TECH TRANSACTIONS & DATA PRIVACY

2023 REPORT

We are poised at the beginning of 2023 with keen anticipation for what this next year will bring.

While the global pandemic that altered so many areas of our lives has finally moved to the background, the new normal has yet to fully materialize. Keeping that context in mind, 2022 saw the beginning of a "crypto winter" but also a proliferation of new technology in areas such as edge computing and artificial intelligence.

The ever-increasing collection, sharing and use of data this past year led to an increasing recognition of the importance of data protection and responsible data handling practices. Public awareness of the risks associated with the collection and use of personal information has never been higher and, consequently, governments around the world implemented or proposed a number of new privacy laws and regulations in 2022. We expect that trend to accelerate this year.

Polsinelli's Technology Transactions & Data Privacy 2023 Report mirrors the growth and depth of our legal practice in this area. Over 40 lawyers have contributed to 19 thought-provoking articles covering a range of important issues – from data rights and usage, analysis of new privacy laws and regulations, ransomware developments, blockchain technology, non-fungible tokens and the latest privacy litigation trends.

As we look toward the future, our attorneys will continue to be at the center of these developments. We take pride in our roles and responsibilities as we work with our clients in 2023 on the complex challenges of the technology and data privacy landscape.

Sincerely,

Greg Kratofil, Jr.
Chair – Technology Transactions & Data Privacy
Note: The above was written with the help of the ChatGPT chatbot launched by OpenAI in November 2022.

Survey of International Privacy Laws

Pavel (Pasha) A. Sternberg
Principal
Los Angeles, San Fransisco

Christina Hernandez-Torres
Associate
Chicago

Introduction

Recent years have brought a dramatic increase in the number of countries that have comprehensive privacy and data security laws. As the world has become increasingly digital, privacy and data protection have become a greater concern for consumers and governments alike. A regulatory scheme that was — as recently as only a few years ago — found primarily only in Europe is now seen across the globe.

It is no surprise then that companies whose business spans the globe are finding international privacy laws confusing and burdensome. This is going to be especially true in 2023 when countries like China, Brazil, India and Canada are set to further complicate the global data privacy stage. This article is focused on providing an overview of these upcoming changes to better orient companies toward compliance obligations.

China's notable cross-border data transfer rules update

As discussed in Polsinelli's Tech Transactions & Data Privacy 2022 Report, China's Personal Information Protection Law was passed in 2021 and requires companies to have a comprehensive privacy compliance framework. Included in that framework is a restriction on cross-border data transfers. In June and July 2022, two regulators — the Cyberspace Administration of China and the National Information Security Standardization Technical Committee — issued regulations for transferring data out of China.

The PIPL provides that personal information can be transferred outside China only after the data subjects have given their informed consent, the company carries out an impact assessment and an appropriate transfer mechanism is used. The transfer mechanism that is required depends on the type of data being transferred, the volume of individuals whose personal information is being transferred and the role played by the company conducting the transfer in the Chinese economy.

In many cases, this analysis will result in a company having to get a security assessment approved by the CAC. This is the case if: (1) the data being transferred is "important data";[1] (2) the company is a "Critical Information Infrastructure Operator"; (3) the company processes the personal information of more than one million individuals and transfers any of it abroad; or (4) in a calendar year it transfers either 100,000 individuals' personal information or 10,000 individuals' sensitive personal information abroad. To get an approved security assessment, a company will have to submit an application containing a self-assessment to the provincial CAC office, which will conduct an initial check and then send it to the national CAC office for approval. The entire process is supposed to take approximately 60 days.

In situations where a security assessment is not required, a company can conduct a cross-border transfer after either obtaining a personal information protection certification from a professional institution designated by the CAC or entering into a regulator-approved standard format data transfer agreement with the overseas recipient of the data being transferred. These cases are primarily for internal cross-border transfers within one multinational company or one economic/business entity, as well as for cross-border transfers by non-Chinese entities that analyze and assess the behavior of the individuals located in China subject to the extraterritorial jurisdiction of the PIPL.

The Chinese government's focus on data localization is made evident by these regulations. At a minimum, all three transfer mechanisms require controls around data security and the further use or disclosure of

1 The regulations define this as "data that, once tampered with, destroyed, leaked, illegally obtained[] or illegally used, may endanger national security, economic operation, social stability, public health and safety, etc."

Table of Contents

CONTINUED ON PAGE 3

CONTINUED FROM PAGE 2

data once it leaves China. In cases where it is appropriate, the standard format data transfer agreement is going to be the easiest and simplest approach for cross-border transfers, but it brings with it the burden of ensuring that the contract is held up. To that end, companies should be aware that noncompliance with the PIPL is subject to hefty fines and has already been used aggressively. Most prominently, in July 2022, the CAC fined the company Didi Global just over 8 billion yuan ($1.2 billion) for violating cybersecurity and data laws.

Brazil's website cookies and personal data protection guidance

An overview of Brazil's General Personal Data Protection Law was also included in Polsinelli's Tech Transactions & Data Privacy 2022 Report and noted that Brazil's National Data Protection Authority was charged with issuing regulations to clarify the statute's requirements. Since then, the ANPD has issued a few guidance documents related to the statute. First, in January 2022, the ANPD issued a resolution that reduced the compliance obligations for so-called small-sized processing agents, including removing the requirement to appoint a data protection officer, simplifying the policies that they must have and lengthening the statutory timelines to respond to customer inquiries and data incidents.

Additionally, in October 2022, the ANPD provided nonbinding guidance on cookies and other tracking technologies that process personal data. This guidance provides that:

- Personal data is broader than basic identifiers like names and phone numbers, and the definition includes behavioral profiles that can be cross-referenced to other data sets.
- The only two legal bases for use of cookies are consent and legitimate interest.
- Cookie collection subject to a legitimate interest basis is subject to opt outs only in some situations. The guidance also suggests that analytics tools are acceptable on a legitimate interest collection basis.
- Advertising and behavior tracking cookies are not "necessary" tools and are therefore subject to consent.
- Notice informing individuals about the categories of cookies, their purposes, third parties involved, retention period, data subjects' rights and other requirements under the LGPD should be provided.
- First-level banners (user-facing banners on landing pages) with basic information followed by second-level banners (opened through first-level banners) can be implemented to simplify users' viewing experience.

As in China, companies should be aware that noncompliance with the LGPD will result in fines of up to 2% of a business's annual revenue to a maximum of 50 million Brazilian reais per violation (approximately $9 million).

Other pending international privacy updates for 2023

Canada

Canada is a country that has had a prominent privacy law, the Personal Information Protection and Electronic Documents Act, for many years. In June 2022, new laws — the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act — were proposed to modernize the current federal privacy framework. Together, these new laws recognize individuals' privacy rights while acknowledging the benefits of data collection and use, and they create an enforcement mechanism to balance these sometimes competing interests.

The proposal has to go through the legislation process and many changes may result from this, but at a high level, the goals of the statutes are to: (1) give consumers more visibility into how personal information is collected and used, and the ability to exert more control over those activities; (2) provide minors with extra protections and impose more limitations on the collection and use of their personal information; and (3) allow for the safe and regulated use of artificial intelligence when it comes to data processing.

Canada has traditionally been at the forefront of privacy law regulation, so monitoring the progress of this legislation will be important to understanding how regulations in this space will evolve over the coming years.

India

In August 2022, India withdrew a 2019 privacy bill because of the negative feedback received from businesses and privacy advocates on its stringent cross-border requirements. Just three months later, in November 2022, a replacement bill — the Digital Personal Data Protection Bill 2022 — was proposed. The updated proposal would create more user-friendly cross-border data transfer requirements for certain countries and territories, and it removes the requirement to store critical personal data in India that was included in the 2019 bill. The 2022 bill would also narrow the scope of data protection afforded to consumers compared with what was in the previous version.

Takeaways

As we begin 2023, it is becoming increasingly important for businesses to assess the countries from which they collect data and how they are transferring that data internally if those transfers involve crossing international borders. As always, they must also review and understand what data they collect as well as how that data is processed, used, shared and sold. The places where these activities occur and what those activities are will determine the rules that companies will have to abide by as compliance increasingly becomes a complicated and burdensome endeavor.

U.S. State Privacy Law Update

Catherine (Cat) Kozlowski
Counsel
Seattle, Los Angeles

Aaron A. Ogunro
Associate
Chicago

In 2023, new comprehensive data privacy laws come into effect in five states — California, Colorado, Connecticut, Utah, and Virginia. The California Privacy Rights Act of 2020 (CPRA) and the Virginia Consumer Data Protection Act (VCDPA) kicked in on January 1, 2023, to be followed by the Colorado Privacy Act (CPA) and the Connecticut Personal Data Privacy and Online Monitoring Act (CTDPA) on July 1, 2023, and the Utah Consumer Privacy Act (UCPA) bookending the year on December 31, 2023 (collectively, the Acts). The Acts implement several new compliance obligations for applicable entities. We highlight the most important ones below.

Vendor agreements

One of the bigger undertakings that entities will have to tackle is updating downstream vendor agreements. The Acts contain a host of mandatory contract requirements for downstream vendors, including:

- Imposing a duty of confidentiality on vendors.
- The right for a controller to:
  - Assess/audit a vendor's privacy and security obligations.
  - Object to a vendor's new or replacement subprocessors.
- Requirements for a vendor to:
  - Identify specifics about the vendor's data processing (e.g., the nature and purpose of processing, the duration of processing, and the types of data being processed).
  - Return or delete personal information at the controller's direction.
  - Implement appropriate technical and organizational measures.
  - Assist with data protection assessments.
  - Notify the controller if the vendor determines that it can no longer meet its obligations.
- Prohibitions against:
  - The reidentification of de-identified data.
  - The service provider or contractor selling or sharing personal information it receives from or on behalf of the entity.
  - Uses other than those expressly permitted in the contract.
  - The combining of personal information that the vendor receives from other persons or customers.

To comply with the Acts, entities must include these terms in their template data processing agreements and work to amend the data processing agreements they currently have in place with downstream vendors.

The Acts also provide that an entity must pass down a consumer's request for access, deletion, or correction across all vendor data flows. CPRA regulations specifically call out a business's obligation to instruct all service providers and contractors that maintain the personal information at issue, pursuant to their written contract with the business, to make the necessary corrections in their respective systems. Service providers and contractors must comply with the entity's instructions to correct or delete the personal information or enable the entity to make the changes directly. Vendors must also provide assistance to the entity in responding to a verifiable consumer "request to access/know" by providing the consumer's personal information it has in its possession, which it collected as a result of providing services to the entity or by enabling the entity to access that personal information directly.

> **Action items:** Review existing data processing agreements to determine whether appropriate terms are included or need to be amended; draft template data processing agreements to use with new vendors.

Data subject requests

Each of the Acts empowers a consumer to exercise certain data subject rights. These include the rights to:

- Access/know.
- Correction.
- Erasure.
- Opt out of behavioral advertising.
- Opt out of the sale and sharing of personal information.
- Opt out of profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer.
- Limit the use of sensitive personal information.
- Nondiscrimination.
- Data portability.

Under comprehensive U.S. privacy laws, many of these rights are new, particularly the right to correction. Entities will therefore need to update their internal processes in order to adequately and timely respond to these requests. Entities must respond within 45 days, with the option of a 45-day extension upon notice to the individual. Additionally, Virginia, Colorado, and Connecticut provide individuals with the ability to appeal an entity's initial decision.

It is important to note that entities need not comply with all data subject requests — each law (or its draft regulations) provides applicable exceptions. For example, an entity does not have to delete personal information if the information is needed to continue providing services to the individual. Further, an entity may decide not to act on a correction request if the entity contends the data is accurate, with varying degrees of conviction required by the Acts. Such determinations still must be defensible and communicated to the consumer.

> **Action items:** Establish policies and procedures for the submission and quick intake of customer requests; ensure personal information is accessible, portable, and editable.

CONTINUED ON PAGE 5

CONTINUED FROM PAGE 4

Sensitive personal information

While sensitive personal information is not an entirely new concept under U.S. privacy laws, the Acts introduce new categories of sensitive information and include new obligations for entities. Under existing U.S. state breach notification laws, categories of information such as Social Security numbers, financial account information and drivers' license numbers are treated as sensitive. Now, comprehensive U.S. state privacy laws introduce new categories of sensitive information that more closely align with the categories found under Article 9 of the European Union's General Data Protection Regulation. These include racial or ethnic origin, religious or philosophical beliefs, precise geolocation, genetic data, biometric data, and health information.

The expanded identification of sensitive personal information under these laws means entities need to take additional steps when collecting, using and disclosing such information. With limited (and varied) exceptions, the CPA, CTDPA, and VCDPA require entities to obtain consent, or provide a clear opportunity to opt out, prior to processing sensitive personal information (and sensitive personal information inferences under the CPA). Consent must be separate from any broad or general terms, actively assented to and freely given, regularly refreshed, and revokable. The UCPA is more business-friendly, requiring clear notice to the consumer and an opportunity to opt out.

The CPRA does not require consent for the collection of sensitive personal information; however, it does grant the consumer the right to limit the use of sensitive personal information if the entity is using the information for purposes that do not align with the services to the individual or commonly accepted business practices (e.g., to prevent or detect security incidents or to resist fraudulent or illegal actions).

> **Action items:** Identify whether sensitive personal information is collected (or inferred) from individuals; implement, maintain and annually renew consumer consents and notices; operationalize opt-out links.

Cookies

There is no question that the Acts have taken a deliberate approach to challenging the collection and use of personal information through cookies and other tracking technologies. The CPRA has introduced the concept of sharing, which addresses the disclosure of personal information for cross-context behavioral advertising. Similarly, Virginia, Colorado, Connecticut, and Utah also now address targeted advertising.

If an entity is selling or sharing personal information or conducting targeted advertising, directly or through a vendor, the Acts require additional compliance measures. Entities must provide adequate notice of such processing activities in the entity's privacy notice (including identifying the categories of third parties to whom information is being sold or shared), implement opt-out links and be able to comply with opt-out preference signals. While it is clear that these state regulators are looking to give consumers more control over tracking technologies, the more nuanced expectations for entities are still murky. At least in California, there have been a couple of lessons. For example, the California Privacy Protection Agency (CPPA) has expressed that cookie banners are not an adequate opt-out mechanism for the selling or sharing of personal information. The California attorney general's enforcement action against Sephora also showcased that a business's backend privacy practices must align with its public-facing privacy notice. This is a fairly easy way for a regulator to confirm whether a business is complying with applicable requirements.

> **Action items:** Conduct cookie scans; analyze whether personal information is disclosed to third parties; implement opt-out links and recognize opt-out preference signals if needed.

Employee data

Businesses subject to the CPRA need to address a key difference from the other Acts — employees are included in its definition of consumers (and the previous partial exception expired January 1, 2023). Employers will need to tread carefully in navigating the unique ways employee and applicant data is utilized as a part of regular operations against the rights and obligations established by the CPRA.

Employers will need to provide their California-resident employees and applicants notice at collection, explaining:

- The types of personal information it collects.
- The purposes of collection.
- The individual's rights, including:
  - Data subject requests.
  - Nondiscrimination.
  - Opting out of the sale or sharing of information.
  - Limiting the use of sensitive personal information.
- Retention periods.
- To whom employers may further disclose the personal information.

All the rights established in the CPRA will apply to employee and applicant data, including performance reviews, payroll, etc. Businesses will need to ensure the appropriate personnel are trained and ready to respond to requests within the CPRA's time constraints, particularly when and how a business vets the validity of and is permitted to deny such requests.

Much of what human resources collects about applicants and maintains on employees falls in the categorical definition of sensitive data under the CPRA. The definition also includes "the contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication." CPRA § 1798.140(ae)(1)(E). However, if sensitive data is collected or processed "without the purpose of inferring characteristics about a consumer," it is treated as personal information. CPRA § 1798.121(d). Employers will need to carefully review how they utilize HR data and how they communicate with employees if they want to avoid the additional obligations carried by sensitive data.

A hot topic with regard to employee data is the conflict between the CPRA and federal and state law retention requirements. The CPRA contemplates such a conflict by stating that it "shall not restrict a business's ability to … [c]omply with federal, state, or local laws." CPRA § 1798.145(a)(1). Businesses will need to analyze their obligations under these retention requirements with the deletion and correction requirements under the CPRA.

For example, federal employment law requires entities to maintain personal information related to applicants for a period of at least one year. 29 C.F.R. § 1602.14. Further, federal law also mandates every employer keep personnel or employment records for a period of one year. 29 C.F.R. § 1627.3(b)(1)(i). While an employer would

CONTINUED ON PAGE 6

CONTINUED FROM PAGE 5

therefore not have to comply with an applicant's data deletion request given its obligation to retain such personal information under federal law, the employer will still need to meet the CPRA's timely response and explanation requirements in its notice of request denial to the applicant.

> **Action items:** Review applicant and employee data uses; revise employee notices to California employees; review retention requirements under state and federal laws and incorporate them into data request response processes.

Conclusion

On top of the new compliance obligations above, further regulations from the CPPA regarding automated decision making, cybersecurity audits, and privacy risk assessments remain outstanding. Limited privacy laws targeting topics like biometric data and reproductive tracking continue to further complicate the U.S. privacy law landscape. And while it is seeming more unlikely, a federal privacy law may also add a wrinkle or offer consistency in this regulatory topography. What is clear is that there will be no shortage of privacy compliance steps that organizations will have to take in 2023.

