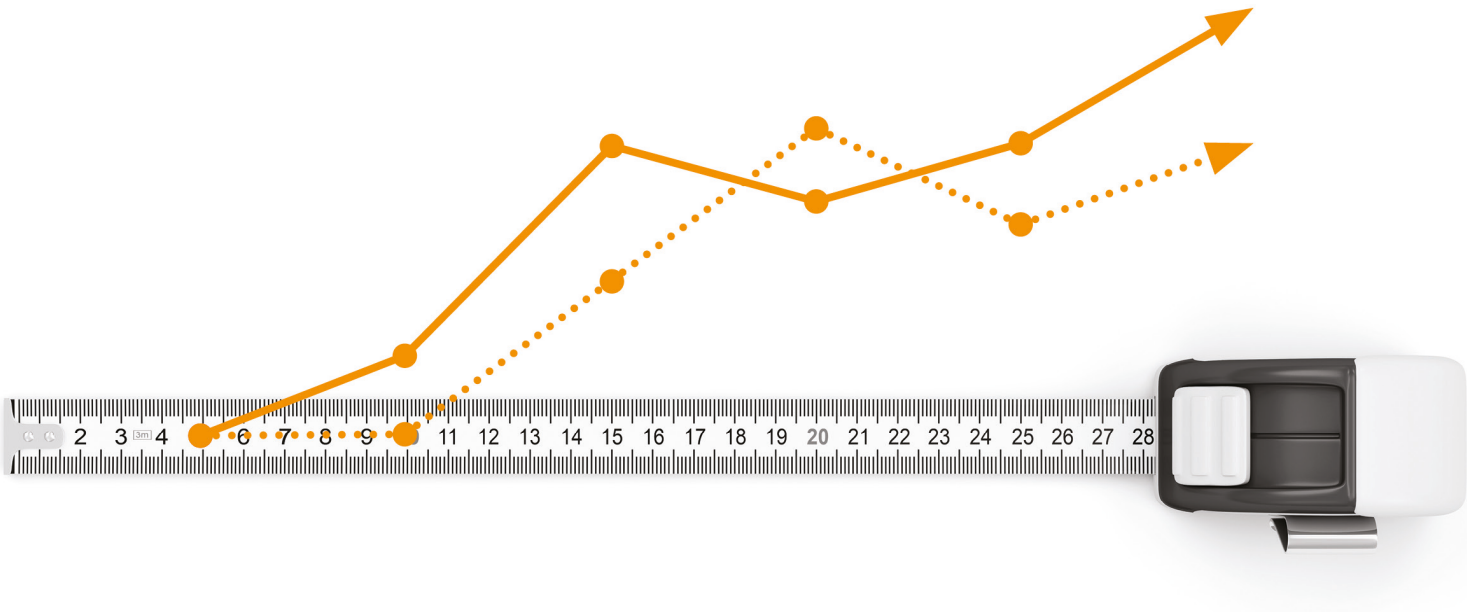
EVERSHEDS SUTHERLAND

A measured approach

US Cybersecurity and Data Privacy review **and update:** Looking back on our 2022 articles and planning ahead for 2023



Executive summary

A look back on US Cybersecurity and Data Privacy in 2022 and planning ahead for 2023

By: Michael Bahar, Eversheds Sutherland Co-Lead of Global Cybersecurity and Data Privacy

The year 2023 will continue to have cybersecurity and data privacy front of mind for General Counsels. With sweeping new US and global laws and regulations coming online and the California Privacy Protection Agency (CPPA) standing up, regulatory expectations on the protection and appropriate use of data will only intensify in 2023. In addition, there is an approaching tidal wave of class action litigation concerning the collection of tracking and targeting cookies, the use of chatbots, and the deployment of high-tech security features like voice authentication and fraud prevention.

Looking at the defining words and concepts of 2022 reveal what is to come in 2023, oftentimes in greater force.

Disclosure

With the California Privacy Rights Act (CPRA) and other enhanced state data privacy laws in or coming into effect this year, companies will find an increased regulatory and litigant focus on the ***transparency and completeness*** of privacy and cookie policies. The laws in California, Virginia, Utah, Colorado, and Connecticut require increasingly detailed and prescriptive policies, especially when it comes to the collection, use, and disclosure of sensitive personal information such as biometrics and precise geolocations. In addition, under the CPRA, employee and B2B personal information are now fully in scope, a development that promises to lead to a proliferation of employee privacy rights requests, including those as a prelude to litigation. Human Resources team as well as in-house lawyers need to quickly get a handle on these new employee rights, when they apply, the critical exceptions, and the implications.

