Inside 3Q2018

ACC Association of Corporate Counsel
BALTIMORE

FOCUS

President's Message

Karen Davidson

Greetings and welcome to the Q3 2018 newsletter! It's hard to believe that by the time this letter is circulated our Fall calendar will be in full swing.

ACC Baltimore enjoyed a great social in June at Urban Axes with Premier Sponsor Womble Bond Dickinson. A good time was had by all as we enjoyed tacos, beer, wine, and critiquing our axe throwing skills, all the while wondering what our Torts Professors would think.

July brought us co-branding with Premier Sponsor Miles & Stockbridge for the Miles Minority Network event. This annual event is a great way to celebrate the strides made in inclusivity, while being mindful that there is more to be done. As always, it was a wonderful party.

In my opinion the best part of being in-house counsel is the ability to concentrate on our client and to be their legal and business partner. However, we can miss the opportunity to "bounce things off" of someone else that private practice can afford; especially those who are in small/solo legal departments. ACC membership gives us the ability to connect locally, nationally, and internationally with other in-house attorneys who have "been there and done that." There are three opportunities in September alone to meet up with your fellow in-house lawyers: on September 13th join Shawe Rosenthal for a timely Labor and Employment discussion while you enjoy lunch; on September 20 we will have a Sponsor Appreciation Happy Hour in Exelon's beautiful new headquarters at Harbor Point; and our Chapter's Day of Service will also occur in September. Come out and have fun while doing good!

As always, we thank our sponsor firms for their generosity and for providing topical legal updates.

Best Regards,
Karen Davidson

If you ever want to share any ideas or comments with the board, here is the current list of officers and directors:

Karen Davidson — President
Prabir Chakrabarty — President elect and Treasurer
Larry Venturelli — Secretary
Joal Barbehenn
Cory Blumberg
Taren Butcher
Dee Drummond
Dana Gausepohl
Joseph Howard
Kaidi Isaac
Raissa Kirk
Kimberly Neal
Noreen O'Neil
Christine Poulon
Daniel Smith
Whitney Washington Boles
Matthew Wingerter

Upcoming Events

September 13
Luncheon sponsored by Shawe Rosenthal

September 20
Sponsor Social

October 21-24
ACC Annual Meeting in Austin, TX

Street Law Brings Together ACC Chapters and Local Schools for Legal Learning

The lack of diversity in the legal profession is not a new issue, but Street Law, ACC, the ACC Foundation, and ACC members are working to put the issue behind us once and for all.

The Corporate Legal Diversity Pipeline Program, a national partnership between Street Law and ACC, encourages diverse students to pursue careers in law. The hope is to foster a next generation of more diverse lawyers, bringing new and needed perspectives to the legal profession. Students gain exposure to the law and have the opportunity to receive counseling on the steps they can take to pursue a legal career. Corporate law departments share their knowledge and make connections with up-and-coming students. The hope is that these connections will serve as a pipeline for future diverse legal leaders.

The four tenets of the Corporate Legal Diversity Pipeline Program are: 1) training, 2) classroom visits, 3) a conference at a corporate legal department, and 4) extensions (mentoring, internships, etc.). While more than a dozen ACC chapters currently participate, ACC headquarters also undertook this initiative in the spring. As long champions of this program, it was wonderful for ACC staff to interact with students directly.

In late March, students from Potomac High School in Oxon Hill, Maryland, visited the new ACC national headquarters office to participate in their class of the ACC/Street Law Corporate Legal Diversity Pipeline Program. All of the students are members of the Law, Education, and Public Service Academy at their school.

Each of the legal volunteers spoke about how he or she became a lawyer. The students were able to hear first-hand that it's truly achievable if that is their goal. It's certainly hard to study, prepare, and be accepted into college and then law school. But it is attainable with planning, mentoring, and access to the right role models.

Much of the day was spent on legal simulations, interactive ways for the students to learn about the practice of law. This included discussing and practicing how to review and analyze facts in a case, and how to present before a judge. The volunteers also covered other public speaking skills, like delivering information calmly and confidently.

Many of the students only knew about lawyers from what they'd seen on TV, so time with real lawyers provided them with a more realistic understanding of a legal career. It's not always as exciting as what's on TV, but it's also a lot more approachable. One student shared that he'd previously thought that all lawyers were always "aggressive," but the time spent with ACC showed that lawyers don't have to be aggressive – or at least that they are much more than just that!

