Q1 – 2023

Data Privacy & Cybersecurity Quarterly Briefing

In This Issue:

Benesch Welcomes Michael Vatis....1

Data Privacy and Security Legislation....2

Data Privacy and Security Trends Across Industries....6

Other Trends in Data Privacy and Security....9

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

Benesch Welcomes Michael Vatis

Benesch is pleased to welcome Michael Vatis as a partner in the firm's New York office. A privacy and cybersecurity counselor and a litigator with deep appellate experience, Vatis joins from Steptoe, where he chaired the Privacy & Cybersecurity practice. Vatis has nearly 20 years of experience assisting clients in navigating U.S. and international privacy and data security laws and regulations, helping clients prevent or respond to data breaches, and representing clients in high-stakes litigation and in enforcement actions by the Federal Trade Commission and state attorneys general. Prior to that, Vatis served in key operational and policy roles in the federal government in the areas of cybercrime, cybersecurity, counterterrorism, counterintelligence, and critical infrastructure protection. Vatis was the founding head of the FBI's computer crime and infrastructure protection program; Associate Deputy Attorney General for national security matters in the Department of Justice; and Special Counsel in the Office of General Counsel at the Department of Defense, where he received the Secretary of Defense Award for Excellence. Following government service, he served as the first Director of the Institute for Security Technology Studies at Dartmouth, the founding Chairman of the Institute for Information Infrastructure Protection (I3P), and Executive Director of the Markle Task Force on National Security in the Information Age.

Michael Vatis
mvatis@beneschlaw.com
646.328.0494

Data Privacy and Security Legislation

Data privacy laws have been progressing globally, but federal legislation in the U.S. has been lacking

Businesses are facing a growing number of data privacy regulations. This is especially apparent among those in highly regulated sectors, including financial services, healthcare, and government, as well as those that operate in multiple countries. Rules governing how data should be stored, used, and shared can be taxing on cybersecurity and risk-management departments, resulting in the need for businesses to better manage their compliance operations.

Since 2018, the year the European Union's General Data Protection Regulation (GDPR) went into effect, there has been a constant increase in these types of regulations. Approximately 100 countries around the world now have some form of data privacy or security rules in place. Further, proposed legislation surrounding artificial intelligence and data governance includes requirements for how personal information is used.

Although many U.S. states have either considered or enacted privacy laws, federal legislation has been lacking. The American Data Privacy and Protection Act is currently the most prominent proposed regulation, but if it fails to pass it could leave a vacuum at the federal level. As such, states could continue to develop regulations without national consistency.

The lack of uniformity within regulations and the volume of regulations create challenges for compliance teams as they consider the compliance needs of their organizations.

In contrast to the EU's rights-based approach to data privacy laid out in the GDPR, to date U.S. laws have been primarily focused on preventing or mitigating harm in specific sectors. The GDPR's rights-based approach provides individuals with ownership of their personal information, as well as the legal right to control it.

GDPR-inspired statutes in California, Colorado, Connecticut, Utah, and Virginia will begin to be enforced in 2023. More states are expected to do the same, representing a shift in the data privacy protection framework in the U.S.

- Montana (October 1, 2024)
- Tennessee (July 1, 2024)
- Iowa (January 1, 2025)
- Indiana (January 1, 2026)

The new laws represent a comprehensive approach to privacy protection, applying to businesses across numerous sectors, in addition to the sector-specific laws that remain in place.

The rights of individuals set forth by the GDPR, which parallel those among the U.S. laws, include:

- The right to request access to inspect their personal information
- The right to request that errors in their personal information be corrected
- The right to request that their personal information be transferred to another entity
- The right to request that their personal information be deleted
- The right to appeal a business's denial of their request

continued on next page

Data Privacy and Security Legislation (continued)

The Governing principles laid out by the GDPR include:

- Data management systems should be designed with privacy protection in mind.
- Adequate records should be maintained regarding the collection, processing, and use of data.
- Data should be minimized. Personal information should only be kept long enough to serve its purposes, if kept at all.
- Personal information should be used with informed consent from the data subjects, in a way that is understandable to them, and only for legitimate uses allowed under law.
- Trained personnel should be monitoring compliance with privacy protection requirements.
- Data should be protected using best practices for cybersecurity to minimize the risks of data breaches.
- A response plan should be in place to provide notifications of data breaches.
- Employees should be trained in privacy protection practices.
- Appropriate contractual language is required.

