end of May 2017.

Take the survey.

Join Our LinkedIn Group

DLA Piper Victim of Massive Malware Attack

Bloomberg Law **reports** that the global law firm DLA Piper fell victim on Tuesday to a widespread cyber attack, which reportedly disabled networks at dozens of companies.

“The firm, like many other reported companies, has experienced issues with some of its systems due to suspected malware. We are taking steps to remedy the issue as quickly as possible,” according to a statement the firm posted on its website.

“But calls and emails to the firm either failed or went unanswered. The U.K.’s Legal Week reported that the attack had ‘knocked out phones and computers across the firm,’ including in Europe, the Middle East and the U.S.,” writes **Gabe Friedman**.

The Petya virus has been spreading, locking companies out of their networks and demanding a ransom in cryptocurrency to unlock them.

Read the Bloomberg article.

Join Our LinkedIn Group

GC Requires Outside Law Firms

to Encrypt Communications

The general counsel of Marsh & McLennan Companies has started requiring the company's biggest outside law firms to use an anti-hacking electronic communication technology known as Transport Layer Security, according to a report from **Bloomberg Law**.

The report quotes Peter Beshar: "What we have done here is gone out to 12 or so of the biggest law firms on the most sensitive matters and insisted, 'You can't communicate with us other than through TLS,' and everyone has signed up by it."

Beshar identified three of the firms are Cravath, Swaine & Moore, Davis Polk & Wardwell and Gibson Dunn & Crutcher.

TLS prevents any unauthorized senders or recipients from entering and intercepting communication – protecting "data in transit" from being hacked, explains reporter **Casey Sullivan**.

Read the Bloomberg article.

Join Our LinkedIn Group

D&O Insurance in a Time of

Technological and Enforcement Uncertainty

Anderson Kill's 15th Annual D&O Conference, "**D&O Insurance in the Era of Technological and Enforcement Uncertainty**," will be presented Thursday, June 8, 2017, 3-5 p.m. EDT.

The event will be in the upper story of the D&D Building, 979 Third Ave., 14th Fl., New York 10022.

Directors and officers face an era of technological and enforcement uncertainty, the firm said in a news release.

Anderson Kill's annual D&O conference will feature a review of 2016 and a look ahead to 2017 for D&O liability and insurance. The conference also will feature a hypothetical D&O claim arbitration to explore key D&O insurance coverage issues in the context of a cyber claim, and will include a panel of policyholder attorneys, an arbitrator and an insurance company attorney.

Every organization faces data breach risk, whether through inadvertent data disclosure, computer system malfunction, or computer hacking. Data breaches cause real and severe peril.

The session will address the interplay of D&O insurance with other insurance policies in cyber claims, including crime insurance, property insurance, GL coverage, and cyber specialty insurance policies.

In addition, a panel of D&O insurance brokers will review major emerging D&O risks and provide a state of the market, highlighting key coverage terms to seek and avoid.

A cocktail reception follows the event (5:00-6:30 p.m.).

The D&O conference is complimentary for general counsel and risk managers: Use CODE AK005

Speakers:

William G. Passannante, Esq.
Shareholder
Anderson Kill
Conference Moderator

Joshua Gold, Esq.
Shareholder
Anderson Kill
Chair, AK’s Cyberinsurance Group

Raymond A. Mascia, Jr., Esq.
Attorney
Anderson Kill

Vivian Costandy Michael, Esq.
Attorney
Anderson Kill

Jonathan E. Meer
Attorney at Law
Wilson Elser Moskowitz Edelman & Dicker LLP

Roger M. Moak
Arbitrator-Umpire-Mediator

R. Damian Brew
Managing Director, FINPRO
Marsh USA, Inc.

James McCue
U.S. Financial Institutions Practice Leader
Aon’s Financial Services Group

Register for the event.

Join Our LinkedIn Group

Invitation: Summer Legal Conference, Berlin

Knowledge Nomads' **Summer Legal Conference** in Berlin July 23-29, 2017, will feature sessions on law in the age of hyperconnectivity, legal issues in the sharing economy, and the legal fallout from Volkswagen's emissions scandal.

The event will be at Berlin's Radisson Blu Hotel.

The CLE-qualified sessions will feature a diverse group of speakers, including a broad range of nationalities, backgrounds and ages.

Interspersed with the the presentations will be an arts and culture day with a choice of seven tailor-made tours, a trip to the home of Volkswagen, and a closing dinner on top of the German Federal Parliament Bundestag building.

Other side events will include guided tours, dinners, receptions, concerts, a gallery tour and more.

Register or get more information.

Law Firm Sues Insurer Over $700K in Lost Billings Due to Ransomware Attack

A small Rhode Island law firm has filed a lawsuit against its insurance company after the insurer refused to pay $700,000 in lost billings following a ransomware attack on the firm that locked down the firm's computer files for three months, reports CloudNine's **eDiscovery Daily Blog**.

Doug Austin's report, based on a story in the ***Providence Journal***, explains that Moses Afonso Ryan Ltd. is suing its insurer, Sentinel Insurance Co., for breach of contract and bad faith. The insurer denied the plaintiff's claim for lost billings over a three-month period when the documents were frozen by a hacker's ransomware attack. The hacker encrypted the law firm's computer files, offering to unlock them if a ransom were paid.

The suit says the infection disabled the firm's computer network, meaning lawyers and staffers "were rendered essentially unproductive."

Read the eDiscovery Daily Blog article.

Join Our LinkedIn Group

Hackers Face $8.9 Million Fine for Law Firm Breaches

Three Chinese stock traders were ordered to pay $8.9 million in fines and penalties for hacking into two law firms and stealing information on upcoming mergers and acquisitions and then leveraging the information to trade stocks, according to a **Dark Reading report**.

A federal court in New York found that the three hackers installed malware on the law firms' computer networks, enabling them to view emails on mergers and acquisitions in which the firms were involved. Then they used that information to buy stock in at least three public companies prior to their merger announcements, according to the Securities and Exchange Commission.

The firms aren't identified in the complaints, but **Law360 reports** they appear to be Weil Gotshal & Manges and Cravath Swaine & Moore, based on information in charging documents.

Read the Dark Reading article.

Join Our LinkedIn Group