

TECH TRANSACTIONS & DATA PRIVACY

2021 REPORT

As we bid farewell to 2020 and look toward the uncharted territory of 2021, it is hard not to take inventory of all that has changed in such a short period. No one at the beginning of 2020 would have predicted what transpired throughout this past year. And while many would like to forget everything about 2020, this past year exponentially accelerated specific industries forward in many ways. The changes we saw in our working environments, education, shopping and social and political engagements were all foreseeable, but the leaps made this past year were transformational.

As Polsinelli's Technology Transactions and Data Privacy Group looks to 2021, our industry's immediate landscape is dominated by the continuing pandemic, rapidly changing regulatory landscape (domestically and globally), data sprawl, cloud access and the diversity and sophistication of security threats and actions. In this report, our attorneys look forward to 2021 and highlight some of the most innovative issues we will face in the new year and beyond.

Today, more than ever before, no industry on the planet is not touched by technology. The importance, sophistication and prominence of technology, privacy and security issues will further accelerate in 2021.

Our attorneys are ready to assist our clients in whatever the new year may bring. We are excited about the future and how we will help shape it.

Sincerely,



Greg Kratofil, Jr.
Chair – Technology Transactions & Data Privacy

PRIVACY AND DATA SECURITY: GENERAL APPLICABILITY

General Counsel's Data Privacy and Security Must-Dos for 2021

Gregory M. Kratofil, Jr.
Co-Office Managing
Partner | Practice Chair
Kansas City



Bruce A. Radke
Shareholder
Chicago



Iliana L. Peters
Shareholder
Washington, D.C.



Caitlin A. Smith
Associate
Washington, D.C.



While General Counsels shifted focus to COVID-19 and the vast changes that it brought to the workplace in 2020, the new year will see a continued focus on the importance of data use and data sharing to business operations, new and changing privacy laws and enforcement, and the proliferation and devastation of cyberattacks on already vulnerable workforces. General Counsels' attention to data privacy- and security-related issues will be at the forefront in 2021. If you are unsure where to begin or want to look back at the end of this year and feel like you have accomplished something tangible, below are the 5 "Must-Dos" for 2021.

Data Knowledge – What, Where, How and Why

A great deal of focus will continue around the requirements contained in the California Consumer Privacy Act ("CCPA"), which was enhanced by the California Privacy Rights Act ("CPRA"), or the European Union's General Data Protection Regulation ("EU GDPR"). The truth is there are a number of privacy-related laws, regulations and best practices that depend on a myriad of factors such as a business' location, products, industry, and clients. Where do General Counsels even begin?

General Counsels should prioritize having complete "data knowledge" in 2021. Every analysis of a company's privacy and security compliance starts with knowing: (1) what data the company has, (2) whether the data is identifiable to individuals, and where such individuals live, (3) where the data itself is located, (4) how the data is used and disclosed, and (5) why the data is needed. Data knowledge underpins every privacy- or security-related action (or inaction) a company will take in its current operations and future planning.

Outside counsel experienced with gathering the right type of information and asking the right questions should be consulted. However, once this analysis is complete, the General Counsels will be surprised how often they utilize this analysis to address day-to-day privacy and security issues and assist the business with discussions of future products or service offerings. The investment here will save time and money in 2021 and beyond.

Employee Cybersecurity Training

Although organizations will spend more than \$100 billion on cybersecurity in 2021, data incidents will continue to routinely occur, because one weak link – employees – will remain a significant vulnerability to an organization's cybersecurity defenses. General Counsels should understand that human error

is one of the prime causes of data incidents. Educating and training employees on privacy and cybersecurity best practices is, therefore, vital – especially in today's remote work environment.

Employee cybersecurity training is essential, given that a recent survey revealed that nearly a third of employees did not have a basic understanding of how to recognize a phishing email and what to do if they received such an email. The survey also found that ransomware was an unknown concept to nearly two-thirds of workers.

Experienced legal counsel should collaborate with General Counsels and human resources departments to develop a tailored privacy and cybersecurity employee training program that teaches employees to:

- recognize potential risks and attack mechanisms (such as email phishing, and ransomware);
- take steps to protect themselves and the company, both with regard to paper and electronic data; and
- understand the process to report an actual or suspected incident promptly.

To be effective, a privacy and cybersecurity training program must cover the types of threats that an organization is most likely to face, such as:

- email scams;
- malware and ransomware;
- password security;
- remote work issues; and
- social networking dangers.

A privacy and cybersecurity training program that addresses these items will reduce the chance that an organization will experience a data incident in 2021 or lessen the magnitude of such an incident by empowering employees to recognize and report an incident or ongoing attack quickly.

CONTINUED ON PAGE 3 ▶

Practice

While there was increased activity among threat actors in 2020, the pandemic also strained resources and shifted IT priorities to account for things like the acceleration of remote work. General Counsels must understand and accept that data security incidents are inevitable despite their organization's best efforts. The question remains, if an incident happens, what is the best course of action?

Near the top of any General Counsels' list for 2021 is to schedule a tabletop exercise and practice incident response. Practice may not make perfect, but practicing incident response before crisis strikes lowers anxiety and gives incident response teams confidence to make the quick and decisive decisions that are so critical at the beginning of any incident.

Even if teams have practiced in the past, such exercises should be a priority to do so again in 2021. Tabletop exercises are low-cost and routinely done on a fixed-fee basis. Experienced outside counsel will tailor the exercise so it incorporates the most common or cutting-edge issues. Outside counsel should conduct a "post mortem" with an analysis of the team's response and make suggestions to improve for the future.

Vendor Risks

As organizations strive to reduce overhead and administrative drains, General Counsels find that achieving this objective often leads their organizations to seek ready-made third-party vendor tools. Companies use vendors to outsource discrete back-office tasks, like payroll or inventory, or entire departments, like IT Security or Human Resources. There could be software-as-a-service (SaaS) solutions used in-house or off-premises services managed entirely by a third party. Unfortunately, when any organization allows third parties to access systems remotely or no longer control the most sensitive data in-house, the risk for a data security incident rises. Vendor-caused incidents are inevitable, but unfortunately, many organizations fail to prioritize data security at the contracting stage. In 2021, the General Counsels should prioritize the vendor-vetting process and strive to negotiate contract terms that address business interruption and data privacy and security.

Since the market is flooded with vendors providing similar tools, companies often have the power to negotiate privacy and

data security terms in contracts or else find other vendors willing to negotiate on terms. Even more often, some provisions are already included in the vendor template, like a time frame in which the vendor must notify customers of an incident or a promise to maintain the privacy and confidentiality of customer data. However, these template contracts rarely include remedies for service outages caused by cyberattacks, failure to meet the contractual obligation to notify a customer of a security event in a timely way, or indemnification for incident response-related costs.

One example of a worst-case scenario for a vendor-caused data security incident was the Blackbaud Inc. data breach from July 2020, which impacted hundreds of college, universities, non-profits, and hospitals, and resulted in notification to millions of people. Blackbaud Inc., a cloud service provider that manages charitable donor information for companies, announced in July 2020 that data was stolen off of its servers from February – May 2020. Many customers had a contractual requirement that Blackbaud must notify them of a data security incident within 72-hours of its occurrence, which was allegedly ignored by Blackbaud. However, most customers found themselves with the legal burden of notifying donors, where required, but without any financial assistance from Blackbaud. Class action lawsuits have piled up, ranging from breach of contract to negligence to failure to timely notify victims of the incident and its scope. While customers could not prevent the incident from happening, counsel could have inserted indemnification or remedy provisions that would have made this ordeal more palatable for many companies.

It is important for General Counsels to understand from internal staff what data the vendor will have access to and what the vendor will be doing with that data in order to tailor the data privacy and security provisions of that contract. Experienced data privacy and security outside counsel can assist General Counsels in deciding which contract provisions should be considered essential when contracting with a vendor to receive certain sensitive data versus provisions that would be "nice to have" when dealing with less sensitive data.

Mergers and Acquisitions

Whether General Counsels help prepare companies for potential sale or support the acquisition of new businesses or products,

there is no denying that privacy and data security will remain critical elements for M&A in 2021. A company's data has increasingly become an important asset having a positive impact on value. Conversely, a company that fails to protect its data through privacy or security compliance creates a meaningful liability that can lead to lower valuations and/or jeopardize the entire transaction. What are some steps General Counsels should take?

Companies that collect, use and store data about customers and employees must be prepared to address the issues proactively and not wait until "caught" in the middle of the transaction. A General Counsel, as either a buyer or seller, should:

- be familiar with an updated due diligence checklist that reflects current best practices in privacy and data security and is tailored to their industry;
- review due diligence materials by someone experienced with the issues, industry regulations and best practices to be aware of potential problems and pitfalls sooner;
- be familiar with updated and appropriate privacy and data security representations, warranties and covenants in deal documents; and
- be prepared to negotiate on more stringent privacy and data security protections through indemnities, holdbacks, escrow accounts and insurance.

Regardless of whether preparing for a sale or making an acquisition, a General Counsel should have M&A lawyers that have access to experienced data privacy and security outside counsel. In 2021, the potential minefield of issues and risk is too great for a generalist or someone "dabbling" in these crucial issues.

What will you do?

Do your priorities for 2021 include the critical issues discussed above? Do you have good outside counsel with whom to discuss these issues? If the answer to these questions is no, we suggest that you reconsider your "Must Do" list for 2021. If the answer to these questions is yes, you're on track for a solid compliance effort in 2021.