SOURCE: *CNBC, Reuters*

Federal legislators are being pressured to act on data privacy

The United States does not have a national data privacy law. Two acts do cover privacy, however:

- The Privacy Act of 1974 was established primarily for federal government agencies as a code of fair information practices to govern the collection, processing, management, dissemination, and destruction of personally identifiable information.
- HIPAA, enacted in 1996, has two key sections: the Security Rule and Privacy Rule. These rules give protected health information providers and processers flexibility in how they protect user data.
- The Childrens' Online Privacy Protection Act
- The Gramm-Leach-Bliley Act
- The Fair Credit Reporting Act
- The Electronic Communications Privacy Act

Privacy advocates have been pushing for a federal privacy law to protect personal information, including information such as political beliefs, habits, interests, and GPS locations. To date, those wanting to prosecute privacy-related claims need to rely on a patchwork of laws. This can make it difficult to prosecute big privacy violation cases.

National legislation is currently being assessed by Congress. The American Data Privacy and Protection Act (ADPPA), if passed, will likely mean companies will have to follow both national and state legislation to ensure they are processing personal data correctly. The ADPPA has been well received by some privacy policy experts.

The ADPPA includes a list of prohibitions, such as biometric data and geolocation data. It also includes a civil rights section preventing organizations from collecting data related to race, color, religion, national origin, sex, or disability. It also requires companies to conduct annual impact assessments for algorithms that could cause harm to individuals. Other notable measures include requirements for organizations to appoint privacy officers to oversee data privacy, as well as the creation of a registry for third-party collecting entities.

continued on next page

Data Privacy and Security Legislation (continued)

Potential issues with passing the law include preemption, which would effectively replace state level legislation. Opposition to preemption has grown as more states pass comprehensive data privacy laws. Another sticking point is enforcement of the legislation. There is concern that a provision for private suits could result in an overabundance of claims.

Efforts at the federal level to pass U.S. privacy legislation have been ongoing for years. Dozens of privacy-related bills have worked their ways through Congress, with legislators making efforts to address all facets of privacy, including individual rights, business obligations, protecting sensitive information, and emerging technologies. Major topics addressed in the bills introduced to date include:

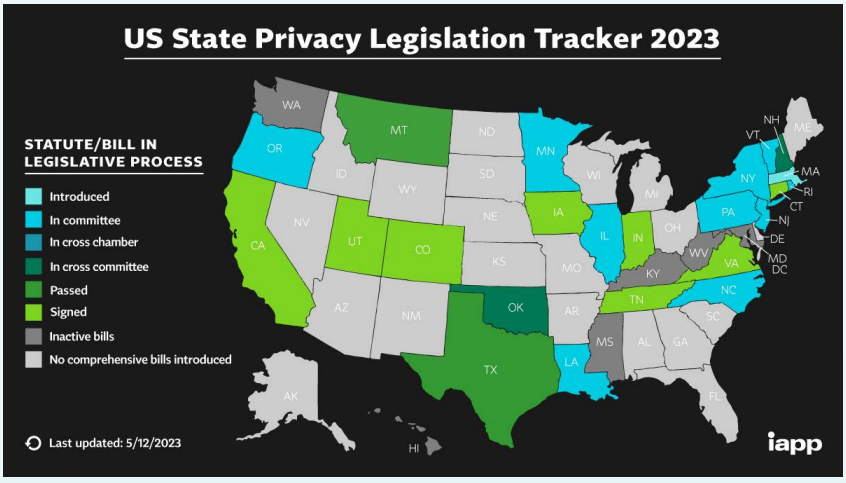
- Consumer and Individual privacy
- Health privacy
- Financial privacy
- Children's and educational privacy
- Federal Trade Commission (FTC) authority and enforcement
- Government restrictions and obligations

The need to strengthen data privacy and platform transparency for Americans was emphasized in the State of the Union address. It was suggested that limits be placed on the ability of companies to collect, use, transfer, and maintain personal data. The President called for stronger transparency requirements and limits on targeted advertising and personal data collection.

