COMPUTER AND TECHNOLOGY SECTION

Circuits

Newsletter of the Computer & Technology Section
of the State Bar of Texas
November 2020

Table of Contents

Featured Articles

Short Circuits

SECTION LEADERSHIP

Leadership at Work

It is with great pride that we announce our 2020-2021 Council, Committee Chairs and Working Groups!

Chair
Shawn Tuma

Chair-Elect
Elizabeth Rogers

Treasurer
Pierre Grosdidier

Secretary
Reginald Hirsch

Immediate Past Chair
John Browning

2020-2021 Council Members

Chris Krupa Downs
Craig Haston
Lavonne Burke Hopkins
Seth Jaffe
Michelle Mellon-Werch
Hon. Emily Miskel
Matthew Murrell
Christine Payne
Gwendolyn Seale
Alex Shahrestani
William Smith
Mitch Zoll

Judicial Appointments: Judge Roy Ferguson and Honorable Xavier Rodriguez

Committees

Budget Committee
Pierre Grosdidier, Elizabeth Rogers

Bylaws Committee
Reginald Hirsch, Mark Unger

Membership, Orientation & Outreach Committee
Lisa Angelo, Sammy Ford IV

Diversity Committee
Alex Shahrestani, Elizabeth Rogers

Social Media, Communications, & Marketing
Mitch Zoll, Shawn Tuma

CLE Coordinator
William Smith, Reginald Hirsch, Hon. Xavier Rodriguez

Circuits Newsletter
Sanjeev Kumar, Kristen Knauf, Pierre Grosdidier

Working Groups

Tech-Bytes
Gwen Seale, Michael Peck, Shannon Warren

In-House & Government Counsel
Michelle Mellon-Werch, Jason Smith

Solos & Small Firms
Craig Haston, Tony Ray

Cyber ADR
Peter Vogel

Cybersecurity & Privacy
Seth Jaffe, Elizabeth Rogers

eDiscovery
Christine Payne, Craig Ball, Michael Curran, Hon. Xavier Rodriguez

Emerging Technology
Lavonne Burke Hopkins, Al Harrison, Ron Chichester, Joseph Jacobson

Table of Contents

Feature Articles:-

Short Circuits:-

Letter from the Chair

By Shawn E. Tuma

Greetings from the Computer & Technology Section! We thank you for being a member and we hope that you will help us spread the word by urging your colleagues to join as well.

Our Section's mission is to be a resource to the legal profession in all matters involving technology. As we look at the extraordinary times we are living in with the COVID-19 pandemic and how it has impacted our society, forcing so many of us to essentially adapt on the fly and learn to manage our practices and lives virtually, it is easy to see the impact that technology has on all of us. One of the impacts this time of social distancing and working remotely has had on many is the loss of personal interaction with friends and colleagues in the workplace and in the profession who we would normally see face-to-face on a more regular basis.

While there is no true substitute for direct face-to-face interaction (yet?), virtual interaction through social media can be a great way to stay connected with other people. We are excited to provide you with five social media channels to interact with others and stay connected to the Section:

- The Section's Facebook Group, *Computer & Technology Section – State Bar of Texas*, https://www.facebook.com/groups/ComputerTechnologySection/, is limited to only active members of the Section and provides a great opportunity to communicate with other members of the Section.
- The Section's Facebook Page, *Computer & Technology Section – State Bar of Texas*, https://www.facebook.com/TXBarTech, is a Page that anyone on Facebook can "Like" and "Follow" and is a great way to stay updated on Section news and events.
- The Section's LinkedIn Group, *Computer & Technology Section – State Bar of Texas*, https://www.linkedin.com/groups/1890047/ is limited to only active members of the Section and provides a great opportunity to communicate with other members of the Section.
- The Section's LinkedIn Page, *Computer & Technology Section – State Bar of Texas*, https://www.linkedin.com/company/computer-technology-section-state-bar-of-texas/, is a Page that anyone on LinkedIn can "Follow" and is a great way to stay updated on Section news and events.

- The Section's Twitter, @TXBarCompTechSection, https://twitter.com/TXBarCompTech, is a Twitter account that anyone can "Follow" and is a great way to stay updated on Section news and events.

- The Section's Instagram, @TxBarTech, https://www.instagram.com/txbartech/, is an Instagram account that anyone can "Follow" and is a great way to stay connected to the Section.

- Follow and use #TxBarTech, the Section's hashtag, on Facebook (https://www.facebook.com/hashtag/TxBarTech/), LinkedIn (https://www.linkedin.com/feed/hashtag/?keywords=txbartech), and Twitter (https://twitter.com/hashtag/TXBarTech) to keep up with and share Section-related content.

Obtaining CLE has been another challenge that many have faced during the COVID-19 pandemic, as we were accustomed to attending CLE conferences in person, but many of those conferences were either cancelled or held virtually. Our Section is committed to helping Texas lawyers meet their CLE requirements and become more knowledgeable of technology issues through the many legal tech education opportunities we offer.

We are very proud of our commitment to promoting access to justice efforts and every year we sponsor "With Technology and Justice for All," a one-day CLE course designed to assist legal aid, pro bono, and new lawyers with using technology to enhance their practices. This course is open to and will be great for all lawyers. This year, this CLE course will be held virtually on December 11, 2020, and you can register online through the Section's website, www.sbot.org, beginning on November 1, 2020. We recently partnered with the Texas Criminal Lawyers Association to co-sponsor the CLE webinar "Conquering Technology in Criminal Practice" which provided 6 hours of MCLE credit, including 0.5 hours of ethics, for $35. This conference was a tremendous success and we are confident the December conference will be as well, so don't miss it!

We have an outstanding variety of educational videos—Tech Bytes—available to all Texas lawyers at https://sbot.org/techbytes/, ranging from 5-10 minute overviews to 45-minute presentations. These videos address areas like encryption, cybersecurity, data privacy, eDiscovery, and investigations using social media. These videos are a great way to obtain self-study CLE credit.

Our Section provides other benefits to our members as well. Members continue to enjoy complimentary use of our Texas Bar Legal App, which gives you access to current Texas rules and codes (with links to relevant case law) right at your fingertips. You can learn more about downloading and using the App here: https://sbot.org/app/.

Of course, we also publish this eJournal, *Circuits*. Each issue is packed with informative articles about cutting-edge topics, and this issue is no different, with topics ranging from tips for working from home during the pandemic to emerging issues in tech law. We would like to encourage Section members like you to submit articles for consideration for publication in *Circuits*.

Finally, we would like to encourage our Members to join and actively participate in one of our Section's Committees and Working Groups. This will allow you to get more involved and contribute to the work of the Section. We are actively seeking new Members for the following:

- Membership, Orientation & Outreach Committee
- Diversity Committee
- Social Media, Communications and Marketing Committee
- CLE Working Group
- Circuits Working Group
- Tech-Bytes Working Group
- The App & Strategic Partnerships
- In-House & Government Counsel Working Group
- Mid-size & Large Firm Working Group
- Solos & Small Firms Working Group
- Cyber | Privacy | eCommerce ADR Working Group
- Cybersecurity & Privacy Working Group
- eDiscovery Working Group
- Emerging Technology Working Group

- Tech Competence in Practice Working Group
- Tech in the Courts Working Group

Thank you again for your membership and for your interest in matters at the intersection of technology and the law. If you would like to become more involved in the Computer & Technology Section or have other ideas you would like to share, please contact our Section administrator at admin@sbot.org.

Shawn E. Tuma
2020-2021 Chair
Computer & Technology Section
State Bar of Texas

Letter from the Co-Editor

By Sanjeev Kumar

Welcome to the first issue of the *Circuits* eJournal for the 2020-21 bar year! As I write this letter, the number of positive cases of COVID-19 is increasing again across our great state of Texas and the country. The Computer and Technology Section has a lot of tools available to help us lawyers remain productive remotely in our practice. Please do not miss the Letter from our Chair, Shawn Tuma, which provides a very convenient list of various ways to connect with the Computer & Technology Section, which is there solely to help our legal community. The accomplished members of the Computer & Technology Section Council are always willing to help in any way possible during these trying times, so please do not hesitate to contact us through our section administrator at admin@sbot.org.

