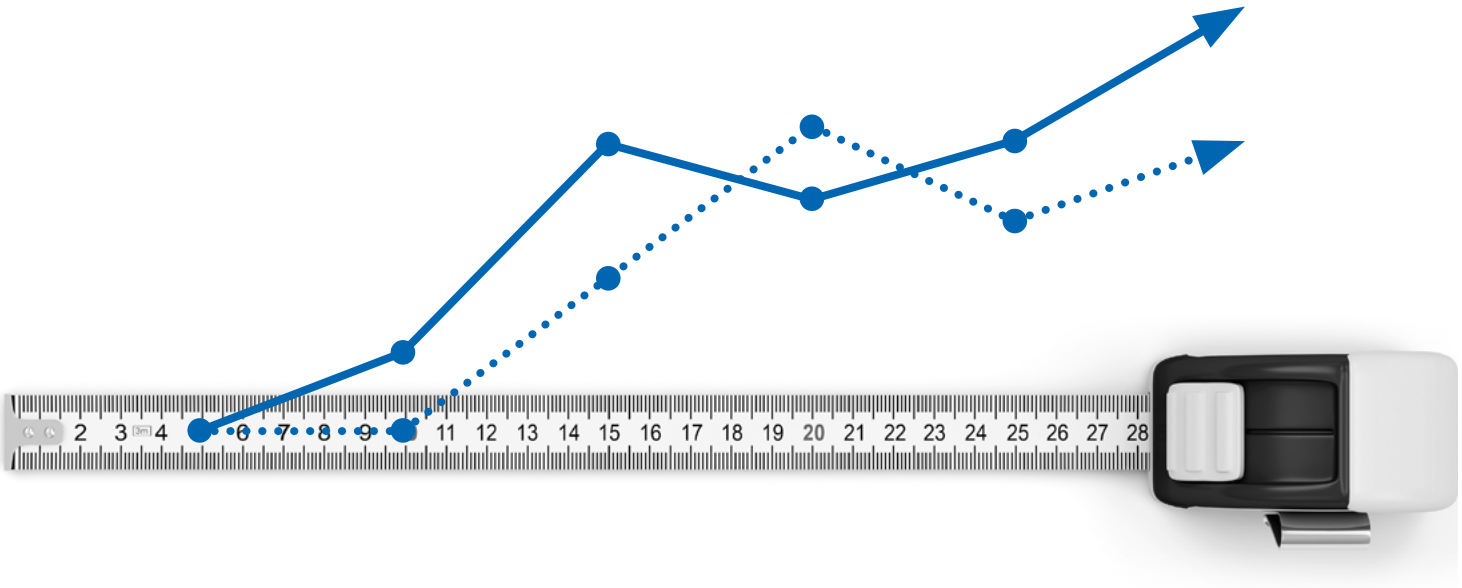
EVERSHEDS SUTHERLAND

A measured approach

US Cybersecurity and Data Privacy review and update: Looking back on our 2023 articles and planning ahead for 2024



Executive summary

A look back on US Cybersecurity and Data Privacy in 2023 and planning ahead for 2024

By: The Eversheds Sutherland US Data Privacy, Security and Technology Team

Technological advances, especially in Artificial Intelligence and quantum computing, will continue to amaze in the coming years. They will open up vast new opportunities while presenting profound regulatory, litigation, and reputational risks for companies and national security risks for countries. At the same time, geopolitical instability coupled with advanced technologies will drive greater cybersecurity threats for companies and governments alike.

As we move into 2024, greater importance will lie in maximizing the upsides of technologies while systematically anticipating and mitigating their risks. The New Year will see forward-looking organizations establishing robust internal Artificial Intelligence safeguards, enhancing efforts and formalizing Board engagement on cybersecurity and resiliency, and reviewing privacy policies and disclosures in light of new legislation and regulations, enterprising class action theories, and consumer protection challenges. Global and public companies will also have to efficiently accommodate a host of cross-cutting and proliferating disclosure obligations as timescales for notifications shrink.

In this year-end compendium of articles, we look back on our analyses and predictions for 2023, while predicting what will come in 2024.