Our program provided the opportunity to teach this class of students more about the law in a few days than they'd likely learned in their entire lives. It was a memorable, fulfilling day for both the students and all of the volunteer leaders.

More than a dozen ACC chapters are active in Street Law nationwide, and the program is now 17 years old. This year, we expect that approximately 5,300 students will participate in the Corporate Legal Diversity Pipeline Program through partnerships with more than 70 companies, law firms, and ACC chapters. Some companies that participate include Coca-Cola, Merck, Verizon, Nationwide, HP, GE, Turner, and Capital One. It's an opportunity for the entire law department, from attorneys, to paralegals, to administrative staff, to collaborate and share their knowledge with the next generation of legal and business professionals.

Volunteer leaders participate in Street Law's half-day training before they begin the program. Street Law helps the leaders to select topics that will interest the students and highlight the volunteers' expertise. The program at ACC focused on immigration and cyberbullying – legal topics in the news today and relevant to the students' daily lives. Other topics frequently covered include: intellectual property, contracts, torts, alternative dispute resolution, employment law, and environmental law.

In addition to classroom learning on civil law and legal careers, the students truly enjoy the experiential components – seeing what a corporate law department looks like, observing the interactions between business colleagues, and even hearing about a typical "day in the life." They come away with a stronger interest in and knowledge of the law, with many new role models.

One of the highlights of the Street Law program is that many corporate law departments stay connected with the most promising students. In fact, these top students may return for another job shadow day, be asked to apply for internships or scholarships, or participate in mentoring. In many cases, it's the start of a strong relationship between the company and the students, a true pipeline for new, diverse legal talent.

If you're curious about starting your own Street Law program on behalf of your ACC chapter, you may find further encouragement in these results: In the post-program survey, between 67 percent and 75 percent (on average) of the participating students said they are more interested in pursuing a legal career than they were before the program. For the program at ACC, the Potomac High students were no exception. Seventy percent said they were more interested in pursuing a legal career than they had been prior to the Street Law/ACC program.

The hope is that more ACC chapters will participate in this worthwhile program. For more information, visit www.streetlaw.org. We are constantly inspired by the in-house community's efforts to give back and we are pleased to partner with so many of our volunteer leaders to increase the pipeline of diverse students entering the legal profession.

ACC News

2018 ACC Annual Meeting: Rates Increase After September 20

The 2018 ACC Annual Meeting, the world's largest gathering of in-house counsel, is scheduled for October 21-24 in Austin, TX. In less than three days you can choose from over 100 substantive sessions to fulfill your annual CLE/CPD requirements, meet leading legal service providers and network with your in-house peers from around the world. Group discounts are available. Visit *am.acc.com* for more information.

Drive Success with Business Education for In-house Counsel

To become a trusted advisor for business executives, it's imperative for in-house counsel to understand the business operations of your company. Attend business education courses offered by ACC and the Boston University Questrom School of Business to learn critical business disciplines and earn valuable CLE credits:

- Mini MBA for In-house Counsel, September 12-14, and November 7-9
- Finance and Accounting for In-house Counsel, September 5-7
- Project Management for in-house Law Department, November 14-15

Learn more and register at *www.acc.com/businessedu*.

ACC Law Department Leadership: A Transformational Leadership Program Presented by ACC and Queen's University

If you are an in-house lawyer looking to develop the transformational leadership behavior to influence, motivate, and inspire your reports, peers, executives, and other stakeholders around you to move forward, this is the ideal opportunity for you. The program is taking place September 28 in Toronto. Register today at *www.acc.com/LDL*.

Are You Conducting Diligence on EVERY VENDOR and Third-party that has Access to Your Systems or Data?

Your vendors are now prime targets for data breaches and small vendors can provide easy access for hackers. Even cleaning crews, HVAC vendors, and food distributors, to name a few, can all lead to data breaches, but are often overlooked in the vendor diligence process. ACC's Exclusive third-party due diligence service should be in your arsenal. Visit *www.acc.com/VRS* for more information.

2018 ACC Global Compensation Report

For companies seeking to stay competitive in the marketplace and lawyers considering career moves, access to detailed compensation data for in-house counsel and legal operations professionals is absolutely essential. Based on responses from more than 5,000 lawyers in corporate legal departments from 65 countries and 39 different industry sectors, this first-ever ACC Global Compensation Report is precisely the resource you need. *Download the free Executive Summary*.