Consent

The days of relying on consumer's to consent at the end of long list of disclosures are waning. Instead, what can be referred to as European-style requirements for ***clear, unambiguous, affirmative consent*** are rapidly proving the best way to reduce regulatory and class action risk. For example, putting in place a "cookie door" and a cookie consent manager, where users are required to actually opt in to the collection of all but essential cookies, will greatly reduce the risk of "selling" or "sharing" cookie data under state privacy laws and can even mitigate the need for having to honor a global privacy control (GPC) or Do Not Track signal, and it can greatly help avoid class action litigation under state wiretapping and eavesdropping statutes, many of which require all-party consent.

Starting in the latter half of 2022, US companies began experiencing a surge of ***consumer class action lawsuits*** alleging businesses and their software providers were violating state anti-wiretapping statutes and invading consumers' privacy rights based on their websites' use of "***session replay***" technologies without obtaining sufficient consent. Session replay, or the ability to replay a visitor's journey on a website or within a mobile application or web application, including what they viewed, clicked on, or hovered over, is relatively new, but the laws under which plaintiffs are suing are relatively old. As a result, in 2023, businesses that operate consumer-facing websites that employ session replay technologies (which is many companies) should strongly consider proactive measures to obtain affirmative consent.

Consent will also be critical for those companies, particularly in the financial services sector, that employ technologies like voice authentication and fraud prevention, or in the consumer sector, who employ virtual try-in features.

Data protection

Increasing geopolitical tensions continue to exacerbate the cybersecurity threat, and new regulations are coming online to protect data and ***enhance reporting under increasingly tight deadlines***, even when personal data is not impacted. For example, New York's Department of Financial Services (NY DFS) expanded the scope of events that trigger mandatory reporting within 72 hours and requires ransom payments to be reported within 24 hours. Further, the new US federal law passed in March 2022 will require (once the accompanying regulations are promulgated) companies providing "critical infrastructure" to report cybersecurity incidents and ransom payments to the Department of Homeland Security (DHS) within the same time frames.

The Securities and Exchange Commission (SEC) has also proposed new regulations regarding mandatory public reporting of cybersecurity incidents within four business days, and the Federal Communications Commission (FCC)

is proposing to reduce the current seven-business-day mandatory waiting period prior to notifying telecom customers of a data breach and to expand the definition of a notifiable breach to include inadvertent, but still harmful, incidents. Moreover, some countries, like India, require certain cyber notifications within six hours!

Even encrypted data is not safe, especially with the emergence of ***quantum computing***, which promises to render traditional cryptographic algorithms obsolete. With the reality of harvest now, decrypt later attacks, countries like Japan, India, and Costa Rica are explicitly requiring regulatory notification for the theft of encrypted data. The US and other nations are looking to proactively defend against these attacks by adopting new cryptographic standards, the use of which may eventually become critical for private organizations via regulation or contract.

Vendor due diligence

Regulators typically ask the same three questions: (1) what other regulators have been told and when were they told; (2) were multifactor authentication and encryption in place; and (3) if the breach involved a third party, what was the extent of the due diligence performed prior to entering the contract and during the life of the contract. Indeed, regulatory expectations over third-party due diligence are rising sharply. They are likely to expect documented due diligence over third parties, including a risk assessment and precise contractual terms in data processing agreements or addenda (i.e., the CPRA requires very prescriptive contractual terms), and they are likely to expect to see how companies ensure those contractual obligations are met. For example, the National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law is becoming widely adopted in the US, which includes requirements for insurers to adopt risk management programs over third-party vendors. Similarly, annual audits of processors are increasingly becoming required contractual terms under comprehensive state privacy laws.

Coordination

While regulators often talk, they do not necessarily coordinate—and no regulator wants to be caught by surprise, putting an increasing premium on ***consistent and coordinated communications***. The ability to coordinate becomes that much more complex when more jurisdictions have data breach notification requirements involving increasingly stringent timescales.

In addition, companies will want to watch very carefully three other developments in 2023:

The contraction of cyber insurance coverage

Cyber insurers are increasingly scaling back coverage for state-sponsored attacks, which can be among the most costly cyberattacks a company may experience. With premiums also increasing as the scope of coverage contracts (and more restrictions are placed), companies are likely to start reevaluating how much to put aside for insurance and how much to invest in improving preparedness, from both a technical perspective and from both a governance perspective, particularly in light of the elevating regulatory requirements and expectations discussed above.