Artificial Intelligence

Generative AI was the story of 2023, which will continue to unfold in exciting ways in 2024. However, no technology is cost-free, and the New Year will surely see increased regulatory, judicial and congressional scrutiny of this transformative technology.

"AI bias," "deep fakes" and "hallucination" entered the legal lexicon in 2023, and regulators and plaintiffs will surely use existing laws and new authorities to challenge the development and implementation of AI.

With the provisional agreement on the European AI Act and its extra-territorial effect, the Biden Administration's issuance of an Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, NIST AI Guidelines and other agency guidance and state-specific requirements, businesses adopting AI must keep up with and meet evolving AI standards. New York, Colorado and California have already put in place measures to protect against bias in AI. We can expect to see other states and industry agencies take a similar position.

At the end of 2023, the Federal Trade Commission used its existing Section 5 authorities to ban the use of automated decision-making at a pharmaceutical company, with one commissioner calling out the "pernicious" effects of algorithmic bias and laying out a roadmap " for what an algorithmic fairness program" should look like – transparency, recourse if harmed, training, detailed assessments of the risks of the tool and its training data, ongoing accuracy testing of the tool, etc.

Therefore, companies would be well served to develop robust internal self-governance over their development and implementation of AI. See, for example, Pillars article.

Cybersecurity

Escalating tensions across the globe are fueling a surge of aggressive cybersecurity attacks, with the financial services, technology and energy sectors an especially common target. This year will likely not see an end to this unsettling trend, and in an effort to mitigate somewhat inevitable damage, states and agencies will continue to attempt expanding cyber reporting requirements.

More robust cybersecurity strategies may need to be deployed to protect the vulnerabilities associated with new technologies such as quantum computing, which continues to advance at rapid speed and the increasingly prevalent adoption of IOT devices.

We can expect to see more guidance around minimum cybersecurity requirements for specific hardware and software in recognition of the increasing prevalence of smart businesses and homes. The scope of privacy protections are also likely to expand to cover previously exempt data, such as encrypted data, which is being harvested in anticipation of unauthorized decryption through the use of new technology. India, Vietnam and Colombia already require data breach notification to the regulator or impacted individual where data is encrypted.

As 2024 unfolds, it will be increasingly important for organizations to update their cybersecurity programs, to stress-test them regularly, to ensure they incorporate the latest threats – including AI-powered deepfakes – to ensure the proper level of Board and C-Suite involvement and oversight, and to further compliance with the latest requirements (see e.g., NY DFS article, SEC article).

Privacy enforcement and litigation

In addition to new AI-based litigation, class action privacy litigation will continue apace. Plaintiffs are breathing new life into old laws like the California Invasion of Privacy Act designed to prevent unlawful wiretapping and pen registers from challenging data tracking via cookies and related technologies. Laws passed decades ago to protect a consumer's VHS rental history or a patient's genetic test results have also been repurposed to provide a cause of action against companies that track, process and maintain personal information. While these actions so far have yielded mixed results, companies can expect the plaintiffs' bar to keep combing through old laws to find new causes of action while eagerly awaiting more purpose-built laws, and even lobbying for greater private causes of action.

Federal Regulators and State Attorneys General are likely to increasingly use consumer protection laws to bring enforcement action where privacy statements diverge from privacy practices or are otherwise deemed misleading, especially when it comes to cookie disclosures, opt-outs of tracking technologies, consents and the use of Artificial Intelligence. Journalists and privacy groups will also keep publishing pieces to further spur on regulatory action.[1]

An ounce of prevention could be worth well more than a pound of cure: Risk mitigation through obtaining consumers' opt-in consent – even when not required by US privacy regulations – and maintaining effective security measures should prove the best defense against this new offense. Relevant article.