The need for working remotely as a result of the pandemic has caused increased use of electronic collaboration tools. It has also resulted in less personal face time with co-workers and increased reliance on electronic mechanisms to accomplish normal business operations. This has also provided novel mechanisms for hackers to penetrate the new but often unhardened new systems being used by businesses for remote operations. We start with our Feature Articles, a contribution from our Section Chair, Shawn Tuma, who discusses how the increased ransomware attacks have turned the need for cyber insurance from a luxury into a necessity.

The COVID-19 pandemic has also brought to focus the interplay between safety and privacy. The second article is penned by our Chair-Elect, Elizabeth Rogers, who discusses the privacy issues resulting from the COVID-19 protocols implemented by employers and educational institutions. This is a timely article for the legal community to better educate our business clients and help them to adopt processes in order to avoid unintentional violation of regulatory regimes.

In the next article, guest author Kirsten Kumar discusses the impact on the legal profession from increasing automation and artificial intelligence in growing areas of legal work.

The Chair of the C&T section's Membership Committee, Lisa Angelo, provides a discussion of some of the decisions and analysis from court cases regarding insurance claims as related to cyber losses. This is an apt supplementary article to our first feature article by our Chair on cyber insurance becoming a necessity instead of luxury, as it highlights the fact that the type

and language of coverage in cyber insurance policies matter when attempting to secure reimbursements for a loss.

We start our Short Circuits section with an article from our former Section Chair and my predecessor as the Editor of *Circuits* eJournal, Pierre Grosdidier, where he highlights the need for obtaining a warrant for search of seized assets in a timely manner. He accomplishes this by discussing a few court cases dealing with the reasonableness of such seizures. This is a continuation of his articles in the previous issues of *Circuits* regarding border searches and seizures.

We end with a Short Circuits article by Lisa Angelo discussing the complexity created due to the invalidation of the EU-US Privacy Shield on the sharing of data from the EU.

Many thanks to all the contributors to this new issue. A big thank you also to Kirsten Kumar for her review of and assistance with this issue's articles. We hope that you enjoy this new edition of *Circuits* eJournal and as always, we welcome any comments that you may have. Please send them to our section administrator at admin@sbot.org.

Kind Regards,
Sanjeev Kumar, Co-Editor

FEATURE ARTICLES:-

With Ransomware Attacks Increasing, Cyber Insurance Now Seen as a Necessity, Not a Luxury

By Shawn Tuma

Threat actors launched a cyberattack against the Texas Office of Court Administration, the IT provider for many Texas courts, and encrypted their computer systems with ransomware, leaving those systems useless. Cognizant, which has a large presence in Dallas-Fort Worth and is one of the world's largest and most sophisticated providers of information technology services for other companies, was hit with ransomware resulting in losses currently estimated between $50 million and $70 million. Dallas-based CyrusOne, a global provider of data center services and managed information technology services for other companies, was hit with ransomware, impacting several of its customers. More than 20 Texas local governments were hit with ransomware, also rendering their computer systems useless.

These are just a few of the high-profile cyber incidents in the past year just for Texas. Similar incidents occur daily across the United States.

While the public learns about attacks like these on well-known organizations, most do not hear about the attacks on small and midsize organizations. Unless the ransomware attack also involves the breach of confidentiality of sensitive personal information or protected health information, there is no general law requiring that such attacks be publicly disclosed or reported.

That does not mean they are not happening. In our experience, they are happening exponentially more to small and midsize organizations all over the United States, and the impact is devastating.

A cyberattack is becoming the one universal risk that can literally destroy overnight an otherwise healthy company. Even with COVID-19, it took days and weeks for the impact to be felt. Not so with cyber incidents; it happens in an instant. If the large, well-funded experts in information technology like Cognizant cannot always defend themselves against these attacks, do you really believe your organization can?

Now is the time for cyber insurance and incident response plans

In reality, there is no "secure" in the cyber world — even when the best security measures are taken. When cybercriminals want to get in and disrupt a business bad enough, they will find a way.

Because a company cannot be completely secure, it must be resilient. Cyber insurance is critical in providing a company with the resources it needs to properly respond to and recover from an attack. However, business leaders need to understand the details of an insurance policy and what it does and does not cover. Only policies specifically designed to cover cyber risk, cover cyber risk.

Standard insurance policies typically do not provide coverage for cyber risk. You must have a policy that is specifically designed to cover cyber risk and, more appropriately, the unique cyber risks your company faces. If you do not know that you have cyber risk coverage, you probably do not.

In addition, businesses should invest in creating a thorough and detailed incident response plan that can be initiated on short notice. Ideally, this plan includes the who, when and how of the response — perhaps most importantly, who leads the response and coordinates all of the steps. The plan should not only include the organization's internal team, but those external service providers who have a critical role in an incident response such as breach counsel (i.e., legal), cyber forensics, and public relations.

For an incident response plan and cyber insurance policy to work, business leaders must educate the key stakeholders, train every member of the team and practice or simulate the actions with the key stakeholders and external providers, all of which are essential members of the incident response team. The most valuable part of an incident response plan is communication and having the right team in place to successfully resolve the situation and minimize the disruptions and associated costs.

Cyber insurance works

Reputable carriers pay claims under cyber policies.

When a policy legitimately covers a claim, the carriers pay. We have handled hundreds of cases where insurance carriers have fulfilled their obligation and paid for the response, mitigation, notification, litigation and regulatory investigation costs. To give you an idea of how many and what kinds of cyber claims are paid each year, the NetDiligence 2019 Cyber Claims Study examined over 2,000 cyber claims that had been paid.

Of course, there may be exceptions and outlier cases where an appropriate claim is not paid or where the claim may fall within a gray area and coverage is not clear. This is true of all insurance for all types of risk.

Cyber is no different.

But these cases are the exception, not the rule. Unfortunately, they are the cases that usually get the most attention and create the perception that cyber claims are not paid. These situations are rare, and those who focus only on them are ignoring the thousands of cases where similar claims are paid.

You manage your company's risk by honestly evaluating the probabilities, not getting hung up on the most unlikely exception. Addressing cyber risk should be no different. When you get a cyber policy from a reputable carrier, the likelihood that the carrier will cover those claims is just as high as the carrier covering any other kind of claim for which you have insurance.

However, before an incident occurs, you should know the answers to all of these questions:

- Do you know you have cyber insurance?
- Where is your policy?
- Who is the carrier and your main contact with that carrier, as well as your broker?
- Were proactive risk management services included?
- How quickly must you give notice of an event?
- Must those on the incident response team be "approved" or "preapproved" by the carrier before you can use their services?
- When must you get preapproval for steps taken in incident response?

Know who you will work with when a cyber incident occurs

Cyber insurance policies typically specify that if your company has an event and makes a claim, you will be required to work with the service providers who are on the carrier's "preferred" or "approved panel" list. This means that if you already have a relationship with an experienced attorney, cyber forensic firm, PR firm, or forensic accounting firm that you know and trust, you probably cannot work with them unless they are approved. This is tantamount to learning that your star players are ineligible to play at the opening whistle of the championship game—not something you want to learn about when a crisis hits.

While this regularly trips up those who are inexperienced in incident response, there is a good reason for this requirement. Little mistakes can have a big impact on the response. Cyber incident response and serving as breach counsel is a highly specialized skillset and the professionals handling this must truly have significant experience in that role or else the consequences — and resulting losses for the client and the insurance carrier — can be catastrophic. The insurance carriers have a strong interest in making sure the professionals they approve have been vetted and can handle the role.

Also, insurance carriers typically have negotiated rates with their approved panel providers that are substantially lower than those same providers would charge on their non-insurance engagements. Because these providers' fees typically erode the insurance policy coverage limits like any other costs, this helps the insured get the most bang for their coverage buck.

Finally, service providers that regularly do this kind of work with insurance companies get better results because they are familiar with the cyber insurance process, have strong relationships and a familiarity in working with the most experienced providers in the other external service provider disciplines (i.e., legal, cyber forensics, public relations), and they all know how to work well together as a team.

This is ultimately much better for the client.

There are solutions to this problem for clients that already have a relationship with an experienced attorney, cyber forensic firm, PR firm, or forensic accountant: Address the issue upfront as part of the incident response planning process. If you know who you want to work with when you are obtaining your policy, make it clear and get a policy with a carrier that will allow you to work with the professionals of your choosing, or have the professionals you know and trust written into your policy.

It may be too late to do this once the policy has been issued, but you should still try because the insurance carriers allow such additions as long as it is before you actually have a claim.