Contact Tracing and Data Protection Laws: What You Need to Know Before You Contact Consumers

INTRODUCTION: To date, over 85 million people worldwide have been exposed to SARS-CoV-2, the virus that causes COVID-19. Governments around the world attempting to slow the spread of COVID-19 have implemented a number of responses. One such method is contact tracing, a process by which public health officials identify individuals who have come into contact with infected persons. **This article will examine how certain data privacy and security laws apply to contact tracing and what pitfalls a company might experience when engaging in contact tracing.**

Kathryn T. Allen
Shareholder
Kansas City



Hale H. Melnick
Associate
Chicago



What is Contact Tracing? The term contact tracing generally refers to the identification and monitoring of people who have been in contact with individuals diagnosed with an infectious disease in order to implement targeted control measures (such as quarantine) to prevent the broader spread of the infectious disease. Contact tracing has been a standard procedure in public health investigations by government officials for many years. However, we are seeing more private businesses employ similar methods for their employees and customers.

Traditionally, contact tracing has been conducted manually through interviews and data collection by public health officials. However, such manual contact tracing has severe limitations—especially with the fast-spreading COVID-19—because the interview process and data analyses required for a successful program can take significant time to perform. Additionally, it can be difficult to locate and quickly notify infected individuals' close contacts because such individuals often cannot identify each person with whom they had close contact, such as passengers on a train. As a result of these limitations, some governments and private sector entities have turned to digital contact tracing methods.

Digital Contact Tracing (“DCT”). Digital contact tracing, or digital exposure notification, refers to the use of technology to identify and notify individuals who may have come into contact with a person who has tested positive for COVID-19. There are two primary methods for digital contact tracing:

- Location tracking apps, which trace a mobile device's movement using location information, such as global positioning system (GPS) or cell site location information; and
- Digital exposure notification or proximity tracking apps, which receive and transmit device identifiers (generally through Bluetooth technology) when two devices remain in close proximity for a set amount of time.

Both of the digital contact tracing methods above use data collected from a digital device to determine whether the user has come into contact with infected persons. When a user is identified as being infected with a certain disease, that information is logged with the device—either in a centralized or decentralized database—and the individual's device notifies all other devices with which it made contact to alert users that they may have been exposed.

Privacy Concerns with DCT. While digital contact tracing can be an effective tool to combat the spread of infectious disease, the technology also raises a number of privacy concerns. Digital contact tracing technology—and location tracking apps in particular—can be invasive, especially when such data is maintained on a central database that others can access. Contact tracing apps also have the ability to collect more than the minimum information necessary to alert users of contact with infected individuals. For example, some contact tracing apps collect biometric data and other sensitive personal data that could cause significant harm to the individual if the data

is breached. Furthermore, even some of the most sophisticated contact tracing app technologies could permit the re-identification of infected individuals.

Data Protection Laws and their Application to DCT. In addition to navigating the privacy and security concerns described above from a public relations perspective, private entities must also navigate federal and state privacy and security laws implicated by the technology. At a federal level, the United States has not adopted a comprehensive federal data protection law, but rather, relies on a “patchwork” of sectoral laws to govern specific types of information. These laws include the following Acts:

- Health Insurance Portability and Accountability Act, which limits certain health care entities' use and disclosure of health information;
- Communications Act of 1934, which limits phone carriers' use of customer data;
- Family Educational Rights and Privacy Act of 1974, which limits educational agencies' and institutions' disclosure of student education records; and
- Children's Online Privacy Protection Act, which limits what personal information operators of online services can collect, use, and disclose from children under the age of 13.

In addition, some states, like California, have adopted their own privacy and security laws, which may be more restrictive than federal laws, although they have more limited jurisdiction. Below, we examine how such laws broadly apply to digital contact tracing technology and the challenges they can bring to a private entity.

CONTINUED ON PAGE 5 ▶

- **Health Insurance Portability and Accountability Act (“HIPAA”).** Pursuant to its authority under HIPAA, the Department of Health and Human Services (“DHHS”) has enacted data protection regulations known as the Privacy, Security, and Breach Notification Rules (“HIPAA Rules”) to protect individuals’ medical records and other personal health information. However, the HIPAA Rules do not apply to all health-related data, but rather only to individually identifiable health information (“protected health information,” or “PHI”) that is created, received, used, or maintained by a covered entity (i.e., a health plan, health care provider or health care clearinghouse) or its business associates (i.e., a person or entity engaged by a covered entity to help the covered entity carry out its health care activities or functions). The extent to which the HIPAA Rules apply to digital contact tracing apps, therefore, depends on whether the parties that develop, operate, or are otherwise involved with the digital contact tracing app, fall within the definition of a covered entity or business associate. If HIPAA does apply, the permissible uses and disclosures of the users’ data will be heavily regulated. For example, a user’s information may not be disclosed to any third party without the user’s authorization (written consent), and breaches of the app’s data security could lead to significant civil monetary penalties (CMPs).
- **The Communications Act of 1934.** The Communications Act of 1934 restricts what “telecommunications carriers”—namely, landline and mobile telephone operators—may do with “customer proprietary network information,” or “CPNI.” Most relevant for digital contact tracing, the Communication Act’s CPNI protections generally prohibit cell phone carriers from disclosing users’ geolocation data to digital contact tracing apps. However, disclosing such data for contact tracing purposes may qualify as an exception under the Communications Act if the geolocation data is provided as an “emergency service” to the contact tracing app and the app is acting as a “provider of information or database management service.” However, the scope of this exception is unclear; it appears that neither the FCC nor the courts have defined the terms “information or database management services” and “emergency services”—nor have they otherwise opined on the nature of this exception.

- **Family Educational Rights and Privacy Act of 1974 (“FERPA”).** As more schools try to reopen, many of them are working with private sector developers and/or public health officials engaged in digital contact tracing. However, under FERPA, any “educational agency or institution” receiving federal funds (“covered entities”) must comply with FERPA’s strict requirements. FERPA imposes privacy protections for student education records, which are defined broadly to include any “materials which...contain information directly related to a student” and are “maintained by an educational agency or institution.” Among other things, FERPA prohibits covered entities from having a “policy or practice” of permitting the release of education records or “personally identifiable information contained therein,” without the parent’s consent (or student’s consent if the student is over 18 or attends a postsecondary institution). This consent requirement is subject to certain exceptions. Most relevant, under the “health or safety emergency” exception, if a covered entity determines that “there is an articulable and significant threat to the health or safety of a student or other individuals,” then it may disclose “information from education records to any person whose knowledge of the information is necessary to protect the health or safety of the student or other individuals.”
- **Children’s Online Privacy Protection Act (“COPPA”).** COPPA is designed to protect the privacy of children under the age of 13 by imposing certain obligations on operators of online services (including apps) that collect children’s information. Specifically, an entity is subject to COPPA if it: (1) collects or maintains personal information from users of the service (or has the information collected or maintained on its behalf); (2) operates the service “for commercial purposes”; and (3) either directs its services towards children or has “actual knowledge that it is collecting personal information from a child.” If a digital contact tracing app is subject to COPPA, the app’s operator must undertake a number of privacy-protecting steps. First, the operator must provide notice as to what type of information is collected and how it is used. Second, the operator may not collect, use, or disclose personal information without receiving verifiable parental consent before the information is collected. Third, operators must comply

with certain data retention and deletion requirements. And fourth, operators must establish and maintain “reasonable procedures” designed to protect the confidentiality, security, and integrity of the information.

- **California Consumer Privacy Act (“CCPA”).** While this article does not go into detail on state privacy and security laws and regulations, it is important to note what is perhaps the broadest reaching and most onerous of them all, the CCPA. The CCPA generally regulates how businesses collect and use consumers’ personal information, and it gives consumers certain rights with respect to their personal information, such as the right to know what personal information a business collects about them and the right to request that the business delete their personal information. A “business” means, generally, a for-profit entity that (i) has annual gross revenues in excess of \$25 million; (ii) buys, receives, sells, or shares the personal information of 50,000 or more consumers; or (iii) derives 50% or more of its annual revenues from selling consumers’ personal information. A “consumer” means any California resident; and “personal information” is defined very broadly to mean “information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household,” which includes, among other things, a consumer’s name or unique personal identifier.

Conclusion. When considering whether to engage in any type of contact tracing, entities should take into account privacy concerns that their employees, customers or other third parties might have with the practice or technology being used, as well as the various federal and state privacy and security laws that may impact such data collection, use and disclosure. When in doubt, it is always best to consult with a privacy expert familiar with the laws and regulations of your industry and your state.

Remote Employee Monitoring: An Accelerating Trend in a Pandemic World

Gregory L. Cohen
Shareholder
Phoenix



Reece Clark
Associate
Kansas City



1. Introduction

As the coronavirus pandemic forced non-essential businesses to close their offices in early 2020, companies were suddenly faced with the unprecedented task of managing a fully remote work force. This was a big change for most companies, which previously had limited or case-by-case experience with remote working configurations. Managers were expected to ensure productivity continued even as they lacked in-person access to their employees or visibility into daily activities. Some tools, such as virtual meetings, were quickly instituted to meet the need for face-to-face interaction.

But understanding remote employee working habits and conditions remained a challenge. As a result, companies gravitated towards remote employee monitoring software and services to provide new insights into their workforce. Demand for such services surged in 2020, and we expect that trend to continue for the foreseeable future. However, with new tools comes new challenges and new risks. We examine what you need to know about employee remote monitoring services in 2021.

2. Evaluating Remote Monitoring Services

Companies considering a remote employee monitoring service will find a wide range of

tools, features and capabilities are available on the commercial market in 2021. Some services track employee time spent on apps, websites, and email. Other services monitor team productivity levels, track time spent on non-work related websites, or focus on enforcing data security policies. The common denominator among these services is that they provide insights into employee activity on a near real-time basis. And once deployed, companies often find these services not only provide visibility into employee productivity and working habits, but also help spot signs of employee burn-out or disengagement.

