TECH TRANSACTIONS & DATA PRIVACY

2022 REPORT

While we were hopeful at the beginning of 2021 that the worst of the 2020 global pandemic was behind us, this did not prove to be the case. The changes in our working environments, education, shopping and so many more areas of our lives were transformed in 2020. As we predicted, that evolution continued throughout 2021.

As Polsinelli's Technology Transactions and Data Privacy Group looks forward to 2022, our industry continues to see explosive growth in technology transactions, data privacy counseling and incident response areas. The increased value and focus on data assets, content distribution, privacy and machine learning will accelerate this year. We anticipate 2022 will have changes in the cyber security insurance market, fallout from last year's exponential growth in ransomware incidents and increased regulatory and contractual attention on vendor management and data security issues.

We are again hopeful that this coming year is when COVID-19 will move to "the rearview mirror," but the importance, sophistication and prominence of technology, privacy and security issues will continue in 2022.

The articles contained in this report highlight the forward-thinking advice and counsel our attorneys provide our clients throughout the year. We remain excited for the future and our continued role in shaping it.

Sincerely,

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

Table of Contents

Top 5 Privacy Issues for 2022

2022 is gearing up to be another pivotal year for data privacy. Organizations, both large and small, will have to prepare for newly enacted laws and regulations and increased regulatory enforcement. A flurry of domestic and international regulatory action is expected in 2022, so we have highlighted five significant key areas of focus.

1. Comprehensive State Privacy Laws

When it comes to U.S. state privacy laws, considerable preparation will be needed in 2022 in order to comply with the laws that come into effect in 2023. On January 1, 2023, the California Privacy Rights Act of 2020 (CPRA) and the Virginia Consumer Data Protection Act (VCDPA) come into effect, closely followed by the Colorado Privacy Act (CPA) which comes into effect on July 1, 2023. We've outlined each of these state's newly enacted laws below to help you identify whether these laws will apply to your business.

California

The CPRA amends the California Consumer Privacy Act of 2018 (CCPA) and will apply to for-profit "businesses" that collect personal information from California residents, do business in the state of California and either (1) had $25 million or more in annual revenue during the prior calendar year; (2) buy, "sell" or "share" the personal information of 100,000 or more consumers or households; or (3) earn at least half of its annual revenue by "selling" or "sharing" consumers' personal information. Importantly, the CPRA expands the definition of covered businesses, whereas the CCPA limited the scope of covered businesses by only applying to businesses that share personal information "for commercial purposes." The CPRA has removed the "commercial purposes" qualifier and will now apply to businesses that merely share personal information of 100,000 or more consumers or earn at least half of their annual revenue by sharing consumers' personal information.

Virginia

The VCDPA will apply to organizations that conduct business in Virginia or produce products or services that are targeted to residents of Virginia and that (i) during a calendar year, control or process personal data of at least 100,000 consumers or (ii) control or process personal data of at least 25,000 consumers **and** derive over 50 percent of gross revenue from the sale of personal data.

Colorado

The CPA will apply to organizations that do business in Colorado and either (i) process or control the personal data of 100,000 or more Colorado residents or households in a calendar year, or (ii) derive revenue or discounts from the sale of personal data and process or control the personal data of 25,000 or more Colorado residents or households.

All three states include varying exemptions in their privacy laws, for example excluding non-profit organizations from their remit, and excluding certain data covered by federal laws such as HIPAA and GLBA. Once an organization identifies whether it is subject to these laws, it will need to implement various operational mechanisms to comply with such laws, including responding to data subject requests, conducting privacy risk assessments and analyzing the transfer of personal data to third parties.

2. Artificial Intelligence

Recent actions of the European Data Protection Board (EDPB) and the Federal Trade Commission (FTC) indicate that the privacy aspects of AI and machine learning will be under increasing focus in 2022.

In June 2021, the EDPB and European Data Protection Supervisor (EDPS) issued a joint opinion to address the data protection implications of AI. The joint opinion aimed to, among other things, (1) harmonize the rules surrounding AI; and (2) identify certain risk areas and prohibit certain uses of AI.

With regard to harmonizing rules surrounding AI, the joint opinion aims to set up a legal framework that aligns with existing laws and regulations, such as GDPR. Primarily, this includes identifying the appropriate legal basis for AI use, ensuring data subject rights are not infringed upon, and promoting transparency in how companies use AI technologies to process personal data. The joint opinion also sets out to identify certain uses of AI that present high levels of risk, focusing on those that may impact human dignity, such as police observation, social scoring and remote biometric identification. In all of these cases, the joint opinion aims to limit these uses to ensure that the private aspects of people's lives are not intruded upon and to avoid discriminatory effects.

Similarly, the FTC has announced that it is considering rulemaking on the commercial use of AI. The FTC has many of the same concerns highlighted in the EDPB and EDPS' joint opinion. FTC's primary goal (and authority) is to curb unfair and deceptive practices. In sticking with this directive, it wants to ensure that the outcomes of AI use remain fair and ethical, and ensure commercial use of AI remains transparent, which includes notifying consumers of the types of data used and the purpose of AI use.

Regulations related to AI are still very much in the infancy stage, but clearer guidelines and restrictions from regulatory authorities are quickly approaching.

3. Global Dealmaking and Due Diligence

Over the past few years, there has been an increased emphasis on privacy due diligence in corporate transactions and global dealmaking. This increased emphasis is due to three main factors: (1) an increase in privacy-related laws and regulations; (2) the costs and fines related to non-compliance with such laws and regulations; and (3) heightened public concerns around the uses of personal data.

As with any transaction, the identification and allocation of privacy-related risks are imperative. In order to understand these risks,

CONTINUED ON PAGE 3 ▸

CONTINUED FROM PAGE 2

purchasers and investors are increasingly focusing on thorough due diligence on the privacy practices of the target and/or its assets. This, for example, involves an analysis of a company's public-facing privacy components, such as its website and privacy policy, along with its internal policies and procedures, including how it handles consumer and/or employee data and data subject requests. Additional focus may also be placed on the target's data breach documentation, the record of processing activity and privacy contracts with vendors and customers (i.e., data processing agreements). All of these components help identify the risks associated with a particular target and whether any additional steps in the dealmaking process are necessary to allocate such risks (i.e., valuation considerations, indemnifications, holdbacks, etc.). For companies anticipating a corporate transaction in the near future, getting the privacy side of the house in order is becoming increasingly important.

4. International Data Transfers

Cross-border data transfer will continue to be a hot topic in 2022 due to recent guidelines published by the EDPB and the implementation of China's new privacy law, the Personal Information Protection Law (PIPL).

The guidelines published by the EDPB clarify the criteria for data transfers that occur pursuant to GDPR. First, the EDPB made clear that personal data collected by a non-EU organization directly from data subjects is not considered a data transfer (and therefore does not require a transfer mechanism as required by GDPR). Second, and perhaps most importantly, the EDPB has identified the three criteria that qualify a processing activity as being a transfer:

a. A controller or a processor is subject to the GDPR for the given processing.

b. This controller or processor ("exporter") discloses by transmission or otherwise makes personal data subject to this processing available to another controller, joint controller or processor ("importer").

c. The importer is in a third country or is an international organization, irrespective of whether or not this importer is itself subject to the GDPR in respect of the given processing.

The above criteria clarify a few points. First, a transfer of personal data to a non-EU importer that is subject to GDPR is still considered a transfer. While this is still considered a transfer for GDPR purposes, the EDPB recognizes that fewer protections are needed considering that the importer is already subject to GDPR and as such the European Commission will publish updated standard contractual clauses that contemplate this type of transfer. Second, a transfer of personal data by an EU processor back to a non-EU controller is also considered a transfer. This second point is not entirely surprising given the extraterritorial scope of GDPR, and the new processor to controller SCCs (published in June 2021) contemplate such transfers.

Further, cross-border transfers that involve the personal data of Chinese data subjects will also be subject to heightened scrutiny. Certain companies, depending on the size of the company and the type and quantity of personal data transferred, will be subject to the PIPL's security assessment requirement, which includes identifying potential risks, ensuring proper safeguards are in place and entering into data processing agreements that address the protection, security and liability surrounding the processing of personal data.

5. Privacy of Children's Data

Enforcement in the children's privacy space has continued to increase. The FTC, in general, has put greater emphasis on data privacy, which has included the continuation of its analysis on public comments related to the Children's Online Privacy Protection Act (COPPA). As a refresher, COPPA aims to protect the personal information of children under 13 years old. While the FTC is reviewing COPPA to ensure its protections are robust enough for today's privacy climate, it has also been active in its enforcement actions. For example, an online advertising platform was recently subject to a two million dollar fine for failing to collect consent from parents for the processing of their children's personal information. A second company (an operator of a coloring book app) settled with the FTC for the misuse of children's personal information, which involved the use of such personal information for behavioral advertising purposes.

Similarly, under the GDPR, the Irish Data Protection Commission has also published guidance on the processing of children's personal data. While the guidance outlines several fundamentals, there are a few key aspects that companies should pay attention to. First, it directs companies to know their audiences. This means companies should take steps to identify their users, and if these users will be children, ensure that child-specific data protection measures have been implemented. Second, when a company directs its products/services to children, it should ensure that any notice should be concise, transparent and intelligible. This does not differ from GDPR's general requirements regarding notice to individuals, but this is especially important when the information is specifically addressed to children.

Conclusion

The above is just a snippet of the regulatory hurdles that organizations face in 2022. As states and countries adopt new laws, increase enforcement and attempt to navigate new technology and trends, organizations will need to adopt a comprehensive and sophisticated approach to identify risk areas and maintain compliance.

Discoverability of Forensic Expert Incident Reports

The discoverability of forensic expert incident reports is often a hotly contested issue in lawsuits. Regulators, such as the Office of Health and Human Services, often demand that they receive copies of forensic reports and companies generally comply. But if the reports are disclosed to a third-party regulator outside the attorney-client relationship, can they nevertheless be protected?

Mark A. Olthoff
Shareholder
Kansas City

Libby Marden
Associate
Kansas City

A. Overview of Attorney-Client Privilege and Work Product Doctrine

1. Attorney-Client Privilege

The attorney-client privilege protects confidential communications between attorneys and their clients that relate to the request for, or the rendering of, legal advice. The U.S. Supreme Court in *Upjohn Co. v. United States* recognized that the attorney-client privilege applies to communications between corporate counsel and a corporation's employees when:

- Employees communicate with counsel at the direction of their corporate superiors.
- Employees communicate with counsel to secure legal advice for the corporation; or provide facts that the lawyer needs to give the corporation legal advice.
- Employees are sufficiently aware that counsel or their agent is questioning them so that the corporation may obtain legal advice.
- The communication concerns matters within the scope of the employees' corporate duties.
- The communication is confidential.

449 U.S. 383, 390-97 (1981). Courts have held that the privilege also extends to communications between corporate counsel and former employees if the discussion relates to the former employee's conduct and knowledge gained during employment and counsel's communications with agents and consultants whom counsel retain to help provide legal advice to the client.

2. Work Product Doctrine

The work product doctrine protects from disclosure to third parties documents and tangible things prepared for or by an attorney in anticipation of litigation or trial by or for another party or its representative. Fed. R. Civ. P. 26(b)(3)(A). When determining whether the work product doctrine applies, courts generally interpret "anticipation of litigation" to mean that a document was created because of anticipated litigation and would not have been created in substantially similar form but for the prospect of that litigation. "At its core, the work-product doctrine shelters the mental processes of the attorney, providing a privileged area within which he can analyze and prepare his client's case. But the doctrine is an intensely practical one, grounded in the realities of litigation in our adversary system. One of those realities is that attorneys often must rely on the assistance of investigators and other agents in the compilation of materials in preparation for trial. It is, therefore, necessary that the doctrine protect material prepared by agents for the attorney as well as those prepared by the attorney himself." *United States v. Nobles,* 422 U.S. 225, 238–39 (1975) (footnote omitted).

B. Submission of Confidential Expert Materials to Regulators

3. Attorney-client privilege and waiver

Generally, voluntary disclosure of a privileged communication to a third party will destroy the attorney-client privilege. *See, e.g., Emmanouil v. Roggio,* 499 F. App'x 195, 199 (3d Cir. 2012); *In re Columbia/HCA Healthcare Corp. Billing Pracs. Litig.,* 293 F.3d 289, 294 (6th Cir. 2002); *U.S. v. Bergonzi et al.,* 403 F.3d 1048, 1049 (9th Cir. 2005). However, the Eighth Circuit has adopted the theory of "selective waiver" related to voluntary disclosure of otherwise privileged material to government agencies. In *Diversified Industries v. Meredith,* 572 F.2d 596 (8th Cir. 1978 [en banc]), the court found that a corporation may selectively waive the privilege to an agency such as the SEC without impliedly effecting a broader waiver. No other circuit has explicitly adopted this view. *See also Jo Ann Howard & Assoc., P.C. v. Cassity,* No. 4:09CV01252, 2012 WL 2396423, at *2 (E.D. Mo. June 25, 2012); *City of Pontiac Gen. Employees' Ret. Sys. v. Wal-Mart, Inc.,* No. 5:12-CV-5162, 2018 WL 1558572, at *5 (W.D. Ark. Mar. 29, 2018).

4. Work product protection and waiver

Work product protection does not protect the confidential relationship between an attorney and client but instead furthers the adversary system by safeguarding the fruits of an attorney's trial preparation from the discovery attempts of an opponent. "[D] isclosure of work-product to a third-party does not necessarily waive the protection; only disclosing material in a way inconsistent with keeping it from an adversary waives work product protection." *Blattman v. Scaramellino,* 891 F.3d 1, 5 (1st Cir. 2018).

C. Application of Cases

Courts faced with deciding whether forensic expert incident reports submitted to regulatory authorities lose protections from discovery have reached differing results, often based upon the unique facts presented. The cases discussed below reflect these varying decisions. This discoverability issue will likely continue to be seriously litigated.

5. Successful Invocation of Privilege in Incident Response

In a number of cases, courts have found that materials created by a forensic expert were not discoverable. Factors supporting this conclusion include cases where outside counsel engaged and instructed the consultant, the expert retained was not one generally used, i.e., the expert was specially engaged for the assignment, the consultant was not given a scope of work pursuant to an existing Master Services Agreement, and the work product of the expert was prepared in anticipation of litigation and not widely distributed. *Maldondo, et al. v. Solara Medical Supplies, LLC, et al.,* No. 1:20-CV-12198-LTS, Doc. 36 (D. Mass. June 2, 2021); *In re Experian Data Breach Litig.,* 2017 WL 4325583 (C.D. Cal., May 18, 2017); *In re Arby's Restaurant Group, Inc. Data Sec. Litig.,* No. 1:17-mi-55555-WMR, Doc. 453 (N.D. Ga. March 25, 2019); *In re Target Corporation Customer Data Sec. Breach Litig.,* 2015 WL 6777384 (D. Minn. Oct. 23, 2015); *Genesco v. Visa,* 302 F.R.D. 168 (M.D. Tenn. 2014).