Artificial Intelligence Law and Policy Roundup

Leslie F. Spasser
Office Managing Partner
Atlanta

Brennan Carmody
Associate
Atlanta

As artificial intelligence ("AI") has moved from the realm of science fiction to the world of business, companies and regulators alike have grappled with the opportunities and risks that AI presents. Today, AI-powered applications, from chatbots to delivery drones, have changed the way businesses operate and interact with their customers. At the same time, the increasing use of AI technologies to facilitate business decisions and outcomes in areas such as employment, health care, housing and finance has prompted lawmakers and regulators at both the state and federal levels to evaluate whether and how to regulate AI to ensure that it is employed responsibly and in a manner that serves the public interest. Although AI technologies have been in existence for decades, regulations are still catching up to this reality.

This article provides an overview of the current AI law and policy landscape in the U.S. by illustrating how government entities are working to foster innovation while also implementing safeguards to mitigate potential harms caused by unrestricted use of AI technologies.

What is AI?

To understand the regulatory environment surrounding AI, it is important to recognize what AI is and how both human input and machine operations play intersectional roles in its development and performance. AI is commonly understood as technology that can simulate human (intelligent) learning and decision making. AI applications employ algorithmic models that receive and process large amounts of data and are trained to recognize patterns, thus enabling the applications to automate repetitive functions as well as make judgments and predictions. The selection of training data, as well as other training decisions, is human controlled. However, as AI becomes more sophisticated, the computer itself becomes capable of processing and evaluating data beyond programmed algorithms through contextualized inference, creating a "black box" effect where programmers may not have visibility into the rationale of AI output or the data components that contributed to that output.

AI across industries

While AI may seem like an abstract technical concept, AI systems pervade our daily lives. Every time we engage with a chatbot, use autocorrect functions in messaging systems, interact with virtual assistant technologies such as Amazon Echo or Alexa, rely on smart car features such as parking assist, or depend on logical inferencing in tax preparation programs, we are enjoying the benefits of AI.

Similarly, AI technologies play critical roles across many industries. For example, businesses use AI to streamline employment application screenings and replace workers in certain capacities. In the real estate sector, AI is being used to determine the loan amount offered to a particular mortgagee, interest rates and even whether to lend to a prospective mortgagee based on an assessment of risk factors. AI is also being implemented in critical roles in the health care sector with AI applications assisting in the diagnostic process, screening patients and predicting risks for certain diseases and health outcomes.

While these and other innovative uses of AI have driven advancements in efficiency, predictability and cost control, if not employed thoughtfully they may leave companies vulnerable to claims of bias, discrimination or other unlawful conduct. The relative risk involved with AI applications varies across industries and depends in large part on the role AI plays in a business's

CONTINUED ON PAGE 7

CONTINUED FROM PAGE 6

interaction with its customers and decision making. As described below, many of the laws and regulations targeted at AI involve concerns over AI's role in unlawful discrimination, biased decision making and use of information in a manner that violates privacy and data protection laws.

AI regulation on the state level

At this time, the U.S. federal government has not developed a comprehensive or coherent strategy for regulating AI. States have attempted to fill the void by developing their own regulatory regimes to address what they see as the greatest potential risks presented by the use of AI. To date, Illinois, Maryland, New York and California have shown themselves to be the most active in this regard. Illinois' passage of the Biometric Information Privacy Act (BIPA) in 2008 represented one of the first efforts to regulate AI.[1] BIPA requires an entity to provide clear and adequate notice and to obtain consent before collecting the biometric identifiers of a consumer for any use, including AI. BIPA has garnered headlines over the past few years by generating hundreds of lawsuits, not only because of its stringent notice and consent requirements but also because BIPA includes a private right of action and liquidated damages for individuals harmed by BIPA violators, making it a favorable vehicle for class action suits. In addition to BIPA, Illinois enacted the Artificial Intelligence Video Interview Act (AIVIA) in 2019.[2] The law requires employers using AI technology as part of the screening or hiring process to notify applicants (i) that AI may be used to analyze their interview, (ii) how AI technology works and (iii) what characteristics AI uses to evaluate applicants, as well as obtain each applicant's consent to be evaluated by AI.

The State of Maryland enacted a law similar to AIVIA that requires employers to obtain an applicant's consent to use facial recognition technology in interviews.[3] Unlike the requirements in AIVIA, Maryland's law simply prohibits the use of facial recognition technology during job interviews unless the applicant consents to its use.

In 2021, New York City legislators passed a law that regulates the use of automated employment decision tools by employers, requires employers that use AI to audit their AI systems, and penalizes employers that engage in biased conduct arising from the use of AI in the hiring process.[4]

California, like Illinois and Maryland, also has its eye on restricting the use of facial recognition tools and automated systems. In March 2022, California's Civil Rights Council (CRC) (formerly the Fair Employment and Housing Council) published draft modifications to its antidiscrimination law, which would hold employers liable for the use of AI in their employment decisions where such use has a discriminatory impact.[5] The CRC's budget for 2023 indicates that it will help advance its AI initiative. Further, in August 2022, California's attorney general requested information from hospitals in the state on how health care facilities and other providers are identifying and addressing racial and ethnic disparities in health care algorithms.[6]

Other states have followed suit by rolling out their own AI regulations. Starting this year, consumer privacy laws in Colorado,[7] Connecticut[8] and Virginia[9] will provide their residents with a right to opt out of AI profiling activity related to decision making. Further, new laws in Virginia and Colorado will require businesses to offer an opt out regarding the processing of consumers' data. As AI continues to proliferate across various sectors, more states will develop their own regulatory regimes for AI technology.

AI regulation on the national level

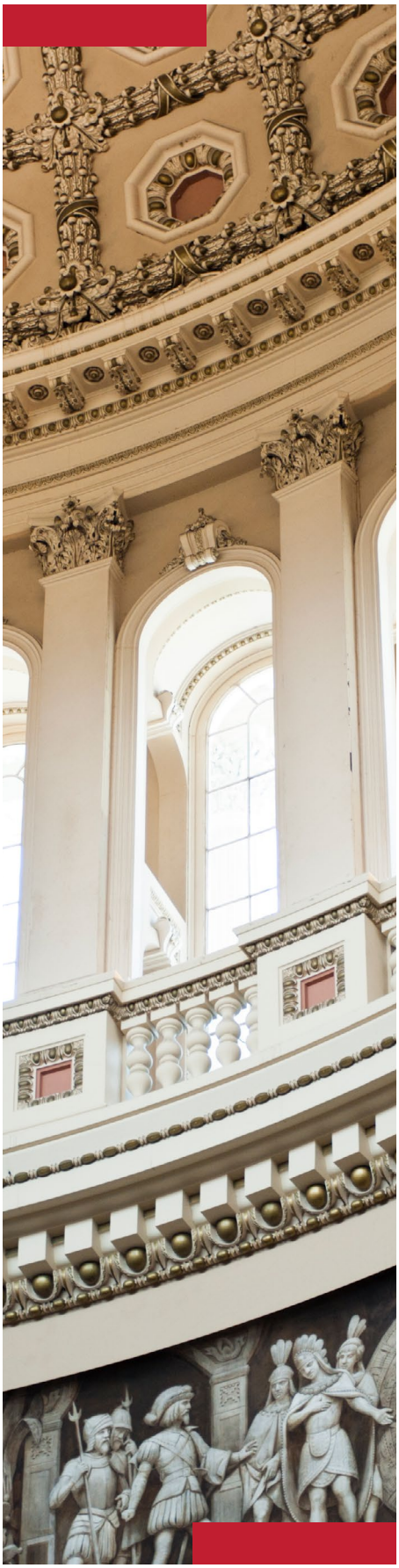
As noted above, Congress has yet to pass legislation regarding the privacy issues and other potential concerns raised by the broad implementation of AI technologies; however, some federal agencies have begun to publish their own guidelines. In May 2022, the Equal Employment Opportunity Commission (EEOC), which focuses on the rights of employees and job applicants, issued guidance outlining how the Americans with Disabilities Act (ADA) may apply to an employer's use of AI.[10] The EEOC stated that an employer's use of AI can violate the ADA where (i) the employer does not provide "reasonable accommodation" as required by the ADA, (ii) the employer intentionally or unintentionally screens out an individual with a disability who is qualified for a position, or (iii) the employer's AI technology violates the ADA's restriction on disability-related inquiries. The EEOC also noted that even in cases where an employer is using a third party's AI, the employer itself could still be held liable for AI technologies violating the ADA.

In addition to the EEOC's guidance on the use of AI in the workplace, the Federal Trade Commission issued its own set of guidelines on the use of AI in 2021. The FTC, which derives its enforcement authority against businesses that engage in unfair and deceptive practices from Section 5 of the FTC Act,[11] has focused on AI from the consumer protection perspective. In that regard, it has advised companies to take a "responsible AI by design" approach, which involves (i) considering ways to improve the data sets used to train the AI as well as to anticipate and solve any shortcomings, (ii) watching for discriminatory outcomes, (iii) embracing transparency and independence by conducting and publishing the results of independent audits, (iv) being open and realistic about what the AI can and cannot

1 Il. St. Ch. 740 § 14.
2 Il. St. Ch. 820 § 42.
3 MD Code, Labor and Employment § 3-717.
4 New York City, Local Law No. 144 Int. No. 1894-A (2021).
5 Cal. Code of Reg. Tit. 2., Div. 4.1, Ch. 5, Subch. 2 (proposed).
6 Press Release, Office of the Attorney General of California, "Attorney General Bonta Launches Inquiry into Racial and Ethnic Bias in Healthcare Algorithms (Aug. 31, 2022), https://oag.ca.gov/news/press-releases/attorney-general-bonta-launches-inquiry-racial-and-ethnic-bias-healthcare.
7 Colorado Attorney General, "Colorado Privacy Act (CPA) Rulemaking," https://coag.gov/resources/colorado-privacy-act/.
8 Conn. Substitute Senate Bill No. 6 Pub. Act. No. 22-15.
9 Va. Code Sec. 59.1-573(A)(5) (2021).
10 U.S. Equal Employment Opportunity Commission, "The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees" (May 12, 2022), https://www.eeoc.gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence.
11 15 U.S.C. § 45.

CONTINUED ON PAGE 8

CONTINUED FROM PAGE 7



do, (v) telling the truth about how data is being used, (vi) doing more good than harm, and (vii) holding themselves accountable. The auditing functions recommended by the FTC play an especially important role in bringing accountability to deep learning or black box AI applications, where developers may not be able to ascertain the basis for the application's decisions or outcomes solely by analyzing the data inputs.

The White House Office of Science and Technology Policy recently published the "Blueprint for an AI Bill of Rights."[12] The Bill of Rights focuses on the development of safe and effective systems, algorithmic discrimination protections, data privacy, the need for notice and explanation, and the use of alternatives or opt-out rights. Specifically, the proposal notes that the public should (i) be protected from unsafe or ineffective systems through the use of extensive testing and risk identification processes, (ii) not face discrimination by algorithms with systems used and designed in an equitable manner, (iii) be protected from abusive practices through the implementation of built-in protections and have the ability to exert control over the use of data, (iv) know that an automated system is being used and understand how and why it contributes to outcomes that impact them, and (v) be able to opt out of automated systems and have a human alternative readily available to assist them.

Key themes to keep in mind

On both the state and federal levels, regulation and guidance focus on the same four pillars: fairness, explainability, transparency and accountability. The fairness principle is codified in the call for AI systems that are free of bias, whether intentional or unintentional. Explainability refers to a focus on laws requiring that companies be capable of explaining how and why AI technologies make decisions. As for transparency, government entities and legislation call for companies to be open about how their AI technology works and when automated systems are being used. Finally, the accountability principle is reflected in the call for companies to continuously inspect and interrogate their AI technologies so they can identify and address any shortcomings.

What's to come?

Over the coming year, we expect to see enhanced enforcement of current laws as well as the promulgation of new laws and regulations relating to AI. Complementing the regulatory process, we anticipate the publication of version 1.0 of an AI risk management framework and institutional guidelines by the National Institute of Standards and Technology (NIST), which focuses on the development of industrywide technology standards.[13] The objective of the framework is to better manage the risks that AI presents to individuals, organizations and society as a whole. Voluntary compliance with NIST guidelines has been used to show good-faith efforts to comply with generally accepted industry best practices, which, in turn, can help mitigate liability in other contexts. Finally, while we have not addressed international developments concerning AI regulations in this article, we expect the continued development of European Union (EU) AI regulations to inform the views of U.S. regulators as they continue to assess AI and develop a more comprehensive regulatory structure to advance the objectives of fairness, explainability, transparency and accountability.

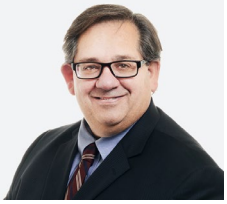
12 White House Office of Science and Technology Policy, "Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People" (Oct. 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.
13 NIST, AI Risk Management Framework Playbook, https://pages.nist.gov/AIRMF/.

The Structure of Data Rights in a Post-On-Premises World

Gregory M. Kratofil, Jr.
Office Managing Partner | Technology Transactions & Data Privacy Chair
Kansas City

Ephraim T. Hintz
Associate
Los Angeles

Gregory L. Cohen
Shareholder
Phoenix



As society moves away from the use of on-premises software into a modern world in which software vendors offer software and services through online, hosted environments, new challenges and trends related to data use and ownership have become more prevalent. This article discusses the relevant historical background of on-premises software, the shift toward subscription-based software or software as a solution, and the new trends arising in such hosted software agreements.

On-premises software

Historically, on-premises software was the only solution available to users. A license to on-premises software grants the user the right to install the software onto their computers or systems for the user's internal use. On-premises software is advantageous for users who enjoy controlling the use of such software, subject to the restrictions in the software agreement. However, users of on-premises software take on significant responsibilities when accessing and using the software, including full responsibility for the implementation of the software, purchasing the network infrastructure (e.g., servers, operating systems) to operate the software, purchasing and maintaining power to access and use the software, controlling any additional external databases necessary to access and use the software, and security and virus protection. Users are responsible for implementing any available updates to the on-premises software, which may be costly, to ensure its functionality meets the users' expectations. In addition, users must maintain the integrity of the software and the safety of their systems to prevent any unauthorized access, use or alteration of the software, or they risk a vendor taking legal action against a user for misuse or misappropriation of such software.

The shift toward hosted software

Although on-premises software solutions remain widely used, in recent years, users have begun shifting toward subscription-based or software as a service solutions (collectively, hosted software) that are hosted off-site by the vendor.[1] There are a multitude of reasons for this shift toward hosted software, including: (a) users pay only for the scope of the solution the user desires to use; (b) users do not have to shell out the extensive upfront costs of implementing on-premises software; (c) hosted software, unlike on-premises software, is capable of quick deployment without a long implementation process; and (d) users are not obligated to purchase and maintain the infrastructure to operate the hosted software; rather, the vendor will collaborate with the user to create the infrastructure that meets the user's needs and will host and monitor the network to ensure the user's access and use of the hosted software complies with the terms of the hosted software agreement. Software vendors also prefer hosted software because the subscription fees provide them with a recurring revenue stream and it gives them greater control over the software.

Legal trends arising from the shift toward hosted software

In conjunction with the rise of hosted software, certain new challenges and legal issues have become prevalent. Specifically, the following legal trends are involved in hosted software agreements: (a) the fight over data ownership (i.e., software vendors' desire to obtain ownership rights over a user's data); (b) users are granting licenses to their data as an alternative to transferring data ownership to software vendors; and (c) users now want to ensure they have adequate rights to claw back their data at the end of the relationship with the software vendor. The intersection of these trends is a two-way street, because software vendors have greater access to a user's data and are aggressively moving to take advantage of such data for a multitude of purposes, including improving or adding features to the hosted software for users' benefits. The result of these intersecting trends in the context of our discussion is that software vendors are asking for or demanding greater rights to access, aggregate, analyze and use a user's data stored in the hosted software.

A. Data ownership

Generally, hosted software agreements between a user and a software vendor will expressly allocate data ownership to the user. For example, the agreement will likely indicate the user is the "sole and exclusive owner" of their data and/or such data is deemed confidential information (i.e., a vendor's misuse or unauthorized disclosure of a user's data would violate the agreement's confidentiality obligations). This type of provision is logical since the user generated the data, then uploaded or shared the data to the hosted software, and thus the user would

1 While there are distinctions between hosted software and SaaS solutions, for the purposes of this article the concepts and issues of such solutions are similar enough that this article treats all the solutions the same.

CONTINUED ON PAGE 10

CONTINUED FROM PAGE 9

likely not enter into an agreement in which it relinquishes control over such data.

However, although the hosted software agreements memorialize a user's ownership rights to their data, recently, software vendors have also been working to include certain provisions or language in the same hosted software agreements that provide the software vendor rights to access, de-identify and use such de-identified data. For example, a software vendor may include language granting the vendor the right to de-identify and commercially exploit a user's data for the provision of the hosted software in order to create new offerings or for other related purposes.

Although it is industry standard to allow vendors the right to monitor data stored and processed within the hosted software for the purposes of providing the software or services and implementing software updates, the agreement's language creates broad rights for a software vendor to derive and own new value (e.g., new revenue streams) from a user's data. For instance, under a provision in the agreement, a software vendor would have the right to use a user's data to create new software or data products that the vendor can sell as stand-alone products and/or develop as new machine learning algorithms.

In response to a software vendor's attempt at obtaining broad rights to a user's data, there are various approaches a user can take to protect themself and their rights to such data, including (a) expressly restricting the vendor's access and use of the user's data to the limited purpose of providing the contracted software or services; (b) granting the software vendor a right to extract, de-identify and commercially exploit de-identified user data for the vendor's commercial purposes, provided that the vendor compensates the user either in the form of actual payment or discounted subscription fees for the hosted software; or (c) granting the software vendor a right to extract, de-identify and commercially exploit de-identified user data for the vendor's commercial purposes, provided that the vendor grants the user a nonexclusive, perpetual and irrevocable license to use any products or services created by such de-identified data.