We expect companies will more actively consider deploying remote monitoring software in 2021. Companies report they are increasingly worried their remote workforce will lose a sense of shared purpose without in-person proximity to colleagues. As shared purpose erodes, productivity may languish. Taking these concerns in stride, a company should consider the following threshold question when evaluating the right remote monitoring service: what behaviors does a company wish to identify and address using these services and, more generally, what are the company objectives for implementing a remote monitoring service?

3. Identifying Objectives

Some companies have a regulatory need to monitor employees. In those sectors, such as healthcare and finance, companies and employees are aligned in the need for employee monitoring given the sensitivity of the information and work. Other sectors lack such regulatory rigors, and so the choice to monitor employees becomes a business decision. In identifying a company objective for monitoring, the reasons are varied. Some companies report wanting to improve productivity or working conditions. Other companies want to apply greater employee oversight, police company equipment, or gain behavioral insights related to remote work. Whatever the reason, a company should document its reasons, formulate clear objectives, and seek internal buy-in from key stakeholders.

In seeking buy-in, companies should not forget the employees themselves. Without transparency in decision-making, employees may not understand the business reasons for employee monitoring, and may be surprised to learn they are or will be monitored. To avoid damaging employee trust, companies thinking about instituting remote employee monitoring should be transparent in their business objectives, and make clear what actions will be monitored and why. If employees understand, for example, that they are being monitored to ensure they are receiving the support and resources they need to continue to be productive, they are likely to be more comfortable with the practice. Likewise, managers should understand what the company objectives are with respect to the monitoring services, and use the insights derived from the services exclusively to carry out those objectives.

4. Software Acquisition Issues

Even with a clear objective for employee monitoring services, legal risks remain. Consider first the contractual risks that a company may undertake in securing access to employee monitoring services. Employee monitoring services generally involve a mix of hosted and on-premises solutions, and may also require establishing secure data flows, hosting environments, and security solutions. These pieces all involve license and service agreements of varying natures. If not careful, companies may unknowingly agree to onerous legal terms that involve, for example, heavy risk shifting, sweeping disclaimers, difficult termination provisions, data ownership transfers, payment penalties, or lax service levels. The data ownership and usage provisions within the license or service agreement will be particularly important considering the nature of the information that is being monitored, collected and stored. These risks may manifest themselves in a poor return on investment through underperforming services, overpayment of fees, security incidents, or worse. Employers should consult with their technology counsel

CONTINUED ON PAGE 3 ▶

to identify these risks on the front end, negotiate the software agreement, and mitigate these potential risks.

5. Legal and Regulatory Risks from Employee Monitoring

Beyond software matters, there are regulatory risks to consider as well. For example, the Electronic Communications Privacy Act of 1986 (“ECPA”) is federal law that, with key exceptions, restricts employers from intentionally intercepting employees’ electronic communications. And while the ECPA sets forth minimum restrictions on monitoring employee communications, many states have enacted their own restrictions. Thus, companies should perform a regulatory analysis of the states in which they do business to evaluate the privacy-related risks they may face in implementing employee monitoring systems. Employers should also consider the implications of common-law tort claims involving invasion of privacy. Some important issues to consider include:

- Whether employees are working from company-supplied computers or other devices or their own personal computers;
- Whether employee acknowledgment is obtained regarding the monitoring;
- Whether and how the monitoring is disclosed to employees and whether it is discussed in the employee handbook or other employee documents;
- Who within the company will have access to the monitoring information;
- How the monitoring information is used within the company including whether it will be used to take disciplinary action; and
- How long the monitoring information is kept and how it is stored or maintained.

Here, employers should consult with their labor and employment counsel and data privacy counsel to develop disclosures and administrative measures that create transparency in the types and uses of monitoring services to mitigate and reduce company risk from both statutory and common law privacy violations.

6. What to Expect in 2021

In 2021, we expect the demand for employee monitoring to continue to increase as the workforce remains remote or enters into a hybrid phase. With increased demand, we expect more employers to face organizational and legal challenges in the implementation and use of remote monitoring services. Companies should take care in rolling out remote employee monitoring services to mitigate potential privacy and regulatory issues and strive for transparency at all levels. From the outset, companies should seek counsel experienced in managing technology and privacy risk to help develop a plan for implementing remote employee monitoring services safely and effectively.

Van Buren v. United States and the Future of Redress Against Malicious Insiders that Access Company Data

Kayleigh S. Shuler
Associate
Kansas City



Pasha A. Sternberg
Associate
San Francisco



What happens when an employee or other company insider uses legitimate access to

company information to further his or her own personal ends? For example, a curious employee may search her company’s database for information about a neighbor, or a departing employee may search the same database for information useful to her potential new employer. In either case, might the employer be able to sue the former employee? And might the former employee have committed a crime?

These are questions the Supreme Court of the United States may answer in a decision expected later this year in *Van Buren v. United States*, in which the Court has been asked to interpret the scope of a federal law known as the Computer Fraud and Abuse Act (or “CCFA”).¹

The CCFA

The CCFA is a federal statute initially passed in 1986 that makes it illegal for a person to access a computer without authorization. A person violates the CCFA when he or she “intentionally access[es] a computer without authorization or exceed[s] authorized access, and thereby obtain[s]...information” from that computer.² This standard, while on first glance fairly straightforward, has in the last decade created vigorous debate among academics, and a circuit split in federal court, and is now up for review by the Supreme Court.

The primary focus in *Van Buren v. United States* is the scope of the second clause cited above. The law itself provides limited guidance on the clause’s meaning, telling us only that

¹ Supreme Court of the United States case number 19-783.
² 18 U.S.C. § 1030(a)(2).

a person “exceeds authorized access” by accessing a computer with authorization and then using that access “to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.”³

Lower courts are divided as to the CCFA’s reach when it comes to individuals that misuse information that they would have been allowed to use for some other purpose. Some courts have concluded that the CCFA applies only to conduct that involves a person doing something akin to “hacking” into a computer,⁴ while others have concluded that the CCFA also applies where a person accesses information rightfully available to him or her (i.e., where the individual views information without any form of “hacking”) but the information is then misused.⁵

Part of the challenge in interpreting the law no doubt arises from the environment in which its text was written. Congress passed the CCFA in 1986 and, while it has subjected the law to limited amendments since then, it has never undertaken a wholesale update. As a result, this law meant to regulate activity on computers was written largely before the age of the modern Internet.

Nevertheless, because there are so few cybersecurity and cybercrime statutes on the books, public and private employers alike have turned to CCFA for potential redress against company insiders. As it provides for both criminal and civil remedies (including, in the latter case, both compensatory damages and equitable relief), some have seen the law as a means of pursuing federal redress against company insiders when other laws, such as those applicable to trade secret theft, are a poor fit. The facts of *Van Buren*, however, illustrate the challenge in applying the law

in today’s world where accessing company information on computers is the dominant part of many American’s daily work activities.

The Facts of the *Van Buren* Case

Nathan Van Buren was a police sergeant who, as part of his job, was given access to a database maintained by state and federal law enforcement agencies. The database included information identifying certain individuals as police officers. At the request of, and in exchange for payment from, an acquaintance named Andrew Albo, Van Buren used the database to lookup a woman and report back to Albo whether she was an undercover police officer. Unbeknownst to Van Buren, Albo himself was working with police and had asked Van Buren to run the search as part of an FBI sting operation against Van Buren.

Van Buren was subsequently found guilty of violating the CCFA in a conviction upheld by the Eleventh Circuit. On this appeal to the Supreme Court, Van Buren is admitting that his purpose for accessing the police database was inappropriate, but contends that his conduct does not violate the CCFA. Specifically, he argues that the CCFA applies only to computer hackings, and thus does not apply to his activity since he was lawfully allowed to access the database at issue. In contrast, the United States argues that the CCFA prohibits not just hacking, but also the type of abuse of privilege engaged in by Van Buren.

The Implications of the Court’s Decision

The Court’s decision in *Van Buren* will likely turn on whether the law is sufficiently clear in prohibiting the type of activity at issue. Oral

argument in the case suggested the Court may reference legal principles like *lenity*, which demands that ambiguous criminal laws be interpreted favorably for defendants, although it is not clear how the Court might apply that principle here.

Whatever reasoning the Court ultimately invokes, a decision confirming the expanded view of the CCFA advocated by the government could provide employers a viable path for using the CCFA to pursue action against former employees who access company information before departing (i.e., at a time when they have legitimate access to that information) for an inappropriate purpose, such as gaining information useful for a competing business or harming the company’s reputation. In that case, the next important question will likely be around how to define the activity that “exceeds” legitimate access (e.g., whether this would be based on company policy, an employment agreement, or something else).

