Crowell

Privacy and Cybersecurity Outlook:

THE 2024 LANDSCAPE

Contents

Introduction

Crowell & Moring's *Privacy and Cybersecurity Outlook: The 2024 Landscape* offers clients forward-looking analysis on the biggest trends impacting their work across the world. This first edition marks a milestone for our premier Privacy and Cybersecurity group, which was recognized in 2023 as one of the leading U.S. practices for organizations and individuals facing cybersecurity incidents, data breaches, compliance concerns, and other privacy risks.

With articles assessing legislative developments across the U.S., the EU, and the Asia-Pacific region, the *Outlook* reflects our practice's global footprint. The *Outlook* also contains pieces covering best practices to test incident response plans, a review of litigation driven by the rise of artificial intelligence, and considerations for corporations and Chief Information Security Officers to ensure compliance with data regulations.

As the privacy and cybersecurity landscape continues to evolve in 2024, we hope you turn to this publication as a trusted resource. All of the articles from the *Outlook* are available here.

U.S. Privacy Legislation

More States Put Laws on the Books

By Sarah Rippy*

State privacy law developments continued on a similar trajectory as previous years, marked by a legislative focus on data privacy issues. At the beginning of the 2023 legislative session, five states (California, Colorado, Virginia, Utah, and Connecticut) passed comprehensive privacy laws, all of which are now effective and enforceable

By the end of 2023, seven additional states passed privacy legislation (Delaware, Indiana, Iowa, Texas, Montana, Oregon, and Tennessee). While the substance of each law varies, they share a common trend of following the broad terminology and structure set by the Colorado Privacy Act rather than the California Consumer Privacy Act—as amended by the California Privacy Rights Act (collectively the CCPA). For example, these laws use the GDPR language of controller/processors rather than the business/service provider distinction found within the CCPA.

At the federal level, while legislators continue to demonstrate an interest in creating a federal privacy framework, comprehensive privacy bills introduced in 2023 made very little traction. Though both the Data Care Act of 2023 and the Online Privacy Act of 2023 were comprehensive privacy bills, neither received the level of publicity and support seen in 2022 when the American Data Privacy and Protection Act was introduced.

Regulatory Updates

Other notable privacy developments in 2023 included the finalization of the new CCPA regulations from the California Privacy Protection Agency (CPPA) and the Colorado Privacy Act rules from the Colorado Attorney General. Originally intended to be effective on July 1, 2023, the implementation of new CCPA regulations was pushed back to March 29, 2024 due to a delay in releasing the finalized version. The new regulations provided guidance on obligations such as:

- Required disclosures to consumers;
- Business practices for handling consumer requests;
- Obligations regarding service providers, contractors, and third parties;
- Request verification;
- Rules regarding children's data;
- Non-discrimination obligations;
- Training and record keeping; and
- Investigations and enforcement.

However, one area was notably absent from the regulations: guidance on risk assessments and automated decision-making technology. Instead, the CPPA released draft regulations on these issues separately in September 2023 and November 2023.

As previously noted, the Colorado Attorney General also finalized its rules for the Colorado Privacy Act. The Colorado Privacy Act rules provide guidance on items such as:

- Required disclosures;
- Document retention schedule obligations;
- Purpose specification and secondary data use;
- Sensitive personal data;
- The definitions of biometric data and biometric identifiers;
- User consent;
- Data protection assessment obligations;
- Providing the right to opt out (including universal opt out mechanisms);
- Dark Patterns; and
- Consumer rights.

*Former Crowell attorney Christiana State contributed to this article.

EU Privacy Legislation

New Act to Ease Data Sharing Barriers

By Yung Shin Van Der Sype

On January 11, 2024, the Data Act entered into force. This marks a significant milestone in the evolving landscape of digital regulation. The Data Act is part of the broader European data strategy and plays a significant role in advancing the EU's digital transformation objectives outlined in the Digital Decade Policy Program 2030.

The widespread use of internet-connected products—the so-called Internet of things or "IoT," from cellphones to smart doorbell cameras—has notably increased the volume and potential value of data for consumers, businesses, and society at large. The recognition that barriers to data sharing hinder optimal data allocation for societal benefit led to the drafting of the Data Act.