SOURCE: *IAPP, TechTarget, White House, Infosecurity*

An increasing number of states have either passed or introduced legislation to help address the absence of federal laws

State-level momentum for comprehensive privacy bills is at an all-time high. Although many of the proposed bills will fail to become law, comparing the key provisions helps to understand how privacy is developing in the United States. Comprehensive state privacy laws have been enacted in California, Colorado, Connecticut, Indiana, Iowa, Montana, Tennessee, Virginia, and Utah. Other states have statutes/bills at various stages of the legislative process.



With consumer privacy issues growing in importance, 140 consumer privacy bills have been introduced or considered in at least 25 states and Puerto Rico in 2023. Comprehensive legislation is being considered in at least 25 states.

continued on next page

Data Privacy and Security Legislation (continued)

Some of the other more common types of consumer privacy legislation concern the collection of data from consumers by commercial entities, online services, or commercial websites. Website privacy or children's privacy on the internet, direct-to-consumer genetic testing, ISP and information/data broker regulation, and other consumer privacy issues have been covered by these bills.

California has been a leader in data privacy legislation, enacting more laws than any other state:

- The California Consumer Privacy Act (CCPA) ensures that residents may ask businesses to disclose the type of information they collect, why they are collecting the information, and the source of the data.
- California Privacy Rights Act (CPRA), which took effect Jan. 1, 2023, builds on the CCPA. It gives residents the ability to prevent businesses from sharing their personal data, request that inaccuracies in their personal data be corrected, and prevent companies from using sensitive data.

The Colorado Privacy Act, which will go into effect July 1, 2023, adds provisions regarding the collection, processing, and dissemination of personal data to the existing Colorado Consumer Protection Act.

The Connecticut Personal Data Privacy and Online Monitoring Act will be effective July 1, 2023. It governs how personal data privacy is protected and how data is collected and processed, and delineates penalties for noncompliance.

The Utah Consumer Privacy Act, in effect Dec. 31, 2023, will protect the collection, processing, and distribution of personal data.

The Virginia Consumer Data Protection Act, effective Jan. 1, 2023, provides guidelines and penalties regarding how personal data is collected, processed, and distributed. It affects government and nongovernment organizations that process specific quantities of personal data.

Lawmakers in Kentucky, Mississippi, New York, Oklahoma, and Oregon propose bolstering company disclosure and consumer consent over how their information is collected and processed. New Jersey privacy legislation introduced in 2022 carries over into the second year of the state's session. Similar laws have already passed in Montana, Tennessee, Iowa, and Indiana.

The state bills present similar privacy rights but differ in their specific requirements, implementation, and enforcement.

SOURCE: *IAPP, National Conference of State Legislatures, Bloomberg Law*

Data Privacy and Security Trends Across Industries

Concerns exist regarding the impact of AI technologies on personal data privacy

As Artificial Intelligence (AI) continues to advance, it has brought about a number of concerns regarding personal data privacy. AI systems often rely on large amounts of personal data to learn and make predictions, which raises concerns about the collection, processing, and storage of such data. This data can include personal information such as names, addresses, financial information, and sensitive information such as medical records and social security numbers. Concerns exist about how this information is being used and who has access to it.

The main privacy concerns surrounding AI are the potential for data breaches and unauthorized access to personal information. With so much data being collected and processed, there is a risk that it could fall into the wrong hands, either through hacking or other security breaches.

Another concern is the use of AI for surveillance and monitoring purposes. Facial recognition technology, for example, has been used by law enforcement agencies to identify suspects and track individuals in public spaces. This raises questions about the right to privacy and the potential to abuse these technologies. With the ability to analyze vast amounts of data, AI can be utilized to monitor individuals in ways that were previously impossible, including tracking their movements, monitoring their social media activity, and analyzing their facial expressions and other biometric data.

