Benesch

Q2 – 2023

# Data Privacy & Cybersecurity Quarterly Briefing

**In This Issue:**



Benesch Data Meets WORLD

Be sure to check out Benesch's Data Meets World blog for timely information and updates related to optimizing, managing and protecting data globally across the full spectrum of industries, technologies, and regulatory requirements. www.datameetsworld.com

## Data Privacy and Security Legislation

### Efforts to Address the Lack of Federal Data Privacy Legislation in the U.S. Have Continued

The need for federal data privacy legislation was reiterated in the House Energy and Commerce Committee's Subcommittee on Innovation, Data, and Commerce meeting in April 2023. The hearing focused on the need for comprehensive privacy legislation to replace the 'piecemeal sector-specific approach' within existing U.S. laws. It was stated that these laws do not consistently protect consumers. The House Energy and Commerce Committee sent the comprehensive American Data Privacy and Protection Act to the full House of Representatives last year following a near-unanimous 53-2 vote, but the bill did not advance from there. It is anticipated to be reintroduced this year.

In another effort to establish comprehensive privacy legislation, the Online Privacy Act (OPA) was recently reintroduced. The OPA creates user data rights, places limitations and obligations on the ability of companies to collect and use user data, and institutes a Digital Privacy Agency to enforce privacy laws. The updated legislation includes several expanded provisions and additional privacy protections, including a section that sets the OPA as the federal floor, allowing states to legislate only when state action would provide greater protection than what is in the OPA. The updated legislation additionally supports privacy education, research, and development.

Apart from comprehensive legislation, Congress is considering a number of specific rules for tech companies. Although most legislators agree that the federal

*continued on next page*

## Data Privacy and Security Legislation (continued)

government should improve regulations for the biggest technology companies, there is little consensus on how it should be done. Among regulations that are gaining momentum are those related to data privacy. Legislation has been introduced to expand online privacy protections, prohibiting companies from collecting personal data from younger teenagers and banning targeted advertising to children and teens. Broader legislation has been introduced to give adults more control over their data and set a national privacy standard.

Efforts have also been made to ban TikTok, a popular video-sharing app, around which data security and harmful content concerns have arisen. There are additional concerns over the app's connections to the Chinese government. Further legislation has been introduced to create a framework to block any foreign apps deemed hostile.

Recently, A bipartisan group of senators and House members introduced legislation to protect American data from being used by U.S. adversaries. The bill is the latest in a series of proposals aimed at addressing concerns about the data of Americans using foreign-owned social media apps like TikTok. The bill would prevent data from being sent to unfriendly nations, stop TikTok from sending Americans' personal information to China, and allow nations with strong privacy protections to strengthen their relationships.

### Regulation of Artificial Intelligence

A new question for Congress is whether lawmakers should move to regulate artificial intelligence, as rapidly developing products, like AI chatbot ChatGPT, begin to enter the marketplace and can mimic many human behaviors, including some human interaction. A general framework of what AI regulations could look like has been released. The framework includes increased disclosure of the people and data involved in developing the technology, more transparency, and an explanation for how AI bots arrive at responses and how they 'learn.'

Although new regulatory efforts for AI are progressing, it has been suggested that existing data privacy laws, regulations, and policies may already directly regulate many key data-related aspects of AI. Existing U.S., state, and international privacy laws related to advertising technology and consumer marketing; authentication and biometrics; evaluations for credit, employment, insurance, and housing; cybersecurity monitoring; and others may directly apply to AI.