ACC Chief Legal Officers 2018 Survey

The ACC Chief Legal Officers Survey offers an opportunity to get data that supports the imperative for the CLO to report directly to the CEO. Other notable findings include what keeps CLOs up at night, reporting structures, how CLOs view the future of departmental budgets and staffing, litigation and contract workload, and where data breaches and regulatory issues have the greatest impact. Download it today at *www.acc.com/closurvey*.

2018 ACC Foundation: The State of Cybersecurity Report is now available.

Cybersecurity touches every aspect of consumer and corporate culture and is a chief concern for individuals and corporate leaders. Learn what more than 600 corporate counsel say about their cybersecurity experiences, role, and practices. Download the free executive summary at *www.acc.com/cyber*.

Thomson Reuters Practical Law Connect is the first-of-its-kind solution that integrates Practical Law legal know-how resources with essential Westlaw legal research. More than 230 Practical Law attorney-editors handpick resources and organize them into our proprietary task-based menus so you can get right to work. *Learn more about Practical Law Connect*.

NAVEX Global helps protect your people, reputation, and bottom line through a comprehensive suite of ethics and compliance software, consulting, and services. These include whistleblower hotlines, case management software, online training, policy management, and advisory services. ACC members receive an exclusive 10 percent discount off of their first year subscription fee when they purchase one of the Online Training Compliance courses. For More Information, visit *http://trust.navexglobal.com/ACC* or call +1.866.297.0224

Getting GDPR Standards to the Finish

By Michele Cohen and Veronica Jackson, Miles & Stockbridge

Despite the risks associated with failing to meet the EU General Data Protection Regulation (GDPR) standards that took effect on May 25, many companies are still working toward compliance. If you are among this group, it is critical to not give up but, rather, to focus on actively continuing efforts to achieve (and maintain) compliance. Potential fines for violating the GDPR include up to four percent of an organization's annual profits or €20 million ($23 million), whichever is greater. Two key areas to consider and address for GDPR compliance are your privacy policies and data mapping.

Privacy Policies

GDPR Impact: Under GDPR, the privacy policy on your website and other media channels may require updates to address GDPR notice and disclosure requirements, including those regarding an individual's rights with respect to your data collection and use practices. This may include required and affirmative consents from users, including your use of cookies and other tracking mechanisms. Remember that GDPR applies to all data collection, including through your website and also other channels, such as mobile applications and physical data collection.

Potential Actions: Review your existing business operations and data collection practices for GDPR applicability. Where appropriate, update your existing privacy policy to address GDPR considerations. Notify users of the changes to the privacy policy and, if warranted, create a mechanism for affirmative consent to your collection practices.

Data Mapping

Rights of Data Subjects to their Personal Data: GDPR expands the rights of data subjects to obtain information on whether and how their personal data is collected and processed. Data subjects also have the right to request copies of their data and the right to erasure (i.e., the "right to be forgotten"), meaning the deletion of their personal data from the data collector's possession for any ongoing use.

GDPR Impact: Under GDPR, you are responsible for knowing what personal data you collect or receive, the purposes for which the data is used, and where it resides (both within your organization and with third parties to whom you have transferred the data). Remember that GDPR applies to all data collection, including through websites and other channels, such as mobile applications and physical data collection. Data mapping is a critical step in compliance with these obligations.

What is Data Mapping?: Data mapping is the process of developing an inventory detailing all personal data collected and/or received by your organization, where this data comes from, where it goes (internally and externally), who has access to the data, how it is used, and where it is stored. Remember that data often flows in multiple directions and without conscious intent or realization. For example, a single email order from a customer might contain a host of personal information, from their name, phone number, personal address, etc. This email might be touched by the sales representative processing the order, a billing representative processing the credit card information, a support team member registering the account, and a data analyst processing survey data or website information that includes the customer's account information. Each of these touch points involves different storage types, including paper form. Some of these touch points likely also involve data transfer to a third party processor, such as the shipper of goods to the customer.

Potential Actions:

- Review existing business operations and data collection needs and practices for GDPR applicability.
- Initiate a data collection inventory, including an internal survey of processes in all organization departments. (You might also consider using an automated classification tool to facilitate this process.)
- Once complete, analyze your data collection practices to determine whether your inventory includes data collection or retention practices that are prohibited under GDPR.
- Consider whether your organization actually needs to collect and retain all of the data currently captured, which is required under GDPR's data minimization requirement.