CONTINUED ON PAGE 5

CONTINUED FROM PAGE 4

6. Unsuccessful Invocation of Privilege in Incident Response

On the other hand, a number of courts have reached the opposite result and held that forensic reports are discoverable and must be produced in litigation. Key factors in these cases were whether the reports were generated in anticipation of litigation or merely in the ordinary course, whether the primary motivating factor to engage the consultant and create the report were the prospect of litigation, the scope of work and services provided were essentially the same before and after the breach, the stated purpose of the engagement set forth in the engagement agreement, whether the report would have been generated regardless whether a suit was filed, whether the report was created to assist legal counsel, *i.e.,* offered guidance for providing legal advice, the timing of the engagement, whether the expert was already under a contract for services, whether the payment for the vendor's services was reflected as a business or legal expense, how widely distributed the work product was made, and whether the report was used for non-litigation purposes, *In re Rutter's Data Sec. Breach Litig.,* No. 1:20-CV-382, Doc. 95 (E.D. Pa. July 22, 2021); *In re Capital One Consumer Data Sec. Breach Litig.,* 2020 WL 3470261 (E.D. Va. June 25, 2020); [1] *Guo Wengui v. Clark Hill, PLC,* 2021 WL 106417 (D.D.C. January 12, 2021); *In re Premera Blue Cross Customer Data Sec. Litig.,* 296 F. Supp. 3d 1230 (D. Or. 2017); *In re Dominion Dental Servs. USA, Inc. Data Breach Litig.,* 429 F. Supp. 3d 190 (E.D. Va. 2019); *Fero v. Excellus Health Plan, Inc., et al.,* No. 6:15-cv-06569-EAW-JJM, Doc. 304 (W.D.N.Y. 2019).

D. Considerations for Maintaining Privilege of Expert Incident Reports

7. Consider Employing a Dual-Track Investigation

Consider setting up a dual-track investigation with separate teams to (1) conduct an ordinary course of business, non-privileged investigation, and (2) provide the organization with legal advice and protect the organization's interests in litigation. Two separate reports, one reflecting a post-breach mitigation investigation and one reflecting a post-breach analysis in preparation for litigation could be created. The non-privileged mitigation investigation report should not include analysis or interpretation. This report should reflect facts and technical information only. Conversations of next steps, effects of the breach, and characterizations of the attack that may occur during the investigation should be done orally until findings are solidified, at which point such findings should be presented either within the legal investigation report or within a privileged attorney letter.

8. Structure Consultant Engagement Agreements Carefully

Hire an outside cybersecurity firm to investigate the breach and, if possible, a different cybersecurity firm than the company previously hired to conduct any prior review of the company's data management systems. If it is impossible or impractical for the company to retain a new firm, the company and the cybersecurity firm should use a separate team of experts dedicated exclusively to investigating the breach and dealing with any litigation that may arise.

Persist operating under one Master Services Agreement with subsequent SOWs referencing the original MSA, citing *Capital One* as justification. The organization, outside legal counsel, and forensic investigator should jointly create an accurate evidentiary record in the agreement that clearly demonstrates that the investigation report is prepared primarily for legal privilege purposes, and not for ordinary business purposes. The forensic investigator's engagement should be limited to work relevant to assisting outside legal counsel to provide legal advice and prepare for litigation. Creating a SOW that differs from broader SOWs or retainers and is perhaps more limited and directed toward work that is legal (as opposed to business) will be beneficial.

9. Counsel Involvement and Direction

The forensic investigator should be hired by outside legal counsel expressly retained to advise the organization regarding the incident and related litigation, and the payment should come out of the company's legal budget. The forensic investigator should deliver its report to, and communicate with, outside legal counsel only. The forensic investigator should not communicate directly with the organization's in-house legal counsel or the incident response team. The investigation report should be based on an analysis of documents and data (e.g. server images) that are preserved for subsequent disclosure in litigation.

10. Restrict Communications and Report Access

Avoid sharing the legal investigation report as much as possible. The investigative report should only be shared on a "need to know" basis and should not be shared with regulators. For others outside of the legal investigation, such as vendors, regulators, or auditors, they should only be provided the non-privileged report. Sharing only the non-privileged report in this manner will help demonstrate that the investigative report was created for purposes of litigation and not for regulatory or business purposes.

Because communications between consultants and businesses are also potentially discoverable, organizations should also take care to limit such communications (especially written communications) to only what is necessary and consider the following techniques:

- Include counsel on all communications concerning the data breach (although that does not guarantee that a court will deem the communication privileged).
- Document investigation-related business matters separately from legal matters.
- Date documents to assist in any later claim of privilege or work product protection.
- Mark documents as "Protected by the Attorney-Client Privilege," "Prepared at the Direction of a Lawyer," or "Prepared in Anticipation of Litigation" when appropriate.
- Prepare a separate, non-privileged report or multiple iterations so only a limited audience receives the full report.

E. Conclusion

Preservation of attorney-client confidences and work product is important in any circumstance but, given the prospect of litigation and class action lawsuits arising from a data compromise, it is even more critical to protect communications, strategies, and analyses as much as possible. Because government regulators often demand forensic reports, structuring and documenting the relationships and work product appropriately may help maintain the privileged nature of documents created. Nevertheless, we expect to see these issues remain hotly contested in 2022 and beyond.

[1] In a separate decision, the District Court held that Capital One's general counsel engagement of PricewaterhouseCoopers was significant in finding that report was not discoverable. The PWC report was created to assist with fiduciary and legal duties in anticipation of litigation. *See In re Capital One Consumer Sec. Breach Litig.,* 2020 WL 5016930 (E.D. Va. Aug. 26, 2020).

Market Changes in Cyber Liability and Options for Your Business

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

Kathyrn T. Allen
Shareholder
Kansas City

Kelsey L. Brandes
Associate
Kansas City

I. Introduction

For the first time ever, cyber insurance is facing a hard market. Since the product line's inception about twenty years ago, carriers, brokers and policyholders have reaped the benefits of soft market conditions. Policies were cheap, and they provided generous coverage and low retention. Losses were minimal, and therefore, cyber insurance books were very profitable. Over the last few years, the cyber risk landscape has shifted. The frequency and severity of losses have grown astronomically, forcing carriers to constrict their offerings, which can put policyholders and potential policyholders in tight positions.

II. Why are we in a hard market?

When carriers began selling cyber insurance, the risks facing large companies were one-off incidents like lost unencrypted laptops, misfired emails containing lists of employee information, and the occasional malicious insider. Smaller companies had even fewer issues. Over time the threats evolved and grew to include more email compromises and small ransomware interruptions. But even those could be resolved quickly by restoring from backups and resetting passwords.

However, in the last few years, the attack landscape has transformed significantly. Companies of all sizes started experiencing significant email compromise events that very often involved the expensive combination of large-scale data breach investigation and notification and the loss of funds through misdirected wire transfers or ACH payments. Phishing and social engineering campaigns exposed a lack of employee training, technical safeguards and data retention policies across many companies. Each of these incidents may cost tens of thousands of dollars to resolve on average, and the frequency led to huge loss ratios for cyber carriers. Further, small companies were not immune to these issues, and the costs associated with the investigations and response compared to the premiums paid for the policies exposed the small business space.

Just as carriers and brokers seemed to wrap their arms around business email compromises, by pushing extensive training and technical solutions, ransomware events exploded much larger than ever anticipated. Early on, ransomware was typically used to encrypt data in place. Attackers would access a network, quickly encrypt what they could, and demand a few hundred or a few thousand dollars in exchange for a decryption key. For many companies, restoring from backups was a way around having to pay, and for others, the demand was so minimal compared to the potential cost of the interruption that it made more sense to pay for the decryption key.

But as attackers saw companies responding rather successfully to these events, they shifted the nature of their attacks. Instead of simply locking users out of a network the moment access was acquired, attackers instead saw the potential for larger paydays with some additional effort. They sat stealthily in a network performing reconnaissance to understand the company's backup strategy and to steal important company data, ultimately using internal phishing campaigns to escalate user privileges to gain access to critical systems. Once sufficient network administrator-level access was obtained, the ransomware attack was launched, finally encrypting the network a few days or months later. When these types of attacks hit companies, they were not only dealing with an overwhelming hit to critical systems and data and backups being encrypted, but also the added concern of data being accessed or stolen, and potentially exposed. This allowed attackers to demand much higher ransom payments—to the tune of millions of dollars per event.

Between the business interruption, extortion demand, data restoration and incident response, policies with $5 million or $10 million in coverage that had never been touched were exhausted on a weekly basis. Further, unlike a typical data breach matter, ransomware matters are immediately public events that draw attention from regulators and class action attorneys, especially when downstream services to customers are interrupted as a result.

III. What does that mean for the market?

Carriers have responded to the new landscape by increasing premiums, decreasing policy limits, and being more conservative in their underwriting process. Where it was previously hard to convince certain markets with minimal data collection and personally identifiable information that cyber insurance is essential for business, the demand for policies in those markets now outsizes supply.

At renewal, carriers have updated application questions, oftentimes with assistance from forensic experts, to better understand a company's preparation for ransomware attacks and the subsequent business interruption. Carriers are now requiring additional technical safeguards, like multi-factor authentication (MFA) and endpoint detection and response tools (EDR), where previously organizations that implemented these tools were considered leagues ahead of their peers. The sudden shift towards requiring these protections as a prerequisite for coverage has left many organizations scrambling to find time and money in their IT budgets to implement these services ahead of a policy renewal.

In addition to increased premiums, limited coverages and higher security expectations, many carriers are outright declining risks in certain markets that have proven to be susceptible to expensive attacks. Manufacturing, technology supply chain providers, and healthcare institutions have especially faced an uphill battle in finding carriers willing to underwrite their businesses.

CONTINUED ON PAGE 7

CONTINUED FROM PAGE 6

This forces those organizations to purchase more expensive policies with lower coverage and build more complex towers of insurance in order to maintain the amount of risk protection enjoyed for many years prior.

IV. What can companies do?

A. Determine What Coverage You Have. The question of whether other insurance policies provide coverage for cyber incidents is hotly contested, but one that can be expensive to litigate. Thus, businesses need to have a clear understanding of whether their current policies cover cyber incidents, and if so, to what extent. These are questions you should ask of your cyber insurance provider:

1. *Does my policy cover my vendor's errors in addition to mine?* Vendor management is becoming increasingly important for businesses, especially those that deal with sensitive information (i.e. financial services or health care). It is important to identify whether your cyber policy covers your loss of data when it is in someone else's possession. For example, a policy may reference coverage for "your computer system" but the definition of "your computer system" might exclude (or not reference specifically) the cloud or networks run by third parties.

   Practical Consideration: Require your vendors to carry their own cyber insurance policy that covers your data in their possession through contract.

2. *Does my policy cover "inside the house" risks?* Employees are the single greatest threat to a business' cyber security. Many cyber policies only cover the malicious theft or destruction of data from an outside source, but studies have found that many times it is employees who are unintentionally and unwittingly contributing to data loss and breach.

   Practical Consideration: Have written, up-to-date information security policies that employees are trained on annually and install proper physical and electronic safeguards on all business electronics that employees use (laptops, tablets and smartphones).

3. *Does my policy cover cloud-related risks?* Certain insurers have used "sub-limits" or lower limits of coverage that cap the amount available for claims specific to cloud-based risks for cloud users. Also note that some policies will have an exclusion for liability assumed through contract by the cloud provider. This means that your cloud provider may have far less liability coverage for your data than you assumed.

   Practical Consideration: Review your policy's sub-limits to ensure that you have sufficient available coverage and never limit liability in contracts with vendors or partners to "insurance limits."

4. *Does my policy apply retroactively?* It takes an average of 256 days for most businesses to identify a malicious attack. If the attack occurred prior to you obtaining the policy, you may run the risk of your insurance not covering it. Some insurers will offer retroactive coverage for an additional premium.

   Practical Consideration: Conduct penetration testing on your system prior to obtaining any cyber coverage. Through these tests, previous breaches or attempts on your network may be identified.

5. *Is my policy limited geographically?* Some policies limit coverage to the United States or put restrictions on how far from your place of business events or incidents must take occur in order to be covered. If you are using cloud-based services, those servers could be located outside of the U.S. or could be thousands of miles from your business's headquarters.

   Practical Consideration: Review your cyber insurance policies for geographic limitations and make sure all agreements with vendors or partners prohibit transmitting your data outside of those limitations.

6. *Does my policy cover physical breaches?* Claims relating to a cyber attack on your systems are covered, but what about physical breaches? Phone systems, security cameras and other systems that are controllable through the internet are all exploitable.

   Practical Consideration: Have a clear understanding of which insurance product covers the physical aspect of a breach. If your policy does not cover the physical aspect of a breach, consider adding additional policies that do cover the physical aspect.

7. *Who is my contact in the event of a breach?* A set claims process following a cyber-security incident is something an increasing number of insurers are implementing. It is important to understand your insurer's policy and know who your point of contact will be in the event of a breach.

   Practical Consideration: Your insurer may also have breach response services available that you can take advantage of as a customer. Discuss with your insurer what, if any, breach response services are available to you before a breach occurs.

8. *Can I get a reduction in premiums if I implement certain policies/procedures?* Many insurers will offer you lower premiums or renegotiate your existing premiums if you can demonstrate you have taken concrete steps to manage your information security risks. Ask your insurer if they do this and have them identify what measures they like to see.

   Practical Consideration: Consult with an information security professional to develop internal corporate information protection policies, draft template agreements to use with vendors that include provisions around information security and conduct penetration testing and other diagnostic steps to identify any risks in your system.

9. *Does my policy cover PCI-DSS Assessments?* One of the more common, and expensive, cyber liability risks is card payment processing information. The Payment Card Industry Data Security Standard (PCI-DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express and Discover. From these standards, the credit card industry sets assessments for data breaches involving credit card information, and fines and penalties for violation of the PCI-DSS. Coverage for such liabilities often requires a specific policy or coverage type.

   Practical Consideration: If your business handles credit/debit card information, review your policy for specific coverage provisions for both fines and penalties resulting from non-compliance with PCI-DSS and fraud-recovery and reimbursements regardless of compliance with PCI-DSS.

CONTINUED ON PAGE 8

CONTINUED FROM PAGE 7

B. Make Your Business More Insurable.
Carriers are expecting organizations to have, at minimum, basic modern IT security controls and data protection policies in place, and to be able to demonstrate that they are implemented correctly and enforced constantly.