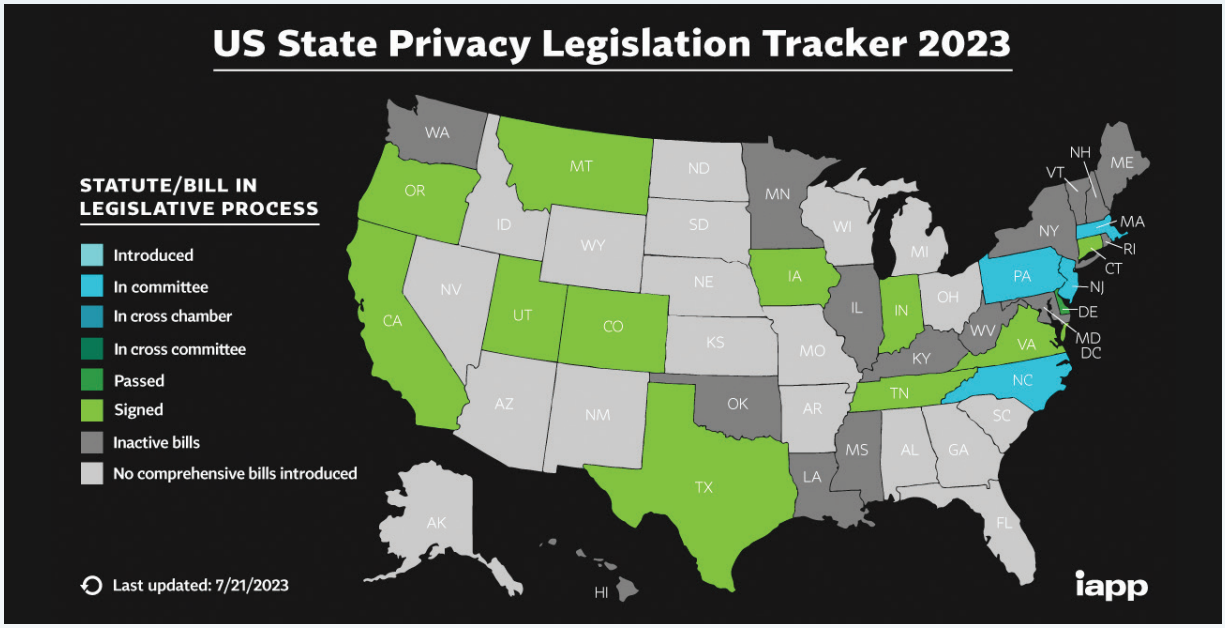
The European Parliament has approved draft legislation to regulate AI technology. Once approved, the European Union (EU) AI Act is expected to set a comprehensive standard for the AI industry that will have a global impact. Through the act, EU lawmakers seek to limit or prohibit AI technology they classify as unacceptable or high-risk. The act would also require that generative AI systems disclose what copyrighted material is used to train its models. Furthermore, AI-generated content must be identified to mitigate the spread of misinformation. Other governments have also been moving to regulate AI tools, including Australia, the U.K., China, France, Ireland, Israel, Italy, Japan, and Spain.

*Sources: IAPP, PBS, Reuters, Benesch, Congresswoman Anna G. Eshoo*

## Data Privacy and Security Legislation (continued)

### An Increasing Number of States Are Continuing to Pass or Introduce Legislation to Help Address the Absence of Federal Laws

State-level momentum for comprehensive privacy bills is at an all-time high, according to analysis by the IAPP. A significant portion of the proposed bills will not become law, but comparing the key provisions can highlight how privacy law is developing in the United States. Comprehensive state privacy laws have been enacted in California, Colorado, Connecticut, Indiana, Iowa, Montana, Tennessee, Texas, Virginia, and Utah. Other states have statutes/bills at various stages of the legislative process:




Indiana became the seventh U.S. state to enact a comprehensive data protection law in April 2023. This continues a trend of Midwest States enacting data protection laws. With an effective date of January 1, 2026, the Indiana Law provides a long runway for in-scope entities to come into compliance. The Indiana Law is most similar to Virginia's data protection law, particularly in terms of data privacy rights for consumers and in that a "sale" of personal information is only defined to mean the exchange of such information for money.

Montana and Tennessee followed by enacting their own omnibus data protection laws. The Montana Consumer Privacy Act and the Tennessee Information Protection Act introduce broadly applicable data privacy and data security requirements for businesses. The Montana Law defines "sale" as the exchange of personal information for monetary or other purposes, aligning with California's broad approach to defining the sale of personal information. Under the Montana and Tennessee Laws, consumers will have the rights to:

- Confirm whether a business is processing the consumer's personal information.
- Correct the personal information a business holds about them.
- Have their personal information deleted.
- Receive a copy of the personal information held about them in a portable and usable form.
- Opt-out of the sale of their personal information.
- Opt-out of cross-contextual behavioral targeted advertising.
- Opt-out of profiling through solely automated means in furtherance of decisions with legal or similar effect.