For more information about GDPR compliance, see additional posts by the authors on the Miles & Stockbridge Intellectual Property Blog.

Michele Cohen is a principal and co-leader of the Real Estate & Transactional Finance Practice Group of Miles & Stockbridge. Her practice also includes business and information technology counseling for both providers and users of technology on a variety of subjects, including licensing, consulting services, e-commerce and cyber-security and privacy issues.

Veronica Jackson is an associate in the firm's Labor, Employment, Benefits & Immigration Practice Group. She is a Certified Information Privacy Professional by the International Association of Privacy Professionals. In the area of data privacy and security, Veronica counsels clients through incident response efforts, privacy law compliance, privacy policies, and training.

Appellate Courts Are Upholding Policyholder Claims for Coverage of Phishing Scams

By Daniel J. Healy

At the beginning of the year, three cases were pending in U.S. Courts of Appeal that turned on whether losses from phishing scams were covered, even if the scam involved more than just the initial fraudulent e-mail. One appellate court already had ruled in favor of policyholders on the issue before the three current cases were pending. Now, two of the appellate courts have ruled in the policyholder's favor.

Phishing losses are one the most prevalent, if not the most prevalent, cause of losses involving computer-related thefts. Such scams often are covered by crime policies that have specific provisions providing coverage for computer fraud and fraudulent transfers of money. In the increasingly complex world of computer scams, however, insurance companies are looking to avoid coverage. One often-invoked coverage defense against phishing claims increasingly is being found by courts to be an insufficient basis to deny coverage.

Companies that fall victim to these scams typically have a single employee targeted by a sophisticated email. Recently, insurance companies have relied upon causation arguments to deny coverage, claiming that a tricked employee was not intended to be covered and that only hacks that instruct banks to wire money (without the involvement of the policyholder's employee) are covered.

The most recent appellate rulings suggest that policyholders should fight coverage denials for phishing scam claims, particularly when those denials are based on the meaning of terms like "directly," "indirectly" and "caused by." The cases all involved a phishing email sent to an employee of the policyholder. In each case, the employee was deceived by the fraudulent email into believing that the email was a legitimate request for payment, had further contact with the thief who sent it, obtained internal approval to send money, and arranged to pay the fraudulent request.

Each of the cases also involved relatively similar policy provisions. The coverage grant was not identical in each of the policies at issue, but in each case provided coverage for loss directly resulting from computer fraud. The insurance companies denied coverage — with mixed results — by arguing, in essence, that the coverage only applied to losses from a hacker impersonating the policyholder and directing a bank to wire the policyholder's money to the hacker. Of course, nothing in the policies is actually that specific.

Two out of three of the underlying district court decisions had been favorable to the policyholder. The Southern District of New York found the policy language provided clear coverage, subject to resolution of certain facts. The Northern District of Georgia held that the language in the policy at issue is ambiguous, because if it means what the insurance company claims it means, then coverage would be illusory. The Eastern District of Michigan, on the other hand, narrowly construed the policy language to find coverage only when the loss immediately follows the fraud, with no intervening steps.

The Second Circuit Recognized the Reality of Phishing Scams in Medidata

The U.S. Court of Appeals for the Second Circuit ruled in *Medidata Solutions Inc. v. Federal Insurance Co.*, No.17-2492 ("*Medidata*") that the insurance company could not deny coverage on grounds that there were intervening steps from the initial fraudulent e-mail and the point at which the duped employee actually sent money to the thief.[1] *Medidata* involved a cyber loss resulting from a phishing scam that fooled Medidata's accounting personnel. The phishing email was directed to an accounts payable employee, purportedly from a Gmail account belonging to Medidata's president. It included a picture of the president and his email address, as well as a copy email address of a fake attorney. The fake attorney "spoofed" the code in the email to make it look like an email from the president, including in the "From" line. The email requested the transfer of $4.8 million. After writing to and speaking with the fake attorney, the employee obtained management approval and transferred $4.8 million to the fake attorney through a bank. Before further money was transferred, the scam was discovered, but the transferred money has not been recovered and the thief's identity is unknown.