Privacy protection

We will continue to see the patchwork of comprehensive state privacy laws enlarge, with the prospects of federal privacy legislation continuing to dim, except possibly in a lame-duck session of Congress in December 2024. There is likely to continue the strong convergence among state privacy laws, except possibly in states like New York, but there will continue to be important nuances to efficiently accommodate. For example, Iowa and Utah do not provide a right to correct or opt-in for sensitive data processing, whereas other states do. Only if a state passes a dramatically new approach to privacy will we see a lot of additional compliance burdens requiring even more creative approaches to maintain efficiency. That said, what we most need to watch in 2024 is regulatory activity outside of state privacy law, where organizations may become subject to laws they were currently immune from or subject to additional restrictions on the collection and use of consumer data.

There has been a proposal by the Consumer Financial Protection Bureau (CFPB) to modernize Fair Credit Reporting Act (FCRA) coverage and dramatically expand the FCRA to apply to data brokers selling consumer reports. In Colorado, insurance companies are now prohibited from using external consumer data and information sources that unfairly discriminate against specified protected classes. The NAIC Privacy Protections Working Group has also issued a draft model law for comment aiming to expand consumer privacy protection and restrict the use of consumer personal information by insurance licensees.

Further afield, global privacy laws will likely continue to push the limits of their jurisdiction. Several global privacy laws were introduced or amended in 2023, such as the adoption of India's long-awaited Digital Personal Protection Bill, which has extra-territorial reach, and amendments to Australia's Privacy Act 1988, which broadens the extraterritorial application of Australia's privacy law and now captures businesses provided they carry on business in Australia, even if they do not have a foreign subsidiary.

Dark Patterns

Related to the value of enhancing consent and disclosure practices, we are likely to see greater regulatory scrutiny over the use of dark patterns and the development of ethical digital products that do not rely on dark patterns and addictive designs.

Recently, the CFPB and FTC have taken enforcement action to combat the rise of digital dark patterns, suing companies for requiring users to navigate a maze of screens in order to cancel recurring subscriptions, sneaking unwanted products into consumers' online shopping carts without their knowledge, and experimenting with deceptive marketing designs.

From a regulator's perspective, the use of dark patterns is soaring. Dark patterns involve manipulating users by distorting or impairing their ability to make autonomous and informed choices or decisions.

Privacy-Preserving Technologies

Privacy-Enhancing Technologies (PETs) and Privacy-Preserving Data Sharing and Analytics (PPDSA) are now commonly being adopted in an effort to protect consumer data.

PETs "means any software or hardware solution, technical process, technique, or other technological means of mitigating privacy risks arising from data processing, including by enhancing predictability, manageability, disassociability, storage, security, and confidentiality."[2]

PPDSA technologies refer to "a subset of PETs that are essential for enabling data sharing and analytics in a privacy-preserving manner, such as secure multiparty computation." [3]

Organizations are grappling with ensuring that the use of these privacy-preserving technologies, such as differential privacy, federated learning and the use of synthetic data, sufficiently mitigates privacy and security risks. In its March 2023 research paper, the National Science and Technology Council acknowledged the challenges deriving from the

1 See e.g., https://www.consumerreports.org/electronics-computers/privacy/i-said-no-to-online-cookies-websites-tracked-me-anyway-a8480554809/.

2 Section 3 (z) Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence | The White House.

3 National Strategy to Advance Privacy-Preserving Data Sharing and Analytics (whitehouse.gov)

use of PETs and PPDSAs, including an inadequate understanding of privacy risks and harms, such as whether data is legitimately obtained or used (e.g., with meaningful individual consent) or if the nature or quality of the data could create harmful bias. On December 11, 2023, NIST released Draft Guidelines for Evaluating Differential Privacy Guarantees. We will likely see further discussion around the anonymization and de-identification of data and the standards required to effectively use PETs.

Conclusion

Boldly embracing technological innovation while methodically mitigating regulatory, litigation, congressional investigation and reputational risks will likely be the winning formula for 2024. The dexterity required to balance compliance, risk management, and effective business operations will prove even more challenging in the coming year but ever more valuable.

Did you know?