*continued on next page*

## Data Privacy and Security Legislation (continued)

Texas has also recently signed a comprehensive privacy bill into law. The Texas Data and Privacy Security Act will take effect in two stages over the next two years. The act creates a list of rights for internet users over their personal data, including knowing when it is collected, the ability to correct and delete personal data, the right to prohibit the sale of personal data, and protections against being discriminated against or retaliation by companies for using these rights. Companies will also be required to obtain consent before collecting data relating to racial or ethnic origins, health conditions, sexuality, or citizenship status, as well as genetic and biometric data. It also requires consent to be obtained for collecting any data on users under age 13 and limits geolocation data collection without consent.

Data privacy has been noted as a bipartisan issue, with cooperation observed at both federal and state levels. Many of the comprehensive state privacy laws in 2023 have been passed in states controlled by Republicans, including Iowa, Indiana, Tennessee, Montana, and Texas. Florida, another Republican-controlled state, signed new data privacy protections into law. However, these protections have yet to be classified as comprehensive, as they place restrictions and requirements on only a small number of large businesses that have a gross annual revenue exceeding $1 billion.

Washington also recently adopted a law with sweeping safeguards for consumer health data, including location records that could reveal visits to abortion clinics and other healthcare facilities. The measure, known as the My Health My Data Act, was introduced as part of a local legislative effort to protect abortion access after the US Supreme Court overturned Roe v. Wade last year.

Full enforcement of California's data privacy law has been delayed until March 29, 2024, though the law itself is currently in effect. The delay in enforcing the regulations will give businesses more time to bring their data protection programs into compliance.

The Oregon law is similar to the other omnibus state data protection that have passed and been signed into law, including, for example, providing individuals data privacy rights of (1) confirmation of processing; (2) access to their personal data; (3) to correct their personal data; (4) to have their personal data deleted; (5) to opt out of the sale of their personal data; (6) to opt out of the use of their personal data for cross-contextual behavioral advertising purposes; and (7) to opt out of automated profiling in furtherance of legally significant or similar decisions. The Oregon law, like many other similar state data protection laws, requires prior opt-in consent before a business can collect or use an individual's sensitive data.

*Sources: IAPP, Benesch, The Texan, National Law Review, Bloomberg Law*

# Data Privacy and Security Trends Across Industries

## Data Privacy and Cybersecurity Continue to Be Top Priorities for Both Regulators and Companies

With reports of cyberattacks and ransomware threats becoming more prevalent in 2022, organizations need to keep up with the dynamic and increasing legal obligations governing data security, understand how they apply, monitor cyber risks and attack trends, and manage their compliance to minimize risk exposure. Issues that organizations must consider include federal and state guidance, regulations, and enforcement actions; private litigation; federal and state legislation; international developments likely to affect U.S. companies, including cross-border data transfer issues; and other issues as cybersecurity concerns develop.

## Attention on Data Privacy and Security Issues in the Healthcare Industry Has Intensified as a Number of Data Breaches Have Been Reported

The recent proliferation of digital health has led to data privacy concerns around the collection of sensitive personal health information. Consumers have been demanding more rights to access, delete, or withdraw consent for their data. This is reflected in emerging legislation increasing protections regarding collecting, sharing, and selling health data without the consumer's knowledge. This presents compliance challenges for healthcare organizations, as there can be considerable consequences for data breaches.

The hacking of healthcare systems has become a top concern, and healthcare organizations are pressured to proactively protect themselves against these attacks. It has been reported that nearly 80% of data breaches in 2022 were from hacking and IT incidents. It has been suggested that healthcare organizations are being specifically targeted by attackers, as breaches and incidents have the potential to be lucrative. The data possessed by healthcare organizations can be of high value and might include personal and financial information. Additionally, healthcare providers often use legacy infrastructure and hardware, making it difficult to protect against cyber threats.