The best way to get the right cyber risk policy is to work with a reputable broker who is truly knowledgeable about cyber risk and cyber policies. There are a lot of brokers trying to sell cyber policies, but many of them do not truly understand the policies, cyber risk in general, or your company's unique needs.

Contact experienced cyber service providers you know and trust to ask for advice on how to get the right policy that will allow you to work with them. Let them connect you with a good

insurance broker who truly understands your cyber risk and has the relationships that will allow them to find a policy that fits your needs.

How this all fits together

Assessing all of the above allows businesses to know what questions to ask to increase protection and mitigate risk:

- Do we have cyber insurance?
- Is it tailored to our unique risk?
- Does it offer proactive risk management services?
- What is covered? What is not covered?
- What choice do we have in service providers used?
- Are there service providers that we want to use that are not permitted?
- Can we get the service providers we want to use approved under the policy?
- If not, who are the carrier's approved service providers so we can develop a relationship with them to use them in our incident response planning and preparation?

The key to identifying the right coverage to fit specific needs is to find the right policy with the right carrier. Good, knowledgeable brokers and agents can assist in this process. You can then incorporate that policy into your incident response plan and become a company fully prepared for the biggest threat facing your company today and in the future.

About the Author

Shawn Tuma is a partner at Spencer Fane LLP in the firm's Dallas and Plano offices. He helps businesses protect their information and protect themselves from their information, representing a wide range of clients, from small to midsize companies to Fortune 100 companies, across the United States and globally in dealing with cybersecurity, data privacy, data breach and incident response, regulatory compliance, computer fraud-related legal issues, and cyber-related litigation.

Novel Privacy Issues Arising During the Novel Coronavirus

By Elizabeth Rogers

Since the winter of 2020, businesses have been struggling to resolve issues that arise because of decisions to send employees and students home and/or to shut out customers—in the name of public safety—and equally struggling to resolve issues that arise because of the decision to call that same population back to business or campus—in the name of bolstering the economy.

To complicate matters, the unprecedented closing and opening of doors to employees, patrons and student populations has occurred without any consistent or coordinated standards or guidelines among federal, state, and local government. These extraordinary circumstances have bred inconsistent practices and have ushered in a set of novel privacy issues implicated by the collection of data that is intended to promote public health, safety, and/or productivity, among other objectives.

The goal of this article is to provide an overview of these trending privacy issues—arising within a return-to-work campaign in the employment setting and a return-to-campus campaign in the higher education setting—and to share standards and frameworks of analysis that have been developed to address them within those environments. While there are plenty of privacy issues within the context of a virtual work environment and a virtual learning environment, the collection of personal data in the context of re-entry creates more privacy challenges.

Additionally, this article highlights technologies developed or discovered during the coronavirus (COVID-19) pandemic to help organizations across multiple industries safely return to a familiar in-person experience. A due diligence checklist is provided to help weigh the benefits of the technology vs. privacy risks.

I. The Balancing Act: Public Health/Safety Concerns vs. Privacy

A. In the Employment Law Setting

1. The issues

The return of employees to the workplace ushers in the next frontier in employers' responses to the novel COVID-19 pandemic, raising a wide range of novel challenges. One of the most fundamental challenges relates to workplace privacy and data security: namely, developing lawful processes to screen employees for possible COVID-19 infection before they re-enter the workplace.

Before implementing these types of solutions, employers should ensure that they provide the appropriate notice and, where necessary, obtain consent from their employees. For example, the California Consumer Privacy Act (CCPA) requires employers to provide employees with a "notice at collection" before collecting their personal information, such as location information. In addition, some state statutes require consent for geo-tracking, and recent case law suggests some risk of a common law claim based on continuous location tracking over an extended period without prior notice and consent. Even where not legally required to do so, employers should consider providing employees with notice for the sake of preserving positive employee relations.

At other points during this process, organizations also will need to consider whether and how long to retain the collected data. If answers to screening questions and test results are retained, then they should be treated like a confidential record of a serious health condition under the ADA and retained as a medical record separate from the employee's other personnel records.

2. Best Practices

Businesses should create a set of policies that seek the employees' signed acknowledgement of the need for and existence of COVID-19 screening questions and temperature scans and account for the unique set of circumstances under which these practices will occur. The policies should include opportunities for the employees to provide a written expression of consent to answer the questions and to periodically and/or regularly submit to the health screenings. Ultimately, there should also be a separate paragraph for written consent to an anonymous disclosure of the employee's positive test results to the general workforce and written consent to a limited disclosure of the employee's specific identity only to those whom the employee was regularly in direct physical contact with, including customer representatives.

Additionally, organizations should provide reasonably appropriate technical, administrative, and physical security for all confidential information collected in the course of asking employees health questions and/or administering medical screening, which may mean encrypting such results at least for the period of time during which the data is retained.

This best practice will mitigate the employer's exposure to liability not only under the data breach notification statutes of all 50 states, but also under the data breach notification requirements of the Health Insurance Portability and Accountability Act ("HIPAA"). Furthermore, under the recently effective California Consumer Privacy Act ("CCPA"), maintenance of a

reasonable security program is a defense in a private cause of action arising because of a data breach.

3. The Regulatory Response

a. The Equal Employment Opportunity Commission (EEOC).

Ordinarily, the Americans with Disabilities Act forbids an employer from asking medical questions, requiring an employee to submit to medical exams, or from disclosing confidential medical information, including an employee's identity. However, because the WHO and the CDC have declared COVID-19 to be an international pandemic, the EEOC has said that COVID-19 meets the ADA's direct threat standard which allows employers to ask screening questions, take the temperatures of, and test workers prior to permitting them onsite. For example, employers may ask applicants or current employees whether they have specific symptoms currently associated with COVID-19 and also may ask about any additional symptoms which evolve as more information is learned about the effects of the virus.

b. Suggestions for further regulatory response

Regulators and lawmakers should consider providing a safe harbor for employers who enact written policies that provide detailed disclosure of the information that will be collected and who obtain express acknowledgment of and consent to the collection of health information. Furthermore, a written consent to disclose test results and identity to a limited group of people who have a need to know, under the direct threat standard, should be an absolute defense for employers or should at least limit the available remedies.

B. In the Higher Education Environment

1. The issues

As some students and athletes returned to campus and sports in the fall of 2020, the hope is that university dorms, fraternity houses, classroom buildings and locker rooms have learned how to mitigate the risk of a massive outbreak of COVID-19. If an outbreak does occur, the core privacy concern is what information, if any, may officials within the university administration disclose about students who test positive? Furthermore, to whom may it be disclosed? Generally, the Federal Education Records Privacy Act ("FERPA") follows the requirement of a parent's or student's written consent prior to disclosure, by university officials, of personally identifiable information ("PII") from a student's education records in the absence of circumstances giving rise to an applicable exception.

2. The regulatory response from the Department of Education ("DOE")

At the end of March 2020, the DOE issued guidance about what circumstances are permissible for covered schools to disclose the PII of students, under the FERPA, in the context of COVID-19. The DOE's guidance focuses on the extent to which the COVID-19 pandemic qualifies as a "health or safety emergency" exception that would allow disclosure in the absence of consent.

The guidance starts with FERPA's default principle that education agencies and institutions should not directly or indirectly identify a student during instances when a student is diagnosed, exposed, or symptomatic. However, the guidance also recognizes that the health and safety emergency exception allows such disclosure of PII to a limited set of parents and other students when it is reasonable under a narrow set of facts or conditions. For example, the DOE clarified that disclosure of PII to public health authorities is permitted under the exception when the school reasonably determines there is a significant and articulable threat to the student or other individuals.

Whether or not a disclosure under the health or safety exception is reasonable, however, will largely be left to the school, according to the DOE. The guidance describes that the standard for application of the exception is a "flexible standard," and that the DOE will not substitute its judgment for that of the covered school, so long as there is an underlying rational basis for the school's disclosure of a student's PII. For example, the DOE cites a hypothetical case in which the health or safety emergency exception would allow the disclosure of the identity of an athlete, who is on a school-sponsored athletic team, to teammates and their parents because the risk of transmission is higher than it would normally be to the general population.

Yet, the same situation would not justify disclosure of the athlete's PII to other or broader groups, such as a campus newspaper or classmates in all of the athlete's on-campus classes. This is due to FERPA's general principle requiring that disclosure be made only to "appropriate parties" who need to know the student's PII, to protect the health and safety of the student and other individuals, such as health and law enforcement officials or a student's parents.