10. *Effective Backup Strategy, and Testing*
A big reason ransomware has exploded so successfully is that attackers have taken away a company's option to restore without paying the ransom by either encrypting or deleting backups as part of the initial attack. In response, many forensic experts recommend the "3-2-1" approach—3 copies of the data (production, on-site backups, off-site backups), 2 different media types (cloud, disk, snapshot or tape) and 1 offsite copy (cloud, tapes).

When it comes to ransomware, best-laid plans often go awry. All too often an organization implements what they believe is a sound strategy, only to find out during an attack that their backups were not segregated properly, or the daily snapshot stopped functioning months ago. Carriers expect organizations to be able to demonstrate a regular testing schedule and the results of those tests. These tests will enable organizations to better anticipate potential downtime, restoration strategy and prioritization.

11. *Multi-factor Authentication (MFA)*
Most ransomware attacks start with an account takeover. Once credentials are stolen, attackers typically use credential-harvesting malware to escalate privileges in order to gain access to a network administrator account. Companies that properly implement MFA across all users can thwart many of these attacks. Rather than just asking for a username and password, MFA requires one or more additional forms of verification (like a one-time use code sent to a user's phone), which decreases the likelihood of an attacker gaining access to the account. MFA should be implemented on all email accounts, local administrator accounts and domain administrator accounts and on any remote access points. If you work with third-party vendors who have direct access to perform functions on your network, MFA should also be enabled here too.

12. *Data Retention Policies*
As mentioned above, ransomware attacks have shifted from encryption only, to encryption + data access. While much of this article is focused on the business interruption and data restoration issues caused by ransomware attacks, the access and acquisition of sensitive data is another hurdle organizations must overcome. For organizations that can restore from backups and avoid a huge interruption, they still must consider the data breach implications of the stolen data. Most often, attackers will provide a sampling of stolen data at the outset of a conversation with the victim organization, in order to encourage payment for the return and destruction of the information. Organizations that have strong data retention policies and enforce those policies can limit the amount of extraneous data available for attackers to monetize. They can also use the sampling to pinpoint where on the network the attacker may have stolen the data from, in order to get a better sense of what data the attacker might have and to better focus a forensic investigation.

Further, for the ongoing issue of business email compromises, inbox hygiene and email archiving drastically limit the data potentially available in a compromised inbox, substantially decreasing the time and money spent determining what the attacker could have had access to while in the compromised account.

13. *Endpoint Detection and Response (EDR)*
EDR is a next-level antivirus solution. It not only provides real-time monitoring of your endpoints for any anomalous activity, but it can also quickly alert security personnel to security issues, allowing organizations to contain an incident before it becomes catastrophic. Further, when an incident does occur, forensic investigators can use EDR logging to understand the timeline of the attack and any movement that occurred in the network. This can speed up the response and help an organization understand what, if any, data is at risk as a result of the limited intrusion.

However, EDR is only as good as the monitoring of alerts. Because attackers tend to strike at inopportune times, it is important to have dedicated resources to rule out false positives from legitimate threats. There are many 24/7 security companies that offer these services.

C. Negotiate.
Brokers are keenly positioned in the ecosystem to ensure that organizations seeking coverage are prepared for the more stringent carrier expectations and well-positioned to fill out a renewal or new policy application. Having access to applications across the market, brokers are in the best position to educate and prepare clients for the inevitable squeeze. Because many of the required safeguards will require additional IT financing and company buy-in, brokers can help clients by flagging issues they need to be prepared for earlier in the application process. This way, by the time the insured is filling out an application, they can provide answers that will put them in the best possible position to get coverage. In line with that, through their connections to the legal and forensic field, brokers can also help an insured party by putting them in touch with resources that can help them identify gaps in their current cybersecurity posture and remediate those gaps prior to the application process. This includes working with law firms and IT security firms to conduct privileged risk assessments, penetration tests and gap analyses and then implement solutions based on the results of those activities.

Additionally, attorneys skilled in cybersecurity insurance can assist clients in both obtaining and negotiating the policy coverage necessary for the client's business. By analyzing the needs of their client's organization, attorneys can ensure that the policy provides an acceptable level of coverage, both in terms of the amount and scope of coverage. They can identify their client's major areas of cyber-related risks and review their client's policy to ensure that it matches these risk areas. For some organizations, a policy may only need to cover direct damages, yet for other organizations, this amount of coverage would be extremely inadequate. An attorney skilled in cyber insurance can identify additional cyber-related risks and negotiate with an insurer to also include coverage for downtime, breach-related expenses and civil liability, if necessary.

Cyber insurance attorneys can also analyze and review their client's current IT security controls and data protection policies to determine if they are sufficient and properly aligned with carriers' expectations. If these controls

CONTINUED ON PAGE 9

CONTINUED FROM PAGE 8

or policies are lacking, your attorney can identify actions to take that will allow your organization to be more insurable. Further, your cyber insurance attorney can review your insurance policy to determine how your policy compares with those in the marketplace, and if you are renewing your policy or obtaining a policy for the first time, avoid coverage gaps, negotiate enhancements or request modifications to the policy as necessary.

V. Conclusion

While cyber insurance is facing a hard market for the first time in its existence, due to increasingly sophisticated ransomware and other attacks, organizations can still effectively determine what coverage their business needs, implement policies and testing to make their business more insurable and negotiate with carriers to receive the best coverage for their organization. Please contact your Polsinelli attorney for assistance in the process of assessing, obtaining or renewing your organization's cyber insurance policy.

Ransomware Reporting Requirements: A Look Forward into Evolving Security Incident Notification Rules

Michael J. Waters
Shareholder
Chicago

Colin H. Black
Associate
Chicago

Data breach notification laws in the United States have historically focused on notifying individuals, regulators and others in situations in which personal information has been accessed or acquired. Ransomware attacks, while incredibly disruptive, do not always involve data access or acquisition and, as such, are not always reported. As ransomware attacks increase in frequency and the severity of their impact, both law enforcement and industry regulators are seeking greater visibility into these incidents and, through the publication of new guidance and the amendment of notification laws, are starting to require increased reporting.

How Does Ransomware Work?

Ransomware refers to a particular kind of malicious software that utilizes encryption to limit access to the contents of an impacted device until a payment is made to the threat actor in exchange for a decryption key.

Encryption is a legitimate utility for data security and works by transforming plaintext into cipher text using an algorithm which generally has a single known solution. The ciphertext can only be converted back to plaintext by using the solution, often referred to as a decryption key. When used responsibly, encryption is an excellent way to protect the confidentiality of data both at rest and in transit.

Oftentimes, ransomware is not a highly complex malware; in some instances, a ransomware attack can even be achieved by leveraging built-in encryption utilities such as BitLocker. The simplistic and often legitimate uses for encryption software make ransomware extraordinarily difficult to detect until it is too late. Furthermore, threat actors are constantly exploring new attack vectors, making complete protection impossible.

State Breach Notification Laws.

By default, all entities domiciled in the United States are subject to state privacy laws. California passed the first data breach notification law in 2003, and since then, every state in the U.S. has adopted its own breach notification statute. Furthermore, the applicability of each state privacy law is based not on the domicile on the entity but rather on the domicile of the impacted data subject. Thus, an entity that is domiciled in California but holds data on individuals all over the United States will generally be subject to the state privacy law in each state where an impacted individual is domiciled.

While the trigger for notification will vary from state to state, all state data breach notification statutes contain requirements that impacted individuals be notified in a manner consistent with the forum state's notice rules. In addition to notice to impacted individuals, many states also require notice to state Attorneys General, consumer credit reporting agencies (e.g., Experian, TransUnion, and Equifax), and law enforcement.

The mere fact that a ransomware incident has occurred does not necessarily trigger a notice obligation pursuant to state breach notification laws. Rather, most states require either the actual access to or exfiltration of personal information. By contrast, the automated encryption of data will not generally trigger a notification obligation in and of itself.

CONTINUED ON PAGE 10

CONTINUED FROM PAGE 9

Sectoral Privacy Regulations.

Privacy regulation in the U.S. is based on a sectoral model; simply put, different rules may apply depending on the industry in which the impacted entity operates. Sectoral regulations exist at both the state and federal levels as well as in self-regulated industries.

Common examples of federal sectoral privacy regulations include the Health Insurance Portability and Accountability Act (HIPAA) for healthcare providers, Gramm-Leach-Bliley Act (GLBA) for financial institutions, and the Federal Educational Rights and Privacy Act of 1974 (FERPA) for educational institutions.

At the state level, certain industries are subject to additional regulations; for example, many state Departments of Insurance (DOI) require notice to the DOI in the event of a service interruption involving entities regulated by the DOI. These regulations are particularly severe, in some instances requiring notice as soon as forty-eight hours from the initial discovery of a security incident.

Finally, many industries require compliance with certain privacy frameworks that have not been promulgated by law. For example, most enterprises that accept payment cards (e.g., Visa or Mastercard) are required to comply in some capacity with the Payment Card Industry Data Security Standard (PCI-DSS), a body of security standards developed by major payment card processors. Similarly, entities that contract directly with or subcontract under the federal government may be required to comply with cybersecurity standards promulgated by the National Institute of Standards and Technology (NIST).

Trends in Ransomware Reporting Requirements.

Based on trends observed in 2021, we can make some predictions about the future of ransomware breach reporting requirements. First, we expect that data breach reporting timelines will continue to shorten. By way of example, the FDIC, Federal Reserve, and Department of the Treasury issued a rule in November with compliance beginning May 1, 2022, that requires banks and their service providers to notify their primary federal regulator within thirty-six hours of a computer security incident that is reasonably likely to disrupt the bank's operations. Notably, this rule does not predicate notice on data access or acquisition, meaning that entities may have to quickly notify their regulators of ransomware events even if there has not been such access or acquisition.

Second, many breach notification frameworks permit notice upon discovery of a breach, in other words, notice will not be triggered until the entity should reasonably know there has been access to personal information. However, some regulators are beginning to place greater emphasis on the discovery of an incident.

While the distinction is narrow, the implications are significant. In the case of ransomware incidents, businesses can be taken offline for weeks, and in many incidents, are unable to restore access to sensitive information. Even if access to data is restored, it can take weeks to determine the nature and scope of the incident and determine which individuals, if any, had sensitive personal information exposed. In many instances, victims of ransomware are forced to choose between reporting on a speculative basis due to a lack of information or risking sanction by a regulator or private action for failure to effectuate timely notice.

Notwithstanding the difficulties associated with making expeditious notice to the appropriate individuals and regulators, we are continuing to see "point of incident" notification triggers grow in popularity. For example, in 2017, the National Association of Insurance Commissioners (NAIC) issued a model rule requiring notice to the state insurance commissioner within 72 hours of the discovery of a cybersecurity event, which includes the disruption or misuse of an information system. Since its release in 2017, the NAIC model rule has been adopted in approximately ten states, however, we anticipate that additional states will be adopting the rule, either in part or in its entirety, in 2022.

Finally, we expect that we will soon be seeing additional requirements regarding the payment of a ransom. Historically, from a legal perspective, the only substantive impediment to payment of a ransom has been the OFAC sanctions list. While paying a threat actor is never palatable, paying a ransom for immediate decryption may be required in some circumstances, such as when there is a risk of bodily harm as in the case of a healthcare provider. Entities are generally free to pay a ransom so long as the threat actor has not been specifically blacklisted by OFAC.

However, as ransomware has entered the public discourse, greater attention is being given to the aftermath of ransomware incidents. The Biden administration has recently expanded its use of sanctions to target cryptocurrency marketplaces that effectuate payment to threat actors. Law enforcement routinely seeks information regarding ransomware negotiations and payment in its postmortem investigations of ransomware incidents and the Department of Treasury has stated that it will consider whether an organization notified and cooperated with law enforcement in deciding how to proceed against entities that inadvertently make payment to an individual or entity on the OFAC list.

In light of the growing ransomware threat, we anticipate that we will see additional and more formal reporting requirements relating to ransomware events and the payment of ransoms. Presumably, such data would aid law enforcement in its effort to apprehend threat actors and perhaps recapture ill-gotten funds.

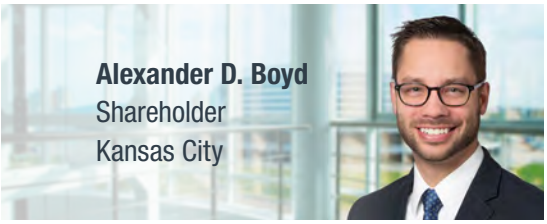
Recommendations for Businesses.

The best way a business can protect itself from ransomware is to create a robust culture around cybersecurity. Security is an ongoing exercise; while no system is impregnable, the vast majority of ransomware incidents we see leverage a combination of the same five or so vulnerabilities, such as open remote desktop protocol ports, unpatched or out-of-date software and Layer 8 failures. Security controls should be constantly assessed for vulnerabilities, configuration errors and proper function.

Second, many businesses do not realize the sprawling nature of data in their control until an incident has occurred. Sensitive information should be segmented appropriately, and if at all possible, encrypted both in transit and at rest. Developing a detailed data flow, both for internal and vendor data, is a critical step in ensuring an expeditious response in the event of a ransomware incident.

Finally, a robust incident response plan is critical, and in many instances, required. The incident response plan should include, at a minimum, procedures for backup validation, key incident response contacts and procedures for the preservation of forensic artifacts. As breach notification rules become more stringent, an incident response plan is invaluable in ensuring a compliant response and restoration.

The FTC's Expanding Role in Cybersecurity and Data Privacy Enforcement in 2022



I. FTC Background

The Federal Trade Commission (FTC) is a federal agency that works to protect consumers from fraudulent, deceptive and unfair business practices. Section 5(a) of the FTC Act broadly authorizes the FTC to investigate and challenge "unfair or deceptive acts or practices in or affecting commerce".[1] The FTC has used this authority to promulgate specific privacy-focused rules, including the Health Breach Notification Rule (*HBN Rule*) and the Standards for Safeguarding Customer Information under the Gramm-Leach-Bliley Act (Safeguards Rule). Congress has provided the FTC authority to enforce privacy-focused legislation like the Children's Online Privacy Protection Act (*COPPA*)[2] and the Fair Credit Reporting Act.[3] Finally, the FTC uses its primary authority under Section 5 of the FTC Act to bring enforcement actions against organizations following data security incidents that the FTC believes involve deceptive practices (often due to misrepresentations in an organization's privacy policy) or unfair practices (often by failing to use reasonable measures to secure sensitive information).