B. Data licensing

Users tend to reject the notion of software vendors owning their data in any manner and generally will push back on the transfer of data ownership to vendors. However, if a user is unable to thwart the software vendor's desire to access and use the de-identified data stored or processed using the hosted software, a good alternative to transferring data ownership is to grant software vendors a limited license to the user's data that restricts the vendor's use of such data to certain limited, agreed-upon uses. Unlike the transfer of data ownership, granting a limited license to the user's data retains the user's right to control their data. Specifically, the user may revoke the data license subject to the terms of the license, prohibit the software vendor from transferring or selling the user's data, restrict access to the data to certain geographical areas, and/or limit the purposes in which the software vendor may access or use such data. The permitted uses of a user's data will likely vary depending on the user's risk tolerance levels and the sensitivity of the data. The limited license may permit a software vendor to use a user's data for any purposes the vendor desires or may limit such permitted uses to only those necessary to monitor and update the hosted software for the provision of services to the user. In addition, the terms of a data license may require that the vendor pay the user compensation or royalties for the vendor's use and misuse of the user's data or the creation of new products from the user's data.

Once a user determines that granting the software vendor a limited license to their data is the best approach to push the deal to closure, the user should consider modifying the applicable definition in the hosted software agreement (generally defined as "user data" or "customer data") to include downstream derivatives that may be developed from the user's data. A broad definition of user data or customer data ensures the user will retain the rights to their current data while establishing rights to any new products or services created from the data.

C. Clawback

Another growing trend is that users now include clawback provisions in hosted software agreements. Clawback provisions grant users the right to retrieve or claw back their data from the software vendor at the expiration or termination of the relationship. Clawback provisions protect users from vendors' continued use of their data after the termination or expiration of the relationship. Typically, clawback provisions will expressly terminate the license to the user's data provided under the hosted software agreement upon the termination or expiration of the user and vendor's relationship and obligate the vendor to destroy or permanently erase all copies of the user's data that the vendor controls at the time of such termination or expiration.

Although clawback provisions provide some certainty for a future return of data, vendors may not have the capability to delete or destroy a user's data. Generally, hosted software solutions take snapshots of the hosted environment (including the user data contained in the environment) and save the snapshots to the vendor's archives or backups, making it burdensome for the vendor to delete the archived user data. If a hosted software agreement grants the vendor the right to retain archived data, users should make sure the agreement (a) extends any applicable confidentiality obligations to the archived data for as long as the vendor retains such data, (b) restricts the vendor's use of archived data to the lawful purposes for such archival (i.e., statutory retention requirements and/or disaster relief plans), and/or (c) sets a reasonable period for the deletion of the archived data once the archival purposes have been fulfilled.

Another key consideration when including a clawback provision in a hosted software agreement is ensuring the vendor remains able to identify the data it receives from the user. If the vendor is incapable of identifying the applicable data from other users' data, the user will be unable to retrieve their data from the vendor at the termination or expiration of the relationship. However, clawback provisions are not without risk — in order to comply with such obligations, vendors must maintain the user's data in an identifiable format that creates risk of accidental identification. In addition, users must conduct a risk analysis and weigh the pros and cons of allowing a vendor to retain their data in an identifiable format for the purpose of the user retrieving the data at a later date.

Conclusion

In this post-on-premises world in which users generate and upload their data to a hosted software environment, vendors are increasingly more aggressive in trying to obtain rights and/or ownership to the user's data. Users of such hosted software should view their data as a commodity and protect their rights to the data and derivatives of such data by restricting the vendor's access to and use of their data through a limited license and, if applicable, express clawback provisions in the hosted software agreement.

Mitigating Your Greatest Data Privacy Risk: How To Establish an Effective Vendor Management Process

Kathryn T. Allen
Shareholder
Kansas City, Dallas

Kelsey L. Brandes
Associate
Kansas City

I. Third-party vendors pose a significant risk

What is the greatest data privacy threat to companies in 2023? It is commonly thought that a company's employees are the greatest data privacy threat, as they may fall prey to phishing attacks, click bait, lost devices and other situations that can compromise company data. Employees can be a threat, but in reality, this threat can be effectively mitigated within the company by implementing solutions such as tighter controls on company devices, employee trainings and internal safeguards.

The greatest data privacy threat companies actually face in 2023 is their vendors: the third-party businesses a company must do business with. Companies are increasingly engaging third-party vendors to provide a host of services. It is often cheaper to outsource key services and infrastructure to cloud services rather than develop and maintain such services and infrastructure in-house. Yet, these vendors are a data privacy threat. Consider the numbers:

- 63% of data breaches are tied to or directly caused by third-party vendors.
- The average cost of responding to large-scale third-party breach is $10 million.

In addition to response costs, data breaches can lead to a number of other challenges for companies, such as:

- Increased operational costs associated with asset recovery and system downtime.
- Regulatory investigations or actions.
- Litigation.
- Reputation harm.
- Customer loss.
- Decrease in shareholder value.

II. The concept of vendor management

Can companies manage vendor risk in a way similar to how they have begun to manage employee risk? The answer is yes, if they follow a comprehensive third-party vendor management program. Many companies rely on their procurement department to gather information on vendors and/or to establish a risk profile through vendor assessments. But as more and more vendors have cloud-based or Internet of Things components (even for the most mundane products and services), it is time to pull vendor management away from the procurement team and implement different measures.

Vendor assessments and surveys are no longer enough to protect a company, as they may not provide a complete picture. Assessments and surveys are often based on moments in time (i.e., what the vendor is doing or not doing at that particular moment when they complete the assessment or survey). Vendors rarely go back and update customers when they make changes to their security policies. Assessments and surveys are a great way to get to know your vendors from a technical standpoint as of the date of completion of the assessment or survey, but the vendor selection process cannot stop there. Additionally, there might not be repercussions associated with assessments or surveys if the vendor experiences a data breach. This is where written agreements between your company and its vendors can protect your company in ways that an assessment or survey cannot.

III. The information security agreement

Based on the type of company and what it does, the company must be the party establishing parameters for its risk tolerance and legal and regulatory obligations. But how does a company do so while contracting with hundreds of vendors each year?

We recommend a written document, whether a stand-alone agreement or an exhibit or addendum to the underlying relationship agreement, that sets forth specific physical and technical standards as well as ongoing obligations by your vendors to keep your data safe. There should also be legal remedies in the event vendors fail to keep their obligations. This document is commonly referred to as an information security agreement ("ISA").

At a minimum, an ISA should address the following:

- **Certifications.** Certain industries have required certifications (e.g., the Health Information Technology for Economic and Clinical Health Act), while others follow industry standards (e.g., SOC2). Vendors should provide copies of their certifications.
- **Data breach notification.** How will the vendor notify you if your data is breached? When must the vendor notify you of a breach? What does the vendor have to do for you and the data subjects post-breach?
- **Encryption of data.** Does the vendor encrypt data only at rest or also in transmission? What level of encryption is used?
- **Audits.** Do you want to be able to audit the vendor's compliance with the ISA? What about after a data breach?
- **Employee/subcontractor management.** Do vendor employees need background checks? Can the vendor engage subcontractors without your approval?
- **Data storage/destruction.** Where can and can't the vendor store your data? What happens to your data when your agreement with the vendor is over?
- **Malware.** What internal processes does the vendor have in place to detect malware and prevent cyberattacks? Does the vendor regularly scan its systems (and make the results of those scans available to you upon request)? What happens if the vendor passes a virus on to you?
- **Disaster recovery/business continuity.** If the vendor experiences a major interruption in business, how long will it need to recover? This is particularly important to infrastructure vendors.
- **Regulations.** Examples may include the

CONTINUED ON PAGE 12 ▸

CONTINUED FROM PAGE 11

European Union's General Data Protection Regulation and the California Consumer Privacy Act.

- **Insurance.** Does the vendor have sufficient insurance in place that will make you whole in the event the vendor experiences a data breach? Is the vendor properly capitalized to stand behind its liability?
- **Liability.** What is the minimum liability your company will be comfortable with accepting in the event of a vendor's data breach or breach of the ISA? The vendor's liability for breaches must be higher or uncapped for regulated businesses.

IV. The vendor management process

Prework. Draft a template ISA that reflects your company's actual needs, considering various factors such as the company's industry, data collected, regulatory environment, and products or services. With the onslaught of new data privacy legislation both domestically and abroad, Polsinelli recommends consulting with your privacy counsel on any data privacy provisions. Prework action steps:

1. Establish written criteria that define when vendors will be required to sign an ISA (i.e., when the vendor will have access to your data, infrastructure or network).
2. Work with the legal and information security teams to draft a form ISA.
3. Establish written parameters for tolerance on vendor-requested changes to the ISA.

Your Polsinelli attorneys can assist with ISA prework, including drafting an ISA that includes requirements and risks your company is comfortable with.

Internal rollout. When rolling out the ISA to your company, you must educate those who are part of the vendor selection process and work with vendor management and legal and compliance to ensure all individuals understand what the ISA is, what it does and the importance of it. Polsinelli recommends hiring an external party to present required trainings for all relevant internal stakeholders for maximum impact and adoption. Internal rollout action steps:

1. Educate internal stakeholders about the ISA, its purpose and its effectiveness.
2. Modify the company's internal process so that an ISA is now provided to any new vendor that meets the established criteria.
3. Establish who has authority within the organization to approve vendor-requested deviations to the ISA.

External rollout. Sending the ISA to prospective vendors is easy. But what will you do when vendors request to negotiate certain provisions, or decline to review your ISA altogether and instead provide their own set of information security terms (which may not be in the form of a legally binding agreement)? Polsinelli recommends establishing a relationship with outside counsel that has expertise in data privacy and information security and who can assist in identifying and quantifying the risk associated with a vendor's changes or terms. External rollout action steps:

1. Send the ISA to vendors with clear messaging that explains the ISA's purpose and relationship to other legal documents.
2. Create a process for the receipt of vendor changes and establish who will negotiate with the vendor.
3. Establish a repository of ISAs that can be called on easily when there is an issue with the vendor.

Your Polsinelli attorneys can assist with responding to any proposed changes by vendors and determining the risk associated with such changes.

V. Conclusion

Facing a regulatory body or your customers after you experience a data breach will be less painful when you can point to a comprehensive, all-encompassing vendor management process. And the process will be even less painful when you can get relief from the vendor that is responsible for the breach instead of paying out of your own pocket.

Cybersecurity To-Dos in 2023

Colin H. Black
Associate
Chicago

Bruce A. Radke
Shareholder
Chicago

Anna K. Schall
Attorney
Kansas City

Introduction

The cybersecurity threat landscape continues to evolve and present new challenges pertaining to the protection of electronically stored information. Innovative "hacking" tactics constantly emerge and metamorphous; however, threat actors continue to target common system vulnerabilities – where available – to gain initial unauthorized access to an organization's computer networks, systems, servers, email accounts, etc. This means that initial unauthorized access oftentimes can be prevented by implementation of known security controls and practices to erase common vulnerabilities, which may incentivize threat actors to simply move on to easier targets. This article outlines common vulnerabilities exploited by threat actors to gain unauthorized access to an organization's environment and electronically stored information, as well as recommended privacy and security controls to mitigate the risk and severity of potential cyber security incidents and/or data breaches.

Business Email Security

Business email compromise ("BEC") is the most common, financially devastating category of cybersecurity incidents. As reported in its 2021 Internet Crime Report, the FBI received approximately 20,000 BEC complaints with losses of close to $2.4 billion in 2021, and it is anticipated that the figures reflected in the FBI's annual report for 2022 will increase significantly.

Threat actors typically rely on one of two methods to effectuate BECs: phishing emails or credential compromises. In the phishing email context, a threat actor sends an email from a "spoofed" email account – i.e., using an email address with slight variations from the legitimate email address or via a different domain – to trick recipients into thinking that the spoofed email address is legitimate. Alternatively, in the credential compromise scenario, the threat actor utilizes malicious software to gain unauthorized access to an organization's systems and email accounts, allowing the threat actor to then interject into and/or intercept legitimate email threads.

Phishing emails or credential compromises allow the threat actor to perpetuate various fraudulent and unlawful acts. The contents of a spoofed email may induce the email recipient to click on a malicious link or open a malicious file. Depending on the sophistication of the threat actor, the malicious link or file may grant the threat actor unauthorized access to an email account by one or more of the following methods: redirecting the email recipient to a fake login page, prompting the email recipient to enter valid login credentials, subsequently instigating exfiltration of the contents of the email recipient's inbox, and/or initiating malware installation for the threat actor's subsequent unauthorized access, exfiltration, etc.

Once within the account, threat actor may attempt to gain additional access to other accounts using the legitimate email address, promulgate additional malware to email contacts, or attempt social engineering attacks to facilitate financial transactions.

While BECs account for most cyber-attacks, they are among the easiest to prevent, for example, by implementing the following recommended technical and operational protocols: First, multi-factor authentication ("MFA"), where a system requires a user to provide a combination of two or more credentials to verify the user's identity for login. MFA is easy to implement, minimally intrusive, and affordable. MFA is often also a requirement for coverage under cyber insurance policies. Second, forced password resets on a routine basis and across all user accounts are invaluable in mitigating the risk of attacks originating from acquisition of compromised credentials. Third, the implementation of policies for data retention, storage, and electronic transfer. Finally, organizations should strongly consider implementing cybersecurity awareness training with emphasis on phishing training (to spot suspicious links and domain/email address inaccuracies). A combination of protections can deter a threat actor from pursuing unauthorized access to an organization's systems and data.

Ransomware Prevention

Ransomware refers to the unauthorized encryption of data, with a decryption utility available for a fee payable to a threat actor. Encryption is a legitimate utility for data security, and works by transforming plain text into cipher text using an algorithm which generally has a single known solution. The cipher text can only be converted back to plain text 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. Ransomware presents a malicious use case for an otherwise-valid (and highly effective) security tool.

The overwhelming majority of ransomware attacks begins with one of three attack vectors: unauthorized or unknown use of Remote Desktop Protocol ("RDP"), phishing attacks, and vulnerabilities or misconfigurations of legitimate software pre-existing in the environment.

Once within the environment, threat actors will typically attempt lateral movement to systems which appear to be mission-critical, contain high-value data, and in particular, will target intra-network backups. Once their initial reconnaissance efforts are complete, the threat actor will deploy the ransomware binary on each infected machine, and drop a ransom note (typically a .txt file), which will contain a link to a TOR/dark-web site, with an invitation to contact the threat actor.

If well-prepared, an organization can thwart a ransomware attack at the intrusion phase. Beyond the anti-phishing measures described above, a significant volume of ransomware

CONTINUED ON PAGE 14

CONTINUED FROM PAGE 13

incidents could have been averted by removing access to RDP (typically by closing Port 3389 to outside traffic). Relatedly, remote access tools such as TeamViewer, AnyDesk, and SupRemo should be blocked unless absolutely necessary. Relatedly, software patching should be routine to avoid the exploitation of outdated versions. While patching will not necessarily defend against Zero-Day attacks (attacks where the software developer learns of a vulnerability after exploitation in the wild), routine patching can mitigate the exposure of such vulnerabilities.

Third Party & Regulatory Risk Mitigation

Another significant area of cyber risk exists from outside the organization altogether. While most cybersecurity and data privacy professionals are generally familiar with the prevalence of third-party risk, Polsinelli continues to see incidents arising as the result of a compromise of a third-party.

As a preliminary matter, it is important to note that an organization will not be discharged of its privacy and security obligations because another party processes or hosts its data. In most instances, as a matter of default, the data owner will ultimately be responsible for the appropriate response, investigation, and notification to individuals in the event of a cybersecurity incident or data breach. Thus, it falls to the data owners themselves to ensure adequate privacy and security controls are in place or be subject to the harms of a data breach.

As a result, sophisticated enterprises are increasingly requiring its vendors and business partners to maintain certain cybersecurity minimum requirements, carry sufficient cyber insurance, and to notify the data owner on an expedited basis in the event of a cybersecurity incident. By contrast, less agile or sophisticated organizations continue to rely on outside business partners, and often fall victim to the self-inflicted harm associated with the failure to appropriately measure and account for risk.

Public companies face even greater exposure. Publicly-traded companies have heightened privacy and security obligations in that they must comply with industry best practices as well as meet standards of prudence, including on issues of privacy and security. For example, a fictional entity might have thirty to sixty days from the point that it determines a reportable breach has occurred to notify impacted individuals. By contrast, if this entity happens to be publicly traded, the same entity might only have four days from the point it reasonably should have determined that it has experienced a material cybersecurity incident to file an 8-K or 10-K as appropriate under proposed rules by the SEC. Further, reasonable security measures are increasingly becoming components of state and federal law for all organizations.

Going into 2023, every organization should be reviewing its contractual agreements to confirm its potential exposure, with particular emphasis on data retention, indemnity, and notification. Additionally, agrowing number of states' laws, and industry guidance, require organizations to include specific language in their vendor contracts related to cybersecurity protections for sensitive information. Organizations should require their data processors to maintain cyber insurance commensurate with their exposure. 2023 is a good time to revisit an organization's vendor due diligence program to adequately and systematically vet vendors before they gain access to an organization's sensitive data to reduce the risk of third-party incidents.

For organizations that are publicly-traded, operate in highly-regulated or infrastructural sectors, or that own or process personal data, it is strongly recommended that organizations develop and/or update their incident response and data retention plans. In order to be prepared to comply with the SEC's proposed rules on cybersecurity risk management and cybersecurity incident report, public companies must have an established incident response plan to identify potential incidents, contain, remediate and respond to such incidents and quickly assess the materiality of such incidents (both individually and in the aggregate). Public companies should also to develop and implement cybersecurity risk assessment programs and collaborate with SEC and cybersecurity counsel to draft required disclosures for inclusion in their 10-K.

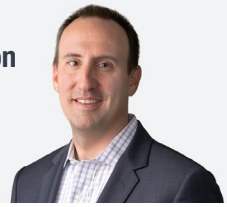
Cybersecurity To-Dos for 2023

The below list, while not comprehensive, will go a long way toward mitigating the risk of a cybersecurity incident or data breach.

- Implement (and enforce!) application-based MFA for all users.
- Implement Office 365, Office 365 Defender, or similar email applications that automatically flag and delete suspicious emails and/or provide alerts regarding sender verification.
- Implement cybersecurity awareness training with emphasis on phishing training (to spot suspicious links and domain/email address inaccuracies).
- Implement regular ethical phishing testing.
- Establish and implement a records and data retention and disposition policy, including email retention.
- Confirm that credentials meet certain length, age, and sophistication requirements.
- Block all non-essential RDP access.
- Block all non-essential Remote Access Tools.
- Implement a routine patch schedule for **all** software.
- Conduct an immediate review of all vendor agreements to confirm data protection, data retention, indemnity, notification, and insurance provisions.
- Update incident response plans to comply with upcoming abbreviated reporting obligations.
- Update data retention policies to adhere to data minimization principles.
- Talk to and educate employees and business partners about their cybersecurity practices.

Data Scraping Update: 'LinkedIn v. hiQ' Answers Some Questions but Leaves Many More Open

Gregory J. Leighton
Shareholder
Chicago



Bari L. Rascoe
Associate
Chicago

2022 provided companies with further clarity and insight regarding legal claims that might be viable to stop data (or web) scraping and those that likely won't work. Data scraping continues to become an increasingly popular method for obtaining structured data that is intentionally made public on websites (as opposed to data that inadvertently may be made public or made public through hacking or other illegal means). Many companies have employed the use of automatic tools to obtain large amounts of structured data in an efficient manner. On the other hand, many website owners are continuing to seek legal tools to prevent or limit this practice. This has resulted in a fair amount of litigation activity in the United States over recent years, typically involving two primary causes of action for website owners: (1) a violation of the Computer Fraud and Abuse Act, a federal law that prohibits intentionally accessing a computer without authorization or in excess of authorization; and (2) breaches of contract claiming violations of website terms and conditions of use that prohibit data scraping. Looking back on this past year's developments, CFAA claims based on data scraping no longer appear to be viable. Thus, the legal evolution in this area is now likely to shift to breach of contract claims, which remain available at least in some circumstances but with questions surrounding what type of remedies might aid website owners going forward.

CFAA claims

The question of the applicability of CFAA claims against data scraping has now largely been resolved by the long-running litigation between LinkedIn and hiQ. Historically, many courts had interpreted the CFAA's "without authorization" and "exceeds authorized access" language broadly to encompass violations of terms and conditions or other contractual restraints put in place by the data owner. However, in LinkedIn's case against hiQ, the U.S. Court of Appeals for the Ninth Circuit took a narrower approach to interpreting the CFAA, viewing it as an "anti-intrusion statute" rather than a "misappropriation statute." *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (9th Cir. 2019). In 2019, the Ninth Circuit affirmed the District Court's holding that the CFAA cannot prevent a party from accessing and using publicly available data simply by revoking its permission via a demand letter. In affirming the District Court's decision, the Ninth Circuit made a key distinction between publicly available information and private information, reasoning that use of public information was unlikely to cause damage or violate any reasonable expectation of privacy held by LinkedIn users. The court also expressly stated that the CFAA should apply only to conduct analogous to breaking and entering rather than to violations of terms of use or other corporate use restrictions.

In March 2020, LinkedIn appealed the Ninth Circuit's ruling to the Supreme Court. In June 2021, the Court vacated the opinion and remanded the case to the Ninth Circuit for further consideration in light of the Court's decision in *Van Buren v. United States*. In *Van Buren*, the Supreme Court adopted a narrow interpretation of what it means to "exceed unauthorized access" under the CFAA, holding that a person "exceeds authorized access" when they access a computer with authorization but then obtain information located in particular areas of the computer such as files, folders or databases that are off limits to them. *Van Buren v. United States*, 593 U.S. __ (2021).

On remand in April 2022, the Ninth Circuit upheld hiQ's ability to scrape publicly available data from the LinkedIn website, holding that scraping such public information likely does not constitute accessing a computer "without authorization" under the CFAA and that a violation exists only if authorization is required and has not been given. On a publicly available website, the Ninth Circuit ruled, there are no rules or access permissions to prevent access and, therefore, accessing that publicly available data cannot violate the CFAA. Accordingly, CFAA claims based on scraping publicly available data no longer appear to be viable.

Breach of contract claims

Although CFAA claims have now been removed as a tool to prevent data scraping, website owners can likely bring and successfully pursue claims for breach of website terms of use that expressly prohibit data scraping. Recent developments in the *hiQ* case have been a potential silver lining to website owners on this point. Indeed, on Nov. 4, 2022, the U.S. District Court for the Northern District of California ruled on LinkedIn's motion for summary judgment on its breach of terms claim. While the court ultimately denied the motion due to factual issues surrounding hiQ's affirmative defenses, it strongly signaled in its opinion that the claim is likely to succeed at trial. Thus, it appears this type of claim remains at least nominally useful to a website owner seeking to prevent data scraping.

However, there are still material questions for LinkedIn (and other website owners) regarding what its remedies will be if it does prevail on a breach of terms claim. Injunctive remedies such as specific performance are generally disfavored in breach of contract claims because it may be difficult to show irreparable harm under typical data scraping fact patterns. Moreover, it may be challenging to show or quantify a significant damages award that would create a disincentive to data scrapers given that most scraped data is not particularly proprietary in nature. Courts may also be hesitant to unintentionally create strong protections for data that does not otherwise fall into already enumerated

CONTINUED ON PAGE 16

CONTINUED FROM PAGE 15

categories of intellectual property protection under U.S. law. As LinkedIn's claim proceeds to trial, website owners will need to watch and see what LinkedIn is ultimately able to recover.

Conclusion

In sum, this past year's developments in the *hiQ* case effectively barred potential CFAA claims based on scraping publicly available data. While website owners still hope to maintain a claim for breach of contract, a key question remains about what remedies are available to them. Of course there are other potential claims website owners could theoretically bring against data scrapers, including copyright infringement, misappropriation or conversion, but these claims would appear to require the website owner to have some proprietary interest in the data or not have the data be publicly available. That said, creative website owners may find ways to breathe new life into these or other claims as they continue to battle against data scraping. This space will continue to be one to watch in 2023 and the future.

'Alkutkar v. Bumble': Securing Active Consent for Updated Terms of Service

Reece Clark
Associate
Kansas City

Benjamin Bira
Associate
Kansas City

I. Overview

The District Court for the Northern District of California recently provided guidance in *Alkutkar v. Bumble Inc.*, No. 22-CV-00422-PJH (N.D. Cal. Sept. 8, 2022), reconsideration denied, No. 22-CV-00422-PJH, (N.D. Cal. Nov. 16, 2022), regarding the steps a business should take to secure end-user consent for updates to terms of service agreements. In lieu of passive email or browsewrap notices, *Alkutkar* affirms that businesses should secure consent through an active means of acceptance. This article provides background and guidance regarding effective methods of securing consent for terms of service updates as well as discusses what we can expect for businesses in 2023.

II. Background: Browsewrap and passive consent

As software has moved to the cloud, so has electronic contracting. Businesses routinely employ "terms of service," "terms of use" or simply "terms" agreements to govern their hosted solutions. From time to time, businesses will update their terms to evolve with changes in technology and the law. In doing so, businesses face a hidden issue involving whether end users have actually agreed to and accepted the new terms.

A common practice in revising terms is to simply post the new terms with an "effective date" set to the date of posting. While administratively easy to do, this "browsewrap" approach generally does not require existing end users to affirmatively consent to the new terms. Some operators implement an extra step or two to announce the new terms via email and/or site banner notices. But even with these passive notices, courts have increasingly disfavored browsewrap approaches. For example, in *Wilson v. Huuuge, Inc.*, 944 F.3d 1212 (9th Cir. 2019), the court stated: "In the absence of actual knowledge, a reasonably prudent user must be on constructive notice of the terms of the contract for a browsewrap agreement to be valid. … A reasonably prudent user cannot be expected to scrutinize the app's profile page with a fine-tooth comb for the [t]erms."

In other words, enforceability of a browsewrap increasingly depends on whether the end user is or should have

CONTINUED ON PAGE 17

CONTINUED FROM PAGE 16

been aware of the new or revised terms in the first place. Email and site banners may not be viewed by end users, so they may not create the type of actual or constructive knowledge contemplated by the court. That has shifted responsibility back to the site operator to build in new technologies, such as "blocker cards," "gateways" and "pop-up" functionalities, which put the end user on active notice of the updated terms. The gravity of such functionality was at the centerpiece of *Alkutkar*.

III. *'Alkutkar v. Bumble'*: Active consent demonstrated with blocker card technology

In January 2021, Bumble updated its terms of service to add an arbitration clause. Bumble then provided notice of the update to its end users via email and by implementing a "blocker card" that end users encountered when first opening the app. To fully access the app, an end user was required to affirmatively consent to the updated terms by checking a consent box presented with the blocker card.

Alkutkar, a Bumble user, filed a class action against Bumble on Jan. 22, 2022, for violations of consumer protection laws based on misleading advertisements. Bumble then filed a motion to compel arbitration based on the mandatory arbitration clause included in Bumble's updated terms of service. In response, Alkutkar asserted that he did not consent to Bumble's updated terms of service, including the mandatory arbitration clause.

Following development of an extensive evidentiary record, the court granted Bumble's motion on Sept. 8, 2022. In ruling for Bumble, the court heavily relied on the strength of Bumble's argument respecting the blocker card functionality, stating: "access and use of the app is a demonstrable consequence of Alkutkar's assent to the updated [t]erms. … Bumble's records indicate that plaintiff was shown the blocker card on his mobile Bumble app on March 4, 2021, at 22:27:35 GMT. … [P]laintiff's activity on the app on March 4, 2021, including adding photos and swiping on profiles, would not have been possible unless he first clicked to accept the updated [t]erms. … Plaintiff additionally accessed and used the app on March 5, 7 and 11, activities only achievable following clicking assent on the blocker card."

IV. *'Alkutkar v. Bumble'*: Motion for reconsideration denied

On Nov. 16, 2022, the District Court issued an order denying a motion for reconsideration brought by Alkutkar, claiming, in part, that there was a genuine dispute of material fact as to whether he viewed or agreed to the blocker card. Alkutkar asserted that either the blocker card did not appear or it did appear but someone else using his phone saw it and clicked the "I agree" button. The court was unpersuaded, however, and dismissed Alkutkar's claims as both "equivocating" and "self-serving."

The court reasoned that even if other people had access to Alkutkar's phone and clicked the "I accept" button on the blocker card, Alkutkar wouldn't know whether or not the blocker card appeared, rendering a key part of his claim as "mere speculation." Further, the fact that Bumble could not prove that it was Alkutkar and not someone else using Alkutkar's phone who clicked the button was unpersuasive. Alkutkar could have easily corroborated his claims with declarations from other users of his device explaining that they saw (or did not see) the blocker card. Instead, Alkutkar chose not to name the alleged other users or provide the dates they hypothetically used his phone to access his Bumble account. Interestingly though, in a footnote, the court stated that if the alternative explanation that someone else clicked "I accept" on the blocker card had been corroborated by Alkutkar, it might have created a triable issue.

In the final analysis, the court reaffirmed that Alkutkar had previously admitted that he accessed the app in March 2021 (after the date the blocker card had been implemented) and provided no corroboration at the time that the blocker card failed to work as intended. Therefore, even though Alkutkar claimed a genuine dispute of material fact as to whether he viewed and clicked on the blocker card, his inconsistent and contradictory statements necessarily precluded any reconsideration.

V. Looking ahead

Alkutkar and prior cases demonstrate that passive updates to terms (e.g., via browsewrap), standing alone, are likely insufficient. Therefore, implementing a mandatory clickthrough requirement designed to affirmatively secure consent to updated terms is now a best practice. Technologies like the blocker card used by Bumble present an effective means of securing consent and help create an evidentiary record of when a particular end user's account has accepted the terms.

However, businesses should be aware that arguments as to whether it was the account holder who actually manifested consent may be asserted in litigation. As such, we recommend using multifactor authentication methods to help strengthen the evidentiary record that it was the account holder — and not a third party — that consented to the revised terms.

In 2023, companies should be actively considering how to architect and implement sufficient mechanisms and technologies to ensure end users actively consent to updated terms of service. Polsinelli's technology attorneys are experienced in counseling on workflows for terms of service agreements, including how to secure consent for new and revised terms in both B2B and B2C agreements.

Cyber Incident Reporting for Critical Infrastructure Act: Significant Changes to Incident Reporting Are on the Horizon

Michael J. Waters
Shareholder
Chicago

Caitlin A. Smith
Associate
Washsington, D.C.

In May 2021, Colonial Pipeline, a privately held oil pipeline responsible for nearly half of the oil supply for the U.S. East Coast, was crippled by a DarkSide ransomware attack.[1] DarkSide is widely believed to be a Russian-based cybercriminal enterprise. Two days into the incident, President Joe Biden declared a state of emergency, which led to national fear of a gas shortage, panic buying, price spikes and gas lines. People were storing gas in trash bags and other unsafe containers, requiring the government to issue a warning about the dangers of these practices. Colonial Pipeline paid a $4.4 million ransom to DarkSide in exchange for a decryption key, partly because there was no sense of the impact when all systems were offline or how long it might take to recover without the decryption key.[2] All in all, the systems moving oil were only offline for five days, but the cascading effects on airline travel and consumer panic highlighted the vulnerability of U.S. infrastructure. While cyberattacks on the nation's infrastructure are not new, this event accelerated the U.S. government's efforts to address how the immediate and long-term harm caused by cyberattacks threaten national security.

In response to the ransomware attack on Colonial Pipeline, in March 2022 Congress passed, and Biden signed, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 to emphasize the importance of information sharing through mandated reporting of substantial cyber incidents and ransom payments by certain organizations.

What is CIRCIA?

At a high level, CIRCIA requires the Cybersecurity and Infrastructure Security Agency to create a clear set of regulations that mandate covered entities (1) to report covered cyber incidents and (2) to report ransomware payments to CISA on an expedited basis. CISA has several years to develop and finalize these regulations; however, these initiatives are executive priorities and the timeline to the final rule may be accelerated. From September to November 2022, CISA held a series of public listening sessions across the country to gather input and feedback on definitions, scope, triggers and procedures for covered entities reporting covered incidents, prior to the eventual publication of a "Notice of Proposed Rulemaking and Final Rule."

The act requires CISA to develop regulations around several requirements related to the reporting and sharing of covered cyber incidents, including the following:

- Cyber incident reporting requirements: Covered entities must report to CISA any covered cyber incidents within 72 hours from the time the entity reasonably believes the incident occurred.
- Federal incident report sharing: Any federal entity receiving a report on a cyber incident after the effective date of the final rule must share that report with CISA within 24 hours. CISA will also have to make information received under CIRCIA available to certain federal agencies within 24 hours.
- Cyber Incident Reporting Council: The U.S. Department of Homeland Security must establish and chair an intergovernmental Cyber Incident Reporting Council to coordinate, deconflict and harmonize federal incident reporting requirements.[3]

The act additionally authorizes several initiatives related to combating ransomware to include the following:

- Ransom payment reporting requirements: CIRCIA requires CISA to develop and issue regulations requiring covered entities to report to CISA within 24 hours of making any ransom payments as a result of a ransomware attack. CISA must share such reports with federal agencies.
- Ransomware vulnerability warning pilot program: CISA must establish a pilot program to identify systems with vulnerabilities to ransomware attacks and may notify the owners of those systems.
- Joint Ransomware Task Force: CISA has announced the launch of the Joint Ransomware Task Force in accordance with the statute to build on the important work that has already begun to coordinate an ongoing nationwide campaign against ransomware attacks. CISA will continue working closely with the FBI and the national cyber director to build the task force.[4]

CISA's goals are to "enhance the quality and effectiveness of information sharing and coordination efforts with appropriate entities" and "provide appropriate entities with timely, actionable[] and anonymized reports of cyber incident campaign[s] and trends, related contextual information threat indicators, and defensive measures."[5]

What industries and cybersecurity incidents are covered by CIRCIA?

CIRCIA regulates "covered entities," which are public and private organizations within industry sectors considered to be "critical infrastructure" as defined in Presidential

1 https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html.
2 https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html.
3 https://www.cisa.gov/circia#:~:text=RANSOMWARE%20INITIATIVES&text=Ransom%20Payment%20Reporting%20Requirements%3A%20CIRCIA,federal%20agencies%2C%20similar%20to%20above.
4 Ibid.
5 Division Y — Cyber Incident Reporting for the Critical Infrastructure Act of 2022, Sec. 2241, Cyber Incident Review.

CONTINUED ON PAGE 19

CONTINUED FROM PAGE 18

Policy Directive 21. In total, PPD-21 designated 16 critical infrastructure sectors whose assets, systems and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on national security, national economic security, national public health or safety, or any combination thereof.[6]

When most people think about critical infrastructure, industries like oil, gas, energy, transportation, water and emergency services come to mind. However, PPD-21 also includes the financial services and health care industries, which are already highly regulated under state and federal data privacy regimes.

CIRCIA requires covered entities to report "significant cyber incidents" to CISA within 72 hours of discovery. A significant cyber incident is a cyber incident or a group of related cyber incidents that are likely to result in demonstrable harm to the national security interests, foreign relations or economy of the United States or to the public confidence, civil liberties or public health and safety of the people of the United States.[7] While it is obvious, for example, that a ransomware attack that limits a hospital's ability to deliver patient care is a "significant cyber incident," covered entities have not received much guidance around reporting less disruptive cybersecurity incidents.

How does CIRCIA change existing incident notifications and timelines?

For certain industries, like health care, CIRCIA imposes a quick regulatory notification obligation for the first time. CIRCIA also broadens the definition of a reportable event for health care entities. Currently, under the Health Insurance Portability and Accountability Act, covered health care entities are not required to report ransom payments or incidents to the U.S. Department of Health & Human Services (HHS) if the incidents do not involve access to, or covered entities' inability to access, patient protected health information. Notably, CIRCIA contains an exception to the reporting requirement for entities "required by law, regulation[] or contract to report substantially similar information to another [f]ederal agency within a substantially similar time frame."[8] Since HIPAA-covered entities are not required to report ransom payments or events that do not involve PHI to HHS, health care entities do not meet the exception to CIRCIA's reporting requirement and likely will be required to disclose many more incidents under much shorter timelines.

Other industries, like financial services, will add yet another urgent reporting obligation to the list. Currently, banks are already required to provide notice to federal regulators within 36 hours following a cybersecurity incident that disrupts the bank's ability to serve its customers.[9] Financial institutions licensed in New York are required to report cybersecurity events to the New York Department of Financial Services within 72 hours of discovering an incident. The National Credit Union Association has also proposed a rule requiring federally insured credit unions to notify the NCUA within 72 hours of discovering a substantial cyber incident. It is unclear at this stage whether these timelines will be considered "substantially similar" to those required under CIRCIA or whether CIRCIA has a sharing mechanism in place with the regulators enforcing these reporting timelines, such that these financial institutions meet the exception to the 24- or 72-hour reporting requirement under CIRCIA.

How should organizations prepare for CIRCIA?

While there is still some time before we receive the final rule from CISA, it is important for organizations that fall within one of the 16 critical infrastructure categories to begin planning for CIRCIA as outlined.

Review the list of 'critical infrastructure' industry sectors

Does CIRCIA apply to your organization? Many organizations may not realize the broad scope of CIRCIA. The critical infrastructure sectors defined by DHS include chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial, emergency services, energy, financial services, food and agriculture, government facilities, health care and public health, information technology, nuclear reactors and waste, transportation, and water and wastewater. Organizations that fit within these sectors should be aware of the developing law and understand the applicability of the reporting obligations.

Monitor the rulemaking process

Organizations that are covered by CIRCIA should keep tabs on the rulemaking process. Public listening sessions recently concluded, which could result in changes to the proposed reporting requirements and timelines. Organizations should stay up to date on these changes and understand what provisions make the final rule.

Update incident response plans

Organizations within the scope of CIRCIA should develop or update incident response plans to address these time-sensitive notification requirements. For many sectors, the quick reporting requirements will be unfamiliar and could be easily overlooked in the critical early hours of a security incident response. An incident response plan should include detailed procedures for evidence preservation and collection. For instance, even if you are an organization with no intention or need to pay a ransom payment as part of a ransomware incident, collecting details from the ransom note and encrypted files will be essential for reporting the incident to CISA.

Train an incident response team

Organizations should also ensure their incident response team is briefed on the CIRCIA reporting requirements. Information security and information technology teams are often the first to know about a security incident. It is very important for these teams to understand the new timelines and the internal process for quickly informing in-house and/or outside counsel about a security incident that could be a covered incident under CIRCIA. For organizations that have never experienced a significant cyber event like ransomware, it is hard to comprehend the number of competing priorities within the first few days of responding to an incident. Building an awareness of the CIRCIA reporting requirements across departments will give organizations the best opportunity to be compliant with these new processes.

6 https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
7 https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
8 Ibid.
9 36-Hour Reporting Requirement for Disruptive Incidents (12 CFR Part 304).

The Increasing Risks and Prohibitions Associated With Paying a Ransom After a Ransomware Attack

Alexander D. Boyd
Shareholder
Kansas City

Kayleigh S. Shuler
Associate
Kansas City

Jessica L. Peel
Associate
Kansas City

While all data security incidents have the potential to cause reputational, operational and financial harm to an organization, ransomware attacks are among the most devastating cyberthreats facing organizations. Ransomware victims discover that their critical files are encrypted and inaccessible. They often also receive threats that their data has been stolen. Depending on the organization's level of preparation before an attack, recovery options may be limited. Ideally, the organization will have recent, unencrypted backups that can quickly be used to recover data and restore operations. In many circumstances, however, the available backups are also encrypted, are outdated or will take meaningful time to access and utilize. While no organization wants to pay a ransom to a threat actor, in some circumstances that may be the only viable option to avoid the permanent loss of critical data or significant operational disruptions. Recently, however, states have begun to consider and enact laws prohibiting certain ransom payments. This trend makes it even more important for organizations to invest in their cybersecurity safeguards and preparations.

Ransomware background

Ransomware is a type of malicious software, or malware, where the attacker locks and encrypts the victim's computer files, systems or networks until a ransom is paid. Attackers also increasingly exfiltrate data prior to encryption, thereby allowing the attacker to extort the victim in two ways: (1) by withholding the key to unlock the encrypted data and (2) by threatening to leak sensitive data on the dark web. In 2021, the FBI received 3,729 complaints of ransomware, representing only a portion of the overall ransomware threat landscape.[1]

Existing risks for making or facilitating a ransomware payment

The FBI, not surprisingly, does not advise organizations to pay criminals their ransom demands because the payment contributes to a criminal enterprise, does not guarantee that an organization will regain access to its data and may incentivize more attacks. Moreover, there is typically minimal legal benefit to paying a ransom because payment does not eliminate an organization's potential notification obligations under applicable data breach notification laws.

Notwithstanding these practical considerations, however, paying a ransom has historically been permitted by law unless the recipient of the funds is on the U.S. Department of Treasury Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons List (often referred to as the OFAC List). In those cases, there are potential civil and criminal penalties for making or facilitating ransomware payments. Assessing whether a particular criminal is on the OFAC List is therefore standard practice for cyber professionals involved with facilitating cyber ransom payments. Until recently, however, there were few other legal considerations to the question of whether payment of a ransom is legally permissible.

New state prohibitions on paying ransom demands

On April 5, 2022, North Carolina became the first state to prohibit state agencies and local government entities from paying a ransom demand in connection with a ransomware attack. The North Carolina law also goes a step further and prohibits government entities from even communicating with ransomware groups.[2] Government entities experiencing a ransom request in connection with a cybersecurity incident are also required to notify the North Carolina Department of Information Technology.[3] The applicability of the North Carolina law is broad and includes any "agency, department, institution, board, commission, committee, division, bureau, officer, official or other entity of the executive, judicial or legislative branches of State government" as well as "The University of North Carolina and any other entity for which the State has oversight responsibility."[4] The law's prohibition on communicating with threat actors is notable, as even victims with no desire or need to pay a ransom will often communicate with threat actors to gain information that can aid the forensic investigation (e.g., information about what data was stolen and from what systems) and to buy time to investigate and inform involved individuals before data is leaked.

Similar to North Carolina, Florida amended its State Cybersecurity Act to prohibit state agencies, counties and municipalities experiencing a ransomware attack from paying or otherwise complying with a ransom demand.[5] The amendments went into effect on July 1, 2022. The Florida law also requires state agencies and local governments to report ransomware attacks to the Florida Department of Law Enforcement's Computer Crime Center, the state's Cybersecurity

1 https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.
2 *See* N.C. Gen. Stat. Ann. § 143-800(a).
3 *See* N.C. Gen. Stat. Ann. § 143-800(b).
4 *See* N.C. Gen. Stat. Ann. § 143-800(c).
5 *See* Fla. Stat. Ann. § 282.3186.

CONTINUED ON PAGE 21

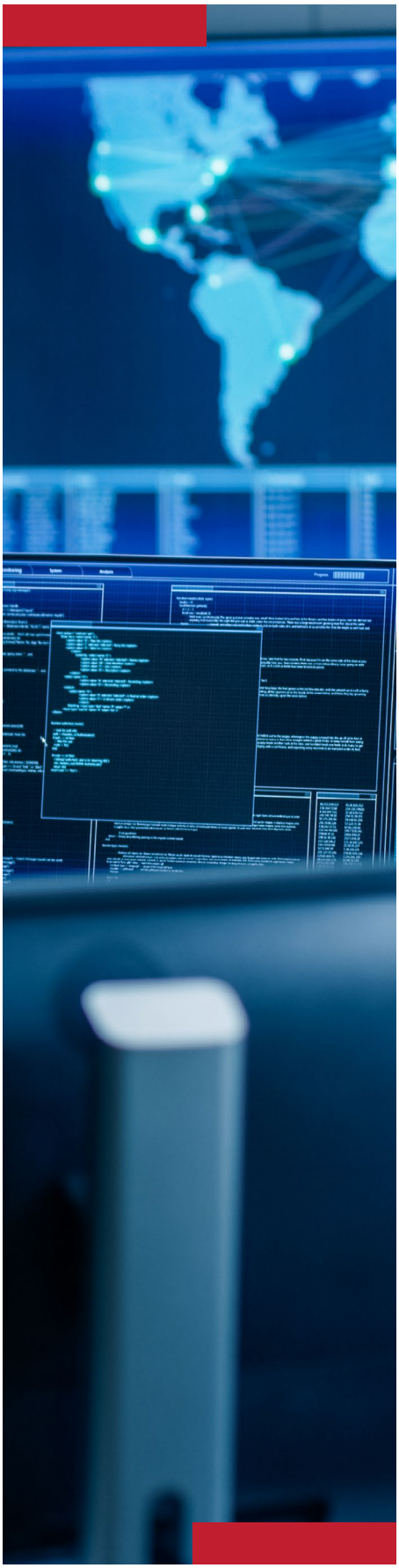
CONTINUED FROM PAGE 20

Operations Center and the local sheriff within 12 hours of a ransomware incident.[6] In contrast to the North Carolina law, the Florida law arguably does not prohibit communications with the ransomware groups and it does not apply to university boards of trustees or state universities.[7]

The rationale behind the North Carolina and Florida laws is twofold. First, some argue that a lack of financial incentive (in the form of ransom payments) will deter ransomware groups from attacking government entities. Second, some argue that constraints on the ability to purchase decryption keys will force government entities to take a more proactive and aggressive approach to cybersecurity designed to prevent successful attacks in the first place. Regardless of the merits of these arguments, in practical terms, an organization subject to these constraints that nevertheless experiences an attack may face permanent loss of sensitive or otherwise important data and critical services that could become unavailable if a secure backup of the impacted systems is not available or if the systems cannot be restored in a timely manner. Additionally, North Carolina's prohibition on even communicating with ransomware groups may hinder government entities from obtaining potentially valuable intelligence regarding the scope and nature of the attack through negotiations.

Following in North Carolina and Florida's footsteps, Arizona, Pennsylvania, New York and Texas have introduced similar legislation banning payments by government entities in connection with ransomware attacks. Pennsylvania's Senate approved a bill banning state agencies from using taxpayer funds to pay ransomware demands, except in cases where the governor declares a state of emergency and authorizes payment. New York is also pursuing legislation that would broadly ban ransomware payments by government entities, as well as by businesses and health care entities. Finally, Texas has introduced legislation that would prohibit government entities or political subdivisions from paying ransom demands. To date, the ransomware payment bans in these states have not yet been enacted.

While the current state prohibitions on ransom payments may impact a relatively small number of organizations, if legislators continue to take aggressive positions on ransom payments, a growing number of organizations may face additional legal hurdles when recovering from a ransomware attack. Organizations should strongly consider investing in their cybersecurity programs and data backup solutions and practicing their incident response plans.



6 *See* Fla. Stat. Ann. § 282.318(3)(c).
7 *See* Fla. Stat. Ann. § 282.3186.

‘Code Is Law’ Embraces Jurisdictional Protections: IP Trends for NFTs in 2022 and 2023

Jonathan E. Schmalfeld
Associate
St. Louis

Daniel P. Mullarkey
Shareholder
Washington, D.C.

Stephen A. Rutenberg
Shareholder
Miami, New York

The summer of 2021 was known by many as the “Summer of .jpgs,” as popular blockchain-based projects like NBA Topshot, Bored Ape Yacht Club and other cryptographically verified digital goods reached mainstream recognition. In 2020, the total estimated sales of non-fungible tokens was $94.9 million. That number grew to $41 billion in 2021.[1]

Even with the cryptocurrency market crash in May 2022, through July 2022 NFT sales had already exceeded the $41 billion in sales from the year before.[2] Many large corporations have also entered the space, with Nike purchasing NFT startup company RTFKT,[3] AB InBev releasing a range of NFT products,[4] Starbucks announcing a plan to put customer rewards on the blockchain[5] and Animoca Brands announcing a new $2 billion fund to invest in metaverse projects. With this increased level of funding and business sophistication, there has also been an increased emphasis on legal protections of intellectual property. While in 2021 “code is law” was the prevailing form of protection over digital assets, in 2022 there was an increased emphasis on jurisdictional laws, especially in the area of IP. This is a trend that we believe will continue into 2023 and beyond.

Trademark applications

In 2022, nearly 6,500 trademark applications were filed with the United States Patent and Trademark Office involving NFTs or digital assets, which is more than three times as many as were filed in 2021 (2,142).[6] While some of these filings were 15 U.S. Code § 1051(a)(1) actual use applications by NFT-focused businesses cleaning up their IP portfolios in 2022, the largest groups of applicants were for established businesses applying for NFT trademarks on a 15 U.S. Code § 1051(b)(1) actual intent to use basis.

In November 2022 alone, BMW, Rolex, Enterprise Rent-A-Car, Indianapolis Motor Speedway, Post Foods, Nike, Home Depot, Reebok, Lionsgate and other household names all applied for trademarks over NFTs and digital asset-related goods and services on a (b)(1) intent to use basis.

It is not altogether clear how the trademark office is going to treat NFT and digital asset-related goods and services. The USPTO and U.S. Copyright Office are currently studying the impact of NFTs on IP rights.[7] Many of the trademark filings include physical goods classes along with software-related goods and services. As the law evolves, it will be interesting to see where digital assets will fall along the Nice Classification system. For now, strategies usually involve filing broadly to cover both physical goods and software-related goods and services.

IP litigation

Similarly, in 2022 we saw a rise in IP litigation, especially in the area of trademarks and copyrights.

In May 2022, the U.S. District Court for the Southern District of New York refused to dismiss a trademark infringement case brought by Hermes International and Hermes of Paris Inc. against artist Mason Rothschild over his sale of NFTs sold as “MetaBirkins” and displaying digital images of faux fur-covered versions of the luxury Birkin handbags.[8] In June, a federal district court in the Central District of California found that a plaintiff’s state law right of publicity claim regarding the use of copyrighted photos in NFTs was preempted by federal copyright law.[9]

In September, Quentin Tarantino and Miramax reached a settlement over their litigation regarding the auction of “Pulp Fiction” NFTs by Tarantino. Tarantino argued that he reserved the rights to “print publication (including without limitation screenplay publication, ‘making of’ books, comic books and novelization, in audio and electronic formats as well, as applicable)” as well as “interactive media,” which included the right to sell portions of his script as NFTs. Miramax, on the other hand, argued that NFTs did not exist in 1996 when their licensing agreement was consummated and

1 Chainalysis, The 2021 NFT Market Report (Jan. 2022), available at https://go.chainalysis.com/nft-market-report.html.
2 Chainalysis, The Chainalysis State of Web3 Report (June 2022), available at https://go.chainalysis.com/2022-web3-report.html.
3 https://about.nike.com/en/newsroom/releases/nike-acquires-rtfkt.
4 https://nft.budweiser.com/.
5 https://stories.starbucks.com/press/2022/starbucks-brewing-revolutionary-web3-experience-for-its-starbucks-rewards-members/.
6 Bannermanquist, Judith, “Trademarks filed for NFTs, metaverse and cryptocurrencies soar to new levels in 2022” (Nov. 7, 2022), available at https://cointelegraph.com/news/trademarks-filed-for-nfts-metaverse-and-cryptocurrencies-soar-to-new-levels-in-2022.
7 https://copyright.gov/policy/nft-study/.
8 Hermes v. Rothschild, Case No. 22-cv-384 (JSR), 2022 WL 1564597 (S.D.N.Y. May 18, 2022).
9 Notorious B.I.G. LLC v. Yes.Snowboards, 2022 U.S.P.Q.2d 526 (C.D. Cal. 2022).

CONTINUED ON PAGE 23

CONTINUED FROM PAGE 22

thus NFTs fell under the catch-all language in the contract granting Miramax "all rights … now or hereafter known … in all media now or hereafter known" in the work.[10]

One of the bigger 2022 NFT-based IP rights cases is an ongoing matter brought by Yuga Labs Inc. (the creators of BAYC) against artist Ryder Ripps and his business partner, Jeremy Cahen, for trademark infringement over their RR/BAYC project.[11] The RR/BAYC project took the images represented in the popular Bored Ape Yacht Club NFTs and sold visually identical NFTs under the RR/BAYC brand. Defendant Ripps has argued, in a motion to dismiss, that his use of the Bored Ape images and associated Yuga Labs trademarks (such as the ape skull logo and the BAYC/BORED APE/BORED APE YACHT CLUB trademarks) is protected free speech under the Roger's test.[12] Yuga Labs, on the other hand, argues that this is a classic case of trademark infringement in which the alleged infringers gained millions by using the Yuga Labs trademarks, harming Yuga Labs in the process. Yuga Labs recently won on those dueling motions, with the court refusing to dismiss Yuga's trademark infringement claims against the defendants.[13] The results of the case may turn on the upcoming decision in *Jack Daniel's Properties, Inc. v. VIP Products, LLC*.[14] The Supreme Court recently granted certiorari to hear this case and it is expected to have implications for the tension between parody and IP.

With the money involved in the NFT industry and the rising level of IP sophistication for companies currently in the space and those entering the space, litigation is expected to increase. This increase is especially anticipated with so many unknowns, such as the protectability of artificial intelligence-generated NFT images,[15] registration of copyrights over large collections (known commonly as "PFP projects"),[16] enforceability of early and unsophisticated license grants,[17] and the effectiveness of terms that include the right to amend subsequent to purchase.

Licensing gets sophisticated

Early in the proliferation of NFTs, particularly in the art space, an interesting and potentially groundbreaking practice developed where certain IP pertaining to the NFTs was licensed to the NFT buyers and passed to their subsequent transferees. The Web3 industry mentality surrounding the decentralization of ownership, including ownership of copyrights and other IP, is a new development that is likely to have legal ramifications across all industries.

The BAYC "commercial use" license in the BAYC terms and conditions was intended by Yuga Labs to allow Bored Ape NFT holders to fully commercialize the images represented in their NFTs.[18] However, this was an exceedingly simple license grant and others have questioned its enforceability.[19]

In March, Yuga Labs purchased the CryptoPunks IP from Larva Labs and promised "[w]ith this acquisition Yuga Labs will own the CryptoPunks and Meebit brands and logos, and as they've done with their own BAYC collection, Yuga Labs will transfer IP, commercial[] and exclusive licensing rights to individual NFT holders."[20] However, when Yuga Labs issued that IP license, it wasn't the two-paragraph license it had used for BAYC; instead, the company went with a more comprehensive and detailed 17-page set of licensing terms.[21]

In August, Andreessen Horowitz, one the biggest venture investors in the Web3 space, released a set of free public licenses designed to be used by NFT project developers as a uniform licensing standard in the space. The self-titled "Can't Be Evil" licenses are a set of six licenses ranging from the most restrictive "Personal Use License" agreement (CBE-PR) to the least restrictive "CC0 1.0 Universal" agreement (CBE-CC0). A16z's stated goal in creating these licenses was to "transparently [codify] the rights of NFT creators, buyers[] and sellers so that every party has a common understanding of the rights associated with NFT ownership."[22]

Conclusion

As with any new form of IP grant, this mass licensing of IP to consumers is likely to evolve over time, especially as more disputes over those terms work their way through the courts. Companies currently in the space or established brands looking to expand into NFTs will need to have attorneys who understand the unique and constantly evolving IP registration and licensing issues facing this new asset class.

10 *Miramax, LLC v. Quentin Tarantino*, Case No. 2:21-cv-08979 FMO (JCx) (C.D. Cal. 2021).
11 *Yuga Labs, Inc. v. Ripps et al.,* Case No. 2:22-cv-04355-JFW (JEM) (C.D. Cal. 2022).
12 *Rogers v. Grimaldi*, 875 F.2d 994 (2d Cir. 1989).
13 *Yuga Labs, Inc. v. Ripps et al.,* Case No. 2:22-cv-04355-JFW (JEM), Doc. #62 (C.D. Cal. Dec. 16, 2022).
14 *Jack Daniel's Properties, Inc. v. VIP Products, LLC*; Case No. 18-16012 (9th Cir. 2020).
15 https://www.copyright.gov/laws/hearings/Letter-to-USPTO-USCO-on-National-Commission-on-AI-1.pdf; Graves, Franklin, "Sorry, Your NFT Is Worthless: The Copyright and Generative Art Problem for NFT Collections" (Feb. 20, 2022), available at https://ipwatchdog.com/2022/02/20/sorry-nft-worthless-copyright-generative-art-problem-nft-collections/id=146163/.
16 https://www.govinfo.gov/content/pkg/FR-2022-11-23/pdf/2022-25211.pdf.
17 Murray, Michael D., "Transfers and Licensing of Copyrights to NFT Purchasers" (July 2, 2022), available at https://ssrn.com/abstract=4152475.
18 https://boredapeyachtclub.com/#/terms.
19 Steiner, Alfred/Dave, "Bored Apes & Monkey Selfies: Copyright & PFP NFTs" (May 21, 2022), available at https://ssrn.com/abstract=4116638.
20 "Yuga Labs Acquires CryptoPunks and Meebits from Larva Labs; Grants IP and Commercial Rights to Individual Owners" (March 11, 2022), available at https://www.businesswire.com/news/home/20220311005470/en/Yuga-Labs-Acquires-CryptoPunks-and-Meebits-from-Larva-Labs-Grants-IP-and-Commercial-Rights-to-Individual-Owners.
21 https://licenseterms.cryptopunks.app/.
22 Jennings, Miles and Dixon, Chris, "The Can't Be Evil NFT Licenses" (Aug. 31, 2022), available at https://a16zcrypto.com/introducing-nft-licenses/.

Blockchain Technology: High-Profile Use Cases in the News and Other Alternative Use Cases

Mark A. Petry
Shareholder
Washington, D.C.

Kyle D. Reather
Associate
Kansas City

Cryptocurrencies and non-fungible token (NFT) news headlines currently focus on the market crash (sometimes framed as a crypto-winter or crypto-extinction), fraud and the collapse of various crypto exchange platforms — or the "wealth" being created or lost through cryptocurrencies and NFTs. Earlier, in 2021 and the first half of 2022, headlines were focused on the meteoric rise in value of cryptocurrencies, digital art marketed as NFTs, and platforms and exchanges that facilitated these transactions using blockchain technology. Looking ahead to 2023 and beyond, further legislation and regulation, along with the enforcement of existing laws and regulations, is inevitable in connection with these financial, investment and otherwise speculative use cases relating to cryptocurrencies, NFTs and blockchain technology.

However, the underlying blockchain technology could be (and is being) used for less headline-grabbing and more mundane, pragmatic and less speculative purposes, and those use cases should not be confused with the use cases typically seen in headlines.

What the future holds for cryptocurrencies, NFTs and other similar uses of blockchain technology is hotly debated, and many people have strong feelings about these developments — especially about the value of new currencies, NFTs and the like. However, regardless of one's feelings and beliefs in this regard, we think everyone should be aware that the legal and business risks vary greatly depending on the use case of the blockchain technology. At its core, blockchain technology is about securely recording and tracking transactions via a ledger that can then be used for many nonspeculative purposes unrelated to cryptocurrencies or digital asset speculation, several of which are discussed below.

Alternative blockchain uses

1. Personal information verification. The ability to both secure and self-authenticate information makes blockchain technology a promising tool to help authenticate and validate who should have access to personal information, including in connection with financial, health care, travel and other data.
2. Welfare and government distributions. With access to self-authenticating, secure personal information using blockchain technology, government distributions could be made more reliable and efficient. Eligible recipients can be verified and obtain access more readily, while ineligible applicants can be more readily identified.
3. Health information. Medical records could be accessed, with sensitive information kept more secure, through blockchain technology used to authenticate an individual's identity. Insurance coverage could be more readily verified, administrative costs and lags could be reduced, and treatment could then be provided more quickly and cost effectively.
4. Media royalties. Blockchain technology can be used to help authenticate who has rights relating to music and video downloads. In addition to mitigating piracy and unauthorized copying, views and playbacks could be more accurately logged. In addition, "smart contracts," typically associated with crypto and NFT transactions, could facilitate automatic royalty payments.
5. Supply chain and logistics. By tracking shipments on a distributed ledger, multiple parties along a supply chain can access real-time and historical information about each shipment. Because blockchain technology could track the chain of ownership and transactions, the presence of counterfeit goods could be more readily identified and mitigated.
6. Loans and insurance administration. The use of blockchain authentication and associated smart contracts in lending and insurance could improve efficiency in connection with various administrative and processing activities, including insurance documentation and coverage, liens, and collateral.

Legal principles to consider

Blockchain is an exciting, promising and relatively secure technology, but like most technology, its use cases and how humans use (or abuse) it need to be considered when entering into transactions, contracts or relationships involving the blockchain. Nothing is perfectly safe or secure, nor is it free from the human element at some level — including error, omission or abuse. For example, people may lose passwords or other credentials or new technologies may arise, which could increase the potential for hacking and the circumvention of encryption mechanisms underlying the blockchain.

Time-tested and basic business, legal and contracting principles should be kept in mind when considering the use of blockchain technology, including (1) counterparty and other due diligence and analysis, (2) legal and regulatory compliance analysis, and (3) robust and thoughtful contractual provisions and protections based on the nature of the use case and application, including the allocation of risks (whether known or unknown).

If you are a vendor providing products or services incorporating blockchain technology, reasonable and appropriate disclaimers about the technology and ancillary human elements should exist in your contracts. Conversely, if you are a customer or consumer purchasing products or services using blockchain technology, be realistic and cautious about the potential benefits and ensure there are appropriate controls, safeguards, remedies and recourse that could be realistically enforced.

CONTINUED ON PAGE 25

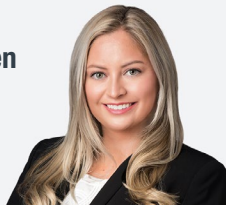
CONTINUED FROM PAGE 24

Conclusion

Just because cryptocurrencies and NFTs, which use blockchain technology, have been in the news grabbing alarming headlines about potential fraud and massive financial gains or losses, there are still other use cases and applications of blockchain technology that, while perhaps less glamorous or newsworthy, may potentially be more profound and beneficial in everyday life in the future.

Will a New Wave of Lawsuits Roll Into a Nationwide Tsunami? Wiretapping Litigation for Website Analytics

Elizabeth M. Marden
Associate
Kansas City



Adam A. Garcia
Associate
Kansas City

Colin H. Black
Associate
Chicago

Elizabeth (Liz) Harding
Technology Transactions & Data Privacy Vice Chair
Denver

2022 has seen a new wave of class action lawsuits targeting companies that use technology to track consumers' interfaces on their websites. These lawsuits generally allege that the use of technologies such as session replay tracking pixels, and chatbots, result in the interception of communications in violation of federal and state wiretapping laws. To minimize potential liability, companies need to be aware of what technologies are used on their platforms, how they are used and what consents need to be obtained from platform users.

Legal background of claims

Plaintiffs often ground their claims in the electronic interception provisions of federal and state wiretapping laws. Under the Federal Wiretap Act of 1968, a person is prohibited from "intentionally intercept[ing] … any … electronic communication." 18 U.S.C. § 2511(1)(a) (2022). The FWA and many state statutes define "interception" as "acquiring the contents of that electronic communication." Id. § 2510(4). "Content" is defined as "any information concerning the substance, purport[] or meaning of that communication." Id. § 2510(8). Under the FWA, a court may require a defendant to pay $10,000 per violation. Id. § 2520(c)(2). Fines under similar state laws range from $1,000 to $50,000 per violation, depending on the state.

While most states generally follow the FWA and its definitions, some states materially differ in their consent requirements. The FWA and some states require consent from only one party to intercept a communication. By contrast, California, Connecticut, Delaware, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Oregon, Nevada, New Hampshire, Pennsylvania and Washington require all parties to the communication to give prior consent to an interception. While litigation most commonly occurs under state laws requiring all-party consent, wiretapping litigation for collection of website analytics has recently been brought under state statutes requiring one-party consent, such as those in Missouri. See *Tucker v. BPS Direct, LLC*, No. 6:22-cv-3285, at *14-15 (W.D. Mo. Nov. 7, 2022); *Tucker v. Cabela's LLC*, No 6:22-cv-3288, at *1 (W.D. Mo. Nov. 9, 2022).

Practices triggering litigation

Session replay

Session replay technologies monitor interactions on websites and other platforms, often recording mouse clicks, keyboard strokes, zooming or cursor movements. Session replay software is designed to capture information at regular intervals to allow the consumer's interface to be re-created by overlaying a consumer's inputs over an image of the website.

These programs assist with consumer experience, compliance and website operation. For example, website owners can use this technology to validate acceptance of contractual terms, identify broken hyperlinks or identify areas of consumer confusion. Depending on the type of software utilized, sensitive information can sometimes be redacted or excluded from capture, depending on which settings are enabled.

Recent decisions in the U.S. Courts of Appeals for the Third and Ninth circuits may

CONTINUED ON PAGE 26

CONTINUED FROM PAGE 25

have opened the door to a potential surge in this type of litigation. See *Javier v. Assurance IQ, LLC*, No. 21-16351, 2022 WL 1744107, at *2 (9th Cir. May 31, 2022) (reversing dismissal of a session replay claim); *Popa v. Harriet Carter Gifts, Inc*., 52 F.4th 121, 128 (3d Cir. 2022) (same). These decisions have spawned numerous session replay lawsuits against companies like Goodyear, Michaels and Cabela's.[1]

Chatbots

Chatbots enable website and other platform operators to engage with users to answer questions and provide information and technical support. Chatbots are often cost-efficient tools allowing companies to communicate with consumers without the need for live website customer service. Many companies record communications between consumers and chatbots. Recording these conversations can improve the user experience by identifying areas of consumer confusion or creating better automated options for the chatbot.

Plaintiffs have recently filed numerous chatbot lawsuits against companies like Columbia Sportswear, Old Navy, Goodyear and M.A.C. Cosmetics.[2] These are original claims and could result in damages of $5,000 per individual violation.

Meta Pixel

Meta Pixel is a tracking code developed by Meta that enables the collection of a website user's activity and links that activity with the user's Facebook ID such that their activity is shared with Meta. Meta Pixel can be implemented with only a few lines of JavaScript and works by collecting data about a user and, in combination with certain fingerprinting technologies, can be connected with other cookie data to compile or add to a "profile" of the given user. Meta Pixel is not visible to an untrained user and is capable of data collection irrespective of whether an individual actively utilizes Meta services such as Facebook, Instagram or WhatsApp.

Recent cases focus on website operators that allegedly use Meta Pixel to record and analyze the user's website usage and as a result enable Meta to access such information. Since the website user did not consent to this tracking, plaintiff's counsel claims that the website operator's recording of it is in violation of various wiretapping and other laws. Claims have also been brought directly against Meta.[3] In the context of state wiretapping laws, website hosts may face exposure if they enable Meta Pixel, thereby allowing Meta to "intercept" electronic communications without prior consent.

In addition to claims under State wiretapping laws, hospitals that have enabled Meta Pixel on patient facing portals are also facing claims under the Health Insurance Portability and Accountability Act (HIPAA). In one recent case, the hospital is alleged to have set Meta Pixel to track patient communications through its patient portal, thus enabling Meta to capture patients' protected health information without obtaining prior consent from the data subjects.[4] This sharing of PHI with Meta was recently disclosed under data breach notification laws and is now the subject of class action litigation related to the unauthorized disclosure of PHI.

What to watch for

Type of consent required

While some courts interpreting state laws have left open the possibility of implicit or contemporaneous consent as a defense to this type of litigation, other courts indicate that prior consent is required. Recently, both the Third and Ninth circuits have signaled that the California and Pennsylvania state statutes may require prior consent before an interception or recording of website analytics can be made. See *Javier v. Assurance IQ, LLC*, No. 21-16351, 2022 WL 1744107, at *2 (9th Cir. May 31, 2022) (determining that the wiretapping provision of the California Information Privacy Act "require[s] the prior consent of all parties to a communication," which standard is not met by providing notice in a linked privacy notice); *Popa v. Harriet Carter Gifts, Inc.,* 52 F.4th 121, 128 (3d Cir. 2022) (determining the same for the wiretapping provision of the Pennsylvania Wiretapping and Electronic Surveillance Control Act). Other courts, by contrast, have left open the possibility of implicit or contemporaneous consent. See, e.g., *Goldstein v. Costco Wholesale Corp.,* 559 F. Supp. 3d 1318, 1322 (S.D. Fla. Sept. 9, 2021) (dismissing a session replay claim on statutory interpretation without considering consent); *Swiggum v. EAN Services, LLC*, No. 8:21-cv-493, 2021 WL 3022735, at *2 (M.D. Fla. July 16, 2021) (deciding the Florida Security of Communications Act does not apply to novel session replay).

Who is a party to the communication

Courts are split on whether third-party technology service providers are "parties" to a communication between a website operator and a consumer for the purpose of determining whether parties gave consent for the interception. In *In Re Facebook Internet Tracking Litigation*, the Ninth Circuit found that Facebook was not a party to the communication when its plug-ins duplicated users' messages to third-party sites. 956 F.3d 589, 608 (9th Cir. 2020) (adopting similar reasoning as the First and Seventh circuits). By contrast, in *In Re Google Inc. Cookie Placement Consumer Privacy Litigation*, the Third Circuit found that Google was a party to the communication because the plaintiff's web browser communicated directly with Google's servers through services embedded in the web browser. 806 F.3d 125, 140-43 (3rd Cir. 2015); see also *In Re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 274-76 (3rd. Cir. 2016) (citing to Google and concluding the same).

What constitutes the 'content' of a communication

State wiretap statutes only prohibit eavesdropping on the "content" of the communications, but courts are divided over what constitutes content. Some courts have determined that recordings of mouse movements, keystrokes and clicks is noncommunicative, comparable to what a security camera detects at a physical storefront. See *Goldstein v. Costco Wholesale Corp*., 559 F. Supp. 3d 1318, 1321-22 (S.D. Fla. 2021) (finding the keystrokes and search terms are the "cyber analog" to in-person movements). Other courts have determined that these recordings could be content because they communicate precisely what the user intended. See *Alhadeff v. Experian*

1 *Alves v. Goodyear Tire and Rubber Co*., No. 1:22-cv-11820, at *1 (D. Mass. Oct. 24, 2022); *Farst v. Michaels Stores, Inc*., No. 1:22-cv-01433 (M.D. Penn. Sept. 14, 2022); *Tucker v. Cabela's LLC,* No. 6:22-cv-3288, at *1 (W.D. Mo. Nov. 9, 2022).
2 *Cody v. Columbia Sportswear Co*., No. 8:22-CV-01654 (C.D. Cal. Sept. 7, 2022); *Licea v. Old Navy, LLC*, No. 5:22-CV-01413 (C.D. Cal. Aug. 10, 2022); *Byars v. The Goodyear Tire and Rubber Co.,* No. 5:22-cv-01358 (C.D. Cal. Aug. 1, 2022); *Valenzuela v. M.A.C. Cosmetics Inc*., No. 5:22-cv-01360 (C.D. Cal. Aug. 1, 2022).
3 See, e.g., *Stewart v. Advocate Aurora Health, Inc. & Meta Platforms, Inc.,* No. 1:22-cv-5964 (N.D. Ill. Oct. 28, 2022).
4 See above.

CONTINUED ON PAGE 27

CONTINUED FROM PAGE 26

Info. Sols., Inc., 541 F. Supp. 3d 1041, 1045 (C.D. Cal. 2021) (finding the defendant obtained information from the plaintiff's movements, such as "personal interests, browsing history, queries[] and habits"). This issue can be an important turning point in litigation because defendants may not violate wiretapping statutes if they are not intercepting "content."

Mitigating risk

The common theme in all these cases, regardless of technology deployed, is that the website user was not aware of, and did not consent to, the monitoring/recording of their communications. The courts have generally held that when a website user is aware of the use of these technologies and provides consent prior to the use of the website, there is no violation of wiretapping laws. In practice, this means providing notice to users of the enablement of Meta Pixel (and other cookies) and session replay technologies on the website via the site's cookie banner and notice. Where chat functions are used, consent language should be included in the chat feature before the user inputs their information. Finally, appropriate language should be included in the site's privacy notice and terms of use, which notice and terms should be affirmatively accepted (or at least acknowledged) by the website user.

Health care providers should also carefully consider the technologies enabled on their websites to understand what information may be collected by, or transferred to, the technology provider. To the extent the technology enables the sharing of PHI, consideration should be given to whether a business associate agreement is in place with the technology provider (and other requirements under HIPAA are complied with) and/or disabling applicable functionality.

Regulatory Overreach/Litigation Remedies To Curtail Regulatory Excess by Federal Trade Commission

Cate A. Green
Associate
Kansas City

With the rise of large-scale, high-profile data breaches, the Federal Trade Commission has expressed its intent to hold companies accountable. (See "Consumer Financial Protection Circular 2022-04," Consumer Financial Protection Bureau, https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/.) But most alarmingly, there has been a move toward enforcement against company executives in their individual capacity. Whether such enforcement falls within the scope of the FTC Act, however, is another question.

The FTC issued a draft complaint against Drizly LLC and its CEO, James Cory Rellas, for violations of 15 U.S.C. s 45(a)(1), which provides that "unfair or deceptive acts or practices in or affecting commerce … are … unlawful." Drizly offers online alcohol delivery services and in its course of business collects and stores customer information such as emails, addresses, phone numbers and unique device identifiers. In 2020, Drizly experienced a data incident where hackers breached an employee's account and stole customer information.

According to the FTC, Drizly knew that its data security practices were inadequate due to a previous data incident in 2018 but failed to properly remedy those issues despite its representations to the contrary. In particular, the FTC claimed Drizly failed to implement simple, inexpensive security measures such as two-factor authentication and limit employee access to customer information. Accordingly, the FTC claimed that Drizly's representations to consumers on its website and mobile app that it had "appropriate safeguards" were false. (*In the Matter of Drizly, LLC*, https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-Complaint.pdf.)

As to Rellas, the FTC claimed he should have hired a senior executive responsible for data security:

> [A]s CEO of Drizly prior to and during the breach, Rellas hired senior executives dedicated to finance, legal, marketing, retail, human resources, product[] and analytics[] but failed to hire a senior executive responsible for the security of consumers' personal information collected and maintained by Drizly (Id.).

The parties entered into a consent agreement in October 2022 thereby waiving judicial review. Most interestingly, the consent agreement follows Rellas for 10 years — even after he leaves Drizly:

> Part VII of the Proposed Order requires Individual Respondent James Cory Rellas, for a period of ten years, for any business that he is a majority owner, or is employed or functions as a CEO or other senior officer with responsibility for information security, to ensure the business has established and implements, and thereafter maintains, an information security program.

("Analysis of Proposed Consent Order to Aid Public Comment in the Matter of Drizly, LLC, and James Cory Rellas," File No. 2023185, https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-AAPC.pdf.)

CONTINUED ON PAGE 28

CONTINUED FROM PAGE 27

"After receiving no substantive comments, the Commission voted 4-0 to finalize the complaint and order against Drizly." ("FTC Finalizes Order with Online Alcohol Marketplace for Security Failures that Exposed Personal Data of 2.5 million People," Federal Trade Commission, (https://www.ftc.gov/news-events/news/press-releases/2023/01/ftc-finalizes-order-online-alcohol-marketplace-security-failures-exposed-personal-data-25-million.) The question remains, however, whether CEOs like Rellas should be subjected to this kind of regulatory reach.

The law is clear that a person may be individually liable under the FTC Act if they: (1) participated directly in the deceptive practice or had the authority to control the practice; and (2) knew or should have known the practices were deceptive. *F.T.C. v. Ross*, 743 F.3d 886, 892-93 (4th Cir. 2014). As the U.S. Court of Appeals for the Tenth Circuit has explained:

> [T]o hold an individual personally liable for consumer redress, the FTC must show a heightened standard of awareness beyond the authority to control. This awareness, however, need not rise to the level of an intent to defraud. In particular, the FTC need only show the individual had or should have had knowledge or awareness of defendants' misrepresentations. The FTC may fulfill its burden by showing the individual had actual knowledge of material misrepresentations, reckless indifference to the truth or falsity of such misrepresentations, or an awareness of a high probability of fraud along with an intentional avoidance of the truth.

F*.T.C. v. Freecom Commc'ns, Inc*., 401 F.3d 1192, 1207 (10th Cir. 2005) (internal citations and quotation marks omitted). This "heightened standard of awareness" could prove difficult in the data incident context.

Regardless, even if the act reaches this conduct, the FTC's decision to proceed against Rellas on an individual basis is surprising. As Commissioner Christine Wilson explained in her Oct. 24, 2022 concurring and dissenting statement:

> The [c]ommission traditionally has exercised its prosecutorial discretion and assessed a variety of factors when deciding whether to name a CEO or principal, including consideration of whether individual liability is necessary to obtain effective relief, and the level of the individual's knowledge and participation in the alleged illegal conduct.

(Wilson Concurring Statement (Oct. 24, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/2023185WilsonDrizlyStatement.pdf.) According to Wilson, none of these factors favored proceeding against Rellas in particular because "the number of issues crossing a CEO's desk on any given day is substantial" and there is no allegation that "Rellas oversaw day-to-day operations of the company's data security practices, had any data security expertise[] or was responsible for decisions about data security policies, procedures[] or programs" (Id.). In doing so, Wilson noted that the FTC has "signaled that [it] will substitute its own judgment about corporate priorities and government decisions for those of companies" (Id.).

While proving an executive's "heightened standard of awareness" may prove difficult, it is not stopping the FTC from filing complaints, which — as in the case of Rellas — could follow executives for years after they leave the company at issue.

Current Turmoil and Future Risks in Resolving Data Breach Class Actions

Mark A. Olthoff
Shareholder
Kansas City

Data incident lawsuits, especially class actions, have the potential to create significant business disruption, loss of marketplace credibility, civil liability or regulatory exposure. Consequently, companies that experience a data incident often want the issues resolved quickly and at minimal cost. In terms of litigation, an early settlement of civil lawsuits in a class action resolution to sweep up all potential claims may be a good strategy. Class action settlements can be structured in a variety of ways, with any number of different terms, to effectuate the desired result.

In the past year, a number of developments occurred with respect to the resolution and settlement of data breach class actions. While some have created peril, opportunities also exist. This article will discuss some of these developments that may impact the future of class action cases and settlements.

First, an increasing number of data breach lawsuits are being filed in state court rather than in federal court. Several possible reasons exist for this development. For one, federal courts have limited subject matter jurisdiction and have generally taken a narrower view with respect to the issue of constitutional standing, particularly where plaintiffs have not pleaded actual existing harm. On the other hand, state courts ordinarily do not have the same strict subject matter jurisdiction requirements. If plaintiffs wish to avoid significant motion practice over standing issues, then state court perhaps provides a more litigant-friendly and less expensive forum. Two, limiting the class definition to mostly in-state residents with a claim against a domiciled defendant can impact whether a case is removable to federal court. And three, the laws, rules and cases in state courts may be less exacting in terms of certifying or settling class action lawsuits.

Second, two federal courts have recently certified classes in data breach cases. The

CONTINUED ON PAGE 29

CONTINUED FROM PAGE 28

U.S. District Court for the Southern District of Florida certified a nationwide negligence class (and a California statutory claim class) of consumers who alleged their personal and payment card information was stolen, finding the Rule 23 class certification requirements were met even though significant causation and damages questions existed. *In re Brinker Data Incident Litig.*, No. 18-CV-686, 2021 WL 140558 (S.D. Fla. Apr. 14, 2021). In its class certification ruling, the court limited the class to those persons whose information had been accessed by cybercriminals and had incurred time or expense to mitigate consequences of the breach, thus attempting to avoid the risk of class members without standing or injury. *Brinker* is currently on a Rule 23(f) appeal to the U.S. Court of Appeals for the Eleventh Circuit. In the consolidated Marriott Hotels data breach litigation in the District of Maryland, where plaintiffs alleged hackers stole the personal information of hundreds of millions of hotel guests, the court certified eight Rule 23(b)(3) damages classes based on an "overpayment" benefit-of-the-bargain damage theory on contract and consumer protection claims as well as Rule 23(c)(4) issue classes on negligence claims. *In re Marriott Intern. Inc. Customer Data Breach Litigation,* Case No. 8:19-md-0278, 341 F.R.D. 128 (D. Md. May 3, 2022). *Marriott* is currently on a Rule 23(f) appeal to the Fourth Circuit. The outcome in both appeals is uncertain but, to the extent settlement negotiations include debate about the viability of class certification in data breach cases, these two decisions may have a future impact.

Third, a recent jury verdict of nearly $230 million in the Northern District of Illinois made headlines. *Rogers v. BNSF Rwy. Co.*, Case No. 1:19-cv-3083 (N.D. Ill. Oct. 12, 2022). While different from typical data breach actions where information is alleged to have been stolen or accessed by a third party, *Rogers* involved claims under the Illinois Biometric Information Privacy Act. Under BIPA, a violation can be found merely by capturing biometric data (e.g., fingerprints) without consent and does not require access to or disclosure of the data. The violation can lead to substantial statutory damages in a class setting as the *Rogers* verdict reflects. It remains to be seen whether the verdict will affect settlements higher in the data breach space.

Fourth, we have seen more courts deny motions to dismiss substantive claims and causes of action. Some courts have allowed variations of the contention that plaintiffs and class members could suffer future harm as a result of a breach. Plaintiffs have increased their attention to pleading the possibility of future harm (e.g., possible dark web exposure allegations) even where actual damage does not exist and often adding more specific allegations tying causation to the data incident. As a result, where parties are trying to resolve cases before or during the motion to dismiss stage, with defendants arguing that the likelihood of dismissal exists, we anticipate plaintiffs will begin to oppose the arguments with more strength given some of these recent decisions.

Last, jurisdictional decisions — whether cases are filed in federal or state courts — can affect the terms included in settling data breach class actions. For example, a number of federal courts have questioned attorney's fees awards and class representative service awards. Some courts have more closely scrutinized attorney's fees requests where class member compensation may be disproportional to the amount of fees sought. That is, where attorneys are requesting substantial fees but cannot demonstrate that the class members are being compensated, courts are considering limits on the amount of fees awarded. For this reason, plaintiffs are aggressively pushing for settlement terms that include nonmonetary classwide relief, such as credit monitoring or certain forms of injunctive relief, to demonstrate the value of the class settlement. The decisions could also lead plaintiffs to negotiate more strenuously for common fund (as opposed to claims-made) settlements to reduce the risk that settlements are not approved because they do not sufficiently compensate class members.

As to class representative service awards, in light of the decision in *Johnson v. NPAS Solutions, LLC*, 975 F.3d 1244 (11th Cir. 2020) (finding service awards impermissible under Rule 23), district courts within the Eleventh Circuit will likely disallow such requests. On the other hand, the Ninth, Sixth and Second circuits have disagreed with the Eleventh Circuit, concluding that class representative service awards are proper. This split of authority will likely lead to a Supreme Court opinion to resolve the differences.

Each of these developments may well impact the future of data breach class action lawsuits and settlements. While some may create new litigation hurdles, there are also opportunities for defendants to search for novel ways to resolve these claims earlier, perhaps in a state court forum that may be more amenable to approving data breach and privacy class action settlements and negotiating settlement terms.

How the Federal Tort Claims Act Extricates Certain Health Care Providers From Data Breach Class Action Suits

John C. Cleary
Shareholder
New York

Shundra Crumpton Manning
Associate
Nashville

Data breach class action litigation continues to occupy center stage in the ongoing struggle to secure compensation and redress for legitimate victims of actionable cybersecurity shortcomings of data owners. The underlying scenarios in these cases encompass criminal hacking episodes, rogue employees, carelessness and unforeseen material gaps in cybersecurity and patch management. The one-size-fits-all approach to typical class actions, however, frequently places health care providers at the mercy of the plaintiff class action bar, and courts may be reluctant to dismiss or meaningfully curtail these cases in the early phases. Yet hope may be on the horizon. For example, in a new wave of cases, certain federally funded community health centers have used the Federal Tort Claims Act as an avenue for substituting the United States as the proper defendant in data breach cases.

Congress and the Department of Health & Human Services have long been aware that federal-sector and federally affiliated providers do not have limitless resources. More to the point, burdening such providers with the types of litigation exposure and costs of defense faced by private-sector hospitals only serves to deplete the federal treasury (directly or indirectly) and divert federal funds from patient care to the types of external players in the litigation ecosystem (most notably, plaintiff lawyers and law firms). Enacted in 1946 after a B-25 bomber crashed into the Empire State Building, the FTCA serves as a mechanism to protect the balance between providing an adequate remedy to aggrieved parties and ensuring that federal-sector and federally affiliated providers are not depleted of the funding needed to provide care.

While these FTCA provisions originated in the area of medical malpractice and other typically non-class action scenarios, they are equally if not more important when a provider faces a class action for a widespread data incident or data breach that is alleged to have caused personal injury to the class representative and putative class members.

Data breaches in the health care sector have proliferated over the years and continue to grow. A recent study by the Identity Theft Resource Center found that in 2021, 1,862 known data breaches occurred resulting in approximately 300 million sensitive records being exposed.[1] Out of the 1,862 recorded data breaches, 330, or 17.7%, were in the medical industry and resulted in the exposure of around 30 million sensitive records.

The FTCA waives sovereign immunity and places the U.S. government on equal footing with private-sector defendants sued for certain types of torts. Additionally, the FTCA imposes liability on the United States for claims against federal entities arising out of "injury or loss of property, or personal injury or death." 28 U.S.C. § 2679(b)(1). According to the terms of the FTCA, this liability is the exclusive remedy for such claims. The Federally Supported Health Centers Assistance Act expanded the scope of this exclusive remedy to Public Health Service employees sued "for damage for personal injury, including death, resulting from the performance of medical, surgical, dental or related functions." 42 U.S.C. § 233(a). Accordingly, "Section 233(a) grants absolute immunity to PHS officers and employees for actions arising out of the performance

1 See 2021 Data Breach Annual Report (ITRC, Jan. 2022), at 6, available at https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited Nov. 30, 2022).

CONTINUED ON PAGE 31

CONTINUED FROM PAGE 30

of medical or related functions within the scope of their employment by barring all actions against them for such conduct." *Hui v. Castaneda*, 559 U.S. 799, 806 (2010). Key factors to consider in data breaches involving health care providers are (1) whether the health care provider has been "deemed" a PHS employee, and (2) whether the alleged data incident arises out of the performance of medical or related functions within the scope of the health care provider's operations.

1. PHS employees

Pursuant to 42 U.S.C. § 233(g), certain eligible community health centers can be deemed employees of the PHS. A community health center is defined as "an entity that serves a population that is medically underserved, or a special medically underserved population comprised of migratory and seasonal agricultural workers, the homeless, and residents of public housing." 42 U.S.C. § 254b. Other health care entities that may qualify as employees of the PHS include migrant health centers, health care for the homeless health centers and public housing primary care health centers.[2]

2. Performance of medical or related functions

In recent data breach cases involving community health centers, defendants have argued that maintaining the confidentiality of patient information is a medical or related function because the statute governing PHS deeming status requires the health center to have "an ongoing quality improvement system that includes clinical services and management, and that **maintains the confidentiality of patient records**." 42 U.S.C. § 254b(k)(3)(C) (emphasis added). The implementing regulations also require health centers to maintain "appropriate safeguards for confidentiality of patient records." 42 C.F.R. § 51c.110. The application that health centers must fill out as a prerequisite to receiving PHS status requires the center to attest that it "has implemented systems and procedures for protecting the confidentiality of patient information and safeguarding this information against loss, destruction[] or unauthorized use, consistent with federal and state requirements."[3]

Accordingly, if a health care entity has been deemed a PHS employee and the data breach arose out of the performance of medical or related functions, then there is statutory and case law support for the health care entity being entitled to immunity under the FTCA. In 2022, three federal courts ordered the substitution of the United States in the place of community health centers based on this analytical approach.[4] We expect these issues to continue to develop at the district court and appellate court levels in 2023.