If the health or safety emergency exception provides the underlying rational basis for the school's disclosure of a student's PII, then the guidance reinforces FERPA's requirement that the disclosure must be recorded in the student's education records and include a description of the articulable and significant threat to the health or safety of a student or other individuals and the parties to whom the school made the disclosure.

3. Best practices

Covered schools who believe that it is reasonably necessary to disclose a student's PII should follow the best practice of seeking written parental or eligible student consent and documenting that consent was given. If consent is not given, or if there is a reasonable basis for believing that disclosure absent consent is warranted, then the covered school should document the safety and health concerns or threats which justify the exception in order to maximize application of the "flexible" standard.

II. Privacy Issues Implicated by Pandemic-Inspired Technology Use

In 2020, there is extensive technology at our disposal and/or in development which may play a crucial role in helping organizations address COVID-19, ensuring a safe and healthy workplace and workforce, and preventing future pandemics. Some examples of the newer applications that have been developed to address COVID-19-specific situations include i) social distance tracking and mask-wearing applications and, ii) digital contact tracing applications.

Nevertheless, organizations must move cautiously and consider the very complex legal risks, questions, challenges, and obligations prior to implementation. Here are a series of questions that may help businesses to assess the privacy risks associated with the technology they are considering:

- *What is the goal for the technology?*

If the goals of the organization are to keep workers who may have COVID-19 from entering its facility, then screening technologies are something the organization may consider. However, if the goal is to identify other workers who may have been exposed to a COVID-19 positive co-worker, then contact tracing technologies may be more appropriate. To this end, it is important to consider the organization's goals prior to selecting technologies for implementation.

- *How does the technology work?*

As a starting point, it is essential that businesses understand what information is being collected by the technology, the purpose for such collection, and where the information will be stored. Some apps are question-oriented and ask people for personal information such as their name, health status, and recent travel. Other apps go much further by tracking employee movements on an automated basis. Additionally, employers should be aware that apps downloaded directly to users' phones may collect other information through cookies and other

tracking technologies. Given these differences, employers must understand exactly what the app is collecting and why the information is being collected.

- *Is notice/consent required?*

The California Consumer Privacy Act went into effect on January 1, 2020, and the state Attorney General started enforcing violations on July 1, 2020. Although the CCPA contains an exemption for employee information, employers still must provide California residents with a notice of personal information collected, along with the legitimate business and commercial purposes for such collection. In this context, that means that employers that deploy COVID-19 apps in California will be required to provide disclosures to and get consent from California employees. Notably, the CCPA's employee information exemption also does not apply to the CCPA's private right of action for a data breach.

- *Will workers participate?*

Do the employees know what the technology does? Is participation voluntary or mandatory? Regardless of whether implementation is voluntary or required, it is important for organizations to communicate with their workers to explain the goals of the technology, answer questions regarding same, and address concerns over privacy and related issues in order to ensure buy-in and effectiveness.

- *How is data collected, shared, secured, and returned?*

Understanding the answers to these questions is imperative in order to help ensure compliance. This is especially true in light of numerous laws that may be implicated when data is collected from workers and others. These include the Americans with Disabilities Act, the Genetic Information Nondiscrimination Act (GINA), state laws, CCPA, and the General Data Protection Regulation (GDPR). In addition to statutory or regulatory mandates, the organization will also need to consider existing contracts or services agreements which may require limitations on the collection, sharing, storage, or return of data.

- *Are employees implementing the technology capable and trained?*

Another important aspect of using these apps will be to implement internal policies and procedures ensuring their proper use. For example, employers should identify which employees need to have access to the information collected by these apps and exclude all others from accessing such information. In these uncertain times, an organization may be left with no choice other than to expand the list of individuals who may have access to workers'

personal information. However, when doing so, organizations still need to be mindful of the ADA's confidentiality requirements and discrimination.

Further, employers should develop strict confidentiality guidelines around the use of this information and should implement clear standard operating procedures to ensure that the information collected does not violate users' privacy rights. Addressing privacy and security obligations through a confidentiality agreement may be one way to help address these concerns.

- *What is the nature of the relationship with the vendor?*

The organization's relationship with the vendor is usually established by way of contract or service agreement. Thus, it is important for these contracts and agreements to include confidentiality, data security, indemnification for data breaches, and similar provisions. This is most important if the vendor will be maintaining, storing, accessing, or utilizing the information collected about the organization's workers.

- *Is there an expiration date for use of the technology?*

As organizations look to the future and the hopeful end to the COVID-19 pandemic, they will need to consider when the state of the pandemic no longer supports the application of EEOC's direct threat exemption for use of technologies that collect employee health information. The EEOC has yet to provide that guidance.

Meanwhile, organizations may still have reasons to continue utilizing some of these technologies. For example, contact tracing may continue to help slow or limit the spread of the virus within an organization. Similarly, organizations may face contractual demands from customers or clients who are looking to limit future risks or outbreaks related to COVID-19.

III. Conclusion

All organizations should carefully consider implementing some form of COVID-19 screening program before returning to "business as usual". When choosing among the wide range of available screening techniques, business leaders must consider a wide range of legal risks, with privacy and data security risks being chief among them. With careful planning, those risks can be reduced to a manageable level, fostering the first steps towards the "next normal".

About the Author

Elizabeth Rogers is an integral member of Michael Best's Privacy & Cybersecurity team. Her extensive experience with a variety of regulatory, cybersecurity compliance, and technology-specific privacy matters from her roles as Partner, Chief Privacy Officer, and General Counsel, provides clients with privacy and cyber risk mitigation steps that achieve business objectives.

Elizabeth focuses on issues including breach responses, privacy risk assessments, and enterprise-wide cybersecurity compliance frameworks across industries such as retail, health care, financial services, retail electric providers, education, and state and local governments. She devotes a significant portion of her practice to the energy sector to assist the firm's clients in the utility industry with their unique cybersecurity concerns.

Outside of her law practice, Elizabeth teaches cybersecurity and privacy law topics for the University of Texas School of Information's Master's Program in Identity Management and Security. She is a thought leader on privacy and cybersecurity matters facing businesses, and frequently speaks and is published on emerging trends in these areas.

Age of the Automated Attorney? An Overview of the Implications of Artificial Intelligence in the Legal Sector

By Kirsten Kumar

Introduction

Given COVID-19's impact on work for many, the narrative that automation is squeezing workers out of employment has resurged from automation theorists, media outlets, and the like.[1] While the debate on the role of artificial intelligence ("AI") and "robots"[2] in destroying or creating jobs is ongoing,[3] we cannot deny the normalization of machines as task-performers across a number of industries. Indeed, machines have been used in auto assembly lines for decades, and the use of robots in routine, repetitive jobs encountered daily, such as self-checkout kiosks at grocery stores and automated tollbooths on highways, have become commonplace for many.

Concern about the proliferation of automation is predominantly centered around the rapid pace at which AI is developing: no longer is it used only for routine and repetitive tasks, but AI is now composing symphonies,[4] writing news articles,[5] and predicting treatment protocols for patients.[6]

---

1 *See, e.g.*, Alana Semuels, *Millions of Americans Have Lost Jobs in the Pandemic—And Robots and AI Are Replacing Them Faster Than Ever*, TIME (Aug. 6, 2020), https://time.com/5876604/machines-jobs-coronavirus/; Will Knight, *The Pandemic Is Propelling a New Wave of Automation*, WIRED (Jun. 12, 2020), https://www.wired.com/story/pandemic-propelling-new-wave-automation/.

2 While "robots" are common in other sectors, this Article primarily focuses on artificial intelligence in the legal sector, loosely defined as "computers learning how to complete tasks traditionally done by humans". Julie Sobowale, *How artificial intelligence is transforming the legal profession*, A.B.A. J. (Apr. 2016), https://www.abajournal.com/magazine/article/how_artificial_intelligence_is_transforming_the_legal_profession.

3 *Compare* Dan Shewan, *Robots will destroy our jobs – and we're not ready for it*, THE GUARDIAN (Jan. 11, 2017), https://www.theguardian.com/technology/2017/jan/11/robots-jobs-employees-artificial-intelligence; *with* Richard Partington, *Robots in workplace 'could create double the jobs they destroy'*, THE GUARDIAN (Sep. 16, 2018), https://www.theguardian.com/business/2018/sep/17/robots-in-workplace-could-create-double-the-jobs-they-destroy.