The financial impact of healthcare ransomware attacks can be substantial, as organizations can potentially have up to 30% of their operating income at risk in the aftermath of a ransomware attack. The average cost of a ransomware attack was reported as $4.82 million in 2021. Healthcare organizations may face financial losses tied to revenue loss and remediation costs, as well as brand damage and legal fees. Beyond financial losses, healthcare organizations may suffer operational disruptions and threats to patient safety due toa cyberattack.

A number of data breaches have recently been reported. PharMerica announced a large health data breach in May of 2023. The national pharmacy network, which serves long-term care, senior living, and behavioral health organizations, notified patients and families that an unknown third party accessed their personal health information in March. NextGen Healthcare also reported in May that hackers had breached its systems, stealing the data of more than a million patients. According to the company, the breach stemmed from unauthorized access to a database from client credentials allegedly stolen from other sources or incidents unrelated to NextGen. The affected information included patients' names, date of birth, addresses, and social security numbers.

MCNA Dental, a Medicaid and Children's Health Insurance Program service provider, also reported a major healthcare data breach in May that impacted more than 8.9 million individuals. The theft included Social Security numbers and personal data. A ransomware group claimed responsibility for the attack. MCNA

*continued on next page*

## Data Privacy and Security Trends Across Industries (continued)

responded to the data breach by taking measures to rectify the situation and bolster its cybersecurity to avert future breaches. Albany ENT & Allergy Services also disclosed a breach, with unauthorized individuals gaining access to its network, exposing more than 200,000 individuals' personal health information.

Data for 11 million people across 20 states was recently stolen in a breach of HCA Healthcare, one of the largest healthcare providers in the country. The provider said the breach was recently discovered and that the stolen data contains information used for email messages. The types of data confirmed as stolen include patient names, city, state, zip code, email, telephone number, date of birth, gender, patient service data, location, and next appointment dates.

In response to concerns regarding privacy and efficacy related to the rapid growth of digital healthcare apps in the U.S., the Federal Trade Commission (FTC) is seeking to update its health breach notification rules. It aims to enhance patient privacy protection for patients utilizing digital health apps. It has proposed the following changes:

- Introducing new definitions to clarify the rule's application to health apps.
- Specifying that a "breach of security" includes unauthorized acquisition of identifiable health information resulting from a data security breach or unauthorized disclosure.
- Modifying definition definitions to align with the rule's scope.
- Providing clarity on how personal health data is collected from multiple sources.
- Authorizing the use of email and other means to provide breach notices to consumers.
- Improving the rule's readability to promote compliance.

The U.S. Department of Health and Human Services (HHS) has announced the release of resources to help address cybersecurity concerns in the Healthcare and Public Health sector, including:

- *Knowledge on Demand.* A new online educational platform that offers free cybersecurity training for health and public health organizations to improve cybersecurity awareness.
- *Health Industry Cybersecurity Practices (HICP) 2023 Edition.* A foundational publication that aims to raise awareness of cybersecurity risks, provide best practices, and help the sector set standards in mitigating the most pertinent cybersecurity threats to the sector.
- *Hospital Cyber Resiliency Initiative Landscape Analysis.* A report on domestic hospitals' current state of cybersecurity preparedness, including a review of participating hospitals benchmarked against standard cybersecurity guidelines.

*Sources: Reuters, Pharmaceutical Technology, Security Intelligence, Healthcare IT News, Infosecurity Magazine, HealthITSecurity, U.S. Department of Health and Human Services*

## Data Privacy and Security Trends Across Industries (continued)

### Data Breaches Have Been Reported in the Retail and E-commerce Sectors, as Retailers and Suppliers Have Become Common Targets for Cyberattacks

The theft of payment card data from retail organizations is on the rise, according to a report by Verizon. The report included data from 406 data breach incidents in the retail sector. The compromised data had payment information, credentials, personal information, and other data. Attacks accounted for 18% of the breaches, with information skimmed from payment forms on checkout pages.