The Data Act, which applies to both personal and non-personal data, encompasses several key elements designed to foster an efficient, fair, and innovative data economy:

- It facilitates data sharing, particularly data generated by connected devices and used by related services. This spans all sectors, underscoring the significance of non-personal data sharing for societal and economic benefits;
- It establishes mechanisms for data transfer and usage rights, with a special focus on cloud service providers and data processing services. This facilitates a more fluid and secure data sharing environment;
- It introduces interoperability standards to ensure data can be accessed, transferred, and used across different sectors, which is crucial for innovation and competitive markets;
- It reinforces the right to data portability, allowing users to move their data across different service providers, which enhances user autonomy and promotes competition;
- It mandates that providers of data processing services, such as cloud and edge services, implement reasonable measures against unauthorized third-party access to non-personal data, thereby fostering trust in data;
- It aims to balance the availability of data with the protection of trade secrets;
- It recognizes the need for public sector bodies, the Commission, the European Central Bank, or Union bodies to use existing data to respond to public emergencies or in other exceptional cases; and
- It provides protections against unfair contractual terms that are unilaterally imposed.

These elements collectively aim to enhance data accessibility and utility, protect individual and business interests, and foster a more competitive and innovative digital market in the EU.

The Data Act entered into force on January 11, 2024, and the provisions will apply starting on September 12, 2025. The timeline for complete enforcement is thus expected to span several years, allowing businesses and stakeholders adequate time to adapt to the new requirements.

Health Care Privacy

Closing the Gaps in HIPAA Regulation

By Jodi Daniel and Brandon Ge

Though general rules established by the Health Insurance Portability and Accountability Act and its implementing regulations (collectively known as HIPAA) are relatively well known, fewer people are familiar with some finer details, such as the fact that HIPAA is somewhat limited in scope. It's also a common misconception that HIPAA applies to all or most individually identifiable health information.

In reality, HIPAA only applies to a narrow set of covered entities—health care clearinghouses, health plans, and most health care providers—as well as their business associates.[1] Given the explosion in the use of health apps, connected devices, and other direct-to-consumer products and services that routinely collect health information, many companies and considerable swaths of health information remain outside the scope of HIPAA and have historically faced little regulation.

The tide began turning on this front in 2023, with many of the year's most important headlines in health privacy generated by federal and state actions aimed at regulating companies and information not subject to HIPAA. Back in February 2023, in the first of a flurry of enforcement actions, the Federal Trade Commission (FTC) imposed a $1.5 million civil penalty against GoodRx under the Health Breach Notification Rule (HBNR) and section 5 of the FTC Act. This marked the FTC's first enforcement action under the HBNR, a rule that took effect in 2009 requiring certain non-HIPAA-regulated entities to notify consumers, the FTC, and potentially media outlets in the event of a breach of health information. In June, the FTC published a Notice of Proposed Rulemaking modifying the HBNR, with many of the modifications aimed at clarifying the FTC's intent to apply the HBNR to health apps and connected devices and to expansively interpret what constitutes a "breach" under the rule.

In 2023, several states also passed data protection legislation focused on protecting consumer health data. Washington state was the first mover by enacting the My Health My Data Act (MHMDA), the nation's first law that specifically protects consumer health data not regulated by HIPAA. Shortly after, Nevada followed suit by enacting its own law similar to the MHMDA, and Connecticut passed an amendment to the Connecticut Data Privacy Act to include specific protections for consumer health data.

Over the coming months, we expect several key developments in the regulation of health information. We anticipate that the FTC will continue to be an active enforcer against digital health companies under both the HBNR and the FTC Act. The FTC could also finalize its proposed modifications to the HBNR. We also expect more states to follow in the footsteps of Washington and others that have passed health-specific data protection laws, adding to the growing patchwork of state data protection laws. Lastly, the Department of Health and Human Services, which recently finalized modifications to 42 C.F.R. part 2,[2] continues to remain active in enforcing HIPAA violations and has proposed modifications to HIPAA and that are still pending finalization.

[1] Business associates are generally service providers that handle individually identifiable health information in providing a service to a covered entity or another business associate.

[2] 42 C.F.R. part 2 is a set of regulations governing the confidentiality of substance use disorder records.

International Data Transfers and Policies

EU Data Transfers to the U.S.