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

$9.5 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

$300 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

$314.28 billion
Estimated worth of cybersecurity market by 2028
Source: Businesswire

$332 million
Average cost of a breach of more than 50 million records
Source: IBM

2023 Cybersecurity and privacy insights

Legal Alerts, Articles and Quarterly Updata Reports

Legal Alerts

Cybersecurity	*What's inside*
Cyber risk strategy: State-backed cyber attacks and trends in cyber policies and risk management (January 31, 2023) Back in March 2022, we detailed the significant risks to both insureds and insurers posed by unclear cyber insurance policy wordings, with a particular focus on war exclusion clauses in the aftermath of the decision... *Click for full article*	Cyber policy coverage is more necessary and prevalent than ever, but caution is required as insurers raise premiums and narrow coverage in an attempt to limit their exposure. This article considers what details both those insured and insurers must clarify in respect of the extent and sufficiency of cyber insurance coverage. For example, where coverage can properly be denied in reliance of a war exclusion, a nation state attack, or because damage results from an attack taking place in another territory. Only then can organizations assess if it is more efficient to spend on a potentially limited insurance policy or if it is better off placed using its resources to improve preparedness in defending against and responding to a cyberattack.
Financial services regulators ramp up cybersecurity reporting requirements (April 27, 2023) US financial services regulators are continuing to enhance cyber reporting requirements in response to increasing geopolitical tensions, emerging technologies, the proliferation of cyber-attacks... *Click for full article*	This article tracks the efforts of US financial services regulators to enhance cyber reporting requirements in response to increasing geopolitical tensions, emerging technologies, the proliferation of cyber-attacks, and larger market events.
SEC adopts new rules to expand public company disclosure relating to cybersecurity by year end (July 31, 2023) On July 26, 2023, the US Securities and Exchange Commission (SEC) released final rules requiring disclosure by public companies of material cybersecurity incidents and policies and procedures related to cybersecurity risk management, strategy, and governance... *Click for full article*	The US Securities and Exchange Commission (SEC) released final rules placing new cybersecurity disclosure obligations on public companies subject to the reporting requirements of the Securities Exchange Act of 1934, as amended, including business development companies (BDCs) and foreign private issuers (FPIs). This article considers the implications of the new requirements.
New York Raises the Bar Again: Revised Cybersecurity Requirements for Financial Services Companies Finalized (November 12, 2023) On November 1, 2023, the New York Department of Financial Services (NY DFS) published its highly anticipated final amendments to its influential cybersecurity requirements for financial services companies (Part 500). These amendments significantly alter New York's cybersecurity standards... *Click for full article*	The New York Department of Financial Services (NY DFS) cybersecurity requirements for financial services companies have been significantly altered in a recent amendment. This briefing analyzes the changes which include (1) greater senior officer and board responsibility for cybersecurity; (2) expansion of the incidents that are reportable within 72 hours; (3) expansion of long-time regulatory expectations like multifactor authentication and encryption; and (4) a revamp of the annual certification process to allow either a certification of material compliance or written acknowledgment of material non-compliance.

A look ahead US Treasury Department announces initiatives for further study of a federal insurance backstop for catastrophic cyber events (November 29, 2023) On November 17, 2023, the United States Treasury Department's Federal Insurance Office (FIO) and the Volatility and Risk Institute at the NYU Stern School of Business jointly hosted a conference on Catastrophic Cyber Risk and a Potential Federal Insurance Response at which... *Click for full article*	This article considers the momentum on discussions for a federal insurance response to the cyber risk against national security and the US economy. The Treasury acknowledges that the private market for insurance against attritional cyber risk from losses other than those related to major catastrophes is dynamic and growing. The Treasury remains focused on policy options for a public-private collaboration or other federal response that "cabins" catastrophic risk alongside the commercial market.