Medidata, a technology company, had purchased crime coverage from Federal Insurance Company that included coverage for "direct loss of money, securities or property" from computer fraud or funds transfer fraud committed by a third-party actor. The policy's definition of computer fraud included fraudulent entry of and changing of data in Medidata's system. It further defined the transfer of funds to include transfers performed pursuant to "fraudulent instructions."

Federal nonetheless denied coverage. It claimed the coverage was not for when an employee was tricked into transferring funds, but only for when a hacker breaks into Medidata's computers and transfers funds. In other words, Federal argued that the loss was not caused by the type of loss the policy covered.

The U.S. District Court for the Southern District of New York ruled that Federal was wrong. It held that there was coverage because Medidata's loss happened when a thief changed computer code without permission to make the phishing email appear to be from Medidata's president, when it was not. Additionally, there was coverage under the funds transfer fraud coverage, because the mere fact that

continued on page 6

[1]Anderson Kill, P.C. partners Joshua Gold and Dennis Nolan represent an a*micus curiae* United Policyholders in the *Medidata* case.

continued from page 5

Medidata's employee "willingly pressed the send button on the bank transfer does not transform the bank wire into a valid transaction."[2]

Federal appealed. The Second Circuit largely upheld Medidata's arguments that the chain of events began with an accounts payable employee's receiving a spoofed email purportedly from Medidata's president, and that but for the receipt of that fraudulent email, the Medidata employee would not have "voluntarily" transferred funds.

In reaching its decision, the Second Circuit found that the phishing e-mail satisfied the New York Court of Appeals requirement, from *Universal American Corp. v. National Union Fire Ins. Co.*, 25 N.Y.3d 675, 680 (2015), that fraud takes place when someone gains "deceitful and dishonest access." The false and manipulated information presented in the phishing e-mail sent to Medidata employees began the chain of events that led to the wiring of funds. The resulting loss was thus covered.

This ruling is particularly useful for policyholders. By asserting that the actions of an employee victim of a phishing scam negated coverage, the insurance company is essentially attacking the weakest link, much like the scammer who sent the phishing email. The argument is that policyholder employees defeated coverage by initiating a transfer of funds. In rejecting Federal's approach, the Second Circuit held that "Medidata is correct that New York courts generally equate the phrase 'direct loss' to proximate cause" and "It is clear to us that the spoofing attack was the proximate cause of Medidata's losses." In other words, an insurance company cannot point to the weakest -- non-covered – step in the chain of events as the cause of the entire loss. In phishing scams, the fraudulent e-mail is the proximate cause.

By holding that fraudulent instructions from a scammer are covered as fraudulent whether sent to the policyholder or to a bank, the decision recognizes the sophistication and reality of phishing scams, and that the policy language does not distinguish between frauds based on how they induce a transfer.

Narrowly Construing "Direct Loss": *American Tooling*

In a case on appeal before the Sixth Circuit, a policyholder suffered a similar attack that the insurance company argued was not directly caused by a hacker or by a hacker impersonating an employee of the policyholder company. The district court ruled in favor of the insurance company, but the Sixth Circuit reversed.

In that case, captioned *American Tooling Center, Inc. v. Travelers Casualty and Surety Company of America*, No. 17-2014 (6th Cir.), the policyholder's employees were tricked into transferring money by fraud. Much like in *Medidata*, the hackers sent American's treasurer a "spoofed" email purportedly from a Chinese vendor and made it look authentic by using an email address very similar to, but not the same as, the vendor's email address. The email instructed American to pay several legitimate, unpaid invoices to a new, foreign bank account. Without verifying the new bank, American paid $800,000 to the identified account. Numerous emails and payments were sent from March through May 2016.

Travelers denied coverage, contending that the policy covered only "direct loss of, or direct loss from damage to, Money …directly caused by Computer Fraud" and the loss was not caused "directly" by computer fraud. Travelers further argued that "computer fraud" is defined as "the use of any computer to fraudulently cause a transfer of Money" and there were several steps, including authorization by personnel at American, from the date of the first email to the dates of the transfers.

The district court ruled in Travelers' favor,[3] finding no coverage by narrowly reading the coverage to apply only when the loss immediately followed the computer fraud as a matter of causation.