II. The FTC's Recent Actions Demonstrate a Trend Towards Increased Cybersecurity and Data Privacy Scrutiny

During the second half of 2021, the FTC took two meaningful actions that signaled the FTC's desire to expand its role in setting and enforcing cybersecurity and data privacy standards: the FTC clarified the scope of the often ignored HBN Rule and the FTC amended the Safeguards Rule to strengthen the data security requirements for financial institutions.

On September 15, 2021, the FTC issued a Policy Statement that clarified the scope of the HBN Rule and signaled that the FTC intends to begin enforcing the rule. Under the HBN Rule, vendors of personal health records (*PHR*) and PHR-related entities, not subject to the Health Insurance Portability and Accountability Act (HIPAA), must notify the FTC and consumers if there has been a breach of unsecured identifiable health information. Notification to the media may also be required in certain cases. The FTC clarified that the rule applies to developers of health apps or connected devices. The FTC attributed the Policy Statement to the recent explosion of apps and connected devices that capture sensitive health data. While the FTC has not enforced the rule in the decade since its issuance, the FTC's Policy Statement signaled that the FTC intends to begin enforcing the rule. Violations of the HBN Rule may result in civil penalties of $43,792 per day.

On October 27, 2021, the FTC announced a final rule amending the Safeguards Rule to strengthen the data security requirements that financial institutions must implement to protect customers' financial information and by broadening the scope of covered financial institutions. Specifically, the FTC modified the Safeguards Rule in the following key ways:

1. The amended Safeguards Rule includes detailed requirements for the development and establishment of the information security program, such as specific criteria for what the risk assessment must include and that the risk assessment be documented in writing. In addition, the amended Safeguards Rule requires financial institutions to address access controls, authentication, secure development practices, data inventory and classification, information disposal procedures, change management, encryption, testing and incident response.
2. The amended Safeguards Rule adds requirements to ensure that financial institutions are effectively training employees and overseeing services providers.
3. The amended Safeguards Rule requires a financial institution to designate a single Qualified Individual to oversee the implementation of the information security program.
4. The amended Safeguards Rule requires periodic reports to boards of directors or governing bodies.
5. The amended Safeguards Rule exempts financial institutions that collect information on less than 5,000 consumers from the written risk assessment, incident response plan and annual reporting to the boards of directors or governing bodies requirements.
6. The amended Safeguards Rule expands the definition of "financial institution" to include entities engaged in activities the Federal Reserve Board determines to be incidental to financial activities. Through this change, "finders" (i.e., companies that bring together buyers and sellers of a product or service) are now within the scope of the amended Safeguards Rule.[4]

Many new requirements under the amended Safeguards Rule became effective on January 8, 2022, and more significant changes will go into effect on December 9, 2022.

III. The FTC's Anticipated Enforcement Role in 2022

In addition to enforcing the HBN Rule and the recently amended Safeguards Rule, the FTC has expressly stated its intent to further expand its role in setting and enforcing cybersecurity and data privacy standards. The FTC is "particularly focused

[1] *See* 15 U.S.C. § 45(a).
[2] 15 U.S.C. 6501–6505.
[3] 15 U.S.C. §§ 1681-1681x.
[4] *See* Federal Trade Commission, Standards for Safeguarding Customer Information (December 9, 2021), https://www.federalregister.gov/documents/2021/12/09/2021-25736/standards-for-safeguarding-customer-information.

CONTINUED ON PAGE 12

CONTINUED FROM PAGE 11

on developing rules that allow the agency to recover redress for consumers who have been defrauded and seek penalties for firms that engage in data abuses." The FTC is considering initiating a rulemaking "to curb lax security practices, limit privacy abuses, and ensure that algorithmic decision-making does not result in unlawful discrimination."[5] The FTC is also looking to complete its ongoing review of public comments related to amendments to COPPA.

The FTC recently announced its intent to further amend the Safeguards Rule to require financial institutions to report to the FTC any security event where the financial institutions have determined misuse of customer information has occurred or is reasonably likely and that at least 1,000 consumers have been affected or reasonably may be affected. Therefore, covered financial institutions may have additional reporting requirements under the Safeguards Rule in 2022.

If Congress enacts a federal privacy law in 2022, there is a meaningful chance that such a law will provide further authority to the FTC to enforce the law's requirements. If no such law is enacted, the FTC will nonetheless use its primary authority and its authority under the specific rules discussed above to ensure that organizations are appropriately safeguarding consumers' personal information and respecting consumers' privacy.

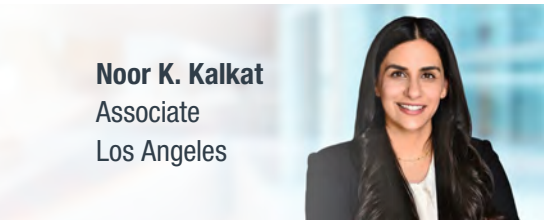
In light of the FTC's recent and likely upcoming actions, organizations should review their operations to ensure they are complying with the FTC's recently amended rules. Organizations should also review and update their privacy policy, implement or review their written information security program and implement or review their incident response plan. Organizations must ensure they are protecting any sensitive data in their possession, or in the possession of their vendors, and ensure they can effectively respond if a data security incident occurs.

[5] See Federal Trade Commission, Trade Regulation Rule on Commercial Surveillance (Fall 2021), https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202110&RIN=3084-AB69.

Third-Party Data Incidents: Preparing and Responding as the Volume of Incidents Rise

Bruce A. Radke
Shareholder
Chicago

Caitlin A. Smith
Associate
Washington D.C.



Noor K. Kalkat
Associate
Los Angeles

Anna K. Schall
Attorney
Kansas City

Preparing for and Responding to Third-Party Data Incidents

I. The Rise in Frequency and Size of Third-Party Data Incident

Many organizations realize that using technology to support both customer-facing and back-office tasks deliver the efficiency and accuracy that employees and customers have come to expect. These technological solutions often reduce overhead internally and allow customers, employees and external third parties to interact with the organization more transparently. However, by incorporating software-as-a-service (SaaS) solutions used in-house, or off-premises services managed entirely by a third party, organizations are exposed to additional potential privacy and security risks.

Year over year, Polsinelli has seen a significant rise in the frequency and severity of third-party incidents. A large reason for the increase is that threat actors are exploiting the technology supply chain—targeting technology providers with direct access to many customer systems, rather than trying to compromise customer systems one by one. The attacks are very clever, and many times go undetected by even the most sophisticated organizations. In late 2020, around 20,000 organizations using the SolarWinds Orion IT monitoring and management software ran what appeared to be a routine update/patch to the software, only to later discover malicious code was pushed through the update that granted threat actors unauthorized access to thousands of organizations. The attack impacted U.S. government organizations, including Homeland Security, and technology giants like Microsoft, Cisco and FireEye.

While the SolarWinds breach was responsible for allowing direct access to customer systems and data, organizations also need to be mindful of data shared externally with third parties. Organizations should understand that state and federal data breach notification laws put the responsibility of notifying individuals of a data breach on the owner of the data, which in these cases is most often the organization rather than the vendor. The vendor's only legal, and oftentimes financial, responsibility is to notify its customer organizations, and in turn, the customer organizations provide legal notification of a data breach to customers or employees.

In addition to the data privacy and access concerns when a security incident occurs, organizations also need to contemplate the potential operational impacts. While technology solutions create efficiencies, an organization could become largely dependent on the software or service functioning properly. When the third-party solution fails, the downstream business interruption could be disastrous. In December 2021, a major HR technology provider announced that it was hit with a ransomware attack that took many of its core services offline. Further, the company reported that the services would have to remain offline for several weeks. Customers reverted to manually tracking time and issuing physical paychecks, a process many employees may have never experienced in their careers. Most companies were able to get paychecks out on time, at a very crucial time of the year, but the longer-term effort of reentering the time, and adjusting for deductions, overtime and hours cannot be quantified.

Gone are the days when an organization can prepare its own privacy and security practices in a vacuum. As discussed mover fully below, organizations are much more dependent on our third-party solutions, and it is imperative that organizations (1) sufficiently vet vendors' privacy and security standards, (2) include contract terms to address outages, data privacy and costs associated with both, (3) continue to train contingency plans for employees who may depend on technology or software solutions to do their jobs and (4) actively seek out network vulnerabilities, in addition to the defensive antivirus and firewall solutions.

II. Federal and State Requirements Related to Third-Party Providers

A. Federal Requirements

In light of the potential risks, federal and state authorities have promulgated regulations addressing third-party vendor relationships. For example, several federal agencies that regulate banking and financial institutions (including federally insured financial institutions) under the interpretive authority granted by the Gramm-Leach-Bliley Act of 1999 issued the interagency Guidelines for Safeguarding Member Information (the "Interagency Guidelines") that, among other things, requires each financial institution to develop and implement an information security program.[1] Under the Interagency Guidelines, the financial institution's information security program must include provisions to "[e]xercise appropriate due diligence in selecting its service providers." To demonstrate the requisite level of due diligence, the Interagency Guidelines

[1] *See* 12 C.F.R. Part 30, App. B A (Office of the Comptroller of the Currency); 12 C.F.R. Part 208, App. D-2 (Federal Reserve); 12 C.F.R. Part 364, App. B (Federal Deposit Insurance Corporation); and 12 C.F.R. Part 748, App. A (National Credit Union Administration)).

CONTINUED ON PAGE 14

CONTINUED FROM PAGE 13

require financial institutions to require service providers by contract to implement appropriate steps to protect the security and confidentiality of sensitive customer information. Additionally, the Interagency Guidelines require, as indicated by the financial institution's risk assessment, the monitoring service providers to confirm that they have satisfied their obligations and as part of the monitoring, the financial institutions should review audits, summaries of test results or other equivalent evaluations of service providers.

In the context of health care, the HIPAA Security Rule mandates that a written contract between a HIPAA covered entity and a business associate must require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronically protected health information. The HIPAA Security Rule further requires the business associate to report to the covered entity any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured protected health information.[2]

B. State Requirements

Likewise, several states have adopted regulations governing third-party service providers as follows:

1. CALIFORNIA

California's Consumer Privacy Act ("CCPA") does not impose specific requirements upon third-party service providers; rather, it requires businesses subject to the CCPA to include in their contracts with third-party service providers certain terms pertaining to the use, retention and disclosure of personal information. Therefore, if a business is not subject to the CCPA, any personal information sent to or shared with a third-party service provider is also not subject to CCPA requirements.

The CCPA defines a "service provider" as a legal entity that processes personal information on behalf of a business.[3] To qualify as a service provider, the legal entity must be party to a written contract with the business that prohibits the legal entity from retaining, using or disclosing personal information for any purpose other than performing services specified in the contract or as otherwise permitted under the CCPA.[4]

In certain circumstances, a legal entity may not qualify as a service provider under the CCPA, including where the legal entity is not party to a written contract with the business or where a written contract exists, but the written contract permits the legal entity to do or more of the following:

- Retain personal information beyond termination of the contract;
- Use personal information for its own purposes; and/or
- Disclose personal information in accordance with its own policies and procedures.

The CCPA does not impose a direct requirement on service providers to delete a consumer's personal information upon request. Instead, the CCPA requires businesses to delete a consumer's personal information upon verifiable request, and the business is thereafter obligated to direct service providers to delete that consumer's personal information from the service provider's records.[5] Deletion of personal information by businesses and service providers is not required in certain circumstances, including but not limited to, where the personal information is necessary to complete the customer's requested transaction or services, to detect and protect against security incidents and/or to comply with other state or federal laws.[6]

Notably, the CCPA does not prohibit a service provider from retaining, using or disclosing personal information received from a business that is "deidentified or in the aggregate consumer information."[7] A service provider with an interest in retaining the personal information originally provided by a business may, therefore, deidentify (e.g., anonymize) or aggregate the information to non-personal information and avoid CCPA restrictions.[8] Furthermore, where a business and service provider have executed a CCPA-compliant written contract, the service provider is not required to indemnify the business for the service provider's mishandling of personal information, nor is the service provider liable if the business fails to comply with the CCPA's requirements.[9]

A service provider that breaches a written contract with a business that prohibits the service provider from retaining, using or disclosing personal information in violation of the CCPA may be subject to an injunction and civil penalties of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation by the State of California's Attorney General.[10]

2. COLORADO

The Colorado Privacy Act ("CPA") defines a "[t]hird-party service provider" as an entity that has been contracted to maintain, store or process personal information on behalf of a "covered entity", defined under the CPA in relevant part as a legal entity that maintains, owns or licenses personal information in the course of its business. [11]

Unless the covered entity agrees to provide its own security protection for personal information disclosed to a third-party service provider, the covered entity must require the third-party service provider to implement and maintain reasonable security procedures and practices appropriate for the type of personal information disclosed from unauthorized access, use, modification, disclosure or destruction.[12]

If a third-party service provider believes a breach may have occurred, the CPA requires that the provider notify the covered entity in the most expedient time possible and without unreasonable delay, if misuse of personal

[2] 12 C.F.R. § 164.314(a)(2)(i)(B), (C).
[3] Cal. Civ. Code § 1798.140(v).
[4] *Id.*
[5] *Id.*
[6] Cal Civ. Code § 1798.105(d).
[7] Cal Civ. Code § 1798.145(a)(5).
[8] The CCPA requires that steps be taken to ensure that such personal information cannot be re-identified. *See* Cal Civ. Code § 1798.140(v).
[9] Cal Civ. Code § 1798.145(h).
[10] Cal Civ. Code § 1798.155(b).
[11] Colo. Rev. Stat. § 6-1-716(1)(b)(i).
[12] Colo. Rev. Stat. § 6-1-713.5(2).

CONTINUED ON PAGE 15

CONTINUED FROM PAGE 14

information about a Colorado resident occurred or is likely to occur.[13] The third-party service provider is also required to cooperate with the covered entity, including sharing information relevant to the security breach.[14]

3. MASSACHUSETTS

Massachusetts' regulations define a "service provider" as a legal entity that "receives, stores, maintains, processes or otherwise is permitted access to personal information" through its provision of services directly to another legal entity subject to Massachusetts' regulations.[15]

Owners or licensees of personal information pertaining to Massachusetts residents, including legal entities as described above, are required under Massachusetts's data breach notification law to develop, implement and maintain comprehensive information security programs that include provisions for overseeing service providers, including:

- Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with state and federal regulations; and
- Requiring third-party service providers by contract to implement and maintain appropriate security measures for personal information.[16]

4. VIRGINIA

Virginia's data breach statute, to the extent that it applies to service providers, only applies to tax preparers, employers and payroll service providers that own or license computerized data related to income tax withholdings.[17] These entities are required to provide notice to the Virginia Office of the Attorney General, without unreasonable delay after the discovery of unauthorized access and acquisition of computerized data containing a taxpayer identification number in combination with the income tax withheld for that taxpayer that compromises the confidentiality of such data and that creates a reasonable belief that the information was accessed and acquired by an unauthorized person and causes, or may reasonably cause, identity theft or other fraud.[18]

III. Proactive Steps to Minimize Third-Party Data Incidents

In light of these regulatory requirements and increased frequency of third-party data incidents, organizations can undertake proactive steps to meet their regulatory obligations and minimize the potential risks and consequences of such incident as follows:

Vetting the vendor: As indicated above, before engaging vendors and providing them access to sensitive information, organizations must properly vet the vendors to ensure that they have implemented appropriate administrative, technical and physical safeguards to protect the data that has been entrusted to the vendors. Additionally, it is important to understand what type of security procedures and protocols the vendor has in place to avoid a potential security incident as well as the vendor's response plans in the event that the vendor has an incident. Not only will proper vetting potentially reduce the likelihood of a data incident, but it could assist the organization in demonstrating adequate due diligence in selecting the vendor in subsequent litigation where plaintiffs allege that the organization was negligent in its choice of vendor.