By Yung Shin Van Der Sype*

On July 10, 2023, the European Commission formally adopted a new adequacy decision for the EU-U.S. Data Privacy Framework (DPF), which provides companies transferring personal data to the U.S. an additional mechanism to legitimize their cross-Atlantic data transfers. The DPF replaces the previously invalidated Privacy Shield and Safe Harbour framework. The DPF is in many ways a "Safe Harbour III" – mainly due to the way that organizations can adhere to it, how it is administered, and the way that its compliance is monitored. However, the legal framework in the U.S. did change to accommodate the requests from the EU and the concerns expressed in the CJEU's Schrems I and II judgments (reflected in the Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities of October 7, 2022 and regulations adopted by the U.S. Attorney General).

Under the General Data Protection Regulation (GDPR), personal data may be transferred from the European Economic Area (EEA)—which includes the 27 EU Member States as well as Norway, Iceland, and Liechtenstein—to a non-EEA country, if that country provides an adequate level of protection for the personal data.

The European Commission (EC) conducts the assessment of the country's level of protection, and it is made concrete in a formal adequacy decision. The first time that the U.S. received such adequacy (still under the GDPR's predecessor, the EU Data Protection Directive) was by the EC decision of July 26, 2000, which created the Safe Harbour framework.

In 2013, Austrian citizen Maximillian Schrems objected to his data being sent by Facebook Ireland to servers in the U.S., arguing that, in light of the 2013 revelations made by whistleblower Edward Snowden, personal data did not receive adequate protection in the U.S., despite of Facebook's formal adherence to the Safe Harbour Principles. In its Schrems I judgment, the CJEU invalidated the Safe Harbour mechanism. On July 12, 2016, the EC replaced the invalidated framework with a new one, the EU-U.S. Privacy Shield. A follow-up complaint from Schrems targeting the validity of the SCCs resulted in an invalidation of the Privacy Shield framework (but not of the SCCs).

A result of the Schrems II judgment was that organizations need to carry out a data transfer impact assessment when using appropriate safeguards such as the SCCs, where the specific data transfers at hand need to be assessed in detail. While completing such an impact assessment was already made easier thanks to changes in the U.S. legal framework (which benefit all data transfers under the GDPR, including those covered by SCCs), having access to a new framework where such assessment is not required represents a victory for trans-Atlantic data transfers.

To rely on the new framework, companies will undergo a self-certification process, as detailed on the U.S. Department of Commerce's new Data Privacy Framework website. Certified companies will commit to a set of privacy obligations without needing to put in place additional safeguards or conduct additional impact assessments. While it seems that Schrems and others have already confirmed that they will challenge this new compliance framework, it does, for now, provide a solid legal basis for cross-Atlantic data transfers, which is a more than welcome breath of fresh air for the digital economy.

*Former Crowell attorney Christiana State contributed to this article.

Artificial Intelligence in the U.S.

Reactions from the Public and Private Sectors

By Jennie Wang VonCannon and Gage Javier*

It's fair to call 2023 the year of artificial intelligence. The 2023 AI boom was largely driven by the widespread adoption of new technologies like ChatGPT, Google Bard, and Microsoft Copilot. Alongside the excitement surrounding these new technologies, alarm over the possible consequences of increased AI use without appropriate guardrails caused both government and private entities to act.

The U.S. government has taken several steps to try to proactively address the possible impact of AI. The Biden Administration demonstrated its commitment to staying ahead of the quickly changing landscape when it released an Executive Order on the *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* in October. The executive order provides guiding principles and priorities that account for various perspectives from agencies, industry, academia, the public, and foreign partners to advance and govern the use of AI. The executive order also aims to maximize the potential benefits of AI while addressing rising concerns about its potential harms, seeking to promote a balance between innovation and protectionary action.

In response, the Office of Management and Budget released for public comment its draft implementation policy on AI use within government agencies, entitled "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," The Department of Defense also began to address AI, releasing its Data, Analytics and AI Adoption Strategy, which focused heavily AI topics including responsible AI and AI-enabled capabilities.

In the private sector, 2023 saw an escalation of litigation as private entities moved to protect their copyrighted assets from the encroachment of AI technology. Several intellectual property suits regarding the alleged use of copyrighted works to train AI models are currently moving through the courts. The defense in one of the earliest of such cases, *Thomson Reuters v. ROSS Intelligence*, will be heard at trial in 2024 and is helmed by Crowell & Moring.