The potential easing of cross-border data flows

With President Biden's executive order of October 7, 2022, companies can expect the return of a privacy shield and further reduce their documented risks of transfers to the US in light of the reforms within Executive Order 14086. That said, given the likelihood of increasing volatility around cross-border data flows from Europe, companies may also want to consider entering into or maintaining their new standard contractual clauses and being intentional about data that needs to flow to the US and data that can stay local. The EU-US agreement is paralleled by a US-UK agreement, but there is no analogous agreement with other countries like China, so companies will still need to navigate global restrictions on cross-border data flows in 2023.

The emerging opportunities and risks of new technologies

Artificial intelligence (AI) can replace human operators in analyzing data and making decisions that historically only a human could make, which raises the question of where responsibility for certain acts and decisions should fall. The US government released the "Blueprint for an AI Bill of Rights," a nonbinding set of guidelines that companies are encouraged to adopt when implementing AI. While widespread use of AI may be on the horizon, companies should anticipate that regulators will keep an eye out for its uses and abuses, especially as it pertains to the type of automated decision-making, or profiling, that privacy laws like the CPRA regulate. As mentioned above, ***disclosure, transparency, and, at times, clear, unambiguous prior consent*** will be crucial.

Conclusion

Overlapping cybersecurity and data privacy regulations will require a deft touch when it comes to balancing compliance, risk management, and effective business operations—never more so than in 2023.

This article was first published on Westlaw Today on 3.1.23.

Did you know?

$10.5 trillion
Global cost of cybercrime by 2025
Source: Cybersecurity Ventures

$5 trillion
Business losses to data breaches by 2024
Source: Juniper Research

75%
Increase in cybersecurity breaches over next five years
Source: Norton

600%
Cybercrime increase due to COVID-19 pandemic
Source: Purplesec.us

$260 billion
Global business spend on cybersecurity solutions by 2026
Source: Cybersecuritydive

$188.3 billion
Global spending on cybersecurity estimated in 2023
Source: Gartner

277 days
Average time to detect and contain a data breach
Source: IBM

$423.56 billion
Estimated worth of cybersecurity market by 2028
Source: Businesswire

$387 million
Average cost of a breach of more than 50 million records
Source: IBM

Visit our GDPR, CCPA and Blockchain/Crypto Assets hubs for one-stop information on each of these landmark privacy issues.

Access BreachLawWATCH, our mobile app, providing easy, consistent access to data breach statutes.

A Focus on Cybersecurity

2022 Cybersecurity and privacy insights

Legal Alerts, Articles and Quarterly Updata Reports

Legal Alerts

Enforcement actions and litigation	*What's inside*
Privacy litigation trend: Session replay software targeted under state anti-wiretapping statutes (October 25, 2022) Recently, US companies are experiencing a surging wave of consumer class action lawsuits alleging businesses and their software providers are violating state anti-wiretapping statutes and invading consumers' privacy rights based on their websites' use of "session replay" technologies... *Click for full article*	After the Ninth Circuit ruling in *Javier v. Assurance IQ LLC* —where the court held that website operators must obtain prior express consent from users in order to escape liability for their use of session replay software - states have seen a significant uptick in the number of lawsuits targeting privacy concerns related to wiretapping statutes and session replay technologies. The majority of litigation has been focused on California, Florida and Pennsylvania, highlighting the fact that this issue is especially pertinent in two-party consent states. This publication discusses penalties related to violation of anti-wiretapping laws, considers potential defenses for companies facing such suits, and suggests that businesses operating consumer-facing websites using session replay technologies consider obtaining affirmative consent in all-party consent states.
The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (March 29, 2022) The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), passed as part of the omnibus spending bill on March 15, 2022, will require critical infrastructure companies - which could include financial services companies, energy companies and other key businesses for which a disruption would impact economic security or public health and safety - to report any substantial cybersecurity incidents or ransom payments... *Click for full article*	Companies within the critical infrastructure sector should consider reviewing the protocols for handling cybersecurity incidents and ransomware attack, with the passage of CIRCIA in early 2022. The act establishes new reporting requirement, and calls for the Cybersecurity Infrastructure Security Agency (CISA) to further define "covered entities." The act also prescribes a stringent reporting timeline for covered entities that experience cyber incidents and that pay ransom to online bad actors, meaning that companies may be required to report before completing investigations. CIRCIA further requires continued reporting as information unfolds, but it does provide exemptions for entities with substantially similar preexisting reporting requirements with other agencies. The passage of the act indicates the federal government's interest in taking an active role in improving cybersecurity in the US.
FinCEN warns financial institutions to be "vigilant" for Russia sanctions violations (March 18, 2022) On March 7, 2022, the Financial Crimes Enforcement Network (FinCEN) issued an alert calling on financial institutions to be "vigilant" in guarding against attempts to evade the recent imposition of expanded Russia sanctions. The latest financial and economic sanctions imposed by the Office of Foreign Assets Control (OFAC) seek to "isolate Russia from the global financial system... *Click for full article*	The FinCEN is warning financial institutions to be cautious in dealing with entities and individuals who may be attempting to circumvent the growing list of sanctions imposed on Russia by the US. In particular, the agency advises that the less traditional financial markets, like those involving crypto and virtual currency, are ripe for exploitation. It also lists a number of red flags to help companies identify sanctions evaders, including nonroutine interactions with Russian banks, newly established accounts attempting to transact with sanctioned institutions, and the use of third parties to shield the identities of sanctioned persons.
SEC proposes mandatory cybersecurity disclosures (March 17, 2022) On March 9, 2022, the Securities and Exchange Commission (the SEC) proposed amendments to certain rules regarding cybersecurity disclosure in order to standardize and to enhance disclosures made by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934... *Click for full article*	The SEC has proposed new rules seeking to establish more consistency in cybersecurity disclosure practices among those public companies that fall within its purview. The act, if passed, will not only attempt to clarify existing guidance, it will also serve to modernize regulations, highlighting the undeniable significance of cybersecurity policies and concerns in the evolving securities industry. It is anticipated that the proposed rules will have a broad impact on a good number of entities, which can prepare for changes by reviewing policies and providing additional training to those responsible for oversight.

New executive order forges path for unified US regulation of digital assets (March 11, 2022)

In an Executive Order (EO) issued March 9, 2022, President Joseph Biden set out the guiding principles for US policy on digital assets and digital asset regulation, including US policy with respect to a US Central Bank Digital Currency (CBDC). The EO is an anticipated and hoped-for development among some in the financial services industry, signaling for the first time... *Click for full article*

After years of unregulated activity and development, the digital asset industry is getting some much needed consideration from the US government, Biden issued an EO setting out principles for US policy on digital assets, including the provision for a US central bank digital currency. The EO marks a change in tide, bringing virtual currencies and crypto assets closer to the main stream and legitimizing the sector. The order calls for interagency cooperation, enhanced national and cybersecurity measures, and improved consumer and investor protections. Looking ahead, US government departments and agencies will need to dedicate programs and resources to abide by the order and build out policies and protections as the digital asset market continues to grow.

SEC proposes cybersecurity risk management rules for investment advisers, funds and business development companies (March 2, 2022)

The Securities and Exchange Commission (SEC) has joined a host of other regulators in doubling down on efforts to protect against the rapidly intensifying cyber threats—with important implications for all SEC-registered investment advisers (Advisers) and SEC-registered investment companies (Funds)... *Click for full article*

A new set of rules and amendments has been proposed by the SEC, in an effort to enhance and regulate cybersecurity practices for investment advisers and investment companies. Information security and defense against cyberattacks have become top priorities for the SEC and other agencies alike, as the worlds of finance and technology become increasingly entwined and threats by bad actors become more frequent and intense. This publication sets out four key requirements under the SEC's proposal and details the opportunities for notice and comment as rulemaking proceeds.

Stablecoins: some key regulatory and enforcement initiatives of US regulators (January 20, 2022)

During the past few months, the US Treasury, the US banking agencies, the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) have pursued several regulatory or enforcement initiatives relating to firms engaging in stablecoin activities... *Click for full article*

A number of US departments and agencies have turned their attention to the stablecoin market, charging firms with regulatory and enforcement initiatives aimed at wrangling the novel and rapidly developing technology. This publication discusses efforts by the US Treasury, banking agencies, the SEC and the CFTC among others, and summarizes support and guidance coming out of the President's Working Group on Financial Markets (PWG) as well as the Federal Deposit Insurance Corporation (FDIC) and the Office of the Comptroller of the Currency (OCC).

US Cybersecurity and data privacy review and update: Looking back on our 2021 articles and planning ahead for 2022 (January 25, 2022)

The past year's trends in privacy and cybersecurity are set to intensify in 2022, with heightened threats, increased regulations, and elevated expectations—as well as new opportunities. To navigate the year ahead, we lay out the articles and lessons of 2021 to help maintain an up-to-date, agile and holistic data strategy... *Click for full article*

This publication collected legal alerts and articles from 2021, providing a look back at the action that has led us to where we are today. With deep dives into cryptocurrency and financial services, enforcement actions and litigation, insurance, and new technology, this compilation is an excellent source to help understand recent updates and trends in the world of cybersecurity and data privacy.

Privacy laws

What's inside

Here we go again: The CPPA kicks off the formal rulemaking for the CPRA (July 21, 2022)

On July 8, 2022, the California Privacy Protection Agency (the CPPA) officially began the formal rulemaking process for the California Privacy Rights Act (CPRA). The CPPA identified three primary goals for the rulemaking... *Click for full article*

The new round of regulations sought to reconcile existing regulations with amendments, operationalize new rights under the CPRA, and clarify statutory requirements. Providing useful insights into the CPPA's evolving interpretation of the CPRA, the proposed amendments give companies a helpful roadmap to compliance leading into the new year when the law goes into effect. In particular, the rulemaking highlighted key considerations like data minimization, user notice and consent, opt-out functions, and expanded due diligence requirements. Businesses must be in compliance with the new CPRA regulations by January 1, 2023.

Connecticut becomes the fifth state to enact a comprehensive data privacy law (May 17, 2022) Connecticut's new consumer privacy law imposes enhanced privacy disclosures and assessment requirements on businesses, and provides consumer rights similar to those in Europe's GDPR, the California Privacy Rights Act (CPRA), the Virginia Consumer Data Protection Act (VCDPA), the Colorado Privacy Act (ColoPA), and the Utah Consumer Privacy Act (UCPA). Scheduled to take effect on... *Click for full article*	Connecticut has joined the ranks of a handful of states that have enacted comprehensive data privacy laws to better protect their citizens. The Act Concerning Personal Data Privacy and Online Monitoring, offers many of the same rights and protections as the laws in Virginia, Colorado, and even the European Union's GDPR. However, Connecticut's law has some unique requirements for the provision of prohibitions in data processing agreements. Nonetheless, the Connecticut attorney general has committed to work with data controllers in the coming years to help them comply with the new law as it takes effect.
Join the club: Utah is the fourth state to enact a comprehensive data privacy law (March 30, 2022) On March 24, 2022, the Utah governor signed a consumer privacy law (the Utah Consumer Privacy Act, UCPA), marking the fourth state law to create enhanced data privacy rights and protections for consumers. The law will go into effect on December 31, 2023... *Click for full article*	The passage of the UCPA continues the trend of state-level regulation of data processing and related privacy concerns. While the new law does contain a number of protections for consumers, the UCPA is narrower and provides more exemptions than privacy laws in California, Colorado, and Virginia. Utah also takes a unique position on profiling and ad targeting, falling short of condemning or prohibiting these practices and instead allowing for consumers to opt out of targeted advertising but not the entire profiling process.

New technology, privacy, and cyber legislation and guidance

	What's inside
Global data privacy and cybersecurity – The data dozen: what's trending now? (November 8, 2022) Key trends that your organizations and boards should be considering in privacy, data and cybersecurity now and over the next 12-24 months... *Click for full article*	The article identifies 12 key trends that will develop in the next 12-24 month including localization laws, proposals around the use of AI, the implementation of non-fungible token regulation, the challenges and opportunities of working with biometrics, and continued developments in global privacy laws. This publication provides thoughtful commentary, and useful insight into some of the biggest issues facing companies today and in the future.
Getting ready for quantum computing: Managing the quantum threat (August 4, 2022) Experts estimate that within the next decade or so, adversaries will have the capacity to use quantum computing to break the encryption on virtually all existing digital databases. This is why it is highly significant that on July 5, 2022, the National Institute of Standards and Technologies (NIST) under the US Department of Commerce announced that it had selected four quantum-resistant cryptographic algorithms... *Click for full article*	Now is the time to prepare for the post-quantum (PQ) era, as current capabilities are being exploited in harvest now, decrypt later attacks. With the rapid expansion of quantum computing technology, bad actors anticipate being able to access encrypted data sooner than later, meaning that companies should be vigilant now to prevent future harm. NIST's move to approve several quantum-resistant cryptographic algorithms highlights that the danger may be closer than it appears. As the algorithms are adopted into the agency's PQ standardization project, it is expected that organizations will utilize the technology to protect sensitive personal and business information as well as any other data that is at risk of exposure unless encrypted with quantum-resistant algorithms. This legal alert discusses a variety of risks that companies need to be aware of and notes existing and upcoming governmental responses to this novel threat.
***Merck and International Indemnity v ACE (et al.)*: war exclusion clauses in an age of cyber warfare** (March 15, 2022) Companies should be aware that, as a result of increasing geopolitical instability, there is a heightened risk of cyber-attacks. Particularly in light of the Merck case, they should therefore consider closely examining the scope of their insurance policies... *Click for full article*	Cybersecurity experts warn companies to prepare, as computer networks are becoming battlegrounds in the wake of geopolitical disputes. Politically motivated cyberattacks are on the rise, and both private and public organizations have been feeling the impact. Data-wiping malware, in particular, has become increasingly popular with bad actors, as it allows for targeted attacks but still has the capacity to have a broad impact. Recent court decisions underscore this threat and suggest that companies consider reviewing and potentially modifying insurance coverage to account for the uptick in geopolitical cyberattacks.

Biometrics

What's inside

Global Biometrics Guide 2022
(February 24, 2022)

Eversheds Sutherland is pleased to send you a digital copy of its 2022 Global Biometrics Guide, authored by more than a dozen of our attorneys from offices around the world... *Click for full article*

This guide walks readers through the basics of biometrics and shares insights on the past, present, and future of the technology as well as potential legal, social and ethical concerns. It also details US and international laws governing the collection, use, and retention of biometric data. For each jurisdiction, experienced attorneys provide in-depth coverage of existing regulations and examples of challenges facing companies using the data, in addition to predictions about the future of governance in this rapidly evolving field. The publication provides helpful guideposts for companies trying to comply with existing and developing regulation in the world of biometrics.

Insurance

What's inside

NAIC report – 2021 Fall National Meeting
(January 5, 2022)

The National Association of Insurance Commissioners (NAIC) held its 2021 Fall National Meeting from December 11 to 16 in San Diego, California. The meeting was held in a hybrid in-person and remote format due to the ongoing COVID-19 pandemic... *Click for full article*

This report covers highlights from select meetings held during the 2021 Fall National Meeting of the NAIC. With key developments in technology and privacy; financial issues; and environmental, social and governance (ESG), the outcomes of the gathering indicate the pervasive impact of evolving capabilities in cybersecurity and data privacy on the insurance industry. Use this publication to take a deep dive into trends and changes coming down the line.

Articles

Raising the Bar on Reasonableness: Your Comprehensive Guide to NY DFS's New Era of Cybersecurity Regulation
(November 1, 2022)

New York Law Journal

Over the past year, the New York Department of Financial Services (NY DFS or the Department) has worked on several fronts to overhaul its approach to regulating the cybersecurity risk and compliance of New York regulated financial services providers (Covered Entities... *Click for full article*

Through supervision, enforcement, and regulation, NY DFS has made considerable efforts in 2022 to heighten expectations around regulatory compliance in cybersecurity. The agency recently proposed rules that would expand breach notification and ransomware reporting as well as require frequent and enhanced monitoring and testing of systems for vulnerabilities. NY DFS has also provided guidance detailing elevated expectations for Covered Entities and on the adoption of an affiliate's cybersecurity program. The agency has made clear that cybersecurity and data privacy are priorities in the financial services market and this article provides details as to how it is acting on those priorities.

On the horizon: More cyber investigations from a growing number of federal agencies
(September 2022)

Global Investigations Review

Cybersecurity and data privacy consistently rank as among the most pressing concerns for general counsel and chief legal officers across industries – and while state attorneys general continue to aggressively file data breach class actions, the US government is... *Click for full article*

While a number of states have begun to enact their own data privacy and cybersecurity laws, the US has notably declined to pass a comprehensive national act. However, that doesn't mean that the federal government is uninterested in regulation. On the contrary, following an EO by Biden in the wake of the Colonial Pipeline ransomware attack, a number of federal agencies have sought to engage more heavily in privacy and cybersecurity enforcement. The FTC, SEC, DOJ, and DHS have all increased efforts to identify and investigate major breaches and attacks, often resulting in fines and sanctions. Experts predict that this trend will continue, and perhaps even expand as novel concerns arise and the possibility of transnational investigations and prosecutions emerge.

The Significance And Legal Risks Of Quantum Computing (August 19, 2022)

Law360

Experts estimate that within the next decade or so, adversaries will have the capacity to use quantum computing to break the encryption on virtually all... *Click for full article*

This article discusses the very real threat that quantum computing poses today, despite being years from realizing the actual potential of the technology. The threat of harvest now, decrypt later attacks has grown over the years, as hackers and bad actors anticipate significant development of quantum technology in the immediate future. As a part of its Post-Quantum Cryptography Standardization Project, the NIST, has selected four quantum-resistant cryptographic algorithms that can be used to protect encrypted databases from quantum attacks. Stakeholders are hopeful that this technology, in conjunction with private and government action, will be useful in thwarting attacks using rapidly developing quantum capabilities.

Advancing Digital Agency: The Power of Data Intermediaries (February 2022)

World Economic Forum

With the integration of screenless technology into everyday life, the data ecosystem is growing increasingly complicated... *Click for full article*

Humans face a myriad of challenges as technology becomes increasingly integral across multiple facets of our lives. Complicated dynamics around data collection, use, notice, and consent stoke fear and perpetuate mistrust of technology among consumers. This report explores the potential to outsource human decision points to an agent or trusted intermediary to act on an individual's behalf, with implications for many companies, including within the technology and financial sectors. The hope is that by leaning into new developments, we will be able to use technology to allay fears and mistrust and to encourage more positive relationships and opinions of its power and potential.

Cybersecurity and data privacy foresight 2022 (January 20, 2022)

Thomson Reuters

Last year's relentless rate of change in the threat and regulatory environments for cybersecurity and data privacy will not soon abate in 2022, necessitating a forward-looking, risk-based and increasingly globalized strategy. At the same time, exciting new technologies continue to... *Click for full article*

This article discusses major themes and trends facing the cybersecurity and data privacy world in 2022. With a number of laws being updated or newly enacted, the rules and regulations governing compliance and enforcement will change for stakeholders. State and federal agencies have also expressed increased interest, requiring diligence on behalf of companies that wish to keep up with regulator expectations. The publication also highlights the impact that new AI technologies and the metaverse will have on the world of data privacy and cybersecurity, and it urges companies to fortify defenses early as data breaches and ransomware attacks continue to rise.

Updata: Your quarterly data privacy and cybersecurity update

Welcome to the latest edition of Updata – the international update from Eversheds Sutherland's dedicated Privacy and Cybersecurity team. These updates cover key US and global privacy and cybersecurity developments.

October – December 2022 – Edition 18
(January 20, 2023) *Click for full update*

July – September 2022 – Edition 17
(October 25, 2022) *Click for full update*

April – June 2022 – Edition 16
(August 1, 2022) *Click for full update*

January – March 2022 – Edition 15
(April 11, 2022) *Click for full update*

Contacts

Michael Bahar
Partner, Co-lead of Global Cybersecurity and Data Privacy
Email | +1 202 383 0882

Frank Nolan
Partner
Email | +1 212 389 5083

Sarah E. Paul
Partner
Email | +1 212 301 6587

Ian Shelton
Partner
Email | +1 512 721 2714

Brandi Taylor
Partner
Email | +1 858 252 6106

MJ Wilson-Bilik
Partner
Email | +1 202 383 0660

Leslie Bender
Senior Attorney
Email | +1 202 383 0274

Melissa Fox
Counsel
Email | +1 404 853 8109

Deepa Menon
Counsel
Email | +1 202 383 0928

Al Sand
Counsel
Email | +1 512 721 2721

Chris Bloomfield
Associate
Email | +1 202 383 0269

Janell Johnson
Associate
Email | +1 202 383 0327

Pooja Kohli
Associate
Email | +1 212 389 5037

Rachel May
Associate
Email | +1 202 383 0306

Jay Patel
Associate
Email | +1 713 425 3530

Melanie Ramey
Associate
Email | +1 404 853 8317

Tanvi Shah
Associate
Email | +1 858 252 4983

Rebekah Whittington
Associate
Email | +1 404 853 8283

eversheds-sutherland.com