EVERSHEDS SUTHERLAND

Pointed in the right direction

US Cybersecurity and Data Privacy review and update: Looking back on our 2020 articles and planning ahead for 2021

2020 Foresight – executive summary

It was a tumultuous year for privacy and cybersecurity, and further uncertainty is all but guaranteed. The key to navigating this volatility, as 2020 proved, is to develop and maintain a proactive, agile and holistic data strategy — not just react when new court rulings, regulations or a data breach hit.

To help with this front-footed strategy through 2021, it is worthwhile to heed the lessons of 2020.

Observe the trends and get in front of them

As seismic as the advent of new privacy regulations, enforcement actions and court decisions are, there are clear trends that successful companies can use to anticipate and accommodate them. For example, in 2020, Brazil, New Zealand and California embraced GDPR-style laws, and 2021 will bring further global privacy requirements, including in Thailand, Switzerland and Canada. One technique to stay in front of these trends is to adopt a high watermark approach to compliance. For example, the EU's General Data Protection Regulation (GDPR) is the emerging global standard and, therefore, a valuable future-proofing tool. Organizations that integrate GDPR principles into their policies and procedures early — even if they do not yet necessarily need to — will be in better positions to weather the inevitable tide of enhanced privacy obligations. Leveraging a GDPR policy to accommodate the LGPD, CPRA or South Africa's POPIA is easier than starting anew each time.

The costs of noncompliance grow at a greater rate than the costs of compliance

Following on from the above, staying ahead of trends and adopting heightened privacy requirements — even when not yet necessary — is more expensive than not acting, but the costs of delay and of noncompliance are growing at a faster rate. Substantial enforcement and privacy-related litigation exploded in 2020 — and this is only the beginning, especially with new privacy regulators in California and Brazil, new privacy class actions developing in the UK and the Netherlands, and new cyber threats striking at systemic levels, like the SolarWinds hack. Accordingly, litigators should proactively join forces with compliance attorneys and their business colleagues to devise pragmatic and realistic risk-based solutions.

Legal resilience is a core component of operational resilience

From the explosion of work-from-home to contact tracing and ransomware attacks, 2020 was a stress test for operational resilience. A key lesson is that organizations that already have a solid understanding of their data practices, including records of processing activity, the ability to map and track their data flows, and sufficiently detailed internal and external privacy policies, are able to make adaptive adjustments more quickly and efficiently. Accordingly, 2021 will again prove that legal resilience is a core component of operational resilience.

Cybersecurity and privacy require cooperation, not competition

2020 saw a devastating state-sponsored cyberattack, an outbreak of global ransomware attacks, Brexit and increasing walls to the free-flow of personal data across borders, particularly after Europe's Schrems II decision. Private organizations should engage in cyber threat information sharing among themselves and with governments, and private organizations should work with governments to limit the rise of data sovereignty laws that curtail the ability to share personal data across borders. The trend of data nationalism is hard to reverse, but it is critical to do so.

Lawyers are leaders

Similar to what emerged as critical in 2020, the ever-increasing importance of the lawyer as leader will be crucial to meeting all the challenges in 2021. General Counsels need to convince executives of the business need to take a proactive, comprehensive and nuanced approach to data, despite its steeper upfront costs, and they need to partner more closely with their security departments. Most important, they need to continue to lead teams through the inevitable personal and professional hardships in the year ahead, and to celebrate together in the successes.

We hope you enjoy this compilation of our 2020 alerts, and we wish you all the best in 2021!

Did you know?

$10.5 trillion
Global cost of cybercrime by 2025
Source

$5 trillion
Business losses to data breaches by 2024
Source

70%
Increase in cybersecurity breaches over next five years
Source

600%
Cybercrime increase due to COVID-19 pandemic
Source

$134 billion
Global business spend on cybersecurity solutions by 2022
Source

$145 billion
Global spending on cybersecurity in 2020
Source

280 days
Average time to detect and contain a data breach
Source

$400 billion
Estimated worth of 2026 cybersecurity market
Source

$392 million
Average cost of a breach of more than 50 million records
Source

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

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

A Focus on Cybersecurity

2020 Cybersecurity and Privacy Legal Alerts

Enforcement actions and litigation

What's inside

Only YOU can prevent IoT network shutdowns (December 8, 2020)

As tens of billions of additional Internet of Things (IoT) devices are poised to enter the market and infuse our supply chains, on December 4, 2020, President Donald Trump signed the first-ever ... *click for full article*

The IoT (Internet of Things) Cybersecurity Improvement Act's new federal procurement rules for IoT devices, along with some state laws, will help solidify IoT security standards across the board.

Once more unto the breach: The Supreme Court weighs in on a circuit split on what constitutes a hack (November 30, 2020)

Working from home since the onset of the pandemic, you check your social media on a work laptop, in violation of your company's Acceptable Use Policy. Have you just committed a federal crime? Under ... *click for full article*

Do you slide past your employer's rule against using Facebook on a work computer? The Supreme Court could hold that you have committed a federal crime by violating the Computer Fraud and Abuse Act — surf with caution.

The US Department of Justice issues Cryptocurrency Enforcement Framework forecasting increased scrutiny of activities involving cryptocurrency (October 15, 2020)

On October 8, 2020, the US Department of Justice (DOJ) Cyber-Digital Task Force issued an 83-page comprehensive "Cryptocurrency: An Enforcement Framework," (Framework), signaling the DOJ's increased ... *click for full article*

A comprehensive framework document issued by the US DOJ Cyber-Digital Task Force positions the agency to tackle cryptocurrency and pursue criminal actions against bad actors in the space.

No rest for the weary: cybersecurity and privacy enforcement actions heat up (August 27, 2020)

Hopes that privacy regulators and litigants would grant a reprieve to businesses during the COVID-19 pandemic may prove ill-founded. On July 21, 2020, the New York Department of Financial Services ... *click for full article*

Hopes that privacy regulators and litigants would grant a reprieve to businesses during the COVID-19 pandemic proved to be premature — enforcement actions showed no signs of slowing, especially those related to the CCPA.

NAIC adopts principles for trustworthy artificial intelligence in insurance that support the avoidance of proxy discrimination against protected classes (August 21, 2020)

On August 14, 2020, the National Association of Insurance Commissioners (NAIC) adopted a set of principles that will guide the work of insurers and entities, including data providers, that play an ... *click for full article*

The National Association of Insurance Commissioners' principles set out expectations that AI systems and actors in the insurance field be fair and ethical, avoid discrimination, be accountable and compliant with the law.

NAIC's Privacy Protections (D) Working Group begins revising privacy model laws (May 28, 2020)

On May 5, 2020, the NAIC's Privacy Protections (D) Working Group met via conference call. The Working Group was formed on October 1, 2019, under the Market Regulation and Consumer Affairs (D) ... *click for full article*

In the wake of the CCPA's novel legal obligations, the National Association of Insurance Commissioners (NAIC) began a review of state insurance data privacy laws to make recommendations for updates to NAIC model laws.

Cybersecurity and coronavirus—Guarding against hackers in this heightened risk environment (March 10, 2020)

Many general counsels, as well as their privacy and cybersecurity teams, are understandably focused on their company's coronavirus safety measures—and that is good news to the hackers. Hackers thrive ... *click for full article*

In collaboration with Eversheds Sutherland attorneys Paula Barrett, Jake McQuitty and Craig Rogers.

As privacy and cybersecurity teams understandably focused on their companies coronavirus safety measures, hackers thrived amidst confusion and distraction. Preparation for these threats is vital to an agile response.

California privacy laws

What's inside

California's new privacy law, the CPRA, was approved: Now what? (November 9, 2020)

On November 3, 2020, California voters passed Proposition 24, the California Privacy Rights Act (CPRA), by approximately 56-44%. This act will amend and supersede the still recent California Consumer ... *click for full article*

CCPA compliance? That's old news. The voter-passed CPRA amends and supersedes the still-new California privacy law — including the establishment of a new regulatory authority. The earlier companies prepare, the easier the compliance.

Proposed CCPA regulations receive second modification (March 20, 2020)

On March 11, 2020, the California Attorney General released a second set of revised draft regulations under the California Consumer Privacy Act (CCPA). The modifications come after the department ... *click for full article*

Filling in the details of the CCPA, the California Attorney General released revised draft regulations to implement the law, notably including greater obligation for companies to disclose the purposes for which they sell personal information.

Accessibility—The hidden A in the CCPA (February 20, 2020)

In the scramble to come into compliance before the January 1, 2020 deadline, companies may have overlooked a key—and potentially costly—requirement in the California Attorney General draft. *click for full article*

As businesses scramble to meet the CCPA compliance deadline, they would be wise not to forget that their updated privacy policies must be reasonably accessible to individuals with disabilities.

Cryptocurrency and financial services

What's inside

A Cybersecurity Storm and Winds of Change: NY DFS requires all New York financial institutions to report effects of SolarWinds hack (December 22, 2020)

The massive SolarWinds security breach, which affected not only the private sector, but federal, state and local governments, has caused some to question whether to share data with the government. On ... *click for full article*

Companies' hesitancy to share data with government entities that were also vulnerable to the massive SolarWinds hack may be understandable, but that impulse is at odds with emerging regulations seeking greater information sharing in the hack's wake.

FinCEN proposes new recordkeeping, verification, and reporting requirements for transactions involving virtual currency and digital assets (December 23, 2020)

On December 18, 2020, the Financial Crimes Enforcement Network (FinCEN) issued a Notice of Proposed Rulemaking (NPRM) to establish new requirements for convertible virtual currency (CVC) and legal ... *click for full article*

In keeping with a greater focus on cryptocurrency, the Financial Crimes Enforcement Network (FinCEN) began the rulemaking process to expand existing reporting, verification and recordkeeping obligations for convertible virtual currency and legal tender digital asset transaction.

NAIC Report – 2020 Summer National Meeting (September 1, 2020)

The National Association of Insurance Commissioners (NAIC) held its 2020 Summer National Meeting virtually from July 28 to August 14, 2020. The meeting was originally scheduled to be held in ... *click for full article*

Highlights of the National Association of Insurance Commissioners' first meeting of 2020 included a focus on race and insurance, AI best practices and updates on key regulatory initiatives.

Cross-border personal data transfers

The seismic shift after Schrems II: The Future of Cross Border Data Flows for US Insurance Companies (August 11, 2020)

If your company, like many other US insurance companies, has an EU or UK affiliate or parent, and you transfer personal data to the US, including employee data or even data of US persons, or if your ... *click for full article*

The seismic shift after Schrems II: The future of cross border data flows for the industrial sector (August 4, 2020)

If you transfer personal data from the EU/UK to countries which lack a so-called "adequacy" determination, like the US or India, or if your trusted service providers do, the Schrems II European Court ... *click for full article*

In collaboration with Eversheds Sutherland attorney Paula Barrett.

The seismic shift of Schrems ll and what you can still do to transfer personal data to the US from the EU (July 28, 2020)

If you transfer data from the EU to the US, or if your trusted service providers do, the Schrems II European Court decision has seismic significance — even if you do not rely on Privacy Shield. On ... *click for full article*

In collaboration with Eversheds Sutherland attorney Paula Barrett.

What's inside

Even for companies that do not rely on the EU-US Privacy Shield, it being struck down by the Court of Justice of the European Union puts significant new due diligence obligations on those businesses that use the Standard Contractual Clauses.

Biometrics

White Paper: Implications of US laws on collection, storage, and use of biometric information (July 16, 2020)

The use of biometric technology in everyday life has increased dramatically over the last few years. As a result, private entities are collecting, using, and storing biometric information from ... *click for full article*

What's inside

While the use of biometric technology in everyday life has increased dramatically over the past few years, the US legal landscape remains in flux and rife with risks for businesses that utilize the technology.

Contact

Michael Bahar
Partner
Email | +1 202 383 0882

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

Frank Nolan
Partner
Email | +1 212 389 5083

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

Ian Shelton
Counsel
Email | +1 512 721 2714

Brandi Taylor
Counsel
Email | +1 858 252 6106

Allison Bailey
Associate
Email | +1 404 853 2601

Giselle Guerra
Associate
Email | +1 713 470 6115

Pooja Kohli
Associate
Email | +1 212 389 5037

Deepa Menon
Associate
Email | +1 202 383 0928

Margaret O'Brien
Associate
Email | +1 404 853 8070

Al Sand
Associate
Email | +1 512 721 2721

Tanvi Shah
Associate
Email | +1 858 252 4983

Andrew Weiner
Associate
Email | +1 212 301 6602

eversheds-sutherland.com