On July 13, 2018, the Sixth Circuit disagreed and ruled in the policyholder's favor.[4] It held that the intervening steps from the first phishing e-mail and contractual obligations were not relevant. Using a hypothetical scenario to unpack Travelers' arguments, the court explained that if "Alex" owes "Blair" five dollars and before Alex pays the five dollars "Casey" "snatches the bill from Alex's fingers," Travelers "would have us say that Casey caused no direct loss to Alex because Alex owed that money to Blair and was preparing to hand him the five-dollar bill."

The Sixth Circuit's common sense ruling takes into account the realities of modern-day fraud and underscores why the insurance companies' simplistic view is unrealistic. The risks include more than just direct hacks into a computer system.

Tie Goes to the Policyholder: Principle Solutions

Further underscoring the issue, in a third case on appeal the district court held that very similar coverage was ambiguous. In *Principle Solutions Group LLC v. Ironshore Indemnity Inc.*, No. 17-11703 (11th Cir.), an employee of Principle (an information technology company) received an email purportedly from the president of Principle asking her to work with an attorney to wire $1.717 million that day. She did; the money was wired after phone calls with the attorney, and of course the email was fraudulent and the imposter attorney was a thief. Ironshore denied coverage and argued that the coverage for "Loss resulting directly from" a "fraudulent instruction" to a financial institution to debit the policyholder's account did not apply when the policyholder's employee undertook acts between the fraudulent email and the debit. Again, Ironshore argued the narrow causation argument based on "directly."

continued on page 7

[2]The cite for the district court ruling is *Medidata Solutions, Inc. v. Fed. Ins. Co.*, No. 15-cv-907 (JAC), 2016 U.S. Dist. LEXIS 178501 (S.D.N.Y).

[3]*American Tooling Center, Inc. v. Travelers Casualty and Surety Company of America*, No. 16-12108 (E.D. Mich. Aug. 1, 2017)

[4]*American Tooling Center*, No. 17-2014, 2018 WL 3404708, — F.3d. — (6th Cir. July 13, 2018).

continued from page 6

The district court disagreed, pointing out that corporate policyholders can only act through the actions of their employees.[5] The court further found the policy language ambiguous. That means it was susceptible to more than one reasonable reading and, because the insurance company wrote it, the tie goes to the runner: there is coverage for the policyholder. Hitting the nail on the head, the district court stated:

If some employee interaction between the fraud and the loss was sufficient to allow Defendant to be relieved from paying under the provision at issue, the provision would be rendered "almost pointless" and would result in illusory coverage.[6]

Now on appeal, Ironshore argues that the district court failed to read the meaning of "directly" into the policy language to cut off any coverage after the point at which the fraudulent email was sent. The causation argument is very similar to those at issue in *Medidata and Principle*. The issue for the appeals courts deciding these issues is how narrowly to read the term "directly" and whether the term denotes that there is coverage only when the sole thing that happened prior to fund transfer was the hacker's fraud. That decision may turn, in part, on whether the policy language requires that the hacker tricked the bank (only) and did not involve the policyholder.

Notably not at issue in these cases are so-called "voluntary parting" exclusions that insurance companies often use to argue that there is no coverage when an employee is deceived. Those provisions should be noted if present in a policy for crime coverage or other first-party coverage that might be relied upon in the event of a cyber loss. Unfortunately, the foregoing cases demonstrate the insurance industry's desire to avoid coverage for cyber losses that involve an employee being tricked into transferring money whether or not "voluntary parting" language is in the policy.

Nevertheless, the appellate decisions handed down in two out of three of these cases are reassuring for policyholders who may suffer ever changing forms of attack. They join some of the prior pro-policyholder decisions in the area. For example, in 2016, the Eighth Circuit found that a malware intrusion, followed by employee steps that allegedly violated company policy, was covered. Along much the same lines of the decisions, the court stated "We agree with the district court's conclusion that "the efficient and proximate cause" of the loss in this situation was the illegal transfer of the money and not the employees' violations of policies and procedures." *State Bank v. BancInsure, Inc.*, 823 F.3d 456, 461 (8th Cir. 2016).

Policyholders should continue to focus on the overriding cause of a crime or theft loss and not on the particular, technological form it took. The foregoing cases demonstrate that insurance is meant to cover those risks that are unexpected and take new forms.

[5] *Principle Solutions Group, LLC v. Ironshore Indemnity, Inc.*, No. 15-cv-4130 (RWS), 2016 WL 4618761 (N.D. Ga. 2016).

[6] Id. at 14.

Europe's Extraordinary Grab For American Business

By Ted Claypoole, Partner, Womble Bond Dickinson

The European Union just began enforcing a set of laws that change how data is managed, and that try to impose those changes on the rest of the world. The General Data Protection Regulation (GDPR) takes extraordinary steps to capture and penalize US businesses that have never operated under the EU's data demands.

Both the EU and US enforce rules to protect the privacy of their citizens. US statutes protect its citizens' health, financial and children's information, and US regulators pursue and penalize companies that commit unfair or deceptive data practices. This targeted system enables business to build new models of data management that could be legally challenged if a consumer or employee is hurt by the activity.

EU regulation starts from a different set of assumptions. Under the EU regime, a resident has a fundamental human right to determine how information relating to the resident is used by others. Casting a complicated, circumstance-dependent concept like data privacy as a fundamental human right when others don't see it the same way is an inherently combative position. Fundamental human rights are essential to a civilized and moral existence. So a society that refuses to recognize such a right is, by definition, immoral.

And this sense of moral certainty encourages the EU to extend its privacy laws to companies thriving on opposite sides of the globe with very little contact with European residents. The privacy beliefs of Europeans or Americans are not questioned here, only the EU's shocking new weapons to impose its privacy beliefs on people who may not hold them.

Much has been written about the Brussels Effect, where the EU allows its economic weight to regulate food safety, chemicals and antitrust matters in a way that affects industry around the world. However, until the GDPR the EU has never passed a law with such striking and unprecedented tools to grab hold and penalize US companies. Viviane Reding, the EU legislator who initiated the GDPR, has been quoted saying that Google, Amazon, Facebook and Apple have historically ignored the EU privacy laws, but that the GDPR would be harsh enough to bring them into line.

Here are the new concepts introduced by the GDPR to force US companies to an entirely different set of privacy rules.

continued on page 8

continued from page 7

Designated Punishment Recipient: Many states require a company to keep a local representative who can receive official messages for the company. Under GDPR the EU becomes the first jurisdiction to require a company to appoint a local representative to be sued and fined in the company's place. Since nothing like this has existed before, no one knows precisely how it will work, except that the EU privacy regulators will collect their fines from someone whether or not that person was actually involved in the underlying behavior that led to the fine.

Regulator Moles Inside US Companies: Certain entities are required by the GDPR to hire a Data Protection Office (DPO), whose role is to teach the company about complying with European laws and to monitor and audit the company's compliance with those laws. In other words, this employee of the company, who by law cannot be fired for harming the company's interests in the pursuit of EU compliance, must be paid to serve as the EU regulator's eyes and ears within the company. The DPO must serve the EU's regulatory interests, even if the DPO's employer disagrees.

Reversed Burdens of Proof: All companies investigated or tried in under the GDPR are subject to reversal of the standard burdens of proving their guilt under the law. Under the EU privacy framework, a company is assumed to owe a duty of care to any EU resident whose data it is holding, is assumed to have caused or participated in any exposure of that data, and is assumed to have caused damages to the EU resident if data is exposed. US businesses that are victims of computer hacking will be presumed guilty on all important aspects of cases brought by EU residents and regulators. Fighting with both hands tied behind one's back is impossible, and soon insurers may recognize this fact and stop selling cybercoverage for EU cases.

Jawdropping Damage Awards: Once a US business is (inevitably) found responsible for exposing data or using data incorrectly under the GDPR, the company is subject to the higher of twenty million Euro fines or four percent of the company's gross annual revenue, which could be as high as $2.8 billion for Facebook or $3.5 billion for Google. This amount is much higher than other charges – even intentional felony matters – when the EU has penalized companies.

US companies may need to evaluate whether the rewards of doing business in Europe are worth the new set of EU hazards that reach across jurisdictions.

Ted Claypoole leads Womble's Privacy and Cybersecurity Team, IP Transactions Team, and FinTech Team, and he just stepped down as chair of the ABA's Cyberspace Law Committee and stepped onto the ABA Business Law Section Leadership Council. He has managed responses to scores of data exposure incidents in all types of businesses and has served as in-house tech counsel for CompuServe and Bank of America. With former White House CIO Theresa Payton, Ted has published the books *Protecting Your Internet Identity: Are You Naked Online?* and *Privacy in the Age of Big Data*. Ted can be reached at Ted.Claypoole@wbd-us.com.

Board Leadership