New actions also resulted from the technologies that emerged in 2023. *Authors Guild v. OpenAI Inc.* and *Tremblay/Silverman v. OpenAI Inc.* involve lawsuits against the makers of ChatGPT for allegedly using copyrighted novels to train ChatGPT AI models. In *Doe v. GitHub Inc.*, developers allege that AI coding tools used the developers' copyrighted code published on the web to develop their models, which the coding platform failed to prevent. Closing out 2023, *The New York Times* sued both OpenAI and Microsoft over allegations of copyright infringement related to the training of their AI models in the last week of December.

With government intervention and litigation likely to continue, there is little doubt the legal landscape of AI will develop throughout 2024.

*Former Crowell attorney Christiana State contributed to this article.

Artificial Intelligence in Europe

The Trailblazing EU AI Act

By Yung Shin Van Der Sype and Maarten Stassen

On Dec. 8, 2023, after lengthy and intense negotiations, European legislators reached a political agreement on the EU Artificial Intelligence Act (AI Act). The EU Parliament formally adopted its position during its plenary session of March 13, 2024, and after legal-linguistic finalization and formal adoption by the EU Council, the AI Act is expected to be published in the Official Journal of the EU before the end of Q2, 2024.

Initially proposed by the European Commission in April 2021, the AI Act positions the EU as a trailblazer in regulating artificial intelligence, as it is the first significant, all-encompassing regulation in the world focused on the development and use of AI. It establishes a uniform legal framework across the EU, with the explicit goals of ensuring that AI used in the European market is legal, safe, and trustworthy. Given its extraterritorial scope of application, certain rules will extend beyond the EU's borders and have, thus, a global impact.

While the AI Act doesn't regulate technology and is in that sense technology-neutral, it sets rules for the development and use of AI in specific cases. The EU legislators have adopted a risk-based approach: AI systems posing minimal-to-no risk do not face restrictions; for limited-risk AI systems, there are some specific transparency obligations, such as the need to mark generated output as artificially generated or manipulated; heavily regulated; "high-risk" AI systems, will carry a more significant regulatory burden; and those considered to pose an unacceptable risk for the health, safety, and fundamental rights of individuals, such as AI systems that manipulate human behavior to circumvent free will, will be banned.

Organizations will need to conduct a thorough mapping of all AI systems to assess whether obligations apply. In doing so, organizations can build on much of the data mapping work that should have been done for GDPR compliance. Consequently, privacy professionals will play a pivotal role in compliance efforts related to AI.

A significant point of contention throughout the interinstitutional legislative process concerned general-purpose AI. While in the past, AI-based applications were designed for specific tasks, recent years have seen the development of AI systems that can be employed for a wide array of tasks (including those previously unforeseen) with minimal modifications, thus serving a general purpose. This has led to the creation of "general-purpose AI models," which serve as the basis for a multitude of different applications. This type of development presents a so-called "single point of failure" risk: if there's a flaw in the model, it can affect all downstream applications built on it. The AI Act imposes specific obligations for providers of general-purpose AI models, and stricter obligations will apply to general-purpose AI models with systemic risk – classified as such if they have (i) high impact capabilities evaluated on the basis of appropriate technical tools and methodologies, including indicators and benchmarks, or (ii) capabilities or an impact equivalent to those set out in (i) regarding specific defined criteria, based on a decision of the EU Commission, *ex officio* or following a qualified alert from the scientific panel.

The EU Commission and supervisory bodies to be created within the EU Member States will play a key role in the enforcement of the AI Act's provisions.

Corporate

Driving New Value with Data

By H. Bryan Brewer III

In 2023, data moved beyond serving as just an "important currency" in the marketplace and evolved into a truly transformative asset class. With this transformation, data requires increased attention and concern by its owners and controllers. Companies are increasingly building, creating derivative works, collecting data, and even focusing on acquiring data through accretive transactions. As a result, stakeholders must understand and address the nuanced legal matters associated with developed or acquired data, which run the gamut from how to actually acquire particular data rights under applicable laws to managing restrictions related to use of tools, such as data analytics and artificial intelligence.