Understand what data is shared and to whom it is shared: Many organizations whose vendors that experienced a data incident are unaware of the full nature and scope of the data that has been shared with their vendors. Accordingly, organizations should understand what and how much data is being shared, with whom and for what purposes. Additionally, organizations need to understand how long they retain the data and whether other parties have access to the data via the immediate vendor. In large organizations, this is crucial, as it is not easy to identify which vendor has access to what data. Further, many third-party incidents frequently occur because a certain vendor has access to more information than they needed to complete the task. Therefore, the amount of sensitive information provided to vendors should be narrowly tailored to only what is required for their services.

Notice requirements: Under state data breach notification laws, if a vendor has a breach, the vendor's only obligation is to notify the owner of the personal information of the incident. Absent any contractual agreement to the contrary, the owner is then obligated to notify affected individuals and regulators. As a result, the language in the vendor contracts will be critical in determining notification obligations. The contract terms should specify, among other things, who is the owner of the data, when and how the vendor must notify its customer of a data incident and whether the vendor is obligated to provide notification to affected individuals and regulators.

Indemnification language and recovery limitations: The contract should also include indemnification language to ensure that the company is not putting itself at risk and will not have to pay reputationally and financially for an incident they did not cause. The contract should include clear language about the costs of covering the breach and the insurance details.

Continuously monitoring: Most organizations forget to continuously check up on their third-party vendors. Companies only check in when they have been notified of an incident. It is important that companies continuously monitor the vendor's new updates and respond when vendors reach out regarding new software or system update within their system.

[13] Colo. Rev. Stat. § 6-1-716(2)(b).
[14] *Id.*
[15] 201 Mass Reg. 17.02.
[16] 201 Mass Reg. 17.03(2)(f) (provided, however, that until March 1, 2012, a contract a person has entered into with a third party service provider to perform services for said person or functions on said person's behalf satisfies the provisions of 201 CMR 17.03(2)(f)2, even if the contract does not include a requirement that the third party service provider maintains such appropriate safeguards, as long as said person entered into the contract no later than March 1, 2010).
[17] Va. Code Ann. § 18.2-186.6.(M).
[18] Id. (applicable only to the employer's employees and not to the employee's customers or other non-employees).

The Current Landscape of Data Sovereignty Laws and A Universal Compliance Strategy

Jeffrey E. Fine
Shareholder
St. Louis

L. Hannah Ji-Otto
Associate
St. Louis

In the past year, we have seen more and more government bodies around the world putting up regulatory barriers to restrict the extraterritorial movement of data. However, heightened restrictions on the flow of information are in direct conflict with the ever-growing need of multinational businesses to move data across borders in an increasingly globalized and digitized economy. This alert provides an overview of the current landscape of data sovereignty laws in the major economic bodies globally and proposes a compliance strategy for multinational companies.

The following is a high-level survey of the current state of data sovereignty laws of five high-profile jurisdictions following a turbulent 2021. We then offer some tips for businesses to keep in mind when shaping their compliance strategies for 2022.

2021 Recap: Data Localization/ Transfer Regulations in Review

While the world continues to grapple with the Covid-19 pandemic, businesses are increasingly pivoting to digital service models that leverage the internet in place of in-person transactions. Many countries have responded by clarifying or amending their regulation of the flow of individuals' data:

Russia. Subject to very several narrowly defined exceptions, Russia requires all companies that collect personal information of Russian citizens to use the databases located within its territory for recording, systemization, accumulation, storage, correction and retrieval purposes. Additionally, personal information collected in Russia can only be moved to a jurisdiction that ensures adequate protection[1] or based on legally permitted conditions (including when the transfer is based on a data subjects' consent or is necessary to perform a contract). In 2021, Russia's Personal Data Law was amended with increased fines for non-compliance, but the fines for violations for data localization requirements remain the same (approximately USD $16,000 - $96,000 for first-time violators and USD $280,000 for repeated violators). The Russian government has not been engaged in widespread enforcement of its data localization requirements, but there have been efforts to compel compliance by blocking high-profile global Internet platform operators.

China. China passed its Personal Information Protection Law and Data Security Law in 2021, which includes strengthened localization requirements, making it more difficult to export data collected in China to other countries. Under the new regime, the types of data that China views as critical to its national and economic interests (defined as "Important data"[2] and "core data"[3]) must be stored in China. Companies operating in enumerated industries[4] and companies that process large amounts of data[5] are subject to heightened data localization and data transfer restrictions. Other types of companies and other less "important" types of data can be transferred and stored abroad when certain conditions are met, which include obtaining certification from Chinese regulators for cross-border data transfers, or executing standard cross-border data transfer contracts (to be provided by Chinese regulators) with the data recipients. For a more in-depth discussion about China's Personal Information Protection Law, please see our previous article here.

The European Union. EU's GDPR does not require data collected in member countries to be confined in the EU, but it prohibits data transfers from the EU to a country that lacks "adequate" data protection unless certain safeguards are provided. The EU Commission has so far recognized 13 countries[6] as providing "adequate" protection of personal data. The U.S. is not considered a country that provides adequate protection. Organizations located in countries other than the EU or those 13 jurisdictions must apply appropriate safeguards on personal data to be able to receive EU data, which include implementing mechanisms including binding corporate rules (BCRs), Standard Contractual Clauses (SCC), an approved code of conduct, or an approved certification mechanism inside the organizations. Following Brexit, the UK is recognized by the EU as a country that provides

[1] Jurisdictions that are deemed to ensure adequate protection include signatories to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and countries that are in a special list approved by Russian privacy regulators from time to time.
[2] Important data is defined as data that poses a threat to China's national and economic interests or impacts the rights of individuals and organizations and has an "obvious cascading effect" across a range of industries and enterprises.
[3] Core data (a subset of important data) is defined as data that poses a "serious threat" to China's national and economic interests.
[4] The following companies are subject to China's data localization rules: (i) companies 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; and (ii) other similarly situated companies. They are referred to as "Critical Information Infrastructure Operators" or "CIIO"s.
[5] The threshold is either processing the personal information about over 1 million people, or cumulatively has exported personal information of more than 100,000 people, or sensitive personal information of more than 10,000 people to offshore jurisdictions.
[6] These 13 jurisdictions are Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the GDPR and the LED.

CONTINUED ON PAGE 17 ▸

CONTINUED FROM PAGE 16

adequate protection to personal data in 2021, meaning that personal data can move freely between the UK and the EU.

The United States. The United States does not have an overarching data transfer regulatory scheme on the federal level. Certain types of data may need to stay in the territory under export control laws, national security laws or sector-specific regulations. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) protects and restricts the use of Protected Health Information, but does not address the issue of offshoring data[7]. On the state level, California, Virginia and Colorado passed or amended data protection laws in 2021, and the trend is expected to continue in the coming years. These state privacy laws have provisions addressing the protection of data subjects' rights but currently have not promulgated any restrictions on interstate or international transfer of data.

A Proposed Compliance Strategy

Companies with business interests across different jurisdictions are challenged to comply with a patchwork of international privacy laws. Moving data across borders is essential under many circumstances to keep the business functioning. For example, companies need to share data internally with their international affiliates subsidiaries to process employee payrolls and transfer data externally with foreign vendors and business partners to perform market analysis or to deliver products or services to local customers. Whichever jurisdictions a company operates in, here are three steps to take when designing a strategy to enable international data transfer in an organization:

- **Conduct Data Mapping.** It is important to have a solid grasp of the data flow in a multinational organization, so the staff implementing the compliance strategy can understand the nature and scope of the issue they are dealing with. In order to take a good inventory of its data, a multinational company should ask its stakeholders the following questions: which jurisdictions does the company operate in? What types of data does the company collect in those jurisdictions? Is the company operating in an industry that is subject to additional restrictions?
- **Analyze Applicable Laws.** Based on the results of the data mapping exercise, a multinational company should be able to compile a list of jurisdictions in and through which its data moves and identify the applicable laws in those jurisdictions. A company's legal department or outside counsel should be consulted to complete this step, as it involves legal analysis.
- **Design A Formal Compliance Strategy.** A formalized compliance strategy is important, especially in those jurisdictions where companies need to demonstrate their compliance to local regulators to be approved to export data and to defend themselves in case of a data breach. A thorough global data sovereignty law compliance strategy should be designed in accordance with the applicable laws and available data maps. For jurisdictions with strict data localization requirements, companies should investigate options to store data locally (for example, setting up local data centers or confining covered data to local servers offered by cloud vendors). For jurisdictions where data may be transferred for processing offshore, a multinational company should confirm whether its current data transfer mechanisms are up to date.

2021 was a very active year in which we saw many changes to nations' stances on international data transfers and 2022 is already shaping up to be just as active. It is important for multinational companies to assess or reassess their data privacy compliance programs when evaluating their business strategies in 2022 and beyond.

[7] The Centers for Medicare & Medicaid Services (CMS) may have some nuanced requirements related to offshoring that might apply to health care providers.

Roundup of International Privacy Laws

Pasha A. Sternberg
Principal
Los Angeles

2021 shaped up to be an active and hectic time in the international privacy law arena, and despite what some privacy professionals may hope for, 2022 is likely going to turn this into a trend. As discussed in more detail in other parts of this report, data localization and cross-border transfers are two topics that have seen a particularly high level of activity. These are not the only areas of law that have seen developments, however.

A New Law in China

A major development in 2021 was China's passage of a comprehensive privacy statute that governs the collection and "handling" of personal information. Similar in many ways to Europe's General Data Protection Regulation (GDPR), China's Personal Information Protection Law (PIPL) was passed in August of 2021 and entered into force on November 1, 2021. PIPL regulates how companies can use the personal information they collect from individuals and requires companies to have a legal basis for these activities. It also provides individuals with rights in the personal information that is collected about them. Notably, PIPL has extraterritorial reach, so even companies that have limited dealings with China could be subject to the law. Additionally, penalties for noncompliance are CNY50 million (approximately $7.8 million as of the writing of this report) , or 5% of a company's annual revenue from the previous year, so the cost of violating the statute can become significant.

More specifically, organizations must provide prior notice to individuals* about: how personal information is going to be collected; the purpose for which collected information will be used; and the ability for consumers to opt into this data collection and use. The law also requires that organizations collect no more personal information than is needed for the business to conduct the task for which the information is being collected. Additionally, it requires that organizations create internal processes such as appointing a data protection officer, entering into contracts with vendors, implementing data security measures, and conducting protection impact assessments on data processing activities. Finally, it gives individuals the following rights:

- The right to access a copy of the information that the organization has about the individual;*
- The right to have an organization correct incorrect information that the organization has about the individual;
- The right to opt-out or object to the use of their information;*
- The right to withdraw their consent for the use of their personal information;
- The right to limit the use of their personal information;*
- The right to have an organization delete the personal information it holds about the individual;
- The right to get a copy of the personal information an organization has about the individual;* and
- The right to freely exercise their other rights without being discriminated against for doing so.

As with other countries' laws in this field, PIPL contains ambiguity which will require follow-up rulemaking from regulatory bodies, so we do not yet have a complete picture of how to comply with the law. Additionally, it is unclear how broadly and aggressively it will be enforced.

A New Law in Brazil

In addition to China's PIPL, 2021 also saw Brazil's comprehensive privacy law come into enforcement. Brazil's General Personal Data Protection Law (the Lei Geral de Proteção de Dados Pessoais) (LGPD) is Brazil's first comprehensive privacy and data protection regulation, and it is also modeled heavily on the EU's GDPR. It originally came into force in September 2020, but enforcement in earnest was delayed until August 1, 2021. As with GDPR and PIPL, the LGPD also has an extraterritorial reach.

Similar to GDPR and PIPL, LGDP requires companies to provide individuals with notice about what information the company is collecting and how it is using that information. It also allows individuals to exercise the same rights as GDPR: accessing the information the company has, correcting inaccurate information, getting a copy of their data and having their data deleted. Like GDPR, LGPD also requires companies to have a legal basis for the data collection and processing, as well as to conduct data protection impact assessments and appoint a data protection officer.

LGPD establishes the National Data Protection Authority, which is tasked with issuing regulations pursuant to the statute, and subsequently enforcing the law. It has to date issued some regulations, but there are still areas where regulations are expected.

Other Statutes

In addition to China and Brazil, a number of other countries and territories (including Australia, Hong Kong, Pakistan, Sri Lanka, British Virgin Islands and the UAE) either passed, amended or considered modifications to their privacy regulations. Additionally, Russia increased the penalties for violations of its privacy laws. These laws vary in their breadth – some are focused specifically on issues such as doxing and data breach notification, while others are more comprehensive, like what we see in the LGPD and PIPL.

Implications

Together, these laws form a mixed bag in terms of the international regulatory picture: some countries have detailed laws with active enforcement, others have general laws with spotty and potentially selective enforcement, a third group has very basic or non-existent laws, while yet another group is working to transition between categories. Of those countries with laws on the books, the approach to enforcement is especially diverse. On one end of the spectrum are those countries that do not have a track record of having the ability or seeming desire to enforce their laws. On the other end of the spectrum are those countries that look to be actively pursuing alleged violations, in some instances to a degree that has observers questioning whether there are underlying political or geopolitical motivations.