Takeaways

1. Discern and update your Federally Qualified Health Center status or other eligible status if available and applicable.
2. Incorporate your FQHC status and related FTCA coverage into overall risk management and purchase of insurance.
3. Identify possibly covered claims or threats of claims and give prompt notice to HHS as required when FTCA coverage is in place.

2 https://bphc.hrsa.gov/initiatives/ftca/faq (last visited Nov. 30, 2022).
3 See Program Assistance Letter 2021-21, Calendar Year 2022 Requirements for Federal Tort Claims Act Coverage for Health Centers and Their Covered Individuals (Feb. 9, 2021), at 16, available at https://bphc.hrsa.gov/sites/default/files/bphc/compliance/pal-2021-01_0.pdf (last visited Nov. 30, 2022).
4 *Ford v. Sandhills Med. Found., Inc.*, Case No. 4:21-CV-02307-RBH, U.S. District Court for the District of South Carolina (Nov. 10, 2022), appeal pending, No. 22-2268 (4th Cir.); Mixon v. CareSouth Carolina, Inc., Case No. 4:22-CV-00269-RBH, U.S. District Court for the District of South Carolina (June 2, 2022); *Jane Doe v. Neighborhood Healthcare et al.,* Case No. 3:21-cv-01587-BEN-RBB, U.S. District Court for the Southern District of California (Sept. 8, 2022).

HIPAA Enforcement: Highlights From 2022 and Expectations for 2023

Noor K. Kalkat
Associate
Los Angeles

Iliana L. Peters
Shareholder
Washington, D.C.

Change in Political Leadership

Some industry publications indicate a pause in enforcement of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations, the HIPAA Privacy, Security, and Breach Notification Rules (the "HIPAA Rules"), by the Department of Health & Human Services ("HHS"), Office for Civil Rights ("OCR"). However, we note that publication of HIPAA-related settlements and civil money penalties always lags after a change in administration or in the Director of OCR, which happened again recently. Therefore, we emphasize that OCR continues to investigate cases involving and enforcing the HIPAA Rules vigorously. We continually see data requests from OCR for cases involving a range of clients, including voluminous data requests addressing the HIPAA Rules requirements and for "recognized security practices," as discussed following. Given the number of investigations we know are ongoing at OCR, we expect there to be more published enforcement activity on cases involving all of the HIPAA Rules during 2023.

Recognized Security Practices

On January 5, 2020, President Donald Trump signed into law H.R. 7898. This new statute amended the Health Information Technology for Economic and Clinical Health (HITECH)

CONTINUED ON PAGE 32

CONTINUED FROM PAGE 31

Act to require HHS to consider efforts by HIPAA Covered Entities and Business Associates to implement "recognized security practices" when assessing fines or penalties under the HIPAA Security Rule. The statute provides that if a HIPAA Covered Entity or Business Associate can demonstrate compliance for the previous twelve months with "recognized security practices," then that entity may benefit in the mitigation of fines related to the incident, an early termination of an audit and, potentially, mitigation of remedies agreed to in an agreement with OCR for violations of the HIPAA Rules.

We note that in any case where OCR requests information about a HIPAA Covered Entity's or Business Associate's implementation of "recognized security practices," such request from OCR may indicate that OCR is considering a settlement or a civil money penalty in that case. We hope the attached sample "Additional Data Request" from OCR referring to and requesting information about an organization's "recognized security practices" is helpful to you. We expect more requests for this information and additional guidance on these "recognized security practices" from OCR in 2023.

Recent Cases

According to press releases and publicly available information, we see a large range of payments being made for violations of the HIPAA Rules, as well as a range in types of entities. We have included examples below of a few of the settlement agreements about which OCR provided information on its website: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html. We note that these settlements range in both dollar amount and entity type and include small to very large amounts. As such, there is no truth to the urban legends that either OCR is not generally enforcing the HIPAA Rules or that OCR does not enforce the HIPAA Rules against small entities. As mentioned above, we expect to see more cases like these in 2023.

According to OCR's website, Oklahoma State University Center for Health Sciences ("OSU-CHS"), agreed to pay OCR a settlement amount of $875,000 and also agreed to implement a corrective action plan in response to settling allegations of potential violations of the HIPAA Rules after a cyberattack. Specifically, OCR stated that on January 5, 2018, OSU-CHS filed a breach report with OCR that stated that an unauthorized third party gained access to a web server that contained protected health information and that the hacker installed malware that resulted in the disclosure of 279,865 individuals' protected health information. Finally, OCR alleged that OSU-CHS failed to do the following: conduct an accurate, thorough risk analysis; perform an evaluation; implement audit controls and security incident response reporting; and provide timely breach notification to the affected individuals and HHS.

Also according to OCR's website, Peachstate Health Management LLC, doing business as AEON Clinical Laboratories ("Peachstate"), agreed to pay OCR a settlement amount of $25,000 and to implement a corrective action plan in response to a review by OCR. Specifically, OCR stated that in December of 2017, it initiated a compliance review of Peachstate to determine its compliance with the HIPAA Security and Privacy Rules and, as a result, OCR alleged Peachstate was not in compliance, as it failed to conduct an enterprise-wide risk analysis, implement risk management and audit controls, and maintain documentation of HIPAA Security policies and procedures. We note that clinical labs, to the extent they bill insurance, must comply with the HIPAA Rules. The OCR Director stated in the press release related to this incident that failing to implement basic HIPAA Security Rule requirements makes entities easy targets for malicious activity and puts patient information at risk. Again, we note that small providers are not immune from investigation or enforcement related to the HIPAA Rules.

Finally, according to OCR's website, Excellus Health Plan agreed to pay a $5.1 million settlement to OCR and to implement a corrective action plan to settle potential violations related to a breach affecting over 9.3 million people. Specifically, OCR stated that in September of 2015 Excellus filed a breach report stating that cyber-attackers gained unauthorized access to its information technology systems. OCR alleged that the hackers installed malware, which resulted in the disclosure of the protected health information of more than 9.3 million individuals. In the press release related to this incident, the OCR Director stated that hacking continues to be the greatest threat to the privacy and security of patient information and "health care entities need to step up their game" to protect the privacy of their patients.

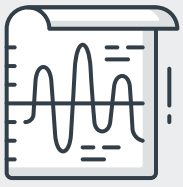
OCR Website

OCR posts all breaches reported to HHS involving 500 or more individuals on its website: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. All cases closed by OCR, usually added to the "Archive" of cases, include "web descriptions." As such, all cases without web descriptions, whether or not they are in the "Under Investigation" section of the website or the "Archive" section, remain open and continue to be investigated by OCR. Accordingly, many reporters, press outlets, plaintiffs' attorneys, researchers, and others frequently use this website to research breaches reported to HHS for a variety of reasons, including for purposes of developing class action litigation. As a reminder, OCR will verify all details of a breach notification submitted to HHS with the entity involved by phone within two weeks of submission, and after confirming the details submitted, OCR will post the information on its website, where it will remain in perpetuity, and automatically start an investigation into potential violations of the HIPAA Rules. OCR does not remove information from this website. We expect to see many more entities notifying HHS of various breaches and OCR posting the information to its website in 2023, thus creating additional resources for reporters, researchers, and plaintiffs' attorneys.

Conclusion

HHS OCR continues to vigorously enforce the HIPAA Rules, and HIPAA Covered Entities and Business Associates should continue to be vigilant about their HIPAA compliance. We expect more activity related to allegations of HIPAA violations by HHS OCR in 2023. Stay tuned!

OCR Recognized Security Practices PDF (Click Icon)



What's up with Illinois' BIPA

Dmitry Shifrin
Shareholder
Chicago

Kevin M. Hogan
Associate
Chicago

The Illinois Biometric Information Privacy Act, 740 ILCS 14/1 through 14/99, was enacted in 2008 to manage the promise of biometric technology for Illinois residents. BIPA seeks to encourage the development and use of biometric technology by imposing requirements on private entities that collect and possess biometric data. 740 ILCS 14/15(a). BIPA safeguards the collection and protection of "biometric identifiers," which are defined as a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face," and also safeguards "biometric information," which is defined as "any information, regardless of how it is captured, converted, stored[] or shared, based on an individual's biometric identifier used to identify an individual." 740 ILCS 14/10. However, the promise of large statutory damages have prompted a series of lawsuits against companies using biometric technology, alleging that such biometric information was collected and retained without the proper policies and disclosures in place. 740 ILCS 14/15. Following are some of the recent developments regarding BIPA litigation in Illinois.

Perhaps most importantly, the first BIPA case finally went to trial, resulting in a large judgment for the plaintiff putative class. The case, Rogers v. BNSF Railway, revolved around BNSF's auto-gate systems at its four Illinois facilities. The auto-gate system requires truck drivers to scan their fingerprints for entry and egress into BNSF's facilities. The court denied BNSF's motion for summary judgment and BNSF chose to proceed to trial, arguing that the auto-gate system technology provider — not BNSF — should be liable. Despite this argument, the class of more than 45,000 truck drivers won a $228 million judgment after a jury found that BNSF violated BIPA by collecting employee fingerprints without proper consent. The result indicates that Illinois juries are willing to award large judgments upon findings of BIPA violations — at least when it comes to employees. The BNSF result reinforces what many companies have suspected thus far: Settling or dismissing BIPA cases early is the preferred route, particularly before large putative classes can be established.

Thus far, the vast majority of BIPA cases have featured similar putative classes as the BNSF case. These classes are namely groups of employees (such as truck drivers) who are required to use their biometric identifiers for employment purposes. A classic — and widely litigated — example of this type of suit is a putative employee class that brings a BIPA action as a result of a company using employees' fingerprints to "punch in" for timekeeping. See, e.g., *Cothron v. White Castle Sys., Inc.*, 477 F. Supp. 3d 723 (N.D. Ill. 2020) (employee class claiming that White Castle committed BIPA violations after requiring employees to use a time-keeping system that required employees to punch in using fingerprint scans without properly adhering to disclosure or retention policies). The litigation surrounding these types of cases has been largely procedural. See, e.g., *Tims v. Black Horse Carriers, Inc.*, 2021 IL App (1st) 200563, ¶ 32 (holding claims brought under BIPA Section 15(c) and (d) are subject to a one-year statute of limitations).

However, aside from these procedural arguments, Illinois' courts have seen an influx of BIPA suits alleging an entirely new type of putative class: customers. This newest spate of BIPA suits focuses on the use of virtual try-on features by companies. These virtual try-on features essentially allow customers to log on to their favorite brand's website and then, using either their camera or an uploaded picture, overlay a desired product onto their own face or body. For instance, the popular makeup brand Estee Lauder uses such technology on its website, allowing customers to "try on" various makeup products before purchasing them (https://www.esteelauder.com/virtually-try-on-makeup-skincare). An Illinois federal judge recently allowed a suit against the company for the try-on product, holding that there was at least a colorable claim that Estee Lauder collected customers' facial geometry to overlay the desired makeup product.

Thus far, it appears that the threshold issue for these cases is how the technology works. Polsinelli attorneys have had success in similar suits (representing companies using identical technologies as those used by Estee Lauder), arguing the specific factual bases of the cases. For instance, Polsinelli represented a hair-coloring product using the same virtual try-on feature and was successful in dismissing the first complaint arguing that "hair" is not a protected feature under BIPA. Similarly, arguments can focus on **how** the technology operates. For instance, courts interpreting statutes similar to BIPA have focused on whether the biometric technology actually captures "biometric identifiers" or "biometric information" or simply operates by coloring pixels to achieve the "overlay" appearance. See, e.g., *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1096 (N.D. Ill. 2017) (discerning between the fact that photographs **themselves** cannot be biometric identifiers, but face templates measuring facial features **on** those photographs may capture biometric information). Companies will argue that while photographs can serve as a **medium** to capture biometric information, they cannot be the underlying biometric identifiers from which that information is derived. Whether this argument gains traction among courts may be of some importance. If these cases regarding virtual try-on features survive past the pleadings stage, then they may require intensive expert witness testimony to sort through the technology, quickly becoming financially burdensome.

In sum, the maxim that companies should get out of BIPA lawsuits early still stands. Plaintiffs have found creative new avenues to assert these claims and putative classes have continued to rise. Coupled with large statutory damages, it is imperative that companies move quickly to settle or dismiss complaints as early as possible.

"Fortnite" Creator Agrees to Pay a Record Penalty for Violating Children's Privacy Laws

John C. Cleary
Shareholder
New York

Tish R. Pickett
Associate
Los Angeles

On December 19, 2022, the Federal Trade Commission ("FTC") and the U.S. Department of Justice jointly announced that Epic Games Inc. ("Epic Games") will pay two record fines, in twin settlements, totaling half a billion dollars. If the settlements are approved by a federal court, Epic Games will pay $275 million in civil penalties for violating the Children's Online Privacy Protection Act ("COPPA"), in the largest fine ever imposed under COPPA. Epic Games will also pay $245 million in refunds to consumers who made unintended purchases, in the largest administrative order in FTC history. FTC's announcement signals a more muscular role in policing the on-line children's game industry for privacy-invasive practices.

FTC's First Complaint - Alleged Online Privacy Invasions

Fortnite, released by Epic Games in 2017, is one of the world's most popular video games with more than 400 million players worldwide.[1] But Epic Games allegedly put those players at risk through its lax privacy practices.[2] In the FTC's privacy complaint and proposed settlement against Epic Games, the FTC alleged that Epic Games (i) violated COPPA by failing to notify parents or obtain verifiable consent and (ii) enabled real-time voice and text chat communications for children and teens by default. Below are brief summaries of the allegations.

- Collecting personal data without parental consent: The FTC alleged that Epic Games actively collected children's names, email addresses, and identifiers that kept track of their progress, purchases, settings, and friends list, without first obtaining parental consent. When parents requested that the company delete their children's personal information, Epic Games failed to honor such requests or made it unreasonably difficult for parents to take steps to protect their children's personal information.[3] The company also implemented a default privacy setting that automatically broadcasted children's display names and matched children and teens with strangers—some of whom were adults—to play Fortnite together.
- Setting default voice and text chat communications: Epic Games allegedly chose to enable live on-by-default voice and text chat communications for players. As early as 2017, company employees allegedly urged Epic Games to change the default settings and require players to opt-in to voice and text chat communications, due to potential harm to children that this practice might impose. However, the company resisted turning off the default settings. Epic Games eventually allowed players to disable the feature, but made it difficult to locate, according to the complaint.[4]

1 Thomas Barrabi, 'Fortnite' maker to pay $520M for allegedly tricking kids into making purchases, New York Post (Dec. 19, 2022, 1:27 PM), https://nypost.com/2022/12/19/fortnite-maker-to-pay-520m-for-allegedly-tricking-kids-into-making-purchases/.
2 Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges, https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations.
3 Id.
4 Id.

CONTINUED ON PAGE 35

CONTINUED FROM PAGE 34

FTC's Second Administrative Complaint - Alleged "Dark Patterns"

In a separate complaint, FTC alleged Epic Games deceived players of all ages into a phenomenon known as "dark patterns." The FTC alleged, for example, that Epic Games made it easy for children and teens to purchase online credits for in-game items, such as costumes and dance moves. Yet, the company made it extremely difficult for players to easily cancel accidental charges. Other examples of "dark patterns" included players being charged while trying to wake the game from sleep mode, while the game was loading, or when a player mistakenly pressed a button when simply trying to preview an item.

The FTC alleged that Epic Games would lock accounts of those who disputed unwanted charges and warned them that they could be banned for life if they disputed any future charges. Epic Games allegedly earned hundreds of millions of dollars through "dark patterns" and billing practices. These practices also resulted in more than one million parental complaints according to the FTC's complaint.

Settlement Terms

If the U.S. District Court for the Eastern District of North Carolina approves the terms of the twin settlements, Epic Games must pay a record penalty in the amount of $275 million for violating COPPA. The company must also refund $245 million to consumers who made unintended purchases. Other terms of the settlement mandate that Epic Games obtain parental consent before the voice and text communications feature is enabled, delete minors' personal information that it obtained in violation of COPPA, establish a comprehensive privacy program, and obtain regular, independent audits. The agreement will last for 20 years from the time it is approved.

The FTC's recent announcement stated that "protecting the public, especially children, from online privacy invasions and 'dark patterns' is a top priority for the Commission, and these enforcement actions make clear to businesses that the FTC is cracking down on these unlawful practices."[5]

For its part, Epic Games did not confirm or deny the FTC's allegations, but the company agreed to revise some of its practices, including the creation of features to protect children such as easier-to-access parental controls, a PIN requirement to allow parents to authorize purchases, and a daily spending limit for kids under 13 years of age.[6] Epic Games stated, "no developer creates a game with the intention of ending up here. Statutes written decades ago don't specify how gaming ecosystems should operate. We accepted this agreement because we want Epic to be at the forefront of consumer protection and provide the best experience for our players."[7]

In May 2022, FTC announced stepped up enforcement in the children's privacy sector and stated that it would "vigorously enforce COPPA." The FTC's investigation and record-breaking fines against Epic Games embody and further that objective, with 2023 presumably headed into yet further regulatory challenges for companies active in the "gaming ecosystem."

5 Id.

6 Epic FTC Settlement and moving beyond long-standing industry practices (Dec. 19, 2022) https://www.epicgames.com/site/en-US/news/epic-ftc-settlement-and-moving-beyond-long-standing-industry-practices.

7 Id.

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 cybersecurity 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, privacy and cybersecurity needs.

Stay Connected

Polsinelli frequently writes about topics related to these materials.
Click here to subscribe to receive news and webinar updates.

Save the Date

2023 Privacy Summit

Thursday, May 11 | 8 A.M. to 5 P.M.

Polsinelli – Chicago

More details coming soon.

Email esterbenz@polsinelli.com for more information.

Editorial Board

POLSINELLI. What a law firm should be.℠