Artificial Intelligence

	What's inside
New NIST AI framework offers guidance on risk management and governance for trustworthy AI systems (February 07, 2023) On January 26, 2023, the National Institute of Standards and Technology (NIST) released its AI Risk Management Framework (AI RMF or Framework.) The AI RMF is a resource for organizations designing, developing, deploying, or using artificial intelligence (AI) systems... *Click for full article*	In response to an increase in the use of AI, the National Institute of Standards and Technology (NIST) released its AI Risk Management Framework (Framework) to guide organizations in designing, developing, deploying, or using artificial intelligence (AI) systems. The Framework aims to help manage the risks of AI and promote the trustworthy and responsible development and use of AI systems. This article identifies the Framework's four (4) core functions that help organizations manage AI risks and develop trustworthy AI systems: (1) Govern; (2) Map; (3) Measure and (4) Manage.
New York City delays enforcement of its artificial intelligence bias audit in employment law as rule-making continues (February 14, 2023) New York City (NYC) has delayed to April 15, 2023 the enforcement of its first-of-its-type law on bias in artificial intelligence (AI) tools used in employment. Local Law 144 of 2021 prohibits employers in NYC from using artificial intelligence... *Click for full article*	This article considers the jurisdictional reach and implications of this New York law prohibiting employers in NYC from using artificial intelligence to screen candidates for hiring or promotion. It also examines how AI is used in hiring and the associated regulatory trends.
The march to regulatory change for artificial intelligence: the commonalities between the EU and US (March 06, 2023) Our global regulatory specialists have put their heads together for this update... *Click for full article*	This briefing explores some commonalities between the EU and US in terms of regulatory changes with respect to AI, focusing in particular on the the EU AI Act proposals, New York employment law and Colorado insurance law attempts to regulate AI.
California's CPRA rulemaking focuses in on automated decision-making tools (March 21, 2023) On March 27, 2023, the California Privacy Protection Agency (CPPA) will close its second phase of rulemaking on automated decision-making (ADM) systems under the California Privacy Rights Act (CPRA)— but not before giving stakeholders a valuable opportunity... *Click for full article*	This article examines California's proposals and outreach on automated decision making (ADM), including which access and/or opt-out rights should be provided to consumers, and how much "access" should access requests provide.
Colorado Division of Insurance proposes significant revisions to its draft algorithm and predictive model governance regulation for life insurers (June 13, 2023) On May 26, 2023, the Colorado Division of Insurance (CDI) exposed, for public review and comment, a significantly revised draft of its proposed regulation (the Revised Draft Reg.) addressing the governance and risk management (GRM) framework requirements for life insurers... *Click for full article*	This article looks at the Colorado Division of Insurance's revised draft regulation on the governance and risk management (GRM) framework requirements for life insurers using external consumer data and information sources (ECDIS), or algorithms and predictive models using ECDIS. The Revised Draft Regulation continues to hold insurers responsible for third-party vendors and other external resources used with respect to ECDIS as well as algorithms and predictive models that use ECDIS.

Colorado Division of Insurance adopts final rule on use of big data and predictive models (September 28, 2023)

The Colorado Division of Insurance (CDI) adopted a new regulation on September 21, 2023 (Final Regulation) providing guidelines governing the use of external consumer data and information sources (ECDIS)... *Click for full article*

This briefing looks at the final regulation adopted by the Colorado Division of Insurance governing the use of ECDIS, as well as algorithms and predictive models using ECDIS (Models), by Colorado-licensed life insurers. The final regulation seeks to ensure that life insurers who use ECDIS and Models are not engaging in unfair discrimination with respect to race.

NAIC releases highly-anticipated draft model bulletin on artificial intelligence systems used by insurers (July 24, 2023)

On July 17, 2023, the Innovation, Cybersecurity and Technology (H) Committee of the National Association of Insurance Commissioners (NAIC) released for comment a highly anticipated model bulletin (Model Bulletin) on regulatory expectations... *Click for full article*

This briefing reviews the the Innovation, Cybersecurity and Technology (H) Committee of the National Association of Insurance Commissioners (NAIC) model bulletin (Model Bulletin) on regulatory expectations for the use of artificial intelligence systems (AI Systems). The Model Bulletin encourages insurers to implement and maintain a board-approved written AI Systems Program (AIS Program) that addresses governance, risk management controls, internal audit functions and third-party AI systems.

The highly-anticipated US Executive Order on artificial intelligence: Setting the agenda for responsible AI innovation (November 09, 2023)

On October 30, 2023, the Biden Administration issued the groundbreaking Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence1 (Order), which sets in motion a comprehensive US strategy for the responsible development and use of artificial intelligence (AI)... *Click for full article*

This briefing looks at the groundbreaking Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (Order). The Order directs US executive departments and agencies (and encourages independent agencies) to develop standards, frameworks, guidelines, and best practices in anticipation of using their existing authority to regulate AI.

Litigation and Enforcement

What's inside

FTC diagnoses common digital practices as both UDAP and breach (February 08, 2023)

In a groundbreaking decision,1 the Federal Trade Commission (FTC) announced it was diagnosing GoodRx's use of tracking pixel codes and analytics, its digital strategy, as not only an unfair or deceptive act or abusive practice but also as a data breach... *Click for full article*

This article discusses the Federal Trade Commission (FTC) determination that, under the Health Care Breach Notification Rule (HBNR), a company's digital strategies (such as tracking codes and related analytics including those that target information presented to consumers) may be held not only as an unfair or deceptive act or abusive practice but also as a data breach. In the GoodRx enforcement action, for example, the company's online and app resources include third-party data analytics and session replay resources, contrary to its privacy promises to users.

From bad to worse: Two Illinois Supreme Court decisions expand scope of potential damages under Biometric Information Privacy Act (BIPA) (March 7, 2023)

For several years, companies that collect, use, and store the biometric information of Illinois residents have lived in fear of violating the Biometric Information Privacy Act (BIPA),1 due to a tidal wave of class action filings resulting in multi-million dollar settlements and verdicts... *Click for full article*

This briefing looks at the implications of the tidal wave of class action filings under BIPA in Illinois, including the establishment of a five-year statute of limitations period, and potential for each independent use of biometric information to accrue, creating the possibility of astronomical statutory damages awards.

Plaintiffs' attorneys discover a new tool in New York City biometrics law (March 29, 2023)

Plaintiffs have filed two putative class action complaints in 2023, alleging violations of New York City's relatively new biometric information privacy law, signaling a new potential avenue for class action plaintiffs' lawyer... *Click for full article*

This articles analyzes the trend of lawsuits seeking recovery under the NYC Biometrics Law which requires covered commercial establishments that collect, store, convert, retain, or share customers' biometric identifier information to disclose the practice in "plain [and] simple language" on "clear and conspicuous" signage near establishment entrances.

A blockbuster privacy law? VPPA's scope remains unclear (April 12, 2023) Enacted in in 1988 after Judge Robert Bork's video rental history was leaked by a store clerk and published in a newspaper profile about the Supreme Court nominee, the Video Privacy Protection Act (VPPA) was the result of public outcry and bipartisan action... *Click for full article*	This article describes the wave of class actions by plaintiffs alleging that web cookies that track user activity for use in analytics and advertising, violate the 1988 Federal Video Privacy Protection Act (VPPA).
Illinois plaintiffs' attorneys find new tool in old genetic privacy law (November 09, 2023) Although the Illinois Genetic Information Privacy Act (GIPA), 410 ILCS 513/1, et seq. was largely ignored by plaintiffs' attorneys until this year, its substantial statutory penalties and recent case law make it an enticing option for plaintiffs' class action lawyers... *Click for full article*	This article looks at the class action complaints against employers under the 1998 Illinois Genetic Information Privacy Act (GIPA), which protects "genetic information" and prohibits anyone from disclosing the results of genetic tests or the identity of persons tested, except under limited circumstances. Employees using pre-employment physicals that include inquiries into family medical histories and genetic predisposition to certain diseases should take caution.

Consumer privacy protection

	What's inside
NAIC proposes new California-style privacy model law for insurance (February 08, 2023) On Wednesday February 1, 2023, the NAIC Privacy Protections Working Group (the Working Group) released a draft of a new model law for comment, the Insurance Consumer Privacy Protection Model Law (#674) (the Proposal), which proposes to substantially limit... *Click for full article*	This article examines the NAIC Privacy Protections Working Group deaft model law, which aims to expand consumer privacy protection and restrict the use of consumer personal information by insurance licensees, in line with the California Consumer Privacy Act (CCPA) and the UK/EU General Data Protection Regulation (GDPR).
Colorado Division of Insurance's first installment of regulations prohibiting the use of external consumer data and algorithms and what's to come (February 09, 2023) On February 1, 2023, the Colorado Division of Insurance (CDI) released a draft of the first of several regulations to implement S.B. 21-169, Colorado's 2021 law prohibiting insurers from using external consumer data and information sources... *Click for full article*	The Colorado Division of Insurance (CDI) released deaft regulations implementing Colorado's 2021 law prohibiting insurers from using external consumer data and information sources (ECDIS) that unfairly discriminate against specified protected classes. This article looks at the proposed requirements, including governance and risk management frameworks, documentation for the use of all aspects of ECDIS, and reporting.
Iowa enacts the sixth state-level comprehensive data privacy law (April 03, 2023) On March 29, 2023, the Iowa Governor signed into law a consumer data privacy law which enters into force on January 1, 2025. Entities already complying with other enhanced state privacy laws... *Click for full article*	This briefing looks at the applicability of and requirements under Iowa's consumer data privacy law which enters into force on January 1, 2025. Entities already complying with other enhanced state privacy laws should not experience any significant, additional compliance burdens.
CFPB proposal signals a dramatic expansion of the Fair Credit Reporting Act to data broker (September 24, 2023) On September 15, 2023, the Consumer Financial Protection Bureau (CFPB) published an outline of expansive rulemaking proposals to modernize the coverage of the Fair Credit Reporting Act (FCRA) to include data brokers, data aggregators and alternative data sources... *Click for full article*	This article discusses the Consumer Financial Protection Bureau's (CFPB) proposals to modernize the coverage of the Fair Credit Reporting Act (FCRA) to restrict data broker activities and remove medical debt from consumer reports.

Movement of data	*What's inside*
Data transfers update: New data bridge available to facilitate UK-US data transfers from 12 October 2023 – despite "qualified" assurance from ICO (September 24, 2023) A new UK-US data bridge will be available to businesses in the UK looking to transfer personal data to organizations in the United States certified under the UK Extension to the EU-US Data Privacy Framework (UK Extension) from 12 October 2023, without the need for an additional transfer safeguard... *Click for full article*	This article considers the UK-US data bridge available to businesses in the UK transferring personal data to organizations subject to the jurisdiction of the Federal Trade Commission or the US Department of Transportation. UK organizations sending personal data to participating importers will not need to carry out a transfer risk assessment. The development also brings the UK's data transfer rules back in step with the EU.
CFPB previews consumer data portability rule meant to accelerate US open banking adoption (November 07, 2023) On October 19, 2023, the Consumer Financial Protection Bureau (CFPB) issued an advance notice of proposed rulemaking (ANPR) with respect to a new consumer financial data portability rule mandated by Section 1033... *Click for full article*	This article analyzes the Consumer Financial Protection Bureau's (CFPB) advance notice of proposed rulemaking (ANPR), which is intended to allow consumers to port their banking and financial services information easily through consumer and developer interfaces.

Articles	*What's inside*
Comparing Iowa's Data Privacy Law With Other States (April 18, 2023) *Law360* On March 29, Iowa Gov. Kim Reynolds signed into law a consumer data privacy law which enters into force Jan. 1, 2025 It is intentionally more business-friendly than other U.S. state privacy laws. It does not apply in the business-to-business or employment contexts, and... *Click for full article*	This article examines the requirements under Iowa's consumer data privacy law, which goes into force on January 1, 2025. Similar to privacy laws in other states, there is no annual revenue threshold so smaller businesses will also be included. However, companies already complying with the laws in other states should not experience any significant, additional compliance burdens.
The Road to Litigation Is Often Paved With Good Intentions (April 20, 2023) *Law.com* For all the laudable developments with new technologies—including artificial intelligence and, at times, biometrics—companies need to be mindful that, despite their best intentions, they may find themselves subject to serious regulatory and litigation risk. Whether it is banks looking to prevent fraud by analyzing the characteristics of a caller's voice, financial institutions looking to authenticate callers through their voiceprint... *Click for full article*	There is a growing surge of actions filed against some of the world's largest companies for alleged consumer harm caused by implementing advanced capabilities and technologies, like artificial intelligence, on their websites and apps without appropriate disclosures and consent. This article highlights how claimants/plaintiffs are using regulations to bring the claims in the US, UK and EU and discusses ways to mitigate against that risk.
A Mayflower Compact for AI: implementing responsible self-governance for US companies (August 25, 2023) *Global Investigations Review* In the absence of clear AI-specific legislation or regulation in the United States, companies should neither heedlessly charge ahead nor timidly wait for greater clarity. Rather, as regulators use existing authorities and private litigants use old laws to bring suits centered on the newest technologies, companies should strongly consider... *Click for full article*	This article advises companies to implement self-governance frameworks, similar to a Mayflower Compact, to insulate them from the risks associated with artificial intelligence and new technological advancements.