4 Kevin Berger, *Digital Composer Records With London Symphony Orchestra*, DISCOVER MAGAZINE (Jan. 25, 2013), https://www.discovermagazine.com/technology/70-digital-composer-records-with-london-symphony-orchestra.

The indication that AI can be used for more creative and complex tasks begs the question: are legal jobs at risk?

The gut reaction of most attorneys to this is likely: no. After all, professional competence requires an advanced degree, Bar certification, and expertise gained from work and continuing education. No machine would be capable of effectively performing an attorney's work. Right?

Well, yes and no. While some attorneys and scholars have marked artificial intelligence as "the next great hope that will revolutionize the legal profession" and look to it as a tool that may change the way legal work is done,[7] others are more skeptical. As Tom Martin, attorney and self-identified legal bot advocate, noted in 2019, we have not yet seen "robots" coming for legal jobs,[8] but AI and automation practices *have* been creeping into the legal sector.

AI in the Legal Sector

Many reading this have probably dabbled in some way with the legal technology market, which offers a range of services for both transactional work and litigation that include some degree of automation. AI is being used to a varying degree in, *inter alia*, contract drafting, discovery document review, and even some legal research.[9] Automated form-filling, for example, can be a useful asset for transactional attorneys to reduce time spent manually drafting repetitive documents. One may wonder how far these more autonomous services can stretch, given the popularity of online "DIY" legal aid sites such as RocketLawyer and LegalZoom.

In recent years, AI researchers have increasingly set their sights on litigation and other forms of dispute resolution. Of course, AI can play a key role in eDiscovery, particularly in document review. In addition, there has been some focus on the decision-making process itself. In February 2019, for example, Canadian company iCan Systems resolved a dispute in the UK

---

5 Nicole Martin, *Did A Robot Write This? How AI Is Impacting Journalism*, FORBES (Feb. 8, 2019), https://www.forbes.com/sites/nicolemartin1/2019/02/08/did-a-robot-write-this-how-ai-is-impacting-journalism/#3b644db27795.

6 Thomas Davenport & Ravi Kalakota, *The potential for artificial intelligence in healthcare*, 6(2) FUTURE HEALTHCARE J. 94 (2019).

7 *See, e.g.*, Sobowale, *supra* note 2.

8 Tom Martin, *How Chatbots Make Room for Lawyer Soft Skills*, A.B.A., 36 No.2 GPSOLO MAG. 56, 57 (March/April 2019).

9 Malcolm Langford, *Taming the Digital Leviathan: Automated Decision-Making And International Human Rights*, 114 AM. J. INT'L L. UNBOUND 141, 142 (2020).

court system using a "robot mediator" in less than an hour.[10] As significant volumes of data become more commonplace in legal disputes, AI may play a more significant role in alternate dispute resolution in the future.

AI has also been applied in predicting legal outcomes in cases. In 2014, attorney and technologist Daniel Katz and colleagues spearheaded a project to do just that, resulting in an algorithm that had 70.2% accuracy in predicting the outcome of U.S. Supreme Court rulings and 71.9% accuracy in predicting Justice votes over the course of nearly two centuries.[11]

Further, there has been a growing discussion on automated judging and administration, although many have expressed rights-based concerns related to issues such as legal accuracy and the possibility for discrimination based on structural background data.[12]

The Rise of Robot Attorneys?

Some argue that the increasing ability of intelligent machines to handle various tasks discussed above may cause some attorneys to find themselves out of work.[13] However, it is important to note that, unlike some other sectors, where a human has been *replaced* by an automated machine or interface, the examples of AI in the legal sector largely entail attorneys and AI working in harmony *together*.

For example, in eDiscovery, technology-assisted review ("TAR") uses AI to flag potentially relevant documents. Studies have indicated TAR results in a higher yield of relevant documents than review conducted solely by attorneys and paralegals.[14] However, TAR depends on human input to help refine its process; the human reviewer will need to provide input on relevant

---

[10] Kate Beioley, *Robots and AI threaten to mediate disputes better than lawyers*, FINANCIAL TIMES (Aug. 13, 2019), https://www.ft.com/content/187525d2-9e6e-11e9-9c06-a4640c9feebb.

[11] Daniel Martin Katz, Michael James Bommarito, and Josh Blackman, *A General Approach for Predicting the Behavior of the Supreme Court of the United States*, SSRN (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2463244.

[12] Langford, *supra* note 9, at 144.

[13] *See, e.g.*, John O. McGinnis & Russel G. Pearce, *The Great Disruption: How Machine Intelligence Will Transfer the Role of Lawyers in the Delivery of Legal Services*, 82 FORDHAM L. REV. 3041, 3055 (2014).

[14] *Myths and facts about technology-assisted review*, THOMSON REUTERS, https://legal.thomsonreuters.com/en/insights/articles/myths-and-facts-about-technology-assisted-review.

documents to guide the system in determining responsiveness.[15] Here, we see AI operating as a useful tool to attorneys, but not posing a threat to job security.

Milan Markovic emphasizes the distinction between routine and nonroutine work in considering legal tasks performed by AI.[16] He notes by way of example, "There is a world of difference between locating an authority for a basic proposition of law [as algorithms in online legal research tools such as Westlaw and Lexis do] versus identifying an authority that best advances a client's position in litigation."[17] Similarly, even those AI systems most adept at deep learning can be led astray if the right data is not fed into them.[18] This indicates that humans still play a key role in legal processes.

TAR and document drafting likely fall closer to the routine and repetitive side of the spectrum of work, where it is now largely uncontested that AI can benefit attorneys so they can more efficiently perform other tasks. Those concerned with the impact AI will have on the legal sector focus more on the increasing ability of AI and robots to operate in more complex and creative ways.

Even though AI is continually evolving in ability and complexity, attorneys are not currently faced with the dilemma of being entirely replaced by robots. Nor does that total overhaul appear likely in the near future.

Attorneys spend a significant amount of time engaged in legal reasoning and analysis, areas that are more challenging for AI to become proficient at, given the fact-intensive nature of many legal disputes, continually changing laws and policies, and perhaps most significantly: the fact that legal disputes are often inherently indeterminate, particularly in the early stages of a dispute.[19] Martin notes, "Humans have emotional intelligence, the ability to listen, and the ability to understand the rapidly changing nature of law and policy,"[20] which sets them apart from even the most advanced AI. Particularly in legal transactions involving emotionally-

---

15 *Id.*

16 Milan Markovic, *Rise of the Robot Lawyers?*, 61 ARIZONA L.R. 325, 333 (2019).

17 *Id.*

18 *Id.*

19 *See* Dana Remus & Frank Levy, *Can Robots be Lawyers? Computers, Lawyers, and the Practice of Law*, 30 GEO. J. LEGAL ETHICS 501, 507 (2017) (finding legal analysis and strategy, legal writing, and court appearances and preparation to comprise the majority of invoiced hours by studied lawyers in mid-size and large firms from 2012-2015).

20 Martin, *supra* note 8, at 57.

charged matters, the inability to listen and adapt to a situation as it develops could be a serious limitation of AI alternatives.

Thus, a response to the perceived threat of robots taking attorneys' jobs centers on the reality that computers lack the same emotional depth and ability to work through intelligible communication[21] as humans and, at least thus far, we have not seen AI come close to that depth of complexity.

Further, there is something to say about client demand. Many clients may prefer to interact with a human over a computer for their legal matters, given the general high-stakes nature of such matters. On the flip slide, today's increase in automation in other sectors, such as the service sector, may bode poorly for the legal profession. It would appear that at least in some circumstances, the value of an in-person, relational experience in the form of a host or waiter at a restaurant, for example, declines in the face of cut costs for businesses, as well as increased efficiency and reduced time for consumers. One need only observe the increase in "self-order" stations cropping up in restaurants and airports, where cashiers are replaced with a touch-screen interface that customers can use to select and purchase food. While attorneys admittedly provide higher-stakes services to clients than the inherently brief, one-time transactions with workers in the service sector, it remains to be seen whether consumer demand for attorneys will remain high in light of cheaper, quicker, and more convenient automated services they can use.

Ultimately, the dystopia of AI attorneys remains tenuous and distant at best, given the significance legal work has for clients and the complex reasoning and analysis required for much of it. Additionally, there are a number of public policy questions on fairness and transparency that arise with respect to AI performing certain tasks in the legal sector. However, practice has shown that AI can be a valuable resource for attorneys and actually make them more efficient at their jobs. Thus, while we are not seeing the rise of robot attorneys just yet, perhaps the legal sector's exploration of AI in various roles is ultimately of benefit.

---

[21] For example, in interpretive challenges of contracts, as in the infamous "chicken" case. Frigaliment Importing Co. v. B.N.S. International Sales Corp., 190 F.Supp.116, 117 (S.D.N.Y. 1960). Here, parties disagreed on the meaning of "chicken" in a contract. One wonders how auto-judging or even a smart contract would have kept up in the messiness of arguments on contextual meaning. *See also* Frank Pasquale, *A Rule of Persons, Not Machines: The Limits of Legal Automation*, 87 GEO. WASH. L. REV. 1, 24 (Jan. 2019).

About the Author

Kirsten Kumar is in her third and final year at the University of Texas School of Law. While in law school, she has worked for a Texas-based non-profit providing legal immigration services to refugees and asylees and for the Office of the Prosecutor at the UN International Residual Mechanism for International Criminal Tribunals, which tries individuals charged with war crimes and other violations arising from conflicts in Rwanda and the former Yugoslavia. Prior to starting law school, she was part of the technology community of Austin and worked in marketing for a local startup that was featured on ABC's Shark Tank. There, she created public-facing messaging, managed content marketing and assisted in producing content for the startup's pitch in SXSW's 2016 Accelerator Pitch Event, which it won.

Kirsten has a background in multimedia journalism, including digital photography, videography, and graphic design and has been published in various media, including lifestyle magazines and KUT Austin radio, an NPR affiliate. She plans to pursue a career in public international law upon finishing her law degree next May.

Court Considers Insurance Coverage for Phishing Attack

By Lisa M. Angelo

A company lost over $1 million after falling victim to what has become known as a run-of-the-mill phishing attack. According to court filings, the company obtained the policy limit under its Social Engineering Fraud coverage.[1] Unfortunately, the policy limit for that particular type of coverage was only $100,000, leaving the company rather short-changed.[2] As you might guess, the company looked to recover the remaining loss under its policy for Computer Transfer Fraud and Fund Transfer Fraud coverage. When its claims were denied, the company filed a lawsuit.

In the Fall of 2017, an employee at a manufacturing company in Mississippi received what appeared to be an email from a vendor the company had done business with for several years.[3] Like many phishing attacks, the "vendor" directed the employee to wire payments to a new bank account due to issues with the old account. The employee initiated the company's three-step wire authorization process that required confirmation from two additional employees, as well as a phone call from the bank's representative obtaining verbal approval from the company's manager.[4] Several days after paying a total of $1,025.881.13, the *real* vendor called the company to collect payment for the now overdue invoice.[5] It soon became clear that the company had fallen victim to a phishing attack.

Phishing attacks are fraudulent attempts to obtain sensitive information and/or money by spoofing emails or texts.[6] Unfortunately, these types of attacks are common. In 2018, victims of reported phishing attacks collectively lost over $48 million.[7]

The Mississippi case presents valuable lessons for companies considering insurance for cyber-related matters. Namely, it highlights the importance of understanding cyber threats and matching such threats to adequate coverage. For many reasons outside the scope of this

---

1 Mississippi Silicon Holdings, LLC v. Axis Ins. Co., 440 F.Supp.3d 575 (N.D. Miss. 2020).

2 *Id.* at 579.

3 *Id.* at 577.

4 *Id.* at 578.

5 *Id.* at 579.

6 *Phishing*, WIKIPEDIA, https://en.wikipedia.org/wiki/Phishing (last visited October 31, 2020.)

7 *2018 Internet Crime Report*, FBI Internet Crime Complaint Center 20 (2018), https://pdf.ic3.gov/2018_IC3Report.pdf.

article, companies are often confused about how insurance coverage applies to phishing attacks and other social engineering-related losses. Many see the word "cyber" or "computer" in a policy and make incorrect assumptions about coverage. Part of the problem is a lack of understanding about how these attacks occur. Without understanding the threat and the mechanism of execution, it is challenging to comprehend what is and isn't covered by insurance.

In the Mississippi case, the Court considered whether there was coverage under the Computer Fraud Transfer or Funds Transfer Fraud provisions by focusing on the plain language of the policy compared to the details surrounding the execution of the attack. The Computer Transfer Fraud provision provided:

> "The Insurer will pay for loss of or loss from damage to Covered Property resulting directly from Computer Transfer Fraud that causes the transfer, payment, or delivery of Covered Property from the Premises or Transfer Account to a person, place, or account beyond the Insured Entity's control, without the Insured Entity's knowledge or consent."[8]

The Funds Transfer Fraud provision provided:

> "The insurer will pay for loss of Money or Securities resulting directly from the transfer of Money or Securities from a Transfer Account to a person, place, or account beyond the Insured Entity's control, by a Financial Institution that relied upon a written, electronic, telegraphic, cable, or teletype instruction that purported to be a Transfer Instruction but, in fact, was issued without the Insured Entity's knowledge or consent."[9]

Ultimately, the Court determined these two provisions provided no coverage based on the plain language of the provisions.[10] Both provisions require the insured lack knowledge or consent, but the insured's employees in the Mississippi case had knowledge of and consented to the wire transfer as demonstrated by the execution of the three-step wire authorization process. The Court also determined that the company's situation did not fall within the definition of "Computer Transfer Fraud". The policy defined a "Computer Transfer Fraud" as "the fraudulent entry of Information into or the fraudulent alteration of any Information within a Computer

---

8 Mississippi Silicon Holdings, 440 F.Supp.3d at 579.

9 *Id.* at 583.

10 *Id.*

System."[11] The Court explained that the definition contemplated a hacking-type scenario involving the manipulation of the company's computer system which apparently, did not occur in this case.

The manufacturing company's tale is not all bad. Before filing the suit, as mentioned earlier, the insurance company found coverage under the Social Engineering Fraud provision, which provided:

> "The insurer will pay for loss of Money or Securities resulting directly from the transfer, payment, or delivery of Money or Securities from the Premises or a Transfer Account to a person, place, or account beyond the Insured Entity's control by:
>
> a. an Employee acting in good faith reliance upon a telephone, written, or electronic instruction that purported to be a Transfer Instruction but, in fact, was not issued by a Client, Employee or Vendor; or
>
> b. a Financial Institution as instructed by an Employee acting in good faith reliance upon a telephone, written, or electronic instruction that purported to be a Transfer Instruction but, in fact, was not issued by a Client, Employee or Vendor."[12]

In the end, it seems the manufacturing company had the appropriate type of coverage for typical phishing attacks but was simply underinsured for the loss. This is a common dilemma because, unlike many other types of insurance, where the value of the insured property is static, cyber and other fraud-related coverage is unpredictable. Consider, on a scale of all-to-nothing, how much will company XYZ lose next year as a result of trickery?

In hindsight, it is notable that all three steps in the wire authorization process were executed on the company's side, with no additional verification from the vendor. Could a step involving authorization from the vendor help protect companies against these types of losses? As we think of more ways to protect businesses, this might be a worth-while extra step.

It is also worth noting that the success of this phishing attack, like so many others, was due largely in part to the impersonation of an established vendor. Could the fraudsters have been aware of the existing vendor relationship? If so, how? It does not take much imagination to

---

[11] *Id.* at 581.

[12] *Id.* at 584.

think the fraudsters may had been monitoring the company's email and/or intercepted an email exchange, giving them the information necessary to launch the phishing attack. Would this open the possibility of coverage under the two provisions that were found inapplicable in this case? Although it is unclear if this issue was raised in the *Mississippi* case, it is something those in similar situations might want to consider.

One thing for certain is that companies seeking coverage for phishing attacks would be well-served by hiring a team with the appropriate technical skills to uncover exactly how the attack was executed. Every technical detail matters and could make all the difference when it comes to recovering under an insurance policy.

About the Author

Lisa M. Angelo is an attorney focused on helping businesses mitigate and manage cyber liability. She advises clients on data privacy, cybersecurity, business transactions, and other areas related to cyber law. Lisa also has a strong background in insurance law and helps clients with cyber insurance disputes. Lisa is the founding attorney of a forward-thinking, "virtual" law practice. She is an elected council member for the State Bar of Texas Computer & Technology Section. She also serves as the Vice-Chair of the State Bar of Texas Business Law Section's General Practice Committee and is a member of the Blockchain Committee. In addition, she is a member of the FBI's InfraGard Houston Chapter. Lisa is a Certified Information Privacy Manager and licensed to practice law in Texas and Colorado. She earned a Juris Doctorate from South Texas College of Law and a bachelor's in psychology from The University of Texas at Austin.