There is also a concern that AI systems may perpetuate existing biases and discrimination. If the data used to train an AI system contains preference biases, the system may learn and perpetuate those biases. This can have serious consequences, particularly in areas such as employment, where AI algorithms may be used to make hiring decisions.

In order to address these concerns, it has been suggested that AI technologies be developed and deployed responsibly. This includes ensuring that data is collected and processed transparently and securely and that individuals have control over it. It also means ensuring that AI systems are designed and tested to identify and mitigate biases and are subject to ongoing monitoring and oversight.

SOURCE: *The Economic Times*

There has been a push to address data privacy and security across industries

Risks and concerns surrounding privacy have increased in recent years for many organizations, as technology transformations have accelerated. However, it has been noted that privacy and legal/compliance teams are understaffed, privacy budgets are underfunded, and gaps in skills exist. It has been predicted that these shortcomings could result in more vulnerabilities among short-staffed companies, which could experience a jump in data breaches and ransomware attacks.

Greater privacy and regulatory pressures are anticipated this year, as governments around the world are advancing their efforts to protect data privacy. Further, cybersecurity disclosure requirements for public organizations have been proposed, obligating them to disclose the cybersecurity expertise of board members and report cybersecurity practices periodically.

SOURCE: *Fortune, Cision, Forbes*

Data Privacy and Security Trends Across Industries (continued)

Data privacy and security issues in the Healthcare industry focus on the protection of patient information and sharing of information by healthcare apps and services

With large quantities of patient data, hospitals and healthcare systems have increasingly become targets of cyberattacks. According to a recent survey, more than one in three healthcare organizations around the world reported being hit by ransomware in 2020. Additionally, the number of victims of healthcare attacks was reported to rise from 14 million in 2018 to 45 million in 2021. It has been suggested that healthcare organizations need to prioritize updating infrastructure and implementing security strategies to protect sensitive patient information.

The surge of cyberattacks on health systems underscores the need for them to reassess security controls constantly as they minimize the risk of hackers obtaining patient data. According to the Health and Human Services Office for Civil Rights, hacking now accounts for 80% of large data breaches. Attackers that deploy ransomware often focus on healthcare organizations, as they hold a great deal of sensitive data about individuals, including demographic information, sensitive medical information, and financial information.

Updated data security strategies could include encryption for healthcare data, backup mechanics and data recovery systems, and two-factor login authentication for those accessing private data.

The National Cybersecurity Strategy issued by the Biden administration is expected to impact healthcare cybersecurity. The strategy outlines the expansion of the federal government's public-private collaboration to defend against attacks and strengthens its offensive role in disrupting cyber threat actors. Further, it seeks to increase the speed at which the government shares intelligence and emphasizes the Administration's goal of improving critical infrastructure security defenses.

Ways in which healthcare is expected to be impacted by the strategy include:

- Growing regulatory requirements are anticipated to shift cybersecurity liability to include both owners and operators, as well as the technology providers that they rely on.
- In order to address the need for shared responsibility for medical device security, the Administration will work with Congress and private sector organizations to develop legislation that establishes liability for software products and services.
- Limits are expected to be placed on what personally identifiable information can be collected and transferred, and protect vulnerable populations from data misuse. Protections for sensitive data such as geolocation and health information will be provided.

Concerns have risen that telehealth companies have allegedly been sharing health data with third-party advertisers. The health data privacy practices of telehealth companies Cerebral, Monument, and WorkIt Health have been questioned. It has been reported that these companies have been tracking their customers sensitive health information and sharing it with advertisers, such as Google.