** Indicates a right that has some limitations based on other statutes or administrative regulations.*

CONTINUED ON PAGE 19 ▸

CONTINUED FROM PAGE 18

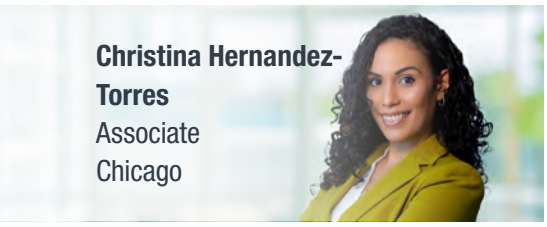
As a whole, these laws reflect a debate about how to regulate a world in which there is an explosion in how much data individuals generate in the course of their daily life and how many ways there is for others to use this data. Among other positions, it reflects the desire of some to limit corporations' ability to harness that data for their own purposes. It also reflects the value that some governments see in being able to keep their citizens' data from leaving their borders and maintaining access to those data assets.

Most likely, 2022 will see more activity on both the legislative and enforcement fronts. Navigating this landscape will be increasingly complicated as the number of laws increases and the enforcement activity continues to get more complex.

Look in on The Status of Passed, Pending and Failed State Comprehensive Privacy Bills

Liz Harding
Shareholder
Denver

Thomas P. Weber
Associate
Denver



Christina Hernandez-Torres
Associate
Chicago

Introduction

After the California Consumer Privacy Act passed in 2018 (CCPA), many states proposed similar comprehensive legislation to protect consumers' data. In light of CCPA, certain states have either enhanced their privacy legislations or drafted new legislation related to consumer data. While not all bills are successfully passed others become laws. The most comprehensive data privacy laws are the California Privacy Rights Act (CPRA), the Colorado Privacy Act (CPA) and Virginia's Consumer Data Protection Act (VCDPA). The laws in these particular states have enacted comprehensive data privacy laws that are comparable.

California, Colorado and Virginia Comprehensive Privacy Laws

Since the passing of the California Consumer Privacy Act in 2018 and the California Privacy Rights Act (*CPRA*), two additional states have followed suit with their own comprehensive privacy laws – the Colorado Privacy Act (*CPA*), and Virginia's Consumer Data Protection Act (*VCDPA*).

The Colorado Privacy Act (CPA) will go into effect on July 1, 2023, and applies to companies that conduct business in Colorado or produces or delivers "commercial products or services that are intentionally targeted to the residents of Colorado," and that satisfies one or both of the following thresholds: (1) controls or processes that personal data of 100,000 or more Colorado residents in a year; or (2) both derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of 25,000 or more consumers.

Virginia's law becomes effective January 1, 2023, the same day as the California Privacy Rights Act (CPRA) which amends the California Consumer Privacy Act (CCPA). The VCDPA applies to businesses that conduct business in Virginia or produce products or services targeted to Virginia residents, and that control or process the personal data of at least 100,000 Virginia consumers. That bar is lowered to 25,000 consumers if over 50% of the business's gross revenue derives from selling personal data.

The recently passed privacy laws in California, Colorado and Virginia have many similarities. For instance, the CPA, VCDPA and the CPRA grant consumers rights, such as rights to access, delete and correct their personal data, data portability, right to know as well as the right to opt-out of the processing of their personal data for certain specified purposes. Like Virginia's CDPA, but unlike CCPA, Colorado's CPA does not contain a private right of action and is only enforceable by the attorney general.

Exemptions

The CPA and the VCDPA adopted the CCPA/CPRA's approach of broadly exempting information governed by the Health Insurance

CONTINUED ON PAGE 20

CONTINUED FROM PAGE 19

Portability and Accountability Act (*HIPAA*) and the Gramm-Leach-Biley Act (*GLBA*). The exact scope of the exemptions varies. For example, the VCDPA creates an exemption for financial institutions and their affiliates regulated under GLBA and for covered entities and business associates governed by HIPAA. This is much broader than the CCPA/CPRA's exemptions for these laws, which apply to regulated information itself rather than to the entities that process them.

Sensitive Information Will Require Special Protection

Like the CPRA and VCDPA, Colorado's CPA provides protection for sensitive data, such as: (1) personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, citizenship or citizenship status; (2) genetic or biometric data that may be processed for the purpose of uniquely identifying a person; or (3) personal data from a known child – an individual under thirteen years of age. Generally, sensitive data may not be processed without consumer consent.

Opt-Out

In addition, identical to the opt-out provision in Virginia's CDPA, Colorado's CPA provides consumers with the right to opt out of the processing of personal data for the following purposes: (1) targeted advertising; (2) sale; and (3) profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer. Beginning on July 1, 2024, controllers that process personal data for the purpose of targeted advertising or the sale of personal data must provide consumers with the ability to opt out through a "universal opt-out mechanism."

The VCDPA also broadens the opt-out right of processing that covers not only sales of personal data but also targeted advertising and profiling. The VCDPA mandates data protection assessments for sales, targeted advertising and profiling or any other processing of sensitive personal data or personal data that presents a "heightened risk of harm to consumers."

Targeted Advertising Growing Area of Concern

While the CCPA/CPRA does not address targeted advertising directly, the CPA and the VCDPA do directly address targeted advertising by requiring controllers to provide an opt-out option for such processing and to conduct a data protection assessment before engaging in the activity.

Obligations for Controllers

Like the CPRA, Virginia's CDPA creates an obligation to confirm processing and broadens its deletion requirement. Unlike the CCPA/CPRA, the obligation to delete personal data covers personal information not only collected from but also collected "concerning" a consumer.

The CPA, similar to the VCDPA, creates a specific duty for controllers. The duties are the following: (1) duty of transparency; (2) duty to avoid secondary use; (3) duty of data minimization; (4) duty of purpose specification; (4) duty of care; (5) duty to avoid unlawful discrimination; and (6) duty to process sensitive data only with the consumer's consent. In addition, similar to the CPRA, the CPA requires companies to conduct data protection impact assessments for certain use cases, including: (1) targeted advertising or profiling that may create risk for consumers; (2) selling personal data; and (3) processing sensitive data.

Conclusion

Although the CPA, VDCPA, and the CPRA privacy laws do not go into effect until the year 2023, the US privacy legislation will likely expand to other states and expand other consumer's rights. Accordingly, businesses should act now to determine their compliance obligations by performing a comprehensive data inventory, reviewing and updating internal and external policies, and reviewing their contracts with vendors and/or other service providers.

Active Bills

As of this writing, there are currently several states with active comprehensive privacy bills. Below is a summary of each pending state bill.

Massachusetts

Bill: S.46 (Massachusetts Information Privacy Act)

The bill applies to businesses that (1) have an annual gross revenue of $10 million or more through 300 or more transactions, or (2) process the personal data of at least 10,000 Massachusetts consumers in a calendar year. Massachusetts's proposed bill contains the following consumer rights: access, correction, deletion, restriction, portability and the right against automated decision-making. Unlike California, Virginia and Colorado, the Massachusetts bill requires opt-in consent before a business can process a consumer's personal data. Covered businesses must provide disclosures to consumers and comply with other transparency requirements, as well as abide by processing limitation requirements. There is a private right of action.

New York

Bill: A 680/ S 6701 (New York Privacy Act)

The bill applies to businesses that (1) have annual gross revenue of $25 million or more, (2) control or process the personal data of at least 100,000 New York consumers, (3) control or process the personal data of at least 500,000 individuals nationwide and 10,000 New York consumers, or (4) derive over 50% of their gross revenue from the sale of personal data and control or process the personal data of at least 25,000 New York consumers. New York's proposed bill contains the following consumer rights: access, correction, deletion, restriction, portability and the right against automated decision-making. Like Massachusetts, the bill contains an opt-in consent requirement. Covered businesses must provide disclosures to consumers, comply with other transparency requirements, and abide by processing limitation requirements. There is a private right of action.

North Carolina (Consumer Privacy Act)

Bill: SB 569

The bill applies to businesses that control or process the personal data of (1) at least 100,000 North Carolina consumers on an annual basis or (2) at least 25,000 North Carolina consumers and derive over 50% of gross revenue from the sale of personal data. North Carolina's proposed bill contains the following consumer rights: access, correction, deletion, restriction, portability and the right to opt out of the processing of personal data for targeting advertising, sales, or profiling. Covered businesses must provide disclosures to consumers, comply with other transparency requirements, abide by processing limitation requirements, conduct data processing assessments and enter into contracts with processors that contain specific requirements for data protection. There is a private right of action.

CONTINUED ON PAGE 21

CONTINUED FROM PAGE 20

Ohio

Bill: HB 376 (Ohio Personal Privacy Act)

The bill applies to businesses that (1) have annual gross revenues generated in Ohio that exceed $25 million, (2) control or process the personal data of 100,000 or more Ohio consumers during a calendar year, or (3) derive over 50% of their gross revenue from the sale of personal data and process or control the personal data of 25,000 or more Ohio consumers during a calendar year. Ohio's proposed bill contains the following consumer rights: access, deletion, restriction, portability and the right to opt out of the sale of personal data. Covered businesses must provide collection notices to consumers, comply with other transparency requirements, and abide by processing limitation requirements. There is no private right of action.

Pennsylvania

Bill: HB 1126 (Consumer Data Privacy Act)

The bill applies to for-profit businesses that (1) have a gross annual revenue of $10 million, (2) annually buy, sell, or share the personal information of 50,000 Pennsylvania consumers, households, or devices or (3) derive 50% of their annual revenue from the sale of Pennsylvania consumers' personal data. Pennsylvania's proposed bill contains the following consumer rights: access, deletion and opt-out of the sale of personal data. Covered businesses must provide collection disclosures to consumers and comply with other transparency requirements. There is a private right of action for security violations by a business.

Failed Bills

The following comprehensive state privacy bills failed in 2021:

Alabama (HB 216), Alaska (SB 116), Arizona (HB 2865), Connecticut (SB 893), Florida (SB 1734 & HB 969), Illinois (HB 3910), Kentucky (HB 408), Maryland (SB 0930), Minnesota (HF 36 & HF 1492), Mississippi (SB 2612), North Dakota (HB 1330), Oklahoma (HB 1602), Texas (HB 3741), Utah (SB 200), Washington (SB 5062 & HB 1433) and West Virginia (HF 3159).

Ransomware Playbook for 2022: Four-Point Plan from the Biden Administration

John C. Cleary
Shareholder
New York

Kayleigh Shuler
Associate
Kansas City

The ongoing ransomware threat continued to capture headlines in 2021, with sophisticated attacks shutting down key sectors of the U.S. economy. A stepped up federal response, drawing upon public and private sector resources, has been rolled out by the Biden Administration.

What happens in a ransomware attack?

In a successful ransomware attack, criminals (typically referred to by privacy professionals as "threat actors") begin their attack by quietly finding a virtual open door into a victim's computer network, such as a vulnerability in the victim's remote connection tools. Once inside, the threat actors move about the victim's network undetected, learning as much as they can about the network's configurations and, in many cases, where "monetizable" or other valuable or irreplaceable information is stored. After surreptitiously extending their reach to as much of the victim's network as possible, the threat actors often steal a copy of data identified as valuable, just before deploying malware that causes all files within its reach to be rendered unreadable (i.e., to be "encrypted"). The threat actors typically drop a virtual ransom note on affected devices, declaring to the victim that it has been attacked and instructing the victim to contact the threat actor and make payment if it (1) ever wants to see its data again, (2) ever wants to re-start or unencrypt frozen data or systems, and/or (3) does not want its sensitive data published on the Dark Web. Although scenarios and outcomes can vary widely, the threat actor is typically motivated by financial gain and has done enough reconnaissance of the victim to understand the types of disruptions and economic loss that can be imposed or threatened to secure such gain.

How was 2021 different?

Ransomware reached the front pages in 2021 and stayed there through two major attacks that caused harm far beyond the targeted company. The oil and gas sector led the way in May 2021 when threat actors shut down operations at Colonial Pipeline – one of the largest gasoline pipeline operators in the country. The outage forced Colonial to shut down operations temporarily, including gasoline shipments to distributors and retailers across the Eastern United States. Markets and consumers took notice, prompting supply constraints, price volatility and innumerable disruptions and economic harms and dislocations over a two-week period.

The meat-processing industry followed the next month, with a ransomware attack on JBS, the world's largest meat processing company, quickly spiraling into shutdowns and other dislocations for farmers, processors and retailers, as well as restaurants and consumers.

These mid-2021 attacks were the most visible of an ever-increasing trend of ransomware attacks with national and international significance, and daunting implications for consumers, public safety and national security.

CONTINUED ON PAGE 22

CONTINUED FROM PAGE 21

What is the current federal government strategy to fight ransomware?

The Biden Administration has indicated that combatting ransomware is among its national security priorities. While the federal sector has long been engaged in the fight against ransomware, October 2021 brought renewed and coordinated efforts by Executive Branch agencies as well as a sizable counter-ransomware coalition, which was convened by the United States in a first-ever 30-nation ransomware summit on October 13-14, 2021. The U.S. Government's four-part counter-ransomware program was outlined on the eve of the conference, as follows (https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware):

- ***Disrupt Ransomware Infrastructure and Actors:*** The Administration is bringing the full weight of U.S. government capabilities to disrupt ransomware actors, facilitators, networks and financial infrastructure.
- ***Bolster Resilience to Withstand Ransomware Attacks:*** The Administration has called on the private sector to step up its investment and focus on cyber defenses to meet the threat. The Administration has also outlined the expected cybersecurity thresholds for critical infrastructure and introduced cybersecurity requirements for transportation critical infrastructure.
- ***Address the Abuse of Virtual Currency to Launder Ransom Payments:*** Virtual currency is subject to the same Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) controls that are applied to fiat currency, and those controls and laws must be enforced. The Administration is leveraging existing capabilities, and acquiring innovative capabilities, to trace and interdict ransomware proceeds.
- ***Leverage International Cooperation to Disrupt the Ransomware Ecosystem and Address Safe Harbors for Ransomware Criminals:*** Responsible states do not permit criminals to operate with impunity from within their borders. The Administration is working with international partners to disrupt ransomware networks and improve partner capacity for detecting and responding to such activity within their own borders, including imposing consequences and holding accountable those states that allow criminals to operate from within their jurisdictions.

This approach has drawn international support but will undoubtedly take time to produce concrete results. There are early signs of progress, however, at least on the U.S. law enforcement front. In Summer 2021, the U.S. Department of Justice announced a new task force aimed at stopping future attacks, known as the Ransomware and Digital Extortion Task Force. And, in the Colonial Pipeline case, the Justice Department used its threat intelligence resources to recover a portion of the ransom payment from the criminal group allegedly responsible for the attack. In another widely publicized ransomware incident involving the software company Kaseya, the Justice Department recently unsealed indictments against a Ukrainian national accused of helping conduct the attack. While these outcomes show promise and may be grounds for a somewhat guarded level of optimism, they remain the exception from prevailing trends. More often, ransom payments are not recovered, and individuals responsible for attacks cannot be located or identified, let alone prosecuted.

Until ransomware attackers are interdicted or deterred, what can businesses do?