Cyber Siege and Artificial Intelligence: These aren't your parents cyber threats – Link needed to PDF from Digital Marketing (September 2023 Newsletter)

NSCP Currents

Remember when companies' biggest cybersecurity fears were whether employees were using "ABC," "123," or "password" as their login password? Well, when Artificial Intelligence (AI) walked in, we moved far beyond those fears. As broker-dealers (BDs) and Investment Advisors (IAs) face increased cybersecurity challenges from AI, which magnifies the complexity and perniciousness of the cyber threat, they are also finding regulatory requirements... *Click for full article*

As new rules and requirements are released to address "constantly evolving" cyber threats, broker-dealers and Investment Advisors should consider reassessing their incident response, information security, and business continuity plans, their cybersecurity disclosures and board agendas and their approach to coordinated communication. This article highlights types of cybersecurity risks and the need to mitigate these risks.

Game Plan: How Sports & Betting Can Prepare For The Coming Cybersecurity Battle – Link needed to PDF from Digital Marketing (November 9, 2023)

LawInSport

Strategy plus ability on the field; loyalty plus trust in the stands. This is a formula for winning and

for profits; but without a comprehensive data security and privacy strategy, both professional and

college sports teams, venues and betting establishments stand to lose both. This article identifies strategies for sports and betting organizations to combat cybersecurity risks and privacy requirements... *Click for full article*

This article identifies strategies for sports and betting organizations to combat cybersecurity risks. With increasing privacy requirements and cybersecurity risks, entities in the sports and betting industries should review their privacy policies, reassess the state of their cybersecurity, and consider their comprehensive data security and privacy strategy.

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 2023 – Edition 22
(January 31, 2024) *Click for full update*

July – September 2023 – Edition21
(November 05, 2023) *Click for full update*

April – June 2023 – Edition 20
(July 12, 2023) *Click for full update*

January – March 2023 – Edition 19
(May 09, 2023) *Click for full update*

Contacts

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

Neal Higgins
Partner
Email | +1 202 383 0168

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

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

Melissa Fox
Counsel
Email | +1 404 853 8109

Al Sand
Counsel
Email | +1 512 721 2721

Pooja Kohli
Senior Associate
Email | +1 212 389 5037

Chris Bloomfield
Associate
Email | +1 202 383 0269

Atiana Johnson
Associate
Email | +1 202 383 0315

Rachel Reid
Partner
Email | +1 404 853 8134

Frank Nolan
Partner
Email | +1 212 389 5083

Brandi Taylor
Partner
Email | +1 858 252 6106

Leslie Bender
Senior Counsel
Email | +1 202 383 0274

Deepa Menon
Counsel
Email | +1 202 383 0928

Janell Johnson
Senior Associate
Email | +1 202 383 0327

Melanie Ramey
Senior Associate
Email | +1 404 853 8317

Soroosh Faegh
Associate
Email | +1 212 301 6587

Ian Jones
Associate
Email | +1 404 853 8051

Contacts *(cont'd)*

Rachel May
Associate
Email | +1 202 383 0306

Claire Scavone
Associate
Email | +1 404 853 8558

Thomas Spring
Associate
Email | +1 404 853 8328

Tanvi Shah
Associate
Email | +1 858 252 4983

Rebekah Whittington
Associate
Email | +1 404 853 8283

eversheds-sutherland.com