Companies should strongly consider the intellectual property protection of data under applicable regimes and statutes. Given the number of statutes and regulations to navigate, the global nature of companies' activities makes this more challenging than ever. As laws and best practices develop at a breakneck pace, owners of data face the additional challenge of tracking and keeping up with evolving data base rights and copyright schemes in a myriad of countries where the data is developed, acquired, or even ultimately transferred.

Companies should also take stock of the legal obligations of the parties under company agreements that impact a company's and counter-party's use of data that is subject to such agreement. Data may be considered a pre-existing work or background technology in a company agreement. If this is the case, as between the parties to the agreement, most often all rights, title, and interest in and to the data remains with the party supplying the data (whether as an owner or licensee from a third party). The parties should ensure the character of the data to highlight whether personal data is contained in the applicable data sets and whether data protection laws have and are being followed.

But the inquiry cannot end with just that previous assessment. Each party's rights need to be carefully understood. Some questions to consider include the following: What rights does a counter-party in your agreement have to use the data, or to combine the data with other data sets? And who owns any derivatives that result from any activity with respect to the data? Any third parties who have access to, or are involved in, outsourced activities related to the data need to have their obligations and rights in the data outlined in separate written agreements that are consistent with the obligations of the primary agreements. In addition, it is important to understand what rights survive the termination of any agreement.

When working with third parties with company data or in acquisitive transactions, there are also a number of legal concerns to consider for companies that own or are acquiring data sets. A few of the key issues include an analysis of the data and related cybersecurity risks, security of all applicable IT systems that are involved, antitrust concerns, foreign investment concerns (CFIUS), and even analysis of the ethical use of data. Companies focusing on these issues will likely be in the best position to extract the most value from these assets now and in the future.

SEC Enforcement

Risk Mitigation for Companies and Chief Information Security Officers

By Laura A. Foggan and Adam J. Singer

With stronger rules requiring disclosure of cyber risk and cyber breaches, 2023 has seen heightened SEC enforcement of companies' obligations in cyber breaches and, notably, enforcement charges brought directly against Chief Information Security Officers (CISOs).

Charges the SEC filed on October 30, 2023, against SolarWinds and its former CISO, Timothy G. Brown, are a key illustration of this risk. The SEC charges alleged fraud and internal control failures related to allegedly known cybersecurity vulnerabilities and risks. The SEC asserts that the defendants defrauded investors by overstating SolarWinds' cybersecurity protections and failed to disclose known risks, violating the antifraud provisions of the Securities Act of 1933 and the Securities Exchange Act of 1934, and that Brown aided and abetted the company's alleged violations.

Given the environment of increased enforcement activity, companies must be aware of potential exposures to themselves and their CISOs related to cyber disclosure, and they should be taking steps to mitigate those risks. Protection for CISOs is particularly important given that they may be individually targeted by the SEC in the aftermath of a cybersecurity incident, as shown in the recent example of Brown at SolarWinds

Companies should implement rigorous training programs that will put them in the best position to avoid enforcement actions for failures to detect and disclose cybersecurity weaknesses. Part of that training should include educating CISOs on the mechanism for promptly reporting cyber incidents to those who need to know and information on how to interact with the company's disclosure committee. Taking these steps will not only protect CISOs when it comes to SEC enforcement activity, but it will increase their effectiveness and performance in protecting their employers against cyber catastrophes.

Along with cybersecurity training, another way companies can protect their CISO is by ensuring that their Directors and Officers (D&O) insurance programs cover CISOs, just as they protect other company officers, including CEOs and CFOs. While cyber liability insurance is important, cyber coverage typically protects against unauthorized access to a company's computer system or data loss or theft, but does not safeguard CISOs against enforcement actions that may arise from decisions and actions taken as part of their duties. Ensuring that CISOs are protected under the company's D&O coverage can provide executive officers with valuable peace of mind and the critical funds needed to defend against what could be very costly enforcement actions following a breach, as well as for indemnity against potential judgments or settlements.

Government Contracts

How Cybersecurity Threats Increase Civil and Criminal Liability

By Jennie Wang VonCannon

The risks faced by companies in light of new federal cybersecurity regulations are particularly acute for government contractors, who must also be aware of compounded exposure from the False Claims Act (FCA). The U.S. government is increasingly scrutinizing corporate cybersecurity programs, and companies are vulnerable to new risks of civil and criminal liability related to data breaches. The specