AMERICAN BAR ASSOCIATION
Tort Trial and Insurance Practice Section

Fall 2020

COMMITTEE NEWS

Cybersecurity and Data Privacy

Cybersecurity And Privacy Issues In The Time Of COVID-19

Glenn A. Brown
Squire Patton Boggs

Kristin Bryan
Squire Patton Boggs

The current COVID-19 pandemic raises some significant issues and risks relating to cybersecurity and data privacy in the US that should be considered carefully and addressed appropriately. Concerns range from cybercriminals targeting a newly remote workforce with clever phishing scams that prey on the environment of uncertainty, to worries that the crisis will give cover to expanded and potentially problematic uses of technologies such as geolocation and facial recognition. Many businesses are unsure of whether and how to collect and disclose their employees' health information under applicable privacy laws during an outbreak of infectious disease. This article explores such data protection-related issues facing businesses as well as some guidance on potential mitigation.

Cybersecurity and WFH Considerations for Employers

Cybersecurity incidents have increased since the COVID-19 outbreak and are expected to increase further during the coming months, as more and more of us

Read more on page 17

A senior member of Squire Patton Boggs' Data Privacy Practice Group, ***Glenn Brown*** *provides business-oriented advice to clients in numerous industries on regulatory compliance and data privacy matters, including cybersecurity risks, internal compliance measures and incident*

In This Issue

Chair Message

Dear Committee Members:

I am honored to serve as your Chair for the 2020-21 bar year. This is a year of great change for me personally as I transition from big law to an independent legal and consulting practice, and for all of us as we continue to address the fallout from the novel coronavirus pandemic on our personal and professional lives. Luckily, we have an active and dynamic Committee that will continue to innovate and provide opportunities to learn and grow in the cybersecurity, cyber insurance and data privacy space.

I want to thank immediate past Chair Michelle Worrall Tilton for her leadership this past year. Michelle took us through our first stand-alone program in March, just before the world shut down, and kept us on track with monthly Zoom calls and guest speakers. I know Michelle intends to stay active, which is a good thing. We have a great legacy of leadership in this Committee's short life, with our founding Chair, Kathy Strickland, and past Chair Janice Mulligan still active and engaged with our Committee.

My route to the Chair seat was an interesting one. I was a member of the original TIPS Cybersecurity Task Force, having been recruited by Kathy Strickland because of our work on the TIPS Disaster Recovery Task Force. While I have an interest in cybersecurity, and in particular cyber insurance and related coverage and risk issues, I am not a data breach response attorney and do not have a cybersecurity advisory practice. Nevertheless, my interest in technology (I chaired the TIPS Technology Committee three times) and cyber insurance kept me engaged. I was not looking to become Chair, but others insisted, so here I am.

Having chaired ESLR and Technology, and having seen the brilliant job done by Kathy, Janice and Michelle, I believe, with your help, we can continue to move this Committee forward to even greater accomplishments. And we have quite a few planned for the next few years.

Some of you recall that I surveyed existing vice chairs about their willingness to serve and their commitment to active involvement. Based on that survey, several original vice chairs have stepped down to make room for several new vice chairs. Earlier this year I circulated, in various stages, a Committee leadership structural matrix. Those of you who agreed to be vice chairs should know your place on that matrix. Some of you are serving as chairs or co-chairs of subcommittees or specific Committee initiatives. Others are serving as subcommittee members. All of you committed to active involvement. And I intend to hold you to that.

Larry P. Schiffer
Chair of the TIPS Cybersecurity and Data Privacy Committee

Larry P. Schiffer is Chair of the TIPS Cybersecurity and Data Privacy Committee. He is a past chair of TIPS ESLR and Technology (3 times) committees. He recently opened an independent legal and consulting practice, where he continues to provide insurance and reinsurance counsel and advice on insurance and reinsurance claims, contract wording, inspections, audits, dispute resolution, commutations and recaptures, insurance insolvency, due diligence for corporate transactions and investments, cyber insurance and related insurance and reinsurance issues, as well as serving as an expert witness, mediator and arbitrator.

Larry can be reached at lpschiffer@yahoo.com

We have our work cut out for us for the 2020-21 bar year given the likelihood that in-person meetings will not happen for some time. But we have lots of plans. First, under the leadership of Randolph Scott, the Committee will start the process of planning for its second stand-alone cybersecurity and data privacy conference to be held in 2022. Many of you, and many of the other TIPS general committees, will be involved in the planning process.

Second, the Committee will be preparing a book on cyber insurance. The book, "A Practical Guide to Cyber Insurance for Businesses," will be unique because it will focus on the policy itself, its components and what various industries want in their policies to meet their coverage needs. The book will provide an overview of cyber insurance. The book will then discuss how cyber insurance interacts with existing business insurance. Next, the book will provide practical advice for policyholders when looking to purchase cyber insurance. Finally, the book will have chapters focused on specific industries and highlight the risks and cyber issues unique to those industries. In these "industry" chapters, the authors will be encouraged to develop scenarios of a data security incident to highlight how insurance played a role in addressing that incident and the specific cyber and data risks attendant to that industry. We will need many authors, so if you focus on a particular industry in the cyber or data privacy space, get ready to sign up. Toni Scott Reed, Michelle Worrall Tilton, Michael Menapace, Lauren Godfrey and I will lead this project, but we will need many of you as authors.

Our goal this year is also to have four newsletters published. That means we need your case summaries and articles on a timely basis. Michael Nitardy and Thomas Kopil will lead that effort. We will also move forward with multiple webinars as we await the return of in-person programming. Melody McAnally will lead the webinar productions, but we need those of you who have webinar ideas to feed them to Melody and the Programming Subcommittee chaired by Joshua Mooney and Carolyn Purwin Ryan.

We also anticipate publishing several articles in TortSource, The Brief and, as part of the Annual Survey, The Journal. Those efforts will be led by the Publications Subcommittee co-chairs Kyle Black and Margaret Reetz, along with Mailise Marks heading up the Annual Survey, Kirsten Soto heading up TortSource and John Okray heading up The Brief. Reach out to them if you have an article.

We have many other subcommittees that will be active with several projects. These include the Membership Subcommittee, headed up by John Stephens and Lauren Godfrey, which includes YLD, Law Student, In-House and Governmental Counsel subcommittees. We need to drive more in-house and government lawyers involved

in cybersecurity and data privacy to our committee. A separate subcommittee for each will help focus that effort.

Our Technology and Social Media subcommittees, led by Robert Stines and Chad Anderson, respectively, will be active in pushing technology and social media efforts on behalf of our Committee. Expect to see lots of Tweets and LinkedIn posts as well as posts on TIPS Connect. Our Committee efforts on Public Policy and House of Delegates Resolutions will be led by Floyd Holloway, who will, I am sure, come up with ways to put our Committee up front as we confront cyber and data privacy laws and regulations.

Finally, I want to address our Diversity Subcommittee led by Deborah Yue. We need to bring some critical thinking to how our Committee can lead by example in addressing racial injustice and diversity within our Committee and our programs and publications. For example, one of the biggest problems facing underserved non-white communities is the inability to access quality wireless services. This is especially important in the face of the novel coronavirus pandemic because many of these students were left out or left behind when classrooms went virtual. What can we do as the Cybersecurity and Data Privacy Committee to help make sure underserved communities have access to technology and at the same time prevent them from falling victim to cyber-attacks and data breaches? If you have an idea, contact Deborah.

I look forward to working with all of you this year and in the years ahead to make our Committee the leading cybersecurity and data privacy forum for in-house, governmental and outside counsel. If you have any questions, ideas, or want to get involved, contact me. Michael Menapace, our Chair-elect, and I are looking forward to a great year.

Larry P. Schiffer
Attorney, Counselor, Consultant, Mediator

Editors Message

We are pleased to present the first TIPS Cybersecurity and Data Privacy Committee Newsletter for the 2020-21 bar year. You will find several interesting articles including two addressing privacy issues presented by COVID-19 by Glenn Brown and Kristin Bryan. Patrick McKnight writes on liability risks presented by contact tracing technology. John Stephens and Mary Grace Guzman discuss lawyer obligations for data breaches. We are also profiling two committee members, John Stephens and Zeshawn Mumtaz.

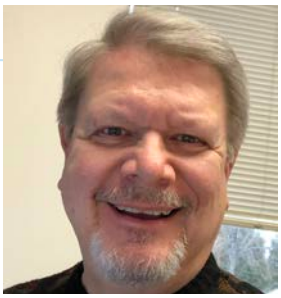
We've obviously been on a long strange trip for some time, and it's unclear when we'll be back to normal and be able to see everyone in person. Nevertheless, the Committee's work has been proceeding full steam ahead. Our outgoing committee chair, Michelle Worrall Tilton discusses the accomplishments of her tenure, and our new chair, Larry Schiffer, presents his vision for expanding on the committee's achievements and establishing the TIPS Cybersecurity and Data Privacy Committee as a leading go-to resource in this expanding area of law.

Call For Authors

We plan to publish a minimum of four newsletters during the new bar year. Since we are in a digital format, we are not restricted by page limits. We welcome submissions from any interested committee members for future issues. This is a great opportunity to establish your reputation in this important growing area. Articles can be as short as 1,000 words, or as long as you like. Non committee members are also welcome to submit articles. If you have questions, or want to submit topic proposals, please contact one of us. If you'd like to write, but can't come up with a subject idea, we'd be happy to can provide you with one or more. If you know of any other interested authors, please encourage them to reach out to us. We are here for you. Let us reserve space for your in our Winter 2020 issue.

Regards,

Tom Kopil and Mike Nitardy



Thomas E. Kopil
Signature Systems, Inc.

Tom Kopil is General Counsel of Signature Systems, Inc., a technology company specializing in data and cyber security solutions for businesses of all sizes, including restaurant point of sale systems. Tom has been a TIPS member for over 30 years, chairing several committees and having recently completed a three-year term on the TIPS Council. Prior to going "in-house", Tom was in private practice in Pennsylvania and New Jersey since 1981. He can be reached at tom.kopil@pdqpos.com.

Michael E. Nitardy
Frost Brown Todd, LLC

Michael is a member in the litigation department of Frost Brown Todd LLC. He represents clients in business and commercial disputes. Michael also helps clients comply with the applicable laws, rules, and regulations governing the proper use and disclosure of personal information. In addition to assisting clients in investigating and addressing potential data breaches, Michael also assists clients in addressing state and federal regulations regarding health law matters. Mike can be reached at mnitardy@fbtlaw.com.

Connect with Cybersecurity and Data Privacy

website

Stay Connected with TIPS

We encourage you to stay up-to-date on important Section news, TIPS meetings and events and important topics in your area of practice by following TIPS on **Twitter** @ABATIPS, joining our groups on **LinkedIn**, following us on **Instagram**, and visiting our **YouTube** page! In addition, you can easily connect with TIPS substantive committees on these various social media outlets by clicking on any of the links.

Contact Tracing Technology May Pose Liability For Employers

Employers have a duty to ensure a safe workplace. This responsibility has become particularly difficult during the COVID-19 emergency. As businesses gradually resume in-person operations, employers are carefully considering the details of their reopening plans.

The focus of reopening plans has, quite understandably, centered around employee and customer safety. However, employee privacy is quickly emerging as another possible cause for concern. Some employers have announced reopening plans involving contact tracing technology to help maintain workplace safety. While this new technology may be valuable, contact tracing technology also presents several potential legal issues.

What is Contact Tracing?

Contact tracing has been used by health officials for at least 100 years to help understand and limit the transmission of infectious diseases. Historically this process has involved a time-consuming process of in-person interviews.

Today, Technology Assisted Contact Tracing (TACT) is being used by some businesses and governments to automate this process. Although TACT is a broad term, much of the attention has focused on the use of mobile phone location data to track the movements of individuals and determine if they have been exposed to the virus. Privacy advocates have raised concerns over the use of TACT by governments. However, for reasons discussed below, employers should also be aware of the risks.

TACT covers a broad range of practices, but the most controversial involves downloading an application to the user's smartphone. The application uses a combination of health and location data to determine whether the user has encountered a person who has tested positive.

Several important technical distinctions in TACT technology have arisen from the initial experience of governments and employers. The most significant distinction is how the technology tracks a user's location data. The use of GPS data can lead to a centralized repository of information more likely to give rise to privacy concerns. Alternatively, the use of Bluetooth technology appears to avoid many of these potential problems.

Read more on page 21

Patrick McKnight
Klehr Harrison

*Author **Patrick McKnight** is an associate in the Litigation Department at **Klehr Harrison**. He focuses his practice on corporate and complex commercial litigation, employment law, and cybersecurity.*

The Coronavirus Task Force at Klehr Harrison stands ready to assist you in your business and legal needs. We will continue to provide additional information and guidance as the COVID-19 situation develops.

This article was original published on the website of the author's firm. Reprinted with permission.

See: https://www.klehr.com/publications/contact-tracing-technology-may-pose-liability-for-employers/

Ethics Are Stubborn Things And The Days Of A Cyber Breach Being Mainly A Client's Problem Are Gone

John Stephens
Hendricks Law, PC,

As a shareholder and lead counsel for data privacy, cyber and live entertainment at Hendricks Law, PC, John Stephens stands at the forefront of information privacy, digital marketing, new media and entertainment-related legal issues. He is known for his wide-ranging practice covering data security, intellectual property licensing, specialty insurance coverage and litigation, and media and entertainment transactions and litigation.

Mary Grace Guzman
Guzmán Legal Solutions

Mary Grace Guzmán of Guzmán Legal Solutions advises lawyers, law firms, and law students on their professional responsibilities and risk management needs. She also teaches legal ethics and professional responsibility at JFK Law School. She works with lawyers and law firms regarding legal ethics issues such as conflict of interest issues, fee disputes, and advises lawyers and law firms as outside ethics counsel to manage risk. Ms. Guzmán recognizes that a lawyer's or law firm's needs are best met by preventing legal ethical issues before they arise or managing an ethical issue once identified. Mary Grace can be reached at marygrace@guzmanlegalsolutions.com

Lawyers don't get a free pass when it comes to data security. In fact, ethical rules impose a series of obligations on lawyers when they or their firms are subject to a data breach. Moreover, the COVID19 pandemic forced many law firms to pivot their practices to either become fully remote or incorporate high levels of remote work opportunities.

Law firms often operate as a repository of sensitive client information, from proprietary trade secrets to personal data, such as social security numbers and medical information. We also store sensitive emails and other communications that clients intend, and prefer be kept, between themselves and the attorney. As a result of COVID19, all areas of law, be it private practitioners, government agencies or courthouses, have been forced to quickly, though often not seamlessly, integrate technology. This pivot includes establishing home offices for all employees, relying upon video conferencing services, or adding online data sharing platforms, all of which requires an attorney to comply with their ethical duties and protect client confidentialities.

In a significant ethics opinion issued more than a year ago, Formal Opinion 483, "Lawyers' Obligations After an Electronic Data Breach or Cyberattack[1], the American Bar Association's Standing Committee on Ethics and Professional Responsibility provided a detailed roadmap to a lawyer's obligations to current and former clients when it is discovered there has been a data breach potentially involving client data. Lawyers must seriously consider the requirements of this opinion as they continue to navigate the demands of law practice during COVID19.

"As custodians of highly sensitive information, law firms are inviting targets for hackers." *See* ABA Formal Opinion 483. Notably, the opinion warns that a lawyer's compliance with state or federal data security laws does "not necessarily achieve compliance with ethics obligations," and identifies six ABA Model Rules that might be implicated in the breach of client information.

The opinion follows Formal Opinion 477R[2], released a year earlier, in which the ABA explained a lawyer's ethical obligation to secure confidential client data when communicating over the Internet.

In ABA Formal Opinion 477, *Securing Communication of Protected Client Information* (May 11, 2017)[3], the ABA draws support from the Duty of Competence

Read more on page 23

Immediate Past Chair Message

Michelle Worrall Tilton
Zurich NA

Michelle Worrall Tilton is a Cyber Product Specialist at Zurich NA and is based in Kansas City. She may be reached at m.worralltilton@zurichna.com.

Dear Committee Members

I wrote my first column at about this same time last year. I remember it clearly because I worked on it in my dad's hospital room. It's been a tough year for so many of us. The past few months have changed the way we care for our loved ones, practice law, educate our children and go about our lives. I have come full circle because my dad's health is once again occupying my thoughts; crowding them, actually. I know from conversations with so many of you, that there are compelling human stories just beneath the surface of our professional titles. I am extremely proud of everything this Committee has accomplished. However, I know that we consistently perform at such a high level because of the personal connections with each other.

I am so very grateful for your hard work this past year. I know that you have other time commitments and that many of you also volunteer for state and local bar associations and other organizations, too. Committee work benefits and enriches our profession. We also know that what we give is returned to us many times over. Every article published and panel moderated, elevates our expertise. Every social event, Zoom Happy Hour and personal outreach develops friendships that extend long after article deadlines have been met and CLE programs have concluded. This is what makes our TIPS family so special.

Admittedly, I was worried at the beginning of the 19-20 bar year. I was concerned about maintaining our high level of Committee activities AND preparing for the stand-alone conference. Kathy Strickland, Jan Mulligan and Larry Schiffer promised that everything would be "fine." (Everybody, but apparently Kathy, Jan and Larry, knows that "fine" is not reassuring). But in short order, sleeves were rolled up. A terrific planning committee was in place. The venue was booked, and Tony Scott, the former Federal Chief Information Officer for the Obama administration, was a lock as our keynote speaker. Our stand-alone conference was scheduled for March 5 – 6, 2020 in Atlanta. Seriously, what could possibly go wrong?

Looking back to early March, we were so naïve – and perhaps blissfully so. We didn't know it at the time, but the pandemic was already spreading in urban areas and would soon threaten lives, livelihoods and our way of life. Many of us attended group dinners after the first day of the conference. Spirits were high because it had been a good first day. We sat close together and enjoyed a wonderful evening. In the Southern style, my dinner companions and I shared plates of food - a lovely and gracious practice; and now, something from the past. Looking back, it was one of those lightning in the bottle moments. It was the last time that I hugged people outside of my family. It was the last normal time as a professional. It was the last normal time, period.

So, where am I going with this? I'm not sure. I don't know what next week holds or the following. Some days, I'm not sure if it is Friday or Monday. I worry about my sons going back to school and about keeping my already vulnerable parents safe. I worry about the human toll of the pandemic. I worry about people of color and the systemic injustice and racism. I worry about people who are out of work. I worry about the environment, too. Yes, there's a lot to worry about right now. But this Committee is not one of them.

We are so fortunate to have an interest in this practice area. Cyber law is fascinating and constantly evolving. A speaker on a recent webinar sponsored by our Committee referred to cyber security as an "ecosystem" because it is dynamic and never static. Another term frequently used in our industry is "resilience." It's the ability of an organization to adapt to persistent cyber threats while maintaining operations, safeguarding people (and their data) and protecting brand equity. The ability to quickly mitigate the impact of a network security or privacy breach and return to normal business operations is crucial for an entity's financial well-being. We've heard from a number of guest speakers over the past several months that ransomware attacks are increasing as threat actors take advantage of the disruption caused by the pandemic. Organizations with remote employees are particularly vulnerable.

If you provide advice about network security and data privacy, it's a crucial time – as well as an opportunity - to contribute to the resilience of your firms, corporate employers and clients. There isn't a better time to share what you know with others and leverage your expertise. Our community of defense, plaintiff and in-house attorneys enjoy sharing information with each other. If you can't decide if you want to become more active on the Committee, there isn't a better time than the present. This is an amazing group of smart, hard-working, compassionate people. If you undertake a project and become overwhelmed because of life-work balance or other issues, there is always someone willing to help. The pandemic has tested and will continue to test our resilience. It's amazing, though, what we can accomplish when we work together.

I am delighted to pass leadership to Larry Schiffer. Larry is a good friend and will be an excellent Chair. He has well more than 30 years' experience as a leader in TIPS. I have leaned on him time and time again this past year. Jan and Kathy will also continue to provide leadership and institutional memory. Kathy did an amazing job organizing the stand-alone conference and serving as Program Chair. I owe her a debt of gratitude. And yes, the conference was "just fine" as she, Jan and Larry promised it would be.

Thanks, again, for all of your hard work and dedication this past year. It has been an honor and a privilege working with you.

Sincerely,
Michelle

AMERICANBARASSOCIATION
Tort Trial and Insurance Practice Section

The Tort Trial & Insurance Practice Section Introduces a New Advertising Opportunity!

The rates for advertising in this publication are:

AD SIZE OPTIONS	DIMENSIONS	COST
Online Lower Rectangle	920 x 90 | 300 x 250	$500
Online Middle Rectangle	920 x 90 | 300 x 250	$650
Online Upper Rectangle	920 x 90 | 300 x 250	$850

Additional information and print/online advertisement opportunities including discount options and complete media kits can be found by reaching out to M.J. Mrvica Associates, Inc., mjmrvica@mrvica.com

TORTSOURCE
A Publication of the Tort Trial & Insurance Practice Section

Member Spotlights

John Stephens

John Stephens
Hendricks Law, PC

As a shareholder and lead counsel for data privacy, cyber and live entertainment at Hendricks Law, PC, **John Stephens** stands at the forefront of information privacy, digital marketing, new media and entertainment-related legal issues. He is known for his wide-ranging practice covering data security, intellectual property licensing, specialty insurance coverage and litigation, and media and entertainment transactions and litigation.

Mr. Stephens together with his law partner, John Hendricks, recently formed "Smart Cyber" which is a practice group within Hendricks Law dedicated to efficient, custom tailored client service regarding cyber and data privacy issues, thus avoiding the one size fits all syndrome that most firms thrust upon their clients. Further, the Smart Cyber group consists of experienced cyber related trial consultants and expert witnesses regarding data privacy and cyber issues that are more and more frequent in today's litigated matters. The group is particularly valuable for clients in the discovery stage of litigation by knowing how and where to obtain key electronic evidence which is often overlooked by most litigators. Mr. Stephens has been a practicing certified CIPP-US for 6 years and is currently studying for his CIPM certification.

Prior to joining Hendricks Law, Mr. Stephens spent nearly 20 years as a media and entertainment litigator and technology/computer law attorney at Sedgwick LLP, forming and chairing the Cybersecurity & Privacy Group.

John can be reached at: JStephens@hendricks.law

Zeshawn Mumtaz

Zeshawn Mumtaz
People's Trust Insurance Company

Zeshawn Mumtaz was born and raised in Miami, Florida. He earned his undergraduate degree in Biochemistry & Molecular Biology from the University of Miami and subsequently worked as a New Development Chemist for many years. While being a chemist he discovered his passion for the legal field. Realizing that his mind was constantly wandering about the law, he decided to trade in his lab coat for a suit and briefcase. He enrolled in law school at Nova Southeastern University's Shepard Broad College of Law in Fort Lauderdale, Florida where he served in leadership positions in several student organizations.

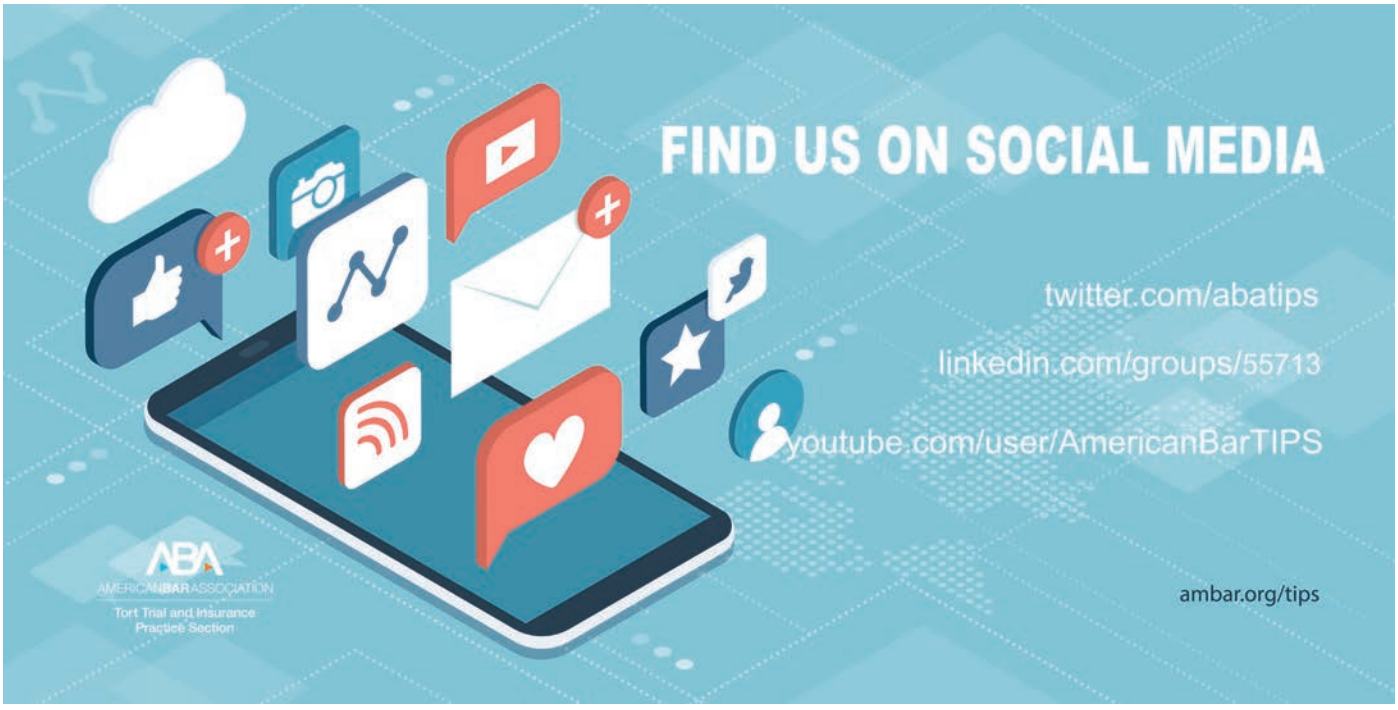
Zeshawn is now in-house counsel for People's Trust Insurance Company – a prominent homeowner's insurance carrier that serves the entire state of Florida.

In his day to day, he assists in transactional matters and helps develop operational efficiencies that improve the carrier's goals and objectives.

Zeshawn is very active with both the Florida Bar and the ABA. He was a fellow in the Florida Bar Leadership Academy and currently serves as a member of the Client's Security Fund Committee. He is also an ABA TIPS Now! Fellow, serves on the ABA Technology and New Media Standing Committee, and is on the ABA Insurance Regulation Committee. Zeshawn joined the ABA to improve his insurance acumen while finding ways to adapt current technology trends to the insurance industry. He is passionate about learning about the harmony between insurance coverage and cybersecurity. Based on his scientific background, and interest in cybersecurity, he felt that the TIPS Cybersecurity and Data Privacy Committee would provide him with excellent exposure to emerging issues.

As most of the world has transitioned to working remotely, Zeshawn has found ways to make the most out of the current circumstances. He maintains a steady workout routine that helps him stay focused. In addition, he always carves out time each day for his favorite hobbies to ensure that a work-life balance is maintained, including baking gourmet cookies!

Zeshawn can be reached at: zmumtaz@pti.insure



Tracking COVID-19 With Geolocation And Facial Recognition: Logistics And Concerns

In an attempt to halt the spread of COVID-19 and enforce social-distancing practices, the US government is reaching out to various companies in the private sector, including social media companies and telecommunications providers, to use existing technology, including app-enabled geolocation features and facial recognition technology. The government hopes that the use of this information will provide them with a better understanding of how the virus is spreading globally and whether or not individuals are practicing appropriate social distancing measures. Unsurprisingly, a variety of privacy considerations have arisen as a result of this information-sharing between the public and private sector.

The CDC is working with Palantir and Google, among others, to model the spread of the virus using data scraped from public social media. A task force has also been developed that is working in conjunction with the government, and includes several companies from the technology sector.

Data analytics company Palantir is working with the CDC to track COVID-19 through the use of data mapping and integration. The CDC previously worked with Palantir during the 2010 cholera outbreak in Haiti to monitor communications within the populace and track the spread of the disease. Similarly, the facial-recognition firm Clearview AI may potentially collaborate with state authorities to use facial-recognition technology to track infected individuals. Clearview reportedly developed its facial recognition algorithm using approximately 3 billion images scraped without permission from various websites. The company hopes to contribute to a greater understanding of "contact tracing", the term given to the practice of identifying individuals that infected individuals may have been in contact with.

The government is also in active talks with technology companies about using location data gleaned from cell phones to track the proliferation of the virus and to track whether Americans are adhering to social distancing protocols. As currently developed, the plan would involve the technology companies sending collected anonymous and aggregated geolocation and facial recognition data from their apps to the federal government as a means to map the presence of the virus. At this time, Google has indicated that the plan would not involve sharing an individual's movement or individual location. The data could be used to demonstrate the impact of social distancing and spread of COVID-19, similar to the way Google is able to store traffic or traffic patterns. The assumption is that the spikes in aggregated geolocation data could help the government track COVID-19, while detecting,

Glenn A. Brown
Squire Patton Boggs

*A senior member of Squire Patton Boggs' Data Privacy Practice Group, **Glenn Brown** provides business-oriented advice to clients in numerous industries on regulatory compliance and data privacy matters, including cybersecurity risks, internal compliance measures and incident response protocols. Having served in-house as Associate General Counsel and Chief Compliance Officer at a large consumer reporting agency, Glenn has a first-hand understanding of the day-to-day issues faced by companies handling significant amount of personal information.*

Kristin Bryan
Squire Patton Boggs

***Kristin Bryan** is a litigator experienced in the efficient resolution of privacy, class action, and commercial disputes, including multidistrict litigation, in courts nationwide. As a natural extension of her experience litigating data privacy disputes, Kristin is also experienced in providing business-oriented privacy advice to a wide range of clients, with a particular focus on companies handling consumers' personal data. Kristin can be reached at Kristin.bryan@squirepb.com*

disrupting, and discouraging gatherings that could result in a dramatic transmission of the virus between infected and non-infected populations.

The use of this data seemingly pushes the bounds of US privacy laws. The data likely is not being used in a manner that has been clearly communicated to users and many obvious questions have yet to be answered:

- What information is being shared with the task force?
- How is the information being kept secure?
- What conditions are being placed on the use of this data?
- What are the processes and procedures in place for destroying the data (or returning it) once it is no longer useful to the task force?
- Will the data be used for additional purposes beyond tracking COVID-19 (e.g., for law enforcement purposes)?

Although the information is being shared for altruistic purposes (i.e., the tracking of COVID-19), opponents of the data sharing practice argue that there needs to be more clarity in how the data is being shared and there must be an emphasis on consumer protection.

These data sharing practices come on the heels of more draconian data sharing practices around the world, including extensive surveillance practices in Singapore tracking where infected individuals have been and the Iranian-state developed app for individuals to check their symptoms but which also includes a geo-tracking feature.

The Tort Trial & Insurance Practice Section Introduces a New Advertising Opportunity!

The rates for advertising in this publication are:

AD SIZE OPTIONS	DIMENSIONS	COST
1/4 PAGE	3.625” × 4.625”	$650.00
1/3 PAGE	3.625” × 3.0625”	$850.00
1/2 PAGE	7.375” × 4.625”	$1,250.00
1/2 PAGE ISLAND	3.625” × 9.375”	$1,500.00
2/3 PAGE	3.625” × 6.25”	$1,800.00
FULL PAGE	8.375” × 10.875”	$2,400.00
INSIDE BACK COVER	8.375” × 10.875”	$2,750.00
INSIDE FRONT COVER	8.375” × 10.875”	$3000.00
BACK COVER	8.375” × 10.875”	$3,500.00

Additional information and print/online advertisement opportunities including discount options and complete media kits can be found by reaching out to M.J. Mrvica Associates, Inc., mjmrvica@mrvica.com

THE BRIEF

Cybersecurity and Privacy... Continued from page 1

are working remotely and as fraudsters look to leverage the uncertainty created by the crisis for phishing attempts and other forms of social engineering. There are reports of cybercriminals (as well as nation-state hackers) using interactive maps displaying Coronavirus statistics and other types of bait documents to plant malware on devices. Fraudsters have also taken to posing as Centers for Disease Control ("CDC") officials in attempts to obtain financial account information. Despite the limited ability to undertake large IT projects at this time, there are some sensible measures that businesses can take to mitigate these threats. Examples of these measures include:

- Reminding employees that phishing attacks are rising rapidly; consider rolling out refresher training on how to detect phishing attacks other forms of social engineering and the organization's procedures for responding to and reporting them.
- Reminding employees of the requirements of your information security, data handling, BYOD (bring your own device), data classification, data destruction, and other relevant policies, and the types of information that they need to continue to safeguard even when working remotely. Sensitive information, such as personnel records and financial information, stored on or sent to or from remote devices should be subject to heightened safeguards, such as the encryption of data in transit and at rest on the device and on any removable media used by the device.
- Reminding employees (if applicable) that they are required to use the company's virtual private network (VPN) when working and accessing company information to ensure that internet traffic is encrypted, especially if connected to a public Wi-Fi network. As more companies rely on VPNs, hackers are identifying and taking advantage of vulnerabilities. Reviewing incident response plans to ensure that the plan's provisions are still practicable when the organization's incident response team is working remotely. You should ensure that the protocols around incident response are clear, that incidents continue to be appropriately flagged and escalated, and that the incident response team can communicate effectively and efficiently. In order to do so, consider using communication techniques that operate outside of regular company communication methods (so-called "off-band" communication methods). Such off-band communication techniques should not be specified in your incident response plan, however, in the event cybercriminals obtain a copy of the plan.

response protocols. Having served in-house as Associate General Counsel and Chief Compliance Officer at a large consumer reporting agency, Glenn has a first-hand understanding of the day-to-day issues faced by companies handling significant amount of personal information.

***Kristin Bryan** is a litigator experienced in the efficient resolution of privacy, class action, and commercial disputes, including multidistrict litigation, in courts nationwide. As a natural extension of her experience litigating data privacy disputes, Kristin is also experienced in providing business-oriented privacy advice to a wide range of clients, with a particular focus on companies handling consumers' personal data. Kristin can be reached at Kristin.bryan@squirepb.com*

- Of course, not all organizations will have adopted the types of dedicated policies and trainings referenced above. So this would be a good time for organizations to review the policies they have to determine whether they adequately address security requirements for remotely accessing company systems. If no such policies address this issue, then we highly encourage communicating to employees some basic guidelines for remotely accessing company systems and using personal devices for company business, even if not in the form of a formal policy.
- Ensuring that your organization has installed all relevant security patches. These patches address known security vulnerabilities and failure to install patches allows cybercriminals to exploit such vulnerabilities to gain access to company systems.
- If your organization hasn't implemented multi-factor authentication, you should strongly consider doing so. Although this may be a larger IT project than is currently feasible, it will ensure greater security of the organization's systems when implemented.

The "Virtual" Conference – More Security and Privacy Concerns

The video conferencing service Zoom reportedly had 10 million monthly active users before the pandemic stay-at-home orders were enacted. Once businesses, schools and organizations rapidly moved to the remote-working and e-learning models, the service reported an increase to *200 million daily* users.[1] And that is when the real fun started. There have been reports of malicious "zoom-bombing," where bad actors were able to "drop in" on meetings or subject an unsuspecting audience to hate speech, profanities, threats or salacious images.[2] Not long after these reports surfaced, the New York state Attorney General, Letitia James, issued a letter to the company asking questions about its security practices. By the beginning of May, the AG had secured an "agreement" with the company for new security measures to be put in place to support and protect consumers, students, schools, governments, religious institutions, and private companies using the application for work, education, prayer, and socializing.[3]

Meanwhile, Microsoft reported its own spike in the use of its Microsoft Teams platform and tried to distinguish its service from others by extolling its security features. Other services like AWS (cloud-computing) and other video communication services like Cisco's Webex also saw a surge in usage.

By April, the FTC issued a bulletin entitled "Video-Conferencing: 10 Privacy Tips for Your Business."[4] The "tips" cover some of the basics – password protections,

limiting access tools, and warning users not to link on unexpected links. The FTC also recommends not using these types of services, if confidentiality "is crucial." Given the ubiquity of the services, the bulletin includes comments on software patches and a review of privacy policies (consent likely to be the key).

Addressing Employee's Health Concerns

The US Equal Employment Opportunity Commission has recently issued additional guidance for employers dealing with the issues presented by the COVID-19 pandemic. This information includes confirmation that employers may ask employees who report feeling ill or who call in sick whether they are experiencing any symptoms consistent with the coronavirus infection and may require employees to submit to non-invasive temperature testing to ensure employees are fever-free, each without violating the Americans with Disabilities Act (the "ADA"). The guidance additionally indicates that, consistent with the ADA, employers may require sick employees to stay home, and that employers may require employees who have been away from work due to illness to provide a doctor's note certifying the employee's fitness to return to duty, although the guidance indicates that with the current demand on the healthcare system, alternatives to physician notes may be necessary. Employers should still ensure that they are acting consistent with state paid sick leave laws, if applicable, to the extent they address return-to-work authorization.[5]

Telehealth Comes into its Own - Relaxation of HIPAA Enforcement

For entities that are covered under HIPAA ("Covered Entities"), the Office for Civil Rights ("OCR") at the US Department of Health and Human Services released a bulletin[6] in February addressing HIPAA Privacy in the context of the COVID-19 public health emergency (the "Bulletin") and issued a notice[7] in March regarding the exercise of its enforcement discretion in the area of telehealth (the "Notice").

Does COVID-19 halt the momentum of data privacy legislation?

Among the unknown impacts of the COVID-19 pandemic is that on the momentum of new data privacy legislation in the US. While state legislatures and Congress are working overtime on addressing the economic fallout from the virus, other priorities are necessarily being pushed aside, including data privacy. In California, where a ballot initiative is pending that would strengthen the California Consumer Privacy Act, it is unclear whether the proponents will be able to gather the requisite signatures to get the proposal on the ballot, given that large parts of California are facing shelter in place orders. In response to pressure from businesses, the California Attorney General delayed enforcement of some of the California Consumer Privacy Act

provisions until January 2022. For unrelated reasons, the Washington Privacy Act failed to pass for a second straight year and it may be that such comprehensive bills were going to lose momentum in any event. But it seems clearer by the day that what was once a flood of new state data privacy bills will likely be reduced to a trickle until the COVID-19 crisis passes.

Endnotes

1 https://www.zdnet.com/article/microsoft-teams-vs-zoom-microsoft-touts-its-superior-security-and-privacy/

2 https://computer.howstuffworks.com/zoom-bombing.html

3 *See* https://ag.ny.gov/sites/default/files/nyag_zoom_letter_agreement_final_counter-signed.pdf

4 https://www.ftc.gov/news-events/blogs/business-blog/2020/04/video-conferencing-10-privacy-tips-your-business

5 https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws

6 https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf

7 https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html

Contact Tracing... Continued from page 7

TACT in the Workplace

Employers face the difficult task of balancing employee safety and employee privacy. Employers have a duty to ensure their workplace is safe for employees and customers. As a result, many employers are considering implementing some form of TACT. As employees gradually return to work and stay-at-home orders are lifted, it is difficult to know which employees have been exposed. TACT offers the attractive prospect of assisting employers maintain a safe workplace during the reopening process.

Employers should be mindful of the potential risks arising from utilizing this technology. Under OSHA, employers have a general duty to provide workers with "employment and a place of employment, which are free from recognized hazards that are causing or are likely to cause death or serious physical harm." OSHA and the CDC do not appear to have provided specific guidance on contact tracing technology. Although the EEOC released updated return-to-work guidance regarding workplace discrimination, it does not address contact tracing technology specifically.

Potential Sources of Liability

Notwithstanding general OSHA and CDC requirements, employers should be aware of the following risks before including TACT in their return to work plan:

1. Employee Privacy Rights

Many states, most notably California, have some form of data privacy laws which may be implicated. The California Consumer Privacy Act (CCPA) contains several exceptions for employee data, but these exceptions are not unlimited. For example, employers with California employees may be required to provide disclosures before implementing TACT. Employers should be aware the CCPA contains a private right of action for violations.

2. Federal Employment Laws

Like temperature screenings and other COVID-related safety procedures, application of TACT in an uneven manner could give rise to discrimination claims. Employers should make sure to avoid targeting policies towards specific groups, even if these groups have been identified by health experts as being at an elevated risk (older workers, etc.). Any reopening plan should ensure compliance with Title VII, the ADEA, the ADA, and other federal laws. Employers considered covered entities under HIPAA will likely face additional restrictions while using contact tracing technology.

3. State and Local Government Requirements

Many state and local governments have Orders specific to businesses operating during the reopening process. Most states also have their own data breach notification laws. These local requirements vary by jurisdiction and often carry significant penalties.

4. Malware and Cybersecurity

Recently, twelve contact tracing apps were reported to contain malware. Hackers used these apps to infect devices with viruses and steal user's data. Although it remains unclear how many users fell victim to the breach, the event underscores the importance of conducting appropriate due diligence on any product before implementation.

5. Practical Problems

Other practical problems can arise, particularly if employers make the use of TACT mandatory for employees. For example, if downloading a contract tracing app is a mandatory component of an employer's reopening plan, employees without smartphones may be unable to resume normal operations. Furthermore, the actual effectiveness of TACT remains unresolved. To be effective, both employees and a large majority of other individuals in the community must carry a smartphone with them at all times. Also, the potential for false positives and other technology malfunctions will need to be addressed.

Conclusion

The level of risk created by including TACT in a workplace reopening plan depends on the details of the program and the technology. Important variables include, but are not limited to; the extent to which the program is mandatory, whether the program allows employers access to employee data, the type of geolocation technology involved, and whether apps are installed to an employer-issued versus an employee's personal device.

It should be noted that competing COVID-19-related data privacy proposals have been introduced in Congress. While the future of these proposals is not clear, their enactment would likely have a direct impact on employers using TACT to maintain a healthy workplace environment.

Employers should ensure the personal health information of employees is kept private and secure. This requires a thorough understanding of any technology prior to implementation in the workplace. Maintaining a balance between employee safety and employee privacy has never been more difficult. Unfortunately, this may be another aspect of the "new normal" for employers for the foreseeable future.

Ethics Are... Continued from page 8

(ABA Model Rule 1.1) and Duty of Confidentiality (ABA Model Rule 1.6) to create an affirmative duty on lawyers to take reasonable measures to ensure that electronic communications with clients remain secure and confidential. ABA Opinion 477, at 4.

At the intersection of a lawyer's competence obligation to keep "abreast of knowledge of the benefits and risks associated with relevant technology," and the confidentiality obligation to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," lawyers must exercise reasonable efforts when using technology in communicating about client matters. *Id.* Yet for many attorneys, the emergency caused by COVID19 allowed little to no time for an attorney to consider these issues.

Given that we are close to 6 months into our new reality, now is good a time for an attorney to assess the very opaque concept of "reasonableness." The ABA adopts a fact-based approach, balancing the need for consistency and clarity with the flexibility to determine what is truly secure in today's technological environment. The factors outlined include: (1) the sensitivity of the information; (2) the likelihood of disclosure if additional safeguards are not employed; (3) the cost of employing additional safeguards; (4) the difficulty of implementing the safeguards; and (5) the extent to which the safeguards adversely affect the lawyer's ability to represent clients. *Id.* (citing Comment [18] to Model Rule 1.6(c)).

Lawyers don't get a free pass when it comes to Data Security.

The ABA emphasizes the need for attorneys to have *knowledge*, both of potential threats and their own systems and data management practices. The days of blissful ignorance when it comes to technology are behind us: lawyers need to be informed consumers of the technology that drives their practices. Ultimately, their ethical obligations to their clients depend upon it.

In ABA Formal Opinion 483, *Lawyers' Obligations After an Electronic Data Breach or Cyberattack* (October 17, 2018)[4], the ABA addresses the uncomfortable question of a lawyer's obligation to notify their clients when a data breach occurs. A core component of any representation is a duty to keep clients "reasonably informed" about the status of the representation such that a client can make informed decisions regarding that representation. *See* ABA Module Rule 1.4.

This duty, in conjunction with a lawyer's duty of competence, provides the basis for the obligation that a lawyer "must employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relating to data and the use of data." *See* ABA Opinion 483 at 5. Without such active monitoring, the discovery of any cyber or

privacy breach would be "happenstance" and effectively, a lawyer would not be able to demonstrate compliance with her duty of competence to the client. Further, once a breach or infiltration is discovered, a lawyer must "act reasonably and promptly to stop the breach and mitigate damage resulting from the breach." *Id.* at 6.

ABA Opinion 483 distinguishes the notice obligation between current clients and former clients. For current clients, lawyers are obligated to communicate a data breach in order to comply with Module Rule 1.4. *Id.* at 10. Curiously, there is no corresponding express obligation to provide notice of a data breach to former clients. Instead, the ABA encourages lawyers "to reach agreement with clients before conclusion, or at the termination, of the relationship about how to handle the client's electronic information that is in the lawyer's possession." *Id.* at 13. Absent such an agreement, lawyers should maintain a data retention schedule in order to reduce the amount of data retained for long periods of time, thereby decreasing the potential that former client data will be impacted by a data breach.

Malpractice Claims and the Liability of Lawyers in Securing Client Data

At this time, there is no way of knowing the malpractice or liability claims involving COVID19 and an attorney's use of technology. Rather, competent attorneys will be cognizant of the ethical implications as they navigate the increased reliance on technology in this uncharted territory.

With the expansion of the Model Rules to require a lawyer to take proactive security and privacy measures, the liability risk for lawyers that fail to meet these obligations increases. "Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession." ABA Opinion 483 at 1. As fiduciaries to our clients, lawyers owe a duty of care to ensure that clients are not harmed by the technology and network infrastructures that lawyers use in their daily practice. The ABA clearly recognizes that an attorney's competence in preserving a client's confidentiality is not a strict liability standard and does not require the lawyer to be invulnerable or impenetrable. Rather, the obligation is one of reasonable efforts. Rule 1.6 is not violated even if data is lost or accessed if the lawyer has made reasonable efforts to prevent the loss or access. *Id.* at 9.

The limitations and boundaries of reasonable care are, as of yet, untested. As the ABA makes clear, there is no one standard that can be used to assess reasonable security and privacy measures: it is a fact-based analysis that will be heavily dependent on the type of information at issue and the resources available to the

firm. However, failing to take any precautionary measures, or not conducting at least a perfunctory review of the measures taken, will likely not pass the test.

The fact that the ABA has issued two formal opinions on the topic of data security in such a short time indicates the importance of ethical principles when lawyers are confronted with the unenviable task of sorting out their own responsibilities in a data breach.

Best Practices:

While the opinion is exhaustive, and certainly worthy of a full read, here are some key takeaways from the opinion's guidance:

- To comply with their duty of competence, lawyers have an "obligation to develop an understanding of the technology." Meaning that even before an attorney begins using a certain technology, they should understand the impact of incorporating the technology in their practice and the impact on their duties of confidentiality and privacy to their clients.
    - A simple example is communication with a client via text message. Has the attorney or law firm considered confidentiality issues with text messaging, especially texts sent from a personal phone? How will the law firm or lawyer maintain a record of a confidential communication? Will certain communications such as settlement offers be communicated via text?
    - Lawyers and law firms should create protocols outlining appropriate use of technology that comply with either their state's Rules of Professional Responsibility and Conduct or the Model rules.
- As part of their duty of competence, lawyers have an obligation to take "reasonable steps" to monitor for data breaches. The opinion defines a "data breach" as an event where "material client confidential information is misappropriated, destroyed, or otherwise compromised, or where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode."
    - Thus an attorney's duty of competency means that the obligation is not only to safeguard confidential information from unauthorized access or loss, but to also supervise subordinate attorneys and staff regarding such measures. This includes proper training and the implementation of cyber security policies and procedures.

- Given that many lawyers and law firms are remote due to COVID19, lawyers and law firms have transitioned to using technology to facilitate working remotely. Law firms may not have supplied their employees with laptops or firm owned computers, thus confidential client information or password protected data bases may be stored on an employee's personal computer. While this may not inherently be a "data breach" as described in Formal Ethics Opinion 483, an employee's use of personal computers puts confidential client information at risk of a data breach. Model Rules 5.1 to 5.3 require an attorney's reasonable efforts to supervise subordinates to conform with Rules of Professional Conduct. This supervision includes the use of technology when handling confidential client information.

- When a breach is detected, a lawyer must act "reasonably and promptly" to stop the breach and mitigate damages resulting from the breach. In order to ensure their ability to do this, lawyers should proactively develop incident response plans that will allow them to respond quickly and appropriately to a data security incident.

    - Bear in mind, the standard for the Model Rule and many of the parallel state rules is a reasonableness standard. An attorney's reasonable response to a data breach includes sensitivity of information, method of communication, and availability of security measures. Further compliance with the reasonableness standard demands that an attorney engage in continual risk assessment, implementation of appropriate measures, and updating and monitoring for effectiveness, all while considering one's rules of professional responsibilities.

- A lawyer must make reasonable efforts to assess whether any electronic files were, in fact, accessed and, if so, identify them. This requires a post-breach investigation where the lawyer gathers enough information to determine that the intrusion has been stopped, and then – "to the extent possible" – evaluate the data lost or accessed. The lawyer must do so in order to allow for full and accurate disclosure to affected clients.

    - If a lawyer relies upon a vendor to assist with a post-breach investigation, the lawyer must make reasonable efforts to ensure that the vendor's services are compatible with the rules of professional conduct. See Model Rule 5.3 or other jurisdiction's parallel rule.

- Lawyers must then provide notice to their affected clients of the breach "to the extent reasonably necessary to permit the client to make informed decisions regarding the representation."
    - As attorneys, we have a duty to communicate with our clients. Model Rule 1.1 (a)(3) requires an attorney to "keep a client reasonably informed of the status of a matter." California's Rules of Professional Conduct ("CRPC") Rule 1.4(a)(3) requires an attorney to "keep a client reasonably informed of significant developments relating to the representation." After an assessment of the breach, a lawyer must disclose the breach to the client as the breach most likely impacts the status of the matter, under the Model Rules, or is a significant development relating to the representation, under CRPC. The post-breach investigation requires that the attorney gather sufficient information to determine that the breach was stopped and the extent to which data was lost or accessed, yet the opinion stops short of opining on how the attorney makes this determination.
- While stopping short of requiring attorneys to notify former clients of data breaches, the ABA notes that an attorney should consider contractual arrangements with previous clients, as well as regulatory or statutory breach notification requirements in determining whether notification is merited, so as to limit liability. In addition, the ABA encourages law firms to adopt a limited document retention schedule that allows them to reduce the amount of information they keep relating to former clients.
    - While the ethics opinion stops short of requiring attorneys to notify former clients, an attorney has a continued duty to protect current and former clients' confidential information, thus notification to a former client should be done on a case by case basis. For example, if an attorney maintains copies of a former client's trade secrets, information pertaining to trade secrets, copyrights or intellectual property, at the very least, the best practice is to notify the former client of the breach.
- The ethical guidelines set forth in the opinion could apply to any client data that may interfere with the representation, instead of being expressly limited to only legally protected information, such as personally identifiable information (PII) or personal health information (PHI).
    - Model Rule 1.15 applies to all client property and is not limited to client funds. In California, for example, the attorney may be subject to

discipline or at the very least open to a potential malpractice suit, if the attorney's use of technology resulted in the mishandling of confidential client information or electronic client property.

For lawyers who are somewhat aware of the issues regarding cybersecurity and data protection, these affirmative requirements to protect client data may seem overwhelming. Many attorneys approach technology as they do mathematics - they shy away from learning something new and rely on experts to help them maintain their obligations. As trusted advisors to our clients, lawyers have a responsibility to embrace security and privacy protections and to continue to maintain client trust.

COVID 19 has reinforced that the law increasingly depends upon technology. Law firms are forced to become trusted information repositories that take security and privacy seriously in order to continue to practice while complying with Stay Safe Orders or remote practices. The law firm's own network infrastructures, document management, and third-party relationships are now on the front line of data privacy and security.

The ABA's opinion is well warranted and should serve as a wake up call to inform lawyers and law firms, as we navigate the demand of remote practice due to COVID19. Lawyers, like other professionals and businesses that deal with sensitive information, must exercise vigilance when it comes to cybercrime. But unlike other businesses and professionals, lawyers are required to deal not only with the aftermath of a breach but with all the ethical and legal obligations that may come with it.

Endnotes

1 https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf
2 https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.pdf
3 https://www.americanbar.org/content/dam/aba/administrative/law_national_security/ABA%20Formal%20Opinion%20477.authcheckdam.pdf
4 https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf

Calendar

October 26, 2020	**The Federal Program to Deregulate Slaughterhouses and It's Effects on Animals, Workers, & Consumers** Contact: Danielle Daly – 312/988-5708	Virtual Programing
November 5-6, 2020	**Fidelity & Surety Law Fall Conference** Danielle Daly – 312/988-5708	Virtual Programing
November 10, 2020	**Toxic Torts & Environmental Law Conference** Contact: Janet Hummons – 312/988-5656 Danielle Daly – 312/988-5708	Virtual Programing
November 18, 2020	**Insurance Regulation Federalization of Insurance** Contact: Danielle Daly – 312/988-5708	Virtual Programing
December 7, 2020	**Preparation, Risks, and Controls of Reopening in a Covid World: It's a Small World After All** Contact: Danielle Daly – 312/988-5708	Virtual Programing
January 2021, TBD	**Life Health & Disability** Contact: Danielle Daly – 312/988-5708	Virtual Programing
February 3-5, 2021	**Fidelity & Surety Law Midwinter Conference** Contact: Janet Hummons: 312/988-5656	Virtual Programing
February 10-14, 2021	**Insurance Coverage Litigation Midyear Conference** Contact: Janet Hummons – 312/988-5656 Danielle Daly – 312/988-5708	Omni Resort Montelucia Scottsdale, AZ
February 17-22, 2021	**ABA Midyear Meeting** Contact: Janet Hummons – 312-988-5656	Hyatt Regency Chicago Chicago, IL
March 10-12, 2021	**Transportation Mega Conference XV** Contact: Janet Hummons – 312/988-5656	Sheraton New Orleans New Orleans, LA
March 12-13, 2021	**Admiralty Maritime Law Conference** Contact: Danielle Daly – 312/988-5708	Sheraton New Orleans New Orleans, LA

Member Roster

Chair
Larry Schiffer
Schiffer Law & Consulting PLLC
10301 Beech Tree Lane
Plainview, NY 11803
(516) 650-1827
larry.schiffer@schifferlc.com

Chair-Elect
Michael Menapace
Wiggin and Dana LLP
20 Church St
Hartford, CT 06103
(860) 297-3733
Fax: (860) 525-9380
mmenapace@wiggin.com

Immediate Past Chair
Michelle Worrall-Tilton
4835 W 87th St
Shawnee Mission, KS 66207-1847
(913) 909-9419
mwtilton@mediariskconsultants.com

Diversity Vice-Chair
Deborah Yue
Law Office of Deborah Yue
1991 Crocker Rd, Ste 600
Westlake, OH 44145
(216) 245-9832
Fax: (216) 223-5064
DeborahYue@dwylaw.com

Law Student Vice-Chair
Nolan Hendricks
GSU College of Law
204 Spring Creek Ln
Sandy Springs, GA 30350-3808
(678) 986-0631
nhendricks3@student.gsu.edu

Membership Vice-Chair
John Stephens
1061 Audrey Dr
Palm Springs, CA 92262-6171
Fax: (213) 426-6921
jstephens@hendricks.law

Social Media Vice-Chair
Chad Anderson
PO Box 63333
Phoenix, AZ 85082
(602) 904-5485
chadknowslaw@gmail.com

Technology Vice-Chair
Robert Stines
Freeborn & Peters LLP
201 North Franklin St, Ste 3550
Tampa, FL 33602
rstines@freeborn.com

Council Representative
Kathleen Strickland
Ropers Majeski Kohn & Bentley
150 Spear St, Ste 850
San Francisco, CA 94105
(415) 972-6328
kathleen.strickland@rmkb.com

Scope Liaison
Patricia Hughes
41815 Primrose Lane
Novi, MI 48377
(248) 4256941
Fax: (248) 324-1489
Ph1500@AOL.COM

Vice-Chairs
David Becker
Freeborn & Peters LLP
311 S Wacker Dr, Ste 3000
Chicago, IL 60606-6679
(312) 360-6391
Fax: (312) 360-6594
davidsbecker@gmail.com

Andrea DeField
Hunton Andrews Kurth
1111 Brickell Ave, Ste 2500
Miami, FL 33131-3126
adefield@hunton.com

Brian Findley
Mulligan, Banham & Findley
2442 Fourth Ave, Ste 100
San Diego, CA 92101
1 (619) 2388700
findley@janmulligan.com

Robert Flowers
Travelers
1 Tower Sq, Ste S202A
Hartford, CT 06183-0001
(860) 277-7150
Fax: (860) 277-5722
rflowers@travelers.com

Kim Hogrefe
Kim Dean Hogrefe LLC
746 Pascack Rd
Washington Township, NJ 07676
(201) 218-8041
Fax: (201) 722-0107
kimdhogrefe@gmail.com

Floyd Holloway
State Farm Insurance
1 State Farm D
Concordville, PA 19339-9300
(610) 361-4150
Fax: (610) 361-4152
floyd.holloway.clxm@statefarm.com

Justin Kahn
Kahn Law Firm, LLP
562 Savannah Hwy
Charleston, SC 29407-7210
1 (843) 5772128
Fax: (843) 577-3538
jskahn@kahnlawfirm.com

Michael Kassak
White and Williams LLP
457 Haddonfield Rd, Ste 400
Cherry Hill, NJ 08002-2227
(856) 317-3600
Fax: (856) 317-1342
kassakm@whiteandwilliams.com

Thomas Kopil
Signature Systems, Inc.
760 Veterans Circle
Warminster, PA 18974
(215) 776-0338
Fax: (215) 757-3048
tom.kopil@pdqpos.com

Chantel Lafrades
Ropers Majeski PC
150 Spear St, Ste 850
San Francisco, CA 94605-3857
(415) 909-0316
Chantel.Lafrades@ropers.com

Amber Locklear
Ropers Majeski Kohn Bentley
750 3rd Ave, 25th Fl
New York, NY 10017
(650) 243-1692
alocklear@rmkb.com

Mailise Marks
Segal McCambridge Singer & Mahoney Ltd
15 Exchange Pl, Ste 1020
Jersey City, NJ 07302-4938
(201) 209-0393
mmarks@smsm.com

Melody McAnally
Butler Snow LLP
PO Box 171443
Memphis, TN 38187-1443
1 (901) 6807322
Fax: (901) 680-7201
melody.mcanally@butlersnow.com

Angela Meyer
1 W Edith Ave, Apt D130
Los Altos, CA 94022-2786
(650) 743-6779
Fax: (650) 688-7077
ameyer@exponent.com

Joshua Mooney
White and Williams LLP
1650 Market Stree
One Liberty Place, Ste 1800
Philadelphia, PA 19103-7395
(610) 649-3886
Fax: (215) 864-7123
mooneyj@whiteandwilliams.com

Ndidi Moses
US Attorney Office
1000 Lafayette Blvd, Fl 10
Bridgeport, CT 06604-4759
(203) 821-3700
Fax: (860) 275-8299
ndidi.moses@usdoj.gov

Michael Nitardy
Frost Brown Todd LLC
7310 Turfway Rd, Ste 210
Florence, KY 41042-1374
(859) 817-5914
mnitardy@fbtlaw.com

John Okray
Solovis Inc
5030 Riverside Dr, Ste 350
Irving, TX 75039
1 (617) 8214867
jokray@solovis.com

Member Roster | continued

Jennifer Parrott
Drew Eckl & Farnham LLP
303 Peachtree St NE, Ste 3500
Atlanta, GA 30308-3263
(404) 885-6217
Fax: (404) 876-0992
jparrott@deflaw.com

Toni Reed
Clark Hill Strasburger PLC
901 Main St, Ste 6000
Dallas, TX 75202-3729
(214) 651-4345
Fax: (214) 659-4091
toni.reed@clarkhillstrasburger.com

Margaret Reetz
Mendes & Mount LLP
750 Seventh Ave
New York, NY 10019
1 (312) 9618201
Fax: (312) 382-8910
margaret.reetz@mendes.com

Mario Russo
McCarter & English LLP
4 Gateway Center, 100 Mulberry St
Newark, NJ 07102
(973) 848-5375
marusso@mccarter.com

Alan Rutkin
Rivkin Radler LLP
477 Madison Ave, Fl 20
New York, NY 10022-5843
(516) 357-3277
Fax: (516) 357-3333
alan.rutkin@rivkin.com

Carolyn Ryan
Cipriani & Werner PC
450 Sentry Pky, Ste 200
Blue Bell, PA 19422
(610) 567-0700
Fax: (610) 567-0712
cpurwin@c-wlaw.com

Randolph Scott
CNA
2426 S Mystic Mdw
Houston, TX 77021
(832) 428-0699
rascottjr87@gmail.com

Dan Vinish
Indeed Inc.
6433 Champions Grandview Way
Austin, TX 78750
(607) 760-4246
dvinish@indeed.com

Ryan Weeks
Mills Paskert Divers
100 North Tampa St, Ste 3700
Tampa, FL 33602
(813) 229-3500
Fax: (813) 229-3502
rweeks@mpdlegal.com