In the meantime, in this ever-changing threat landscape, the bottom line for business leaders is: (1) to take all feasible measures to prevent an attack (e.g., frequently reviewing the cybersecurity procedures that both you and your vendors have in place); (2) to maintain and test a comprehensive incident response plan that contemplates legal and law enforcement involvement and that can be engaged as soon as an attack is discovered; and (3) to position yourself to increase cyber resilience and reduce the risk of needing to pay a threat actor if a ransomware attack does occur (*e.g.,* maintaining robust and segregated file backups that can be rolled out if working copies are encrypted).

Data as an Asset: Considerations in Technology Transactions and M&A Due Diligence

Jean Marie R. Pechette
Shareholder
Chicago

Scott M. Tobin
Associate
Chicago

In today's economic environment, it is increasingly important for businesses to derive value from data they collect from and about their customers. This data can be an essential asset in assisting companies to improve or enhance existing products or services, or develop new products or services, identify predictive usage patterns in technology platforms, and target potential sales or marketing opportunities. In addition, technology providers have access to significant amounts of their customers' data in connection with the services they provide, and in many cases seek to use such data for their own business purposes. As a result of this environment, in recent years many companies have sought to acquire businesses that have either robust data sets or strong data analytics capabilities to help develop actionable insights from data.

Businesses need to be prudent regarding their objectives for the collection, use and protection of data, especially in light of stronger enforcement of existing state, federal and international laws and regulations relating to the protection of personal data and the passage and implementation of new privacy laws by various states containing substantially similar requirements to those

CONTINUED ON PAGE 23

CONTINUED FROM PAGE 22

imposed by the European Union's General Data Protection Regulation (*GDPR*) and the California Consumer Privacy Act (*CCPA*), including Virginia's Consumer Data Protection Act (*CDPA*) and the Colorado Privacy Act (*CPA*). While the use of data may present significant opportunities, businesses must be aware of the substantial regulatory, contractual and reputational risks associated with failure to comply with applicable privacy laws. This article will provide tips for best practices for negotiating technology agreements, both from the perspective of technology providers and their customers, as well as guidance regarding key issues to consider with respect to businesses' data use and collection practices in due diligence for M&A transactions.

Data Rights in Technology Agreements

In the negotiation of agreements between software or other technology providers and their customers, it is imperative that terms relating to data collection, use and disclosure clearly state the rights and obligations of the parties. This requires the drafting of carefully crafted language designed to reflect the interests of both parties and to ensure compliance with applicable legal requirements.

Technology providers often seek to secure rights to collect and use a broad range of data from their customers, from metadata relating to the use of any software products to the information disclosed by such customers for processing. Such broad rights permit these providers to develop or enhance their products or services, perform analytics regarding their customer base and otherwise commercialize data for their business purposes. Many companies have begun to utilize a "give to get" model, in which customers must contribute data to be able to use functionality in a software, such as shared databases or analytics dashboards that aggregate data across such providers' customer base to provide benchmarks and other insights. For example, certain procurement management software providers offer functionality to permit their customers to view analytics dashboards comparing payment terms and amounts by type of vendor across the provider's customer base. In "give to get" models, such customers may only access these dashboards if they agree to share data for inclusion within the dashboards. Such models benefit technology companies by removing ambiguity regarding data rights and expressly permitting data usage in a manner that enhances the provider's products and services, but may present difficulties for their customers, as discussed below.

On the other hand, the companies using such technology products or services have an interest in limiting data collection and use for purposes solely as necessary to enable the technology provider to deliver the products or services being purchased. In many cases, the disclosure of data carries risk, whether it is personal information subject to state or federal privacy requirements or confidential financial information that could result in harm to the company if disclosed. Additionally, technology providers often seek broad representations and warranties from their customers regarding the customer's right to disclose data to the vendor and permit certain secondary uses and further disclosures of data by the technology vendor. At times, these terms also pose risk to the extent they conflict with any agreements or understandings between the customer and the consumers or data subjects from whom it collects data (such as a privacy notice or an authorization to disclose data). As a result, customers of technology vendors should attempt to limit any use or disclosure of information to the extent possible and seek additional protections regarding the confidentiality of such data.

Such protections often include requirements that any data used for any purpose other than the direct provision of products or services to the company be aggregated and anonymized (i.e. that the data, as used, does not identify the company, any consumer or any information unique to either the company or any consumer). These limitations provide protection against the improper disclosure of personal information in violation of applicable law and help mitigate the risk of disclosure of any other confidential information. However, the parties must ensure that such aggregation and anonymization is conducted in accordance with the various standards imposed by applicable laws to which they are subject. For example, GDPR imposes certain requirements relating to the "anonymization" of personal data, while entities subject to HIPAA must comply with specific requirements regarding the de-identification of Protected Health Information (PHI) via either the "Safe Harbor" or "Expert Determination" methods of de-identification, and further, Business Associates must abide by the limitation that they only de-identify or aggregate the PHI of multiple Covered Entities upon receipt of explicit permissions to do so from the applicable Covered Entity.

Another issue that arises from the use of aggregated or anonymized data relates to the ownership of such aggregated or anonymized data. The ownership of data is a distinct issue from use and disclosure rights under privacy laws but also plays a key role in the ability of technology providers to derive value from customer data. Generally, customers of technology providers seek to and do retain ownership of the original data disclosed to technology providers in connection with the use of such providers' products and services. The ownership of aggregated or anonymized data is a more complex matter - technology providers often seek to own such data to allow for flexibility in the use of the data for their own business purposes. Conversely, many customers prefer to retain exclusive ownership of any data or new technology derived from the original data (particularly any personal or otherwise sensitive data) they disclosed to the service provider. However, though such customers may not be willing to relinquish ownership, they may instead be willing to grant a limited license to the service provider to permit the use of any anonymized aggregated data in connection with the delivery or enhancement of the products or services used by the customer. This way the customer as well as other customers of the provider benefit from the use of the data.

More broadly, the use of data by technology providers raises a number of issues regarding intellectual property rights in software or other technology created through the use of or derived from the use of their customers' data. If a technology provider uses its customer's data (whether the original data provided or any anonymized or aggregated derivatives of such data) to create any software (or enhancements to existing software), algorithms, models or other commercially valuable materials, the parties will need to determine ownership rights to such newly created intellectual property. The resolution of this issue is dependent on a number of factors, including the nature of the data, relative bargaining power of the parties, whether anything produced is intended to be a work product created specifically for the customer, contributions from the respective parties of assets or other resources in connection with the development of the new technology and scope of intended data use.

In addition to the foregoing, technology agreements which involve the technology provider's access to and use of data also implicate a number of issues relating to the allocation of risk, data security obligations and responsibilities of the parties upon termination of the agreement. The following checklist provides a non-exhaustive summary of potential key issues and questions for review in connection with terms implicating data usage and ownership rights in technology agreements.

CONTINUED ON PAGE 24

CONTINUED FROM PAGE 23

Issues for Review in Technology Agreements

- What is the nature of the data to be disclosed? How sensitive is the data (*e.g.,* does it relate to an individual's medical history)?
- What laws and regulations are applicable to the data, and what obligations to protect the data do such laws and regulations impose?
- For what purposes is the technology provider permitted to use or disclose data provided by its customer?
- Do such uses and disclosures conform with the commitments made by the customer to any consumers or other data subjects (e.g., patients or clinical trial participants) from whom it collected data?
- Does the agreement permit the technology provider to anonymize and/or aggregate any customer data? If so, which party owns this derived data?
- If the technology partner creates any new intellectual property, such as software, algorithms, models or other materials using or derived from customer data, which party owns such new intellectual property? Is joint ownership of such intellectual property with potential cross-licensing rights a feasible alternative to exclusive ownership by one party?
- Upon termination, does the agreement require the technology provider to return or destroy data disclosed by its customer? What is the scope of this requirement (i.e. does it only include the original data or any aggregated or anonymized data as well)? If the technology provider is unable to return or destroy any data (e.g., if it has been aggregated with the data of other customers and thus extraction is not feasible or would change the outcomes or analysis?), what obligations regarding the protection of data will survive termination?
- How will the parties allocate risk for improper use or disclosures of data?
- Is the technology provider obligated to indemnify its customer for claims relating to data breaches or uses of data in violation of applicable law? Is the customer required to indemnify the technology vendor for the customer's disclosure of data to the vendor which it does not have the right to make?

As discussed below, the ownership of any data is a key issue in the performance of diligence in connection with M&A transactions, as acquirers will need assurances that the selling company has appropriate rights to its data.

Considerations in M&A Due Diligence

It is essential that any company seeking to acquire another where the target company's data is a key asset perform thorough due diligence regarding such company's data collection, use and safeguarding practices.

First and foremost, the acquirer must ensure that the target company has the appropriate rights to collect, disclose and use any data that it does collect or has collected and permit use for secondary purposes, such as creating derivative works from the original data collected. If the target company collects personal information directly from consumers, the acquirer must ensure that the target collected and uses such personal information in accordance with applicable law. This includes ensuring, where applicable, that any personal information was collected in accordance with the target's privacy notice and contractual arrangements, that such information is only used for the purposes described in the privacy notice and that any legally-required requests for the deletion or opt-out of the disclosure of such information are honored.

If the target collects data from other businesses in the course of providing services to such businesses, the acquirer should ensure any such data is only used as permitted by the applicable agreements with such customers, as well as applicable law. Additionally, any diligence should identify any restrictions on the disclosure of data to third parties, as such restrictions may limit the transferability of any data depending on the structure of the merger or acquisition. Further, the acquirer should review any terms relating to ownership of any aggregated or anonymized data. If the target's customer retains ownership of such data and is granted a license for its use, such license will likely be subject to any restrictions on the assignment or transfer of the underlying agreement.

Any such diligence should involve the review of the target company's consumer-facing privacy notice (if applicable), internal policies and procedures relating to data collection, use and security, and its relevant contracts. The diligence should also review the target company's history, including any actions taken against it for past violations of privacy law or any data breaches. However, a review of any legally required documentation is likely to be insufficient, as acquirers must have certainty that the target is complying with any privacy notices, contracts or policies in practice. Accordingly, the acquirer should review any books and records of the target company to assess the target's compliance with its stated practices, and perform testing on the target's security controls to review potential vulnerabilities.

Sellers must also conduct diligence regarding their data assets to mitigate risk and ensure the proper transfer of their assets or ownership interest. Most importantly, sellers must ensure that they in fact have the right to sell, license or transfer any data which will be included in the sale. This includes a review of contracts with data providers to ensure the terms of such agreements permit the sale or disposition of any data, and to permit an opportunity to amend such agreements if required before any potential issues impede the ability of the seller and its acquirer to consummate the transaction. Where applicable, such efforts may also include the review and revision of privacy notices to permit the transfer of data to the acquirer, and the remediation of any potential non-compliance with internal policies and procedures regarding data usage and protection.

The purchase agreement in an M&A transaction will likely include a number of representations and warranties with respect to the seller's ability to transfer data, and its data collection, usage and protection practices. Acquirers generally seek strong warranties regarding the seller having the right to sell or transfer the data to be included within the sale, the seller's compliance with applicable privacy law and that there is no pending litigation or enforcement action against the seller relating to its data use practices. Sellers prefer to limit such warranties by adding knowledge qualifiers, limiting the time period for which such warranties are effective (for example, by stating that the seller is compliant with applicable law "as of the effective date" of the transaction).

The following checklist provides a non-exhaustive summary of potential key issues and questions for review in connection with data usage and ownership in M&A transactions.

Issues for Review in M&A Transactions

- What is the nature of the data to be disclosed? How sensitive is the data (*e.g.,* does it relate to an individual's medical history)?

CONTINUED ON PAGE 25

CONTINUED FROM PAGE 24

- What laws and regulations are applicable to the data, and what obligations to protect the data do such laws and regulations impose?
- How will the parties allocate risk for improper transfers or disclosures of data?
- Does the seller have the right to transfer the rights to any data which it owns or licenses under both applicable law and any agreements with the seller's data providers?
- Is the seller compliant with applicable privacy law, and does it comply with its privacy notice and internal policies and procedures? Does the seller have any prior actions taken against it alleging violations of privacy law, or has it suffered any data breaches?
- Do the representations and warranties in the purchase agreement reflect the foregoing?
- Is the selling party obligated to indemnify its purchaser for claims relating to data breaches, violation of applicable privacy law, or failure to obtain the right to sell, license or transfer any data which will be included in the sale?

Conclusion

The use of data provides significant opportunities for businesses yet comes with regulatory risk and many contractual issues to consider. Technology providers and their customers must carefully review data usage and ownership terms in their agreements to address a wide range of issues and meet the needs of each party. Additionally, the parties in M&A transactions must each conduct diligence to ensure the selling party's compliance with regulatory and contractual requirements, internal procedures, and to ensure the selling party has appropriate rights to transfer ownership or license rights to such data. By taking proactive measures to address these issues, businesses can mitigate risk and help realize the potential offered by data.

#Compliance: Legal Pitfalls in Social Media Influencer Marketing


Leslie F. Spasser
Office Managing Partner
Atlanta


Spencer R. Wood
Shareholder
Chicago


Gabriella Mas Bell
Associate
Atlanta


Ephraim T. Hintz
Associate
Los Angeles

As seen in recent years, social media influencer marketing can lead to a meteoric rise in popularity for a company and its brand. Whether an Instagram post by that famous family in Calabasas or a TikTok video from a micro-influencer, influencer marketing can do wonders to promote the visibility of a brand. As a result, it has grown into nearly a $14 billion industry according to Influencer Marketing Hub.

At its core, influencer marketing involves a company leveraging the popularity of an influencer (i.e., a social media personality with a loyal following) to promote its products or services. In exchange, the company compensates the influencer with payment, free goods, services or other benefits.

Influencer marketing extends well beyond celebrities who have millions of followers. Companies frequently engage ordinary people with a small following in a niche category. The industry generally categorizes influencers into four groups based on the size of their social media following: mega (>1 million followers), macro (100k-1M followers), micro (10k-100k followers) and nano (<1k-10k followers).

While companies (i.e., advertisers) are drawn to influencer marketing for myriad reasons, including its lower cost and perceived ability to attract better customers, those engaged in influencer marketing should be cognizant of the legal and regulatory obligations that govern all parts of the ecosystem, including the advertisers, parties playing an intermediary role (e.g., marketing agencies) and the influencers themselves.