Cerebral, a company that provides online therapy services, acknowledged that its customers' sensitive health information had been sent to third-party firms. The telehealth provider sent letters to users about the incident, in which it had been sharing user data with service providers such as Google, TikTok, and others via tracking "pixels."

continued on next page

Data Privacy and Security Trends Across Industries (continued)

The online counseling service BetterHelp also agreed to return $7.8 million to customers to settle with the FTC for sharing health data it had promised to keep private, including information about mental health challenges, with companies including Snapchat. The company revealed data including email and IP addresses and questionnaire information to Snapchat, Criteo, and Pinterest for advertising purposes. The proposed FTC order also limits how the company may share consumer data in the future. BetterHelp will provide partial refunds for customers who used the service.

SOURCE: *Fortune, Forbes, Cision, Security Magazine, Bloomberg Law, Security Week, CPO Magazine, The Washington Post, HealthITSecurity*

Issues faced by Retail and Ecommerce include cyberattacks targeting retailers and the protection of customer data

While the conveniences of the incorporation of technology by retailers have advantages for consumers, some services have been associated with security pitfalls. Vulnerabilities are inherent in retail payment systems, and can be easily exploited by cybercriminals. Risk can be further exacerbated with retailers using multiple vendors. When retailers' suppliers are attacked, it could lead to customer data being compromised.

It has been suggested that risk can be mitigated by retailers remaining vigilant in identifying weaknesses in vendors' systems or processes, and establishing policies to minimize risk in business partnerships.

Retail sector ransomware attacks have experienced an increase, with many big name brands falling victim to ransomware. Retailers are often seen as high-value targets because they store a great deal of customer data. While the retail sector as a whole appears to be implementing more tools to protect itself against cyberattacks, many retailers are still being targeted due to their lack of protection. It has been suggested that bolstering basic cybersecurity defenses and adopting third-generation cybersecurity solutions is essential for retailers to protect customer data and avoid ransomware attacks.

While many retail businesses are embracing ecommerce, it has introduced the complications of data privacy issues and cybersecurity. Although these have become business pillars, many companies have experienced difficulty in dealing with them. Ways in which data can be protected and breaches can be avoided include:

- Examining data collection practices to ensure companies are only gathering what they need
- Examining payment channels and reducing risk through outsourcing payments-related compliance to payment facilitators
- Reviewing which users have access to customer data and updating security measures
- Implementing two-factor authentication
- Reviewing security protocols and using current best practices in data security

SOURCE: *Security Magazine, Security Boulevard, Entrepreneur*

Other Trends in Data Privacy and Security

Increased litigation surrounding biometrics is anticipated

Industry observers expect there will be increased focus on several areas of biometric litigation in 2023. More fines are anticipated for tech and financial companies, with more regulations being introduced, making privacy compliance a priority for companies. Additional privacy, data, and cybersecurity regulations are expected at every level, from local to global. Several federal agencies are considering new regulations.

There has been an uptick in class action lawsuits focused on voice recognition technology, particularly in Illinois. In the past two years, dozens of lawsuits were filed against various companies, including McDonald's, Walmart, and others, alleging that they collect consumer or employee voice data in violation of Illinois' Biometric Information Privacy Act (BIPA).

The BIPA, adopted in 2008, requires companies that collect biometric information such as fingerprints and retinal scans to obtain permission beforehand and to notify workers and consumers of how that information will be used. It is the only law in the U.S. that grants a private right of action to sue over the mishandling of biometric information.

The Illinois Supreme Court recently indicated that workers and consumers have five years to sue for violations of the state's unique biometric privacy law, rejecting a much narrower window pushed by business groups. Nearly 2,000 lawsuits alleging violations of BIPA have been filed since 2017, yielding a series of large settlements and judgments.

A biometric privacy lawsuit was recently settled by Vimeo. It agreed to a $2.25 million settlement in a lawsuit alleging that its artificial-intelligence-based video creation and editing platform collected and stored users' biometric data without consent in violation of Illinois' Biometric Information Privacy Act.

In addition, Tesla is facing a class-action lawsuit in the U.S. District Court for the Northern District of California claiming it violated customers' privacy. The lawsuit argues that employees accessed videos and images recorded by customers' vehicle cameras for their entertainment.