Retail data centers have been noted as a prime target for cyberattacks, which are frequently targeted to steal or destroy data. Credit cards and personal information can be at risk, resulting in costly breach-related expenses for retailers. Cybersecurity, data protection, and privacy are forcing companies to work towards consolidating tech stacks to make them more effective at identifying intrusion attempts, threats, and endpoint breaches.

Western Digital recently reported that hackers accessed customer information after stealing a database used for its online retail store. The stolen customer data included names, billing and shipping addresses, email addresses, telephone numbers, and encrypted data, including hashed and salted passwords and partial credit card numbers.

Cyberattacks are a rising cause of supply chain disruption. Attackers are targeting suppliers in order to reach bigger targets, like major retailers. Supply chain fraud can give attackers access to the target's internal systems to steal or divert funds. A single successful supply chain attack can cause damage on a much larger scale than a fraudulent transaction or return.

*Sources: Security Boulevard, Cybersecurity Dive, VentureBeat, Supply Chain Brain*

## Other Trends in Data Privacy and Security

### Security Concerns Surrounding AI Led Some European Countries to Ban Some AI Tools, With the Potential for Regulation Emerging in the U.S.

Data Security and privacy concerns have grown with the rapid advance of Artificial Intelligence technology. The security of the data used to train and operate these technologies, as well as the privacy implications if the data is mishandled are central issues. In addition to the data that is manually input to the system, ChatGPT scrapes data from the web to bolster its learning models. Data scraping is a process of importing data from other websites without permission or consent. This scraped data is then accessible by any user if the data is responsive to the user's query or prompt. It retains substantial quantities of personally identifiable information and other sensitive information, including but not limited to a user's browsing history, social media activity, credit scores, medical records, trade secrets, and financial data. Therefore, using ChatGPT can lead to the disclosure of sensitive information. Additionally, due to the volume of its data storage, ChatGPT is likely to become a valuable target or tool for cybercriminals. This could lead to major data breaches and violations of privacy.

The data protection debate surrounding AI has begun in Europe. Italy recently became the first Western country to ban ChatGPT, a popular AI chatbot from OpenAI. OpenAI was temporarily ordered to stop processing Italian users' data amid a probe into a suspected breach of Europe's privacy regulations. A data breach was cited, which allowed users to view the titles of conversations other users were having with the chatbot. There are also concerns surrounding a lack of age restrictions on ChatGPT, as well as how it can serve factually incorrect information in its responses.

*continued on next page*

## Other Trends in Data Privacy and Security (continued)

Other governments are also developing regulations for AI, including generative AI, which refers to technologies that generate new content based on prompts from users. It is more advanced than previous iterations of AI. There have long been calls to regulate AI, but the pace at which the technology has progressed is creating difficulties for governments to keep pace. The U.K., the E.U., and the U.S. have indicated their intentions to regulate AI.

France's data protection authority has begun to receive complaints regarding personal data use by ChatGPT, with some suggesting that it violates the E.U. General Data Protection Regulation but should not be banned. It has also been reported that the U.S. Congress has started having conversations on regulating artificial intelligence technologies.

The privacy watchdogs of the G7 countries are set to detail a common vision of the data protection challenges of generative AI models like ChatGPT. The data protection and privacy authorities of the United States, France, Germany, Italy, the United Kingdom, Canada, and Japan have met to discuss enforcement cooperation and emerging technologies. Privacy regulators have pointed out the risks that generative AI tools entail from a data protection standpoint. The starting point is the legal authority AI developers have for processing personal information, particularly of minors, in the datasets used to train the AI models, how users' interactions are fed into the tools, and what information is returned as output. AI developers have been called on to ensure that personal information used by generative AI tools is kept accurate, complete, up-to-date, free from discrimination, and is not unlawful or produces otherwise unjustifiable effects.

*Sources: Benesch Law, CNBC, IAPP, Euractiv*

## The FTC Has Issued a Policy Statement to Address Emerging Technologies, Such as Those That Utilize Biometric Information

The Federal Trade Commission issued a warning that the increasing use of consumers' biometric information and related technologies, including those powered by machine learning, raises significant consumer privacy and data security concerns and the potential for bias and discrimination. Biometric information refers to data that depict or describe physical, biological, or behavioral traits, characteristics, or measurements of or relating to an identified or identifiable person's body.

In a policy statement, the Commission said the agency is committed to combatting unfair or deceptive acts and practices related to the collection and use of consumers' biometric information and the marketing and use of biometric information technologies.

Recent years have seen a proliferation of biometric information technologies. For instance, facial, iris, or fingerprint recognition technologies collect and process biometric information to identify individuals. Other biometric information technologies use or claim to use biometric information to determine characteristics of individuals, ranging from the individuals' age, gender, or race to the individuals' personality traits, aptitudes, or demeanor.

Consumers face new and increasing risks associated with collecting and using biometric information. Large databases of biometric information could also be attractive targets for malicious actors who could misuse such information.

The statement also stands as the first formal position from the federal government on what it will consider as a biometric identifier. It also affirms much of the regulation contained in the Illinois Biometric Information Privacy Act (BIPA), the "gold standard" of biometric data laws. This was the first state-level biometric privacy law and has been suggested to be the most effective and enforceable law by privacy experts. Several other

*continued on next page*

## Other Trends in Data Privacy and Security (continued)

states are attempting to pass their own BIPAs this year. Washington's recent My Health, My Data Act has also been noted for its potential effectiveness in biometric regulation. Although it primarily covers data related to consumer health, its broad definitions of protected data include biometrics.

The statement further clarifies the definition of biometric data to include data derived from depictions, images, descriptions, or recordings to the extent that it would be reasonably possible to identify the person from whose information the data had been derived. The policy statement also includes a non-exhaustive list of what has become traditional biometric information examples. It also gives examples of what is considered "biometric information" that goes far beyond what traditional biometric information laws previously identified, such as an individual's characteristic movements or gestures. Another example of how broadly the FTC's definition of biometric information reaches is that it would include an individual's typing patterns. Tools analyzing typing patterns have become more and more common as a tool for employers to measure productivity. Under the FTC's policy statement, such tools would be subject to biometric information considerations. This will increase the need for employers to consider what is and is not biometric information when crafting employee and job applicant privacy notices.

More stringent enforcement surrounding biometric information is expected with the clarification for biometric use in companies going forward.

*Sources: Federal Trade Commission, Statescoop, Benesch, SC Magazine*

## Website and App Tracking Technologies, Such as Pixels and Cookies, Can Create Compliance and Litigation Risks

In recent months, digital privacy risks resulting from tracking pixels and other web technologies have gained attention. The increasing awareness of data collection and website tracking by businesses has become a key factor in determining risk levels for security leaders. Tracking pixels are used across a spectrum of advertising technologies to understand consumer behavior. Unlikebrowser cookies, pixels can send more personal information to third parties. The potential for class action lawsuits and regulatory investigations is growing, creating a need for organizations to address privacy concerns. Although urgency is of particular concern in healthcare, all organizations can be affected.

Some security leaders have attempted to limit their risks by putting a governance process in place that includes marketing, privacy, IT, and legal departments. However, many organizations appear unaware that they are using pixel-tracking technology.

Tracking pixels have caused continuing data privacy issues in healthcare. Despite the frequent patient data privacy issues that arise around the use of tracking pixels, they are commonly used in healthcare. The US Department of Health and Human Services released guidance on the use of tracking technologies for HIPAA-covered entities. The guidance acknowledges that tracking technology provides beneficial insights but also states that any use of these tools cannot result in impermissible disclosure of personal health information to tracking technology vendors or any other violations of the HIPAA rules.

Appropriate use of tracking pixels in healthcare hinges on enterprises knowing exactly how the technology works, what data is being collected, and where it is going. Healthcare enterprises may now know that personal health information is being leaked to a third party, but ignorance likely will not protect them from regulatory consequences.

*Sources: Infosecurity Magazine, Information Week*

**For more information regarding Data Privacy & Cybersecurity please contact:**

**Ryan T. Sulkin**
rsulkin@beneschlaw.com | 312.624.6398
**Michael D. Stovsky**
mstovsky@beneschlaw.com | 216.363.4626
**Michael Vatis**
mvatis@beneschlaw.com | 646.328.0494