Legal and Regulatory Obligations

Currently, social media influencer marketing is primarily regulated by the Federal Trade Commission (*FTC*) pursuant to its authority under Section 5(a) of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce" (15 U.S.C. Sec. 45(a)(1)). The Food and Drug Administration (*FDA*) is also involved when marketing involves prescription drugs and certain medical devices (see e.g. 21 CFR 202.1).[1]

Federal Trade Commission

In 2009, the FTC published Endorsement Guides ("the Guides") to provide guidance to advertisers, intermediaries and endorsers (including influencers) regarding Section 5's application to advertisements relying upon endorsements and/or testimonials and to give illustrations of best practices to facilitate compliance with Section 5's requirements (see 16 CFR 255). The Guides consider an endorsement to be "any advertising message (including verbal statements, demonstrations, or depictions of the name, signature, likeness or other identifying personal characteristics of an individual or the name or seal of an organization) that consumers are likely to believe reflects the opinions, beliefs, findings, or experiences of a party other than the sponsoring advertiser, even if the views expressed by that party are identical to the sponsoring advertiser." (16 CFR 255.0(b)). As

[1] Potential claims under the Lanham Act for unfair competition are outside the scope of this article.

CONTINUED ON PAGE 26

CONTINUED FROM PAGE 25

more fully explained in the Guides, compliance with Section 5 of the FTC Act requires, in part:

- disclosure of a material connection between an influencer and the advertiser that could materially affect the weight or credibility of the endorsement;that endorsements reflect the influencer's honest opinions and experiences;
- that an advertiser does not distort the influencer's opinion or experience or present an endorsement out of context;
- that an influencer must have been a bona fide user of a product when the endorsement was given and the advertiser may continue to run an ad using such endorsement only if it has good reason to believe the influencer remains a bona fide user;
- that claims regarding the performance of a product or service have adequate substantiation, which may require competent scientific evidence;
- that claims regarding one or more influencers' experience with a product or service are representative of what consumers generally can expect if they use such product or service; and
- if an influencer is held out to be an expert, their qualifications must actually give them the expertise they claim to possess and such expertise must have actually been exercised in evaluating the particular features of a product.

In addition to describing the requirements of Section 5 of the FTC Act, the Guides provide numerous examples of compliant and non-compliant behavior.

Beyond the Guides, the FTC has brought numerous enforcement actions that further inform the steps that advertisers and influencers should take to avoid legal violations. By way of example, in March 2020, the FTC filed a false advertising lawsuit against Teami – a seller of tea and skincare products – alleging the company used false or unsubstantiated claims (including endorsements from social media influencers) about the efficacy of its products and failed to disclose a material connection with the influencers who provided endorsements. In its complaint, the FTC asserted that Teami's advertising (including influencers' social media posts) claimed:

- its tea product treats cancer, decreases migraines and reduces cholesterol; and
- its 30-day detox product results in an average of 5 to 20 pounds of weight loss, and that substantial weight loss could result from only drinking the tea.

The FTC asserted that these and other claims in the advertising were false or misleading or not substantiated when made. The FTC also alleged that Teami failed to adequately disclose that the influencers were paid to endorse the tea products. Teami and the FTC entered into a $15.2 million settlement (all but $1 million was suspended), which included an ongoing obligation to establish a program to monitor influencers and a 10-year compliance reporting obligation.

Notably, advertisers as well as intermediaries (i.e., marketing agencies) and the individual influencers can be liable for violations of Section 5. However, to date, the FTC has focused most of its enforcement actions on the advertisers, not the individual influencers.

In the above Teami case, while not bringing a claim against the influencers the FTC did send them warning letters advising that any endorsement must make obvious the financial or other relationship they have with the brand. In this instance, the FTC alerted the influencers that "clear and conspicuous" disclosure required that their Instagram posts include such disclosure where it can be seen by a consumer without having to click "more" to see the entirety of the post.

Food and Drug Administration

Under the FDA's regulations, advertisements may not (among other things) overstate a drug's benefits, downplay risk information or make a claim that is not supported by adequate evidence. Although the FDA has not adopted formal influencer-specific guidelines like the FTC's Guides, in 2014 the agency prepared a non-binding draft of certain guidance, titled "Internet/Social Media Platforms: Correcting Independent Third-Party Misinformation About Prescription Drugs and Medical Devices" (https://www.fda.gov/regulatory-information/search-fda-guidance-documents/internetsocial-media-platforms-correcting-independent-third-party-misinformation-about-prescription).

Like the FTC, the FDA so far has focused its enforcement actions on advertisers rather than the influencers. In one matter, the FDA sent a warning letter to the maker of Diclegis, a medication used for the treatment of nausea and vomiting during pregnancy. Kim Kardashian partnered with the company to promote the drug and posted favorable comments on Instagram. Although the post included a link to the company's safety information, the FDA requires risks to be included with the promotion and not via a separate link. The FDA required the company to take remedial steps, which included issuing corrective messages through the same media channels. Following the FDA's action against the company, Kardashian issued a subsequent Instagram post that included the drug's risk disclosures.

Other Legal Risks

Influencers and companies that use their endorsements also should take precautions to avoid liability for infringing third-party intellectual property or publicity rights. While a celebrity mega influencer may well have a sophisticated team of advisors helping them craft endorsement messages, oft-used macro, micro and nano influencers may not be familiar with the legal implications of incorporating into social media posts any images, music, video or graphics that do not belong to them.

Similarly, the tenor of social media banter – while possibly a characteristic that endears influencers to their followers – could run afoul of libel laws or implicate individual rights of privacy (e.g., portrayal of someone in a false light).

Risk Mitigation

Influencer Contracts

When engaging an influencer for marketing services, there are several contractual provisions that can help ensure compliance with applicable legal and regulatory obligations and protect against inappropriate conduct. Generally, a company-favorable influencer agreement should include:

- An express obligation that the influencer comply with applicable laws (including, the FTC Guides). With micro and nano influencers, it may be advisable to include more prescriptive compliance requirements (such as the obligation to conspicuously disclose any material connection to the advertiser in clear language within the endorsing post), as these influencers may not be familiar with the applicable requirements.
- A right to audit the influencer posts for compliance and to require the influencer to modify or remove non-compliant posts.
- A morals clause prohibiting the influencer, their affiliates and family members from

CONTINUED ON PAGE 27

CONTINUED FROM PAGE 26

creating or partaking in content or conduct that may reflect negatively on the advertiser. The agreement should include the right to immediately terminate an influencer's contract for breach of the morals clause.

- Clear language designating the influencer as an independent contractor, and not an employee or agent of the advertiser or intermediary. Note, however, that merely designating the influencer as an independent contractor will not control if the actual circumstances show that the influencer was treated as an employee. Although there is no bright-line test, the more control a company exerts over an influencer the more likely a court may find that an employment relationship exists. Also note, in some circumstances, advertisers can be liable for acts of influencers even though they operate as independent contractors.
- A clause obligating the influencer to cooperate with the company in connection with any investigation by a regulatory authority. Such clause should include language that obligates the influencer to take remedial actions directed by regulators, such as issuing corrective social media posts.

A word of caution: Exercising a level of oversight with respect to social media content posted by influencers can be a double-edged sword. On one hand, training and monitoring the content posted by an influencer can help keep a marketing campaign in compliance with regulatory and legal obligations. On the other hand, not only can exerting a high degree of control turn an intended independent contractor relationship into one that is deemed an employment relationship, but such control with respect to content can also risk the advertiser losing immunity that might otherwise apply under Section 230 of the Communications Decency Act. Careful analysis should be undertaken with respect to the terms of a social media influencer agreement.

Insurance for Influencer Marketing

Unlike the traditional, "Mad Men-esque", style of marketing in which companies seek professional advertising firms to create grandiose, elaborate marketing campaigns distributed by the company, the influencer marketing style exists at an informal level with the campaign consisting of the influencer creating and distributing social media posts and brand mentions. Historically, commercial liability policies were created with the traditional style of marketing in mind and protected against losses attributable to a company's direct marketing campaign. These traditional commercial policies may not cover damages attributable to influencer marketing. Prior to engaging an influencer for marketing services, the company should consider purchasing or upgrading its commercial liability insurance to protect against direct, consequential or incidental damages arising from an influencer marketing campaign. For additional protection, companies can also purchase director and officer liability insurance shielding the company, its directors and officers from third-party claims stemming from an endorsing post or an influencer's conduct.

Conclusion

There is no question that influencer marketing can benefit brands, engage consumers and drive sales. However, as we have described in this article, requiring and enforcing influencer compliance with legal and regulatory obligations play a critical role in mitigating the risks associated with influencer campaigns and ensuring that the campaign does not backfire by causing liability or negative publicity. Because the influencer landscape is subject to a complex set of regulations, we recommend consulting legal advice prior to engaging influencers to promote a company's products and services.

Content Distribution on the Blockchain: A Case Study in the Use of Smart Contracts

I. What we Saw in 2021

The year 2021 saw enormous growth in the use, interest and diversification of blockchain technologies. From the rise of non-fungible tokens (NFTs) as a digital art medium to the establishment of numerous bespoke cryptocurrencies, blockchain stood at the nexus of intellectual property, content creation and finance. The year 2022 will be another exciting year in blockchain as the gap between traditional contracting and contracting using blockchain continues to narrow. Polsinelli's Technology Transactions team was at the forefront of bridging that gap in 2021 through a novel fusion of Ethereum's smart contracting capabilities with sophisticated in-bound and out-bound content licensing. This article sets forth the fundamentals of how Ethereum blockchain was used to navigate complex licensing issues arising from the creation and hypothecation of digital assets.

II. How Ethereum Smart Contracts Work

Foundationally, Ethereum blockchain is a platform that uses distributed ledger technology to execute and validate smart contract transactions. Each transaction is called a "block" and connects with the previous transaction as the next link in the chain of transactions (hence the term "blockchain"). Each participant in a blockchain holds a complete copy of the entire ledger and all of its transactional history (NFTs use this feature, for example, to prove digital art ownership and provenance).

CONTINUED ON PAGE 28

CONTINUED FROM PAGE 27

When a new transaction or a change occurs to the blockchain, the new transaction must be approved by the blockchain network using a consensus mechanism. The consensus mechanism used depends on whether the blockchain is privately or publicly accessible. A blockchain is public when it is open to all participants and does not require permission from others. A private blockchain requires permission to transact from a private party authorized to transact on the network. Because of this permission structure, private blockchains may be subordinated to written agreements between parties related to the use of the blockchain.

III. A Novel Approach to Content Licensing

Leveraging the ability to establish top-level written agreements on a private blockchain, Polsinelli developed a novel licensing model for digital assets (Assets) on behalf of an independent gaming platform (Platform). The process starts with a traditional content license and hosting agreement (License Agreement) that transfers Assets to the Platform which are then published on the Platform's web-based digital asset marketplace. The License Agreement further establishes key transactional issues such as intellectual property rights, the division of royalties between the Platform and content creator, the number of License Tokens (described below) available per Asset, the cost of each License Token to an end user and the overall process by which the Platform will sublicense and market the Assets to end users. Once the Asset is published on the Platform, an end user can procure access to the Asset by purchasing a License Token. The License Token serves as the gatekeeper for accessing Assets. If the end user does not have the required License Token, the Platform provides the end user with ability to purchase said License Token and once the License Token is added to the end user's digital wallet, the end user can access the Asset (subject to any stipulations on use e.g., end user license agreements). This process is executed via Ethereum smart contract, which manages both the distribution of the Asset to the end user and the real-time payment of royalties to the content creator and the Platform.

IV. A Bottom-Up Approach to Content Creation

End user use and consumption of Assets is not the only benefit the Platform offers. Through the Platform, content creators can list, sell or license their Assets, which can then be leveraged by other content creators to build new digital content in a collaborative or derivative manner. As digital content creators generate new content, the Ethereum smart contracts tied to the underlying Assets comprising the new content are again leveraged to facilitate real-time royalty payments for the licensing and sale of the new digital content as whole. This process creates a decentralized model allowing for a bottom-up approach to content creation and monetization. This, in turn, creates additional incentive for independent creators to develop new and diverse content. Content creators also have the option of developing new content as a "work made for hire" directly for the Platform under a content authoring agreement. This approach can award a larger initial payment to the creator but a smaller royalty on sublicenses to end users. That gives flexibility to how content creators engage in the development and monetization of their works.

V. Looking Ahead in 2022

We expect the model above will be further refined in 2022 and deployed in other unique ways for the distribution and monetization of digital content. We foresee, for example, the creation and management of decentralized autonomous organizations (DAOs) that leverage smart contracts to raise capital for the creation and sale of digital assets. In theory, a DAO could award voting share tokens (similar to the License Tokens discussed above) to investors according to their respective contributions to the DAO. Investors would then be able to vote their tokens on unique content creation proposals with smart contracts reviewing the votes and the corresponding tokens to determine if the proposal is approved. If approved, funds from the DAO would then flow in real time to content creators to fund their digital asset creation. Naturally, royalties resulting from the sale of these digital assets would be automatically distributed to investors according to their respective voting share tokens.

VI. Conclusion

Using Ethereum smart contracts and distributed ledger technology to execute transactions on the blockchain to establish rights in the use and distribution of content allows both content creators and content hosting services to financially benefit from sublicensing of content to end users and relicensing content to other creators. In 2022, Polsinelli will both assist digital content creators in refining and deploying this model in the distribution of their content and guide platforms through the process of leveraging private blockchains to manage the distribution of digital content to consumers and royalties to content creators.

ABOUT OUR TECHNOLOGY TRANSACTIONS & DATA PRIVACY PRACTICE

Polsinelli's Technology Transactions and Data Privacy team is comprised of over 50 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

Kathyrn T. Allen
kallen@polsinelli.com

Gregory L. Cohen
gcohen@polsinelli.com

Jeffrey E. Fine
jfine@polsinelli.com

Liz Harding
eharding@polsinelli.com

Jean Marie R. Pechette
jpechette@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

Colin H. Black
cblack@polsinelli.com

Kelsey L. Brandes
kbrandes@polsinelli.com

Alexander D. Boyd
aboyd@polsinelli.com

Reece Clark
rclark@polsinelli.com

John C. Cleary
john.cleary@polsinelli.com

Christina Hernandez-Torres
chernandez-torres@polsinelli.com

Ephraim T. Hintz
ehintz@polsinelli.com

L. Hannah Ji-Otto
hji-otto@polsinelli.com

Noor K. Kalkat
nkalkat@polsinelli.com

Libby M. Marden
lmarden@polsinelli.com

Aaron A. Ogunro
aogunro@polsinelli.com

Jessica L. Peel
jpeel@polsinelli.com

Anna K. Schall
aschall@polsinelli.com

Kayleigh S. Shuler
kshuler@polsinelli.com

Caitlin A. Smith
casmith@polsinelli.com

Scott M. Tobin
scott.tobin@polsinelli.com

Thomas P. Weber
tweber@polsinelli.com

POLSINELLI. What a law firm should be.℠