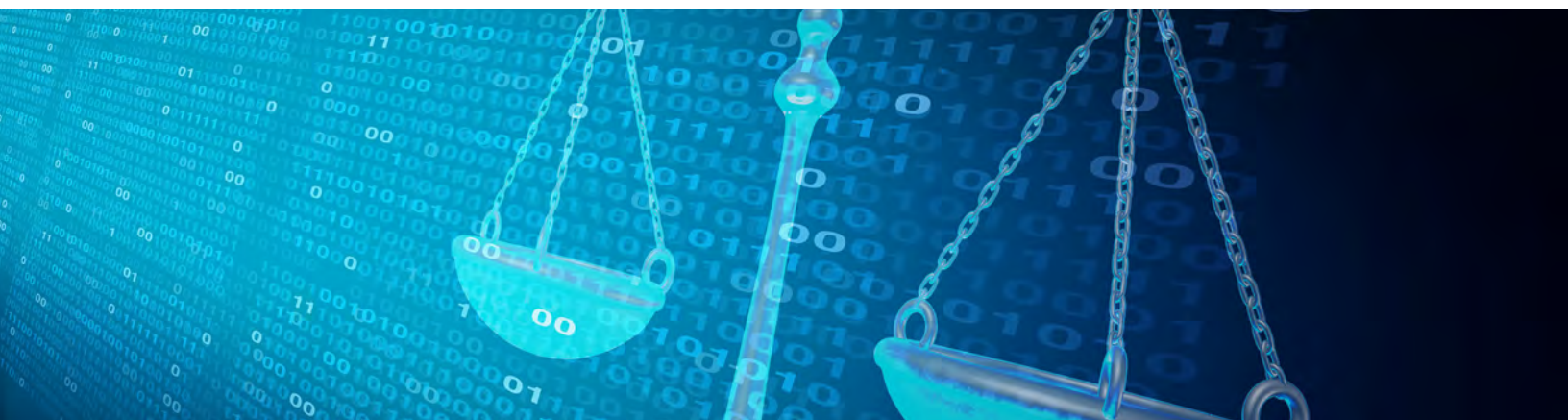
In contrast, a decision rejecting the government’s expanded view of the CCFA and instead ruling that the law applies only where a person has no legitimate means of accessing company information (i.e., that the law only applies where some form of hacking has occurred) may cut off the CCFA once and for all as a potential avenue for redress against malicious insiders. In that case, employers will likely continue turning to sometimes ill-fitting laws around things like trade secret theft, fraud and misrepresentation to pursue former employees in these types of cases.

Polsinelli will continue to watch for the Court’s decision in *Van Buren* and analyze its effect for our clients.

³ *Id.* at § 1030(e)(6).

⁴ See, e.g., *United States v. Steele*, 595 Fed. Appx. 208 (4th Cir. 2014).

⁵ See, e.g., *Van Buren v. United States*, 940 F.3d 1192 (11th Cir. 2019).



PRIVACY AND DATA SECURITY: RANSOMWARE

The Rise of Data Exfiltration in Ransomware Attacks

Michael J. Waters
Shareholder
Chicago



Jane E. Petoskey
Associate
Seattle



Jessica L. Peel
Associate
Kansas City



It can be difficult to prognosticate the data security threats organizations will face in an upcoming year given that threat actors are regularly changing the tools and techniques that they use to attack organizations. Given, however, the unabated increase in ransomware attacks over the past few years, it is safe to say that ransomware attacks will continue to be a major issue in 2021.

In 2020, ransomware attacks were among the top types of data security incidents,¹ as detailed in Verizon's 2020 Data Breach Investigations Report. In the first half of 2020, "no industry was spared from ransomware activity[.]" where the "five most heavily targeted sectors were" telecommunications, managed security service providers, "education, government, and" technology.²

The newest threat with ransomware attacks involves the exfiltration of an organization's data, which is often coupled with data encryption. In such cases, threat actors demand payment of a ransom in exchange for both a decryption tool and an agreement not to publish and/or sell an organization's data.

The most commonly seen ransomware variants are as follows: Sodinokibi, Maze (most recently appearing to be inherited by Egregor), Netwalker, Phobos, DoppelPaymer, Snatch, Conti, Lockbit, Dharma, Nephilim, and Avaddon.³ A primary difference between the variants includes the associated ransomware attack style, as discussed below.

Ransomware Attack Styles

1. System Interruption

One of the most commonly seen styles of ransomware attacks is where a threat actor accesses an organization's computer network (whether through open Remote Desktop Protocol ("RDP"), email phishing, software vulnerabilities, etc.) and then takes down the organization's systems, typically by encrypting the machines with malware. This attack style strikes quickly and often causes the organization to experience a business interruption, which remains the most costly complication from an attack, where organizations averaged nineteen days of downtime in the third quarter of 2020, which rose 19% from the second quarter of 2020.⁴ Ryuk ransomware is an example of a variant that is commonly used in this attack style.

An organization often engages with such threat actor group to compare its cost of downtime (loss of profits, overhead costs, etc.) to the cost of a ransom payment, in order to get its systems back up and running. The organization is hopefully able to restore

its systems from backups, but it can be costly and time consuming to do so. Thus, organizations may opt to pay the ransom demand to get the affected systems back up and running as quickly as possible.

In terms of the potential legal obligations arising from a system interruption ransomware attack, while there is system access, there is often no data access, acquisition, or exfiltration and, as such, the impacted organization may not have breach notification obligations.

2. Backup Data Encryption

Another style of attack involves a threat actor similarly accessing an organization's computer network, but where the threat actor further corrupts the organization's backup data. The Dharma ransomware variant is commonly used in this attack style.

If an organization is unable to recover from backup data, it may negotiate with the threat actor group for the decryption tool or it may risk never having the ability to recover its data. For many organizations, it can be incredibly difficult to conduct business without complete data. In some circumstances, such as a healthcare provider's loss of historical patient data, it can even be dangerous if an organization cannot recover encrypted data. As such, in situations where backup data has been encrypted, organizations may feel that there is no choice but to pay to receive the decryption tool to recover the data on the affected systems.

If data cannot be recovered, an organization may have an obligation to provide notice to individuals and/or regulators. For example, notification obligations may exist if a healthcare provider's ability to safely care for its patients or a law firm's ability to represent its clients has been impacted. Moreover, threat

¹ 2020 Data Breach Investigations Report, Verizon, available at <https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf>. The top six incident threat varieties consisted of (1) DoS (Hacking), (2) Phishing (Social), (3) Loss (Error), (4) Other, (5) DoS (Malware), and (6) Ransomware (Malware).

² August 2020 Global Threat Landscape Report: A Semiannual Report by FortiGuard Labs, Fortinet, available at <https://www.fortinet.com/resources-campaign/quarterly-threat-landscape-report/quarterly-threat-landscape-report-2>.

³ Ransomware Demands continue to rise as Data Exfiltration becomes common, and Maze subdues, Coveware (Nov. 9, 2020), <https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report#dataExfil>.

⁴ *Id.*

CONTINUED ON PAGE 10 ▶

actors utilizing this type of attack often browse systems and files in an attempt to locate sensitive data and backups and such data access can lead to notification obligations.

3. Data Exfiltration

A third attack style similarly involves a threat actor accessing an organization's computer network and encrypting data (possibly including backup data), but adds exfiltrating data from the organization's computer network. Threat actors utilizing this attack method commonly extort victims by claiming that they will publish the data online (often on public shaming websites) and/or sell it on the dark web. Over the past year, there has been a significant increase in the number of ransomware attacks accompanied by data exfiltration, with ransomware variants such as Lockbit, Sodinokibi, and Maze utilizing this technique.

Impacted organizations may choose to engage a threat actor in these situations, even if data was not encrypted or it has adequate backups, because they want to assess what data the threat actor claims to have taken from its computer network and to see what the threat actor intends to do with such data (e.g., sell or publish it). An organization can experience severe reputational damage when its data, or its customers' data, is published on the Internet.

In terms of potential legal obligations arising from the data exfiltration ransomware attack style, if personally identifiable information, protected health information, or other types of sensitive data was acquired, the impacted organization may have notification obligations.

Ransomware Developments in 2020

While ransomware attacks over the past ten years have focused on attack styles one (system interruption) and two (backup data

encryption) above, threat actors' attack methods have shifted in the past year to attack method three (data exfiltration), where a higher number of recent ransomware attacks have involved the exfiltration of data in addition to encryption. Ransomware negotiator and first recovery responder Coveware recently reported that in the third quarter of 2020 nearly "50% of ransomware cases [it worked on] included the threat to release exfiltrated data along with encrypted data[.]" where exfiltration doubled from the second to third quarter of 2020.⁵ Additionally, the average ransomware payment rose to \$233,817 in the third quarter of 2020, "up 31% from" the second quarter of 2020.⁶

While the threat actors who launched the Sodinokibi ransomware variant in 2019 were not known to exfiltrate data, there was a shift in 2020 where there was a significant uptick in data exfiltration in those cases. We also saw this trend with Maze ransomware.

As with most successful business models, in the context of ransomware attacks, a cost-benefit analysis is typically performed, where a threat actor will often assess the cost of exfiltrating data compared to the benefit of doing so. In terms of the cost, exfiltrating data takes time and effort to first find sensitive data and then exfiltrate it undetected. The benefit of exfiltrating data is that it can lead to a larger ransom demand and payment. Take, for example, the difference between two industry sectors: hospitals and law firms. If a threat actor accessed a hospital's computer network, it may be easy to quickly assess what files contain patients' protected health information. Compare this to a law firm, where it may take much more time and effort to assess whether a law firm even has files containing individual clients' personally identifiable information, let alone where such information resides on the computer network.

As threat actor groups continue to learn about their victims and their computer networks over the course of their attacks, given the typical higher payout from the data exfiltration ransomware attack style, it is expected that data exfiltration will continue to rise in 2021 ransomware attacks.

Takeaways

While ransomware attacks will continue in 2021, there are steps that organizations can take to mitigate the attack itself and the potential damage from a successful attack. As Coveware pointed out in its third quarter of 2020 report, RDP compromises remain the highest vector of attack in its observed ransomware cases.⁷ Then comes email phishing and other software vulnerabilities as the next highest forms of ransomware attack vectors.⁸ Again, the cost-benefit analysis weighs into the attack vector, where compromised RDP credentials are trending as the most cost-effective way to compromise a computer network in ransomware cases. Frequent password resets, the implementation of multi-factor authentication across network systems, and the installation of software updates are all simple ways for organizations to combat ransomware attacks.

Apart from preventing a ransomware attack, organizations can take other steps to mitigate against potential damage from a successful attack. Organizations should have full offsite backups of data, as well as a segmented network, to the extent possible, with limited use of RDP, where such access should be monitored. Organizations should further audit active directory and audit logs to assess for unauthorized activity, and limit administrative privileges across the network. Additionally, organizations should prepare and maintain incident response and business continuity plans, including plans that address ransomware preparedness.

5 *Id.*

6 *Id.*

7 *Id.*

8 *Id.*



Alexa, Forget That: Addressing Privacy Concerns Associated with Artificial Intelligence

Mark A. Petry
Shareholder
Washington, D.C.



Stephen D. Fisher
Shareholder
Seattle



Gabriella Mas Bell
Associate
Atlanta



From AI-powered advertising, marketing, and customer support solutions to smart home devices and autonomous vehicles, technologies incorporating Artificial Intelligence (“AI”) are becoming increasingly pervasive in the modern era. AI technologies enable novel business models, products, and services. These technologies also create incredible opportunities, including enhanced efficiency, decision-making, and data analysis that was previously impractical.

AI technologies rely on various mathematical algorithms and models that are “trained” to make decisions and/or predictions using data sets. In order to operate effectively and reliably, the mathematical models that power these AI technologies require tremendous amounts of data, much of which is actually or potentially personally identifiable and subject to one or more privacy laws. Consumer-facing solutions and devices that incorporate AI often (almost always) include mechanisms to collect,

train, and re-train using data, creating several legal and ethical concerns in the process. This article is intended to help legal counsel identify and mitigate these risks.

The Basics

To effectively mitigate risks associated with AI, attorneys need a basic understanding of what AI is and how it works. At its core, AI relies on correlations and probabilities. AI algorithms and models are selected and designed by data scientists for a particular use case, and data is collected and input to initially “train” those AI algorithms and models to make decisions or predictions. Once the algorithm is trained, additional data sets can be used to further train and refine it. The data scientist, the human element, typically acts as a check to refine and validate the AI technologies’ recommendations, decisions or predictions, as applicable.

There are many types of AI with differing levels of human intervention. The more sophisticated the algorithm, the less human interaction is required to train the AI and the lower the mitigating factor. Two general types of AI are machine learning and deep learning. Once data is fed into a machine learning (or “white box”) system, a human can review the AI’s individual decisions. In contrast, deep learning systems typically function as a “black box,” learning from information input over time and making it difficult to correlate specific data sets with specific results.

Key Privacy Issues

AI technologies inherently raise a number of privacy and other legal concerns. These concerns should be considered and addressed at one of three junctures:

- 1. When data is first collected from the source (e.g., the individual consumer).** Companies should consider whether and how the applicable data is regulated, and (if necessary) obtain informed consents or provide a privacy policy governing its rights

and responsibilities relating to the storage and use of such data.

- 2. When the data is provided to a third-party AI technology vendor.** The company and AI vendor should clearly articulate how and when the data may be used and retained. Usually, AI vendors need the data in a granular form, but sometimes data can be provided and used in a de-identified, anonymized, and/or aggregated form. Similarly, while some AI vendors only need the data during the term or for another finite period (to learn from once and delete or return thereafter), other vendors will need to retain some right to use any data to facilitate training and re-training of the algorithms. When a perpetual right to use data is needed for the vendor to train its system, consider the form of data that may be retained (e.g., aggregated and de-identified in such a way that it cannot be used to identify any individual in the future) and the duration of such retention. Finally, because AI applications themselves may not be capable of negligence (fault), the parties should discuss indemnification provisions to address the results of the AI’s conduct, such as misuse of company data, biased results arising from the AI app, faults in the data set provided by the company, misuse of the AI technology by the company, and any related fines or penalties.

- 3. When implementing decisions and activities derived from the AI.** The company or user relying on the AI needs to carefully consider the nature and impact of the AI technology’s decisions and whether disclaimers or procedures to request or require human review are necessary or appropriate. When AI technologies are used for health and safety (such as health care or driving), human oversight is typically imperative so that the AI is not relied upon too heavily. For example, AI might be used to help support a medical decision or identify potentially

CONTINUED ON PAGE 12 ▶

adverse reactions between prescriptions. However, medical professionals should actively engage with the AI, which is not a substitute for professional medical advice, given the consequences of a potential mistake (and health care laws and regulations). Similarly, AI systems in vehicles may identify potential hazards on the road but are not typically a substitute for an attentive human driver (although that is starting to change). In contrast, it may be appropriate for an AI natural language processing tool to expeditiously answer frequently asked questions for noncritical products and services, provided that consumers may have the ability to ask for a live agent if those AI generated responses are not helpful.

For consumer-facing AI technologies, the following should also be considered:

- **Consumer Right to Meaningful Information and Explanation for AI Decisions**

As a general rule, it is best to inform consumers when AI is used to make or support decisions and provide procedures for how consumers may request a further review or information on the decision. The law is not well established on this given that AI is relatively new, but we expect laws and regulations to further mature on this topic over time. Currently in Europe, Article 22 of the General Data Protection Regulation requires companies to provide individuals with meaningful information about certain automated decisions. Similarly, the Equal Credit Opportunity Act in the United States requires creditors to provide applicants with specific reasons to support adverse actions.

For companies that leverage machine learning solutions, it is relatively easy to describe to individuals the categories of information that are being evaluated and how that data may lead to a particular

decision. In contrast, the technicalities involved in deep learning systems often make describing these processes difficult. One of the ways to address the foregoing concerns is a field known as Explainable Artificial Intelligence (“XAI”). Given the virtually infinite applicability of AI, it should not be surprising that data scientists have begun leveraging AI to explain AI to humans. XAI is a broad term that generally describes a human’s ability to understand the decisions made by AI algorithms. XAI seeks both global explicability (by focusing on entire decision-making system) and local explicability (by analyzing what factors led an algorithm to make a particular decision). Data scientists are also developing AI models that can be used to approximate the way a black box system made a certain decision. While academia has hypothesized about the type and amount of this information that should be provided to individuals, the issue of how much of this information is legally required to be included in company’s privacy policy remains open.

- **Implicit Bias**

Initially, AI-based technology was promoted as a tool to create a level playing field by objectively and mathematically processing data and sidestepping the prejudices of human decision makers. However, that has proven not to be the case since the data used to “train” AI models are often biased and/or based on historical correlations or probabilities that are further reinforced by the AI technology. For example, a hiring algorithm can focus only on certain relevant factors (like education and experience) while disregarding others that can lead to prejudice or implicit bias in human recruiters (like names or addresses, proxies for gender, race, and economic status). However, because the data used

to train an AI model is frequently derived from historical information, these systems can easily perpetuate historical biases and discriminate against historically marginalized groups.

Major cities around the United States have recently banned government use of certain facial recognition software, which, to date, has been trained using mostly Caucasian faces, thereby producing disproportionate error rates when applied to non-Caucasians. The leading edge in litigation are claims by wrongfully prosecuted individuals against cities for use by their police of flawed facial recognition software. Additionally, some health care AI algorithms have been found to ignore gender and thus generated sub-optimal results and produced mistakes.

When contracting with an AI vendor, companies should consider:

- a. representations and warranties that the AI vendor complies with applicable laws and regulations and has in place a documented process for detecting and addressing bias, including a meaningful appeals process, as appropriate in the particular situation;
- b. requirements for the AI vendor to review, tune and re-train its AI technologies to mitigate bias; and
- c. notice and approval rights over material changes to the AI system and controls during the course of the agreement.

The potential benefits of leveraging AI technologies cannot be overstated. As companies continue to explore ways to harness these benefits, counsel will need to understand the various legal issues that could arise. By understanding the intricacies of AI, counsel can mitigate their clients’ exposure to privacy and other related risks associated with these new technologies.



Data Localization and Data Transfer Restrictions

Liz Harding
Shareholder
Denver



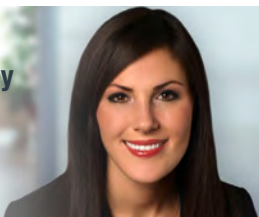
Sal D. Phillips
Associate
Chicago



Lisa J. Acevedo
Shareholder
Chicago



Lindsay R. Dailey
Shareholder
Chicago



In the modern global economy, data is the most valuable resource. Businesses use data to create value for customers and increase profit for its stakeholders. Although these businesses can only maximize their use of the data when it can flow freely across borders, many countries have been enacting measures that would make transferring data more complicated, expensive, time consuming, and at times, illegal.

Data Localization vs. Data Transfer

Data localization laws govern the location where personal data is stored, whereas data transfer laws govern the ability to disclose copies of

personal data outside the borders of a country or region, but do not require local storage. Often, data localization laws incorporate aspects of data transfer laws.

Globally, these rules are not uniform and many countries have adopted their own requirements which can vary based on the types of personal data covered and the scope of their respective requirements. The following are the most commonly seen categories of data localization and data transfer laws:

- 1. Broad Localization Laws:** Cover all categories of personal data and a copy of the data must be stored in country. Cross border transfers are permitted under certain exceptions.
- 2. Specific Localization Laws:** Cover specific categories of personal data and/or certain types of organizations which must comply, and a copy of the data must be stored locally. Cross border transfers are permitted under certain exceptions.
- 3. Combined Localization/Transfer Laws:** Cover specific categories of personal data, and the data must be stored locally unless an exception applies. These types of laws typically do not require storing a copy of the data locally, and cross border transfers are permitted under certain exceptions.
- 4. Pure Data Transfer Laws:** Pure data transfer laws do not require local storage but only permit cross border transfers under certain exceptions.

European Laws

The European Union's ("EU") General Data Protection Regulation, together with (a) the United Kingdom's Data Protection Act 2018 and associated post Brexit implementation laws, and (b) implementing laws of EU member states (collectively, "GDPR"), permit transfers of personal data to locations outside of the European Economic Area ("EEA"), which have not been designated as having 'adequate'

protections for personal data, only in certain circumstances. Below is an overview of the main mechanisms pursuant to which personal data may be lawfully transferred.

- 1. Adequate Safeguards:** In the absence of a transfer to a country deemed to have adequate protections for personal data, a controller or processor may transfer personal data outside of the EEA if adequate safeguards are in place and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. The GDPR lists a number of appropriate safeguards, the most commonly used being:
 - a.** Binding corporate rules – available only for purposes of intercompany transfers;
 - b.** Standard contractual clauses – currently available for controller to controller, and controller to processor, transfers. Draft updated standard contractual clauses are also under review and would also cover processor to controller, and processor to processor, transfers.
 - c.** Approved certification mechanism (such as the recently invalidated EU / US Privacy Shield framework).

The recent Schrems II decision from the European Court of Justice¹ invalidated the Privacy Shield framework, meaning that personal data could no longer be transferred from the EU to the US under that mechanism. In the same judgment, the European Court of Justice confirmed that Standard Contractual Clauses could still be utilized as a method of transfer, but that in certain circumstances additional safeguards over and above those contained within the clauses would be required. This is particularly applicable to transfers of personal data to the United States, where US government surveillance laws such as FISA 702 mean (at least in the consideration of the European Court of Justice) that enforceable rights and effective legal remedies are not available to data subjects. Recent guidance

¹ [https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA\(2020\)652073_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf)

from the European Data Protection Board has provided further clarity as to the type of additional safeguards that may be required, including data minimization, and encryption of personal data in transit and at rest.

2. Derogations for Specific Situations:

In the absence of an adequacy decision, or appropriate safeguards, a transfer of personal data can still take place pursuant to one of a number of derogations, including:

- a. The data subject has explicitly consented to the proposed transfer, after having been informed of the risks of such transfers. It should be noted, however, that there are significant limitations on what is considered valid consent under GDPR, and therefore use of consent for international transfers should be carefully considered in advance.
- b. The transfer is necessary for performance of a contract between the data subject and the controller, or a contract between the controller and a third party where the contract is for the benefit of the data subject.
- c. The transfer is necessary for important reasons of public interest recognized under EU or member state law (note, this is usually only applicable in the case of international data exchanges between government authorities and will rarely apply in the context of transfers for business purposes).
- d. The transfer is necessary for the establishment, exercise, or defense of legal claims.
- e. The transfer is necessary to protect the vital interests of the data subject or

other persons, where the data subject is incapable of giving consent.

It should be noted that transfers undertaken on the basis of derogations should concern a limited number of data subjects only, and may not be repetitive. As a result, reliance on derogations as a mechanism for transfer is appropriate only for occasional transfers and is therefore not a reliable transfer mechanism for most business related transfers (for example, reliance on derogations would not be appropriate for transfers of data to a US based cloud hosting provider, payment processor, or for HR administration purposes).

Laws Outside of the European Union

Below are examples of how various countries outside of the EU have approached data localization and data transfer requirements, and how they fit into the categories of localization/transfer laws described above.

1. Broad Localization Laws:

- Russia requires a copy of the data to be stored on local servers, and cross border transfers are permitted under certain exceptions, such as data subject consent.

2. Specific Localization Laws:

- Japan requires medical care records to be stored within the country.
- China requires certain types of information to be located within mainland China including financial and health or medical information. China's cybersecurity law also requires certain types of organizations to conduct security assessments prior to transferring personal data outside of China.
- Australia requires certain health information to remain inside of the country.

- India requires licensed banks and payment system providers to retain their information locally, and may also be stored additionally outside of India if certain criteria are met.

3. Combined Localization/Transfer Laws:

- British Columbia and Nova Scotia in Canada both require personal information maintained by "public bodies" (e.g., hospitals) to be stored locally unless the explicit consent to transfer such data outside of Canada and be accessed by non-Canadians is obtained from the data subject.

4. Pure Data Transfer Laws:

- Brazil restricts the disclosure of personal data outside of the country unless prior consent is obtained, or another exception applies.
- For private entities, Mexico restricts disclosing personal data outside of the country unless notice is given and consent is obtained, or another exception applies. Note that Mexico also has national security provisions applicable to governmental entities that require local storage of national security and public information within the facilities of the relevant public entities.

Conclusions

With the growth of international enterprises, and the ever increasing digital economy, organizations should carefully consider the application of data localization and data transfer laws to their operations and those of their customers. Consideration of these issues as part of product or service development can save time and money and avoid unanticipated legal risk.

The Newly Released Chinese Privacy & Security Laws

Jeffrey E. Fine
Shareholder
St. Louis



L. Hannah Ji
Associate
St. Louis



With the change in presidential administrations, many corporate leaders are optimistic that the climate for conducting business in China will improve. It remains to be seen what position the Biden administration will take in regards to tariffs and other trade matters. Technology companies that already have made inroads or are looking to expand into China should be aware of recent developments in Chinese privacy and data security laws.

The past three years have seen enormous development in China's data protection policies. In 2017, the People's Congress enacted the Cybersecurity Law of the People's Republic of China (for a deeper dive into the contours of this framework, please review our previous article [here](#)). Now three years later, China has released proposed revisions to these policies in the form of two new statutes: the Data Security Law of the People's Republic of China ("DSL") and the Personal Information Protection Law ("PIPL").¹ If these proposed laws are enacted as expected, they will signal a large shift in China's approach to information governance and magnify the compliance obligations of companies that do business there. While these new laws will amend a number of China's existing regulations, we project that three of these changes will have the biggest impact on our clients.

Chinese Privacy & Data Security Laws will have Extraterritorial Effects

Under China's current regulatory regime, with very few exceptions, national data privacy laws

have little direct impact on organizations that operate outside of the country (i.e., have no physical presence within the nation's territory). However, under the DSL and the PIPL, Chinese regulators will be empowered by new laws with specific extraterritorial application to organizations processing data outside of China's territory under the circumstances described below.

Significantly, the DSL expressly stipulates that organizations located outside of the territory of mainland China can be held liable for any data activities that harm China's "national and public interest" or the interests of Chinese "residents and organizations." It is not yet clear how broadly the country will view these "interests," but there are already concerns that China is signaling its intent to aggressively police data moving through its territory regardless of the source. Similarly, the PIPL regulates all data activities occurring in China's territory and those occurring outside of China when the data processing:

1. provides products or services to customers in China; and
2. analyzes or evaluates the behaviors of individuals located in China.

In other words, China intends to regulate the data of any company performing marketing, transacting business or performing data analysis in China.

New Types of Data will be Regulated with Some Subject to Heightened Scrutiny

Read together, the two proposed laws will expand the types of data regulated by Chinese authorities to include types that are not currently regulated. At the same time, it will add stricter scrutiny to data elements protected by the current legal regime in China.

The current 2017 Cybersecurity Law applies to "personal information," which includes most information about a specific individual. The DSL goes beyond "personal information" and regulates "any record of information in electronic or non-electronic form," as well as any "important data," which could include both de-identified and aggregated information. "Important data" are defined as

data that have the potential of causing harm to "China's national security, the public interest, or the lawful rights and interests of citizens or organizations." As a result, the DSL may apply to almost any type of data a company is using, as well as any metadata associated with it. Organizations collecting data (or storing, processing, using, providing, trading or disclosing data) will be obligated to establish data security policies, conduct employee training, maintain appropriate organizational and technical measures, and report breaches to users and applicable regulators.

The PIPL also takes a step forward in regulating the use of "personal data" and will require organizations to find a specific lawful basis prior to processing personal information. As we have seen in the General Data Protection Regulation ("EU GDPR"), finding a valid legal basis for each and every aspect of data processing can be a complicated and time-consuming process for a company, and expectations are no different for China's proposed system. Additionally, the PIPL introduces a new concept termed "sensitive personal information," which does not exist in the current law. Sensitive Personal Information is defined as "information that once leaked or abused may cause damage to personal reputation or seriously endanger personal and property safety, and includes race, nationality, religion, biometric information, health, financial account, personal whereabouts and other information." An organization is prohibited from processing Sensitive Personal Information unless it has a specific purpose and sufficient necessity to process such data and must obtain separate consent from the data subjects for each piece of data. Further, the organization must also inform the data subject of the necessity of processing sensitive personal data and the impact on the data subject. Depending on how broadly officials interpret this provision, many data elements gathered in China may be subject to these enhanced requirements.

Organizations have Increased Reporting Obligations Under the Proposed Laws

Under the DSL, organizations handling data that may cause harm to "China's national

¹ The draft of DSL was released on July 3, 2020 and its public consultation period was closed on August 16, 2020. Currently, it is waiting for passage. The draft of PIPL was released on October 21, 2020, and its public consultation period was closed on November 19, 2020. The PIPL is currently awaiting its passage as well.

CONTINUED ON PAGE 16 ▶

security, the public interest, or the lawful rights and interests of citizens or organizations” (defined as “important data”) will be required to conduct periodic security risk assessments and submit reports to Chinese regulators. Due to the nature of these assessments, organizations deemed as handling “important data” might be forced to expose confidential and proprietary information (e.g., details of corporate security measures, contents of contracts with other organizations relating to the data, any proprietary algorithms applied to the data, etc.) to the scrutiny of Chinese officials. The proposed law provides that the security risk assessment report must at least include:

1. the categories and quantities of “important data” controlled by the organization;
2. how “important data” is collected, stored, processed and used;

3. the security risks the organization faces; and
4. details of the mitigation measures it has taken.

Similarly, the PIPL contains increased reporting requirements for certain data activities perceived by Chinese regulators as posing higher risks to Chinese individuals or national security. Organizations identified as Critical Information Infrastructures Operators² (“CIIO”) that need to transfer data across borders will be required to pass strict security assessments conducted by the Chinese regulators. Unlike the DSL, China has not yet made clear what this group of assessments could entail, but most assume they will be no less involved than those required under the other law.

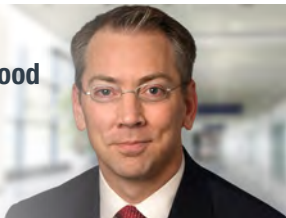
² CIIO is defined as a company in public communication and information services, power, traffic, water resources, finance, public service, e-government, and other critical information infrastructure which—if destroyed, suffering a loss of function, or experiencing leakage of data—might seriously endanger national security, national welfare, the people’s livelihood, or the public interest.

As businesses worldwide recover from the pandemic and strive to return to normalcy, the size and scope of markets in China present enticing opportunities for entrepreneurs large and small. The new privacy and security rules will need to be taken into account as business owners evaluate the risks and rewards of doing business in China. Due to the proposed legislations’ extraterritorial reach, its broad coverage and added scrutiny, and increased reporting obligations, the compliance costs for overseas organizations to operate under the new framework will likely increase. Given China’s desirability as a market and a source of data, many businesses will likely determine that the gain is worth the risk. Any such organizations would do well to start preparing now to shore up compliance programs and make early efforts at mitigating the impact of these new requirements on its business.

TECHNOLOGY: SOCIAL MEDIA & PLATFORMS

Preparing for Reform to Section 230 of the Communications Decency Act

Spencer R. Wood
Shareholder
Chicago



Kelsey L. Brandes
Associate
Kansas City



Ephraim T. Hintz
Associate
Denver



Jean Marie R. Pechette
Shareholder
Chicago



Section 230 of the Communications Decency Act (“CDA”) (47 U.S.C. §230) broadly immunizes online platform providers from liability for what third-party users post or upload to such platforms and gives platform providers certain rights to moderate such user content without being deemed a content creator. Section 230 has come under intense

scrutiny from politicians on both sides of the aisle, but for different reasons. The push for Section 230 reform is highly unlikely to subside in 2021, especially after several social media platforms suspended President Donald Trump’s accounts in the wake of an attack on the U.S. Capitol Building on January 6. With potential changes looming, we provide guidance on what to expect.

What Is Section 230?

The push for Section 230 reform centers on two key provisions. Section 230(c)(1) states:

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

This provision essentially immunizes platform providers from liability for carrying content that third-party users upload or post to the platform. (Note: There are certain exceptions for which Section 230 does not provide protection. See 47 U.S.C. § 230(e).)

Section 230(c)(2) states, in relevant part:

No provider or user of an interactive computer service shall be held liable on account of – (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd,

CONTINUED ON PAGE 17 ▶

lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected ...

This provision protects platform providers from liability for certain actions taken to moderate third-party content.

Section 230 Is Now a Political Battleground

In recent years, Section 230 has been criticized by both Democrats and Republicans. In general, Democrats have urged social media giants (e.g., Facebook and Twitter) to increase moderating to prevent the publishing of content that is factually inaccurate or contains wrongful speech. In contrast, Republicans argue that social media companies should use a more judicious approach when choosing what content to moderate. Republicans contend that since many interactive websites only censor conservative speech, these websites should not be granted immunity under Section 230 because their censoring tactics violate the spirit of the law.

Twitter's recently adopted moderating practice of flagging visible tweets with a warning label that suggests the posted tweet is either "misleading," "contains disputed information," or "is an unverified claim" is an example of platform provider action that has spawned debate. Democratic Senators (such as Senator Dianne Feinstein) argue that Twitter's labeling practice fails to prevent the anticipated harm because users can still view the labeled tweet. Whereas, Republican Senator John Kennedy claims that Twitter is not eligible for Section 230's protection because it is no longer acting as only a host of the content but is now curating and modifying users' content.

Adding fuel to an already scorching debate, President Trump recently vetoed the annual National Defense Authorization Act, a bill that allocates military funds each year, because it did not include the President's requested language terminating Section 230. With overwhelming majorities in both houses, Congress voted to override the veto on January 1 leaving any reform of Section 230 to be addressed in the future. Less than a week later, major U.S. social media platforms suspended President Trump's ability to post content, asserting concerns that his posts incited violence in violation of the platforms' terms of service. This action has fueled further debates on whether the platforms' suspension should be immune under Section 230. Critics

have asserted that these platforms have engaged in improper censorship that should not be protected under Section 230. With this backdrop, Section 230 is assured to remain at the center of political battle in 2021.

Proposed Reform to Section 230

There are currently numerous formal and informal proposals to reform Section 230 coming from across the political spectrum. For example:

- In May 2019, in a letter to Congress, a bipartisan group of forty-seven (47) state attorneys general urged Congress to amend Section 230 to make clear it does not prohibit the enforcement of state or territorial criminal law. This amendment would shrink Section 230's immunity shield and expand the number of criminal actions that could be brought against an interactive online website.
- In May 2020, President Trump issued an executive order instructing the Commerce Department to request that the Federal Communications Commission (FCC) initiate rulemaking procedures to narrow Section 230's protections, including clarifying what constitutes "good faith" moderation practices, clarifying what type of content can be removed and whether amplification of content qualifies for protection, and requiring greater transparency and procedures for content moderation.
- In June 2020, Senator Brian Schatz of Hawaii (D) and Senator John Thune of South Dakota (R) introduced the Procedural Accountability and Consumer Transparency Act ("PACT Act"). The PACT Act's main objectives are to increase transparency and consistency of content moderation and decrease unlawful content on web platforms. Under the PACT Act, hosts of interactive websites would be required to produce quarterly "transparency reports" concerning moderation decisions. In addition, the PACT Act would create a "notice and takedown" regime in which companies would have to remove content deemed unlawful, by a court order, within twenty-four (24) hours.
- In September 2020, the Department of Justice issued a proposed revision to Section 230 that would create an exception for platforms that purposefully facilitate third-party content that violates federal law, remove Section 230's immunity shield

in cases brought by the Federal Trade Commission or the Department of Justice, and require "sunsetting" Section 230 protection after a period of time.

With many reform proposals surrounding it and disfavor from both political parties, Section 230's future remains uncertain. Scholars disagree as to what reform of Section 230 is likely. Jeff Kosseff, assistant professor of cybersecurity law in the U.S. Naval Academy's Cyber Science Department and author of *The Twenty-Six Words That Created the Internet* believes that the most likely outcome is a total repeal of Section 230 due to a lack of consensus over how to reform it. Others, like Mary Anne Franks, professor at the University of Miami School of Law and author of *The Cult of the Constitution: Our Deadly Devotion to Guns and Free Speech*, believe that reform will not be as radical as a repeal and will likely come as an ineffective and complicated bill.

Preparing for Uncertainty

With the change in presidential administrations, President Trump's Executive Order likely will be revoked, and past positions taken by the DOJ are likely to undergo change. Also, outgoing FCC Chairman Ajit Pai recently stated he will not act on President Trump's request for rulemaking to narrow Section 230's protections. However, given the events of early January, there is even greater focus on Section 230 and renewed calls from both parties for reform. The need for bipartisan support may limit the reach of any legislative solution. Whether a compromise can be reached in Congress or challenges continue to be mounted in the courts, it seems inevitable that there will be some reform of Section 230. Here are some proactive steps that can be taken to prepare.

- **Provide Transparency.** Multiple groups have advocated for greater transparency around content moderation practices and procedures. Calls for transparency range from setting forth a notice requirement and procedure for appeal when user content is to be removed or flagged, to establishing periodic reporting requirements that obligate platform providers to disclose what has been removed and why. Thus, Section 230 reform may well include transparency requirements. Adopting practices that provide for such transparency now may make any new requirements easier to implement in the future. There may be less need to adopt transparency policies and procedures

for content that clearly falls within the enumerated categories of Section 230(c)(2) (i.e., content that is clearly obscene, lewd, lascivious, filthy, excessively violent, or harassing). Removing or flagging content that is not obviously within one of those categories or falls within the Section 230(c)(2) category of “otherwise objectionable” has given rise to controversy, and these may be areas where greater transparency should be considered. Responding to a complainant within a reasonable time frame, notifying the user who posted the potentially violating content, and providing users with a meaningful method of appeal provides greater transparency in content moderation. What constitutes a “meaningful method of appeal” will vary, but standards to consider are: using human review as opposed to software review; using reviewers who were not involved in the original removal to review the appeal; providing the creator with a chance to present further information; and providing examples of appropriate content versus inappropriate content. If a user requests information about why a post was removed or an account suspended, provide them with the reason for removal or suspension. Consider providing such information at the time of removal or suspension before the user requests such information. Under the proposed PACT Act, platforms would be required to explain why content was removed to both the user who posted the content as well as the complainant. While the PACT Act would not require notification and explanation of account suspension, best practices include providing such information within a reasonable time to the user whose account was suspended.

- **Use Good-faith Moderation Practices.** Section 230(c)(2) requires that platform providers act in good faith when moderating third-party content. There is not much guidance in the case law as to what constitutes good faith. However, one


court found that a plaintiff’s complaint could survive a motion to dismiss where the plaintiff alleged that the platform provider did not act in good faith when it removed the plaintiff’s videos and terminated the plaintiff’s account. In that case, the plaintiff alleged that defendants (i) allowed videos to remain on the platform for years before being removed, (ii) refused to assist the plaintiff in complying with the platform’s terms of use, (iii) refused to provide an explanation for content removal and account termination, (iv) removed content that was deemed not to be advertiser friendly to increase their profits, and (v) took into consideration videos that the plaintiff already had voluntarily deleted when deciding to terminate the plaintiff’s account. Because Section 230 is an affirmative defense, the platform provider needs to establish its applicability. Accordingly, demonstrating good faith may, in many ways, resemble the steps noted above for providing transparency. In addition, establishing clear community guidelines and following objective procedures for removing or flagging content will be helpful to platform providers seeking to establish that actions were taken in good faith. When identifying content to be removed or flagged or when ranking content for amplifying or de-emphasizing its prominence, platform providers should be able to demonstrate that improper bias did not impact such decisions – whether made by an individual or through the use of algorithms.

- **Adhere to Terms of Service.** If Section 230 were to be repealed, some argue that the First Amendment also protects the right of platform providers to moderate third-party user content, on a theory that the government cannot force a private company to publish speech that it does not want to publish. Platform providers can protect their right to moderate user content by having clear, enforceable terms

of service that forbid certain speech, include the ability to remove user content that violates those terms, and reserve the right for the platform provider to amplify or de-emphasize certain content. Platform providers need to ensure that they comply with such terms of service to avoid a breach of contract or promissory estoppel claim, which would not be shielded by Section 230.

- **Avoid Becoming a Content Creator.** If a platform creates or develops the content at issue, Section 230 may not provide protection. This can occur when the platform provider develops or materially alters content, as well as in less obvious circumstances. For example, in *Anthony v. Yahoo! Inc.*, the court found that Yahoo was acting as an information content provider when it created and sent false dating profiles to users and sent users profiles of previous users who had deleted their accounts. Thus, Yahoo! was not afforded Section 230 protections. In another case, Section 230 did not apply when a website included a drop-down menu that allowed users to select from a list of pre-populated options when looking for a roommate.

In light of the significant political attention that Section 230 has received, it is reasonable to assume that some type of reform is likely. If you are proactively implementing any of the above steps in anticipation of reform, we recommend you consult with one of our attorneys for a review of platform features and functions, terms of service, community guidelines and moderation policies and procedures. If and once Section 230 is revised (or repealed and replaced with an alternative scheme), your Polsinelli attorney can advise you on the new legal requirements and their impact on your business. Polsinelli will continue to monitor developments in this area and will provide updates on any substantial changes.



words have power

The Digital Millennium Copyright Act – Trends in Content Moderation

Leslie F. Spasser
Shareholder
Atlanta



Alexander D. Boyd
Associate
Kansas City



Websites and online service providers play a vital role in the dissemination and storage of third-party-generated content. While much of the recent political scrutiny has focused on the speech-based protections provided by Section 230 of the Communications Decency Act, another federal law that provides broad protections to online service providers that publish and distribute content is also receiving attention – the Digital Millennium Copyright Act (“DMCA”).

Congress passed the DMCA in 1998 to establish protections for online service providers in certain situations if their users uploaded or transmitted materials that violated another party’s copyright. If a service provider met the strict requirements of the DMCA, the service provider would enjoy a “safe harbor” from liability for copyright infringement claims asserted because one of their users stored or transmitted infringing material on or through the provider’s platform. By establishing these procedural requirements, the DMCA relieved the service provider from the burden of determining whether the content was infringing and from assuming the risk of liability if its determination was incorrect.

In order to receive the DMCA’s protections, service providers must comply with several procedural and administrative requirements, including the following:

- Designate an agent with the U.S. Copyright Office;
- Designate an agent on the service provider’s website or platform;

- Comply with takedown request and counter-notification procedures;
- Implement policies to terminate repeat infringers; and
- Accommodate and not interfere with standard technical measures used to identify or protect copyrighted works.

Recent court decisions and jury verdicts have emphasized the need for service providers to strictly adhere to the DMCA’s procedural requirements to benefit from safe harbor protection. Decisions issued by the U.S. District Court for the Eastern District of Virginia and the Court of Appeals for the Fourth Circuit ruled that an internet service provider may not be entitled to the DMCA safe harbor if the service provider does not adopt and enforce a repeat infringer policy. Similarly, a pending class action against YouTube in the U.S. District Court for the Northern District of California alleges that YouTube did not reasonably implement a repeat infringer policy and did not provide all copyright owners with adequate takedown processes. The consequences of determining that a service provider did not comply with the DMCA procedures can be significant. If a service provider fails to qualify for a safe harbor, the statutory damages arising from a contributory or vicarious copyright infringement claim can quickly add up to substantial amounts.

In addition to activity in the courts, Congress has indicated an interest in copyright issues, including the DMCA. Congress recently amended the U.S. Copyright Act as a part of the December 27, 2020, COVID-19 relief and government funding bill. The amendments included permitting felony charges for the live streaming of copyrighted works (bringing the charges in line with existing criminal penalties for the reproduction and distribution of copyrighted works) and creating a Copyright Claims Board that can resolve small claims of copyright infringement. While those revisions did not directly modify the DMCA, they appear to have opened the door for more amendments to U.S. copyright law, including the DMCA.

To this end, on December 22, 2020, Senator Thom Tillis (R) introduced a discussion draft of legislation to reform the DMCA – the Digital Copyright Act of 2021. The law is still in draft

form, with comments solicited until March 5, 2021. Based on the proposed changes, online service providers should monitor the draft bill closely. The proposed bill includes the following categories of revisions to the DMCA:

- Prohibits service providers from taking advantage of the safe harbor if they are willfully blind to infringement or are aware of facts or circumstances indicating infringing activity is likely;
- Requires the Copyright Office to establish best practices that service providers must take to combat online piracy in order to be eligible for the liability safe harbors;
- Authorizes the Copyright Office to develop and maintain a model repeat infringer policy to serve as the minimum baseline standard for service providers;
- Makes it easier for copyright owners to submit takedown requests when it may be difficult to identify the specific location of the infringing material;
- Requires service providers to make available on their website a standardized form copyright owners can use to submit takedown requests;
- Uses the Copyright Claims Board established in the COVID-19 relief bill to resolve certain disputes between copyright owners and counter-notice senders; and
- Requires service providers to take steps to ensure that additional copies of infringing work are not re-posted after a takedown request is processed (unless a valid counter-notification is received).

Whether the DMCA continues as currently written or is reformed, online service providers should review their policies and procedures as well as their enforcement of the same to ensure they are taking the steps necessary to enjoy the benefit of the DMCA’s safe harbors. As the scrutiny on technology companies and online platforms continues to increase, online service providers must be prepared to demonstrate that their policies comply with the DMCA’s requirements and, as importantly, that their implementation of their policies and procedures supports that compliance.

ABOUT OUR TECHNOLOGY TRANSACTIONS & DATA PRIVACY PRACTICE

Polsinelli's Technology Transaction and Data Privacy team is comprised of over 40 lawyers with significant experience in the technology, privacy and security industries.

We work with companies of all sizes and at all stages of development to provide strategic guidance as they create, acquire, use and commercialize technology. Our clients include businesses with domestic and international operations as well as governments, universities, hospitals, financial services institutions, startups and nonprofit organizations.

The Polsinelli team provides industry-leading data privacy counseling, incident response and breach litigation legal services. Our lawyers include former in-house data privacy attorneys, alumni of law enforcement agencies, attorneys with international backgrounds and some of the most experienced incident response lawyers in the country.

Contact one of our team members today to learn how we can help you and your organization with its technology and data privacy needs.

Stay Connected

Polsinelli frequently writes about topics related to these materials. Click [here](#) to subscribe to receive news and webinar updates.

Editorial Board

Gregory M. Kratofil, Jr.
Practice Chair
gkratofil@polsinelli.com

Lisa Acevedo
lacedo@polsinelli.com

Kathryn T. Allen
kallen@polsinelli.com

Gregory L. Cohen
gcohen@polsinelli.com

Lindsay R. Dailey
ldailey@polsinelli.com

Jeffrey E. Fine
jfine@polsinelli.com

Stephen D. Fisher
sfisher@polsinelli.com

Liz Harding
eharding@polsinelli.com

Jean Marie R. Pechette
jpechette@polsinelli.com

Iliana L. Peters
ipeters@polsinelli.com

Mark A. Petry
mpetry@polsinelli.com

Bruce A. Radke
bradke@polsinelli.com

Leslie F. Spasser
lspasser@polsinelli.com

Pasha A. Sternberg
psternberg@polsinelli.com

Michael J. Waters
mwaters@polsinelli.com

Spencer R. Wood
swood@polsinelli.com

Gabriella Mas Bell
gbell@polsinelli.com

Kelsey L. Brandes
kbrandes@polsinelli.com

Alexander D. Boyd
aboyd@polsinelli.com

Reece Clark
rclark@polsinelli.com

Ephraim T. Hintz
ehintz@polsinelli.com

L. Hannah Ji
hji@polsinelli.com

Hale H. Melnick
hmelnick@polsinelli.com

Jessica L. Peel
jpeel@polsinelli.com

Jane E. Petoskey
jpetoskey@polsinelli.com

Kayleigh S. Shuler
kshuler@polsinelli.com

Caitlin A. Smith
casmith@polsinelli.com

Sal D. Phillips
sphillips@polsinelli.com

Polsinelli is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements. Copyright © 2021 Polsinelli PC, Polsinelli LLP in California | All Rights Reserved