SOURCE: *Bloomberg Law, Reuters, IAPP*

Other Trends in Data Privacy and Security (continued)

Website and app tracking technologies, such as pixels and cookies, can create compliance and litigation risks

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) recently issued a bulletin with guidance concerning the use of online tracking technologies under the Health Insurance Portability and Accountability Act (HIPAA). The bulletin followed an uptick in litigation concerning these technologies in industries, including healthcare.

Tracking technologies on websites include cookies, web beacons, and tracking pixels. Mobile apps may use tracking technologies such as tracking codes within the app, as well as captures of device-related information. They are used for various reasons, including to better understand the user experience on their site or app. Technologies developed by third parties may be able to track users and gather information after they navigate away from the original site.

During 2022, litigation concerning the use of website tracking technologies increased significantly. The trend does not just involve HIPAA-regulated entities or HIPAA.

It has been suggested that covered entities and business associates should conduct an audit of any tracking technologies used on their websites, web applications, or mobile apps and determine if they are being used in a manner that complies with HIPAA. They should also review tracking technology vendor agreements and ensure a business associate agreement is in place to avoid potential impermissible disclosure of private health information.

As data breach notifications tied to the use of tracking pixels continue to surface, experts have observed a wave of lawsuits being filed against hospital systems related to third-party tracking technology. Numerous healthcare entities reported breaches tied to their use of tracking pixels. The breach notices commonly state that the healthcare entity had implemented the technology to understand how visitors interact with their websites, but later discovered that it had been inappropriately transmitting sensitive data to big tech companies such as Google.

As data privacy laws continue to expand across the country, HIPAA-covered entities and non-HIPAA-covered entities will need to adjust their compliance programs to adapt to new regulations and evolving technologies.

Enforcement actions by the FTC recently taken against companies like BetterHelp for allegedly sharing user health data with third parties for advertising highlighted the use of third-party tracking pixels. Concerns surrounding the use of pixels include:

- The widespread usage of invisible pixels with no way for consumers to avoid. Traditional controls such as blocking third-party cookies may not entirely prevent pixels from collecting and sharing information. Additionally, many consumers may not realize that tracking pixels exist.
- A lack of clarity around data collection and use. With pixels, any type of personal and identifying information can be collected and shared. Third parties are often covert about how they store the data, and in some cases do not know what kinds of information is being tracked and where it is being stored.
- The possibility that personal information may not be effectively removed. Some pixel tracking methods ostensibly attempt to remove personal information but may still leak enough information to identify an individual.

SOURCE: *National Law Review, Federal Trade Commission*

Other Trends in Data Privacy and Security (continued)

Targeted/Cross-Contextual Advertising

With the California Privacy Rights Act and the Virginia Consumer Data Protection Act coming into effect in 2023, as well as new legislation from Colorado, Connecticut, and Utah, privacy teams from the digital advertising industry are trying to decipher what companies can and can't do under new state privacy laws.

Advertising and marketing are major topics of discussion surrounding federal privacy legislation. Some advertising business models have been built on monetizing the collection, use, and sharing of digital information. The proposed boundaries surrounding data privacy in the proposed American Data Privacy and Protection Act (ADPPA) are expected to alter digital advertising practices. The ADPPA does not ban targeted advertising altogether, but distinguishes between targeted advertising and contextual advertising. Contextual advertising is based on the context in which an ad appears, not on specific information about each individual viewer. The ADPPA would only affect contextual advertising to the extent that limits on the collection of personal data would constrict contextual information.

The constraints on targeted advertising are substantial. The ADPPA would allow entities that collect data directly from an individual to target advertising to those individuals. Individuals would have the right to opt out of receiving any targeted ads, which advertisers, including first parties, would be obligated to offer prominently and to respect if exercised.

The decisions have been suggested to represent a warning to other platforms seeking to ignore EU data protection rules by not providing users with a choice over being subject to tracking for behavioral advertising. The decisions include $410 million in fines, along with orders to correct unlawful data processing.

SOURCE: *IAPP, Brookings, Gizmodo, TechCrunch*

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