SHORT CIRCUITS:-

Seized Digital Devices Cannot Wait Forever

By Pierre Grosdidier

Federal prosecutors in New York almost lost a conviction when the Second Circuit Court of Appeals held that waiting 31 days to apply for a warrant to search a seized tablet violated the Fourth Amendment.[1] The court nonetheless declined to apply the exclusionary rule because the error was isolated and "because an objectively reasonable officer would not have known in light of existing precedent that the delay violated" the defendant's constitutional right.[2]

A state trooper found Smith slumped over the steering wheel of his car and reeking of alcohol. The trooper confiscated Smith's tablet, which displayed a picture that suggested child pornography. Once sober, Smith, a registered sex offender, declined to consent to the tablet's search. The trooper had a busy docket and waited 31 days to secure a search warrant that, once granted, revealed ample contraband, and eventually led to more contraband at Smith's residences. Smith conditionally pleaded guilty and appealed the denial of his motion to suppress on the basis that the police had waited too long to secure the search warrant.

The Fourth Amendment protects persons against unreasonable searches and seizures. A Fourth Amendment seizure occurs when authorities "meaningfully interfere" with suspects' possessory interest in their personal property.[3] Warrantless seizures are legal to protect evidence, but it is assumed that authorities will act diligently to secure a search warrant. This diligence is required to minimize the interference with the suspect's possessory interest in case the search reveals no contraband, or the contraband is segregable, or judicial scrutiny reveals that the seizure itself was improper. An unreasonably long delay in securing a search warrant following a warrantless seizure is, in and of itself, a Fourth Amendment violation.[4]

The Second Circuit analyzed the reasonableness of the delay under its four-factor test, which considers "[1] the length of the delay, [2] the importance of the seized property to the

---

1 United States v. Smith, 967 F.3d 198, 2020 WL 4290005, at *202 (2d Cir. 2020).

2 *Id.*

3 *Id.* at *205.

4 United States v. Mitchell, 565 F.3d 1347, 1350 (11th Cir. 2009); United States v. Lowe, No. H-10-813-2, 2011 WL 1831593, at *2 (S.D. Tex. 2011) (Harmon, J.).

defendant, [3] whether the defendant had a reduced property interest in the seized item, and [4] the strength of the state's justification for the delay."[5]

The court held that a 31-day delay was not presumptively reasonable and weighed substantially in the defendant's favor. The trooper had all the information needed for the warrant on the day he confiscated the tablet and all the facts that supported probable caused filled a single paragraph in the warrant application.

The court started its analysis of the second factor by considering the nature of the seized property. The court acknowledged the wealth of personal information that can be stored on a tablet (in addition to that justifying the search) and the "broader constitutional protection" that the U.S. Supreme Court accorded to seized digital devices.[6] Nevertheless, because Smith acknowledged that he could replace the tablet's functions with other devices and he did not request its return, the court concluded that the second factor weighed in the government's favor.

The court held that the third factor, Smith's reduced property interest in the tablet, was unlike that in a murder weapon or narcotics, which retain their evidentiary value without further inquiry. Instead, the tablet retained its value to the police until it was searched, which in turn hinged on when the police secured a search warrant. Therefore, probable cause to believe the tablet contained contraband reduced Smith's interest only for so long as the reasonable wait time to secure a search warrant. Because Smith never consented to the tablet's seizure and search, the court held that the third factor was either neutral or weighed in Smith's favor.

As to the fourth factor, the justification for the delay, the record showed that the investigator did scant work on the case until he applied for the warrant. The fact that he might have had a busy docket, or covered a large rural area, as the district court found, could not excuse his lack of diligence. The Fourth Amendment imposes a duty to prioritize securing a warrant after a seizure. Only a specific overriding excuse, like an investigation or a police duty, could justify a delay. The alternative would simply invite and excuse more delay. For this reason, the court held that this final factor weighed in Smith's favor. The court held that, collectively, all the factors led to the conclusion that the month-long delay was unreasonable under the Fourth Amendment.

---

[5] Smith, 2020 WL 4290005, at *206.

[6] *Id.* at *207 (referencing Riley v. California, 573 U.S. 373 (2014)).

The court compared this case with the Eleventh Circuit Court of Appeals' decision in *United States v. Mitchell*.[7] In that case, FBI agents seized a hard drive with probable cause to believe that it contained child pornography based on its owner's admission. A forensic investigator waited 21 days to secure a search warrant because he felt no urgency to do so before leaving for a two-week training trip. The court vacated the conviction because, in the absence of overriding circumstances, the delay in securing the warrant was unreasonable. In its analysis, the *Mitchell* court stressed that whether a delay is reasonable must be determined "in light of all the facts and circumstances," and "on a case-by-case basis."[8] For example, in Mitchell's case, the delay might have been reasonable had the assistance of resources been required, or had the agents in charge of the case been absorbed by overriding investigations.

The Fifth Circuit has not had the opportunity to chime in on the issue of the timeliness of search warrants for digital devices.[9] But one judge in the Southern District of Texas has. In *United States v. Lowe*, the court considered a motion to suppress based on, *inter alia*, a 21-day delay in securing a warrant to search a cell phone.[10] The court adopted *Mitchell*'s all-facts-and-circumstances and case-by-case directive. Finding that the investigating officer had satisfactorily accounted for his priorities and that the defendant had never asked for the phone's return, the court declined to find an unreasonable interference with the defendant's possessory interest in the phone, and it denied the motion to suppress. But importantly, the court also considered the fact that the information that can be stored on a phone "is far more limited" than that that can be stored on a personal computer, and the investigation's priorities "outweigh[ed] the temporary interference with stored phone numbers that could have been obtained by other means, text messages that had already been read, and digital photos."[11] The weight accorded to this last factor should be reconsidered in future cases in light of the United States Supreme Court's *Riley v. California* decision.

---

7 *Id.* at *8 (citing Mitchell, 565 F.3d at 1353).

8 Mitchell, 565 F.3d at 1351.

9 *See* Smith, 967 F.3d at *206 n.1 (citing cases from the 3rd, 4th, 7th, 9th, 10th, and 11th Circuit Courts of Appeals that have considered this issue).

10 Lowe, 2011 WL 1831593, at *2.

11 *Id.* at *3.

About the Author

Pierre Grosdidier is an attorney in Houston. He belongs to the first group of attorneys board certified in construction law by the Texas Board of Legal Specialization in 2017. Pierre's practice also includes data privacy and unauthorized computer access issues and litigation. Prior to practicing law, Pierre worked in the process control industry. He holds a Ph.D. from Caltech and a J.D. from the University of Texas. He is a member of the State Bar of Texas, an AAA Panelist, a registered P.E. in Texas (inactive), a member of the Texas Bar Foundation, a Fellow of the American Bar Foundation, and the State Bar of Texas Computer & Technology Section Treasurer for 2020–21.

Companies Transferring Data from the EU to the US May Be Left Scrambling for Solutions: The Invalidation of the EU-US Privacy Shield

By Lisa M. Angelo

Until recently, companies making external data transfer from the EU to the US had essentially two options to make adequately protected transfers under the General Data Protection Regulation ("GDPR"):[1] implement Standard Contractual Clauses or certify under the EU-US Privacy Shield framework. Those that opted for the latter were sent scrambling for solutions after a recent decision of the European Court of Justice invalidated the adequacy of the EU-US Privacy Shield.[2] The pivotal case is commonly referred to in the privacy world as "Schrems II", somewhat of a sequel to another notorious privacy case which invalidated a previously recognized safe harbor for EU-US data transfers.[3] The underlying theme of the case is a serious concern as to whether data can be protected from the eyes of the US government once it is shared with US companies.

With the EU-US Privacy Shield invalidated without mention of a grace period, many companies are quickly turning to execute Standard Contractual Clauses ("SCCs"). For the moment, it is unclear when and how European authorities will take action against companies who were transferring data under the EU-US Privacy Shield if no substitute transfer mechanism is in place. Presumably, the EU authorities would give deference to companies actively pursuing an acceptable transfer mechanism. Of course, nothing is certain until more guidance is issued. The reality is that many companies may face significant business interruption if they were to cease international transfers of data while pursuing a solution. On the flip side, there could be substantial fines and penalties for violating the GDPR.

It seems the most common options involve implementing Standard Contractual Clauses or redirecting the flow of data away from the US. Companies switching to Standard Contractual Clauses might not be out of the woods for long. Since a basis for invalidating the EU-US Privacy

---

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Ch. V, *Transfers of personal data to third countries or international organisations*.

2 Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd., Maximillian Schrems and intervening parties, 2020 E.C.R. I-559.

3 Case C-362/14, *Maximillian Schrems v. Facebook Ireland Limited*, 2014 E.C.R. I-650.

Shield is the existence of laws that make data available to the US government, such rationale might also apply to the Standard Contractual Clauses. For now, guidance provides that companies should evaluate each relationship involving data transfers from the EU to US and consider whether the terms of the Standard Contractual Clauses could adequately protect such data.[4] With so much uncertainty, companies will want to give careful consideration and be able to justify any decision to rely on the Standard Contractual Clauses as a mechanism to protect data being transferred from the EU to the US. For in-house counsels and privacy attorneys, this means reviewing data maps and updating data protection terms as companies return to their data-transfer drawing boards.

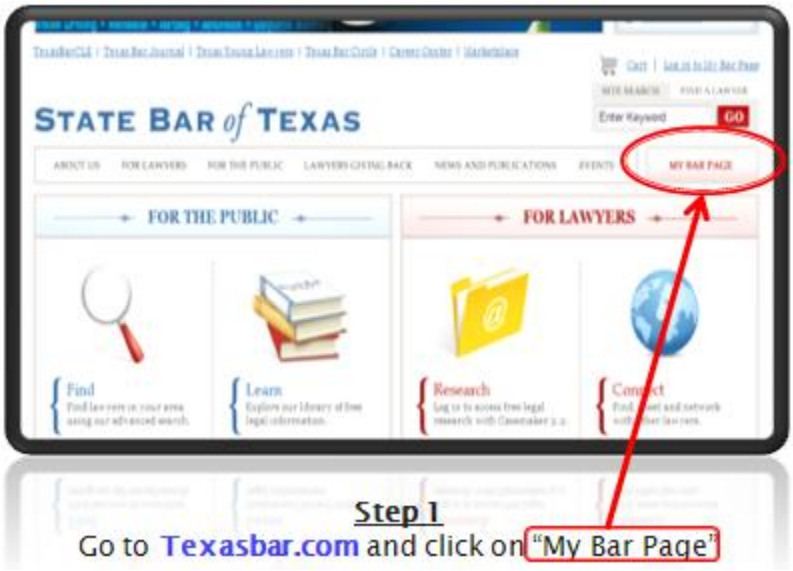
About the Author

Lisa M. Angelo is an attorney focused on helping businesses mitigate and manage cyber liability. She advises clients on data privacy, cybersecurity, business transactions, and other areas related to cyber law. Lisa also has a strong background in insurance law and helps clients with cyber insurance disputes. Lisa is the founding attorney of a forward-thinking, "virtual" law practice. She is an elected council member for the State Bar of Texas Computer & Technology Section. She also serves as the Vice-Chair of the State Bar of Texas Business Law Section's General Practice Committee and is a member of the Blockchain Committee. In addition, she is a member of the FBI's InfraGard Houston Chapter. Lisa is a Certified Information Privacy Manager and licensed to practice law in Texas and Colorado. She earned a Juris Doctorate from South Texas College of Law and a bachelor's in psychology from The University of Texas at Austin.

[4] European Data Protection Board FAQ on the judgment of the Court of Justice of the European Union in Case C-311/18, Adopted on 23 July 2020, https://edpb.europa.eu/our-work-tools/our-documents/ovrigt/frequently-asked-questions-judgment-court-justice-european-union_en (last visited Sept. 13, 2020).

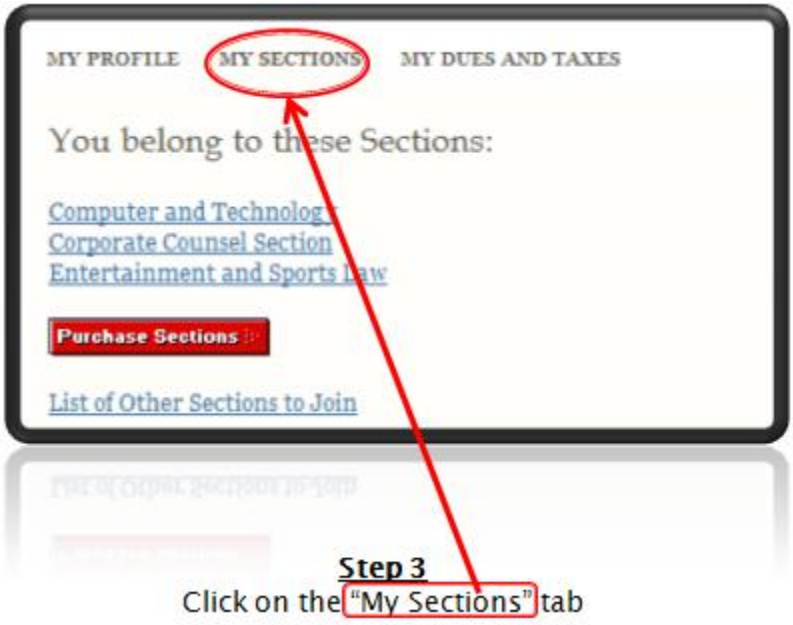
How to Join the State Bar of Texas Computer & Technology Section

Joining the State Bar of Texas Computer & Technology Section is easy. You can join online by visiting the State Bar of Texas Website at www.Texasbar.com. Please follow these instructions to join the Computer & Technology Section online.



Step 1
Go to Texasbar.com and click on "My Bar Page"

Step 2
Login using your bar number and password
(this will be the same information you'll use to login to the Section website)



If you see "Computer and Technology", congratulations, you're already a member.

If not, click the "Purchase Sections" button and follow the instructions to add the Computer and Technology Section. **Please note: It may take several days for the State Bar to process your section membership and update our system.**

You can also complete this form and mail or fax it in.

State Bar of Texas Computer & Technology Section Council

Officers:
Shawn Tuma – Plano – Chair
Elizabeth Rogers – Austin – Chair-Elect
Pierre Grosdidier – Houston – Treasurer
Reginal Hirsch – Houston – Secretary
John Browning – Dallas – Past Chair

Circuits Editors:
Sanjeev Kumar – Austin
Kristen Knauf – Dallas

Webmasters:
Ron Chichester – Houston
Rick Robertson – Dallas

Appointed Judicial Members:
Judge Xavier Rodriguez – San Antonio
Hon. Roy Ferguson – Alpine

Term Expiring 2022:
Lavonne Burke Hopkins – Houston
Gwendolyn Seale – Austin
Alex Shahrestani – Austin
Michelle Mellon-Werch – Austin

Term Expiring 2021:
Chris Downs – Plano
Seth Jaffe – Houston
Judge Emily Miskel – Dallas
William Smith – Austin

Chairs of the Computer & Technology Section

2019-2020: John Browning
2018-2019: Sammy Ford IV
2017-2018: Michael Curran
2016-2017: Shannon Warren
2015-2016: Craig Ball
2014-2015: Joseph Jacobson
2013-2014: Antony P. Ng
2012-2013: Thomas Jason Smith
2011-2012: Ralph H. Brock
2010-2011: Grant Matthew Scheiner
2009-2010: Josiah Q. Hamilton
2008-2009: Ronald Lyle Chichester
2007-2008: Mark Ilan Unger
2006-2007: Michael David Peck
2005-2006: Robert A. Ray
2004-2005: James E. Hambleton
2003-2004: Jason Scott Coomer
2002-2003: Curt B. Henderson
2001-2002: Clint Foster Sare
2000-2001: Lisa Lynn Meyerhoff
1999-2000: Patrick D. Mahoney
1998-1999: Tamara L. Kurtz
1997-1998: William L. Lafuze
1996-1997: William Bates Roberts
1995-1996: Al Harrison
1994-1995: Herbert J. Hammond
1993-1994: Robert D. Kimball
1992-1993: Raymond T. Nimmer
1991-1992: Peter S. Vogel
1990-1991: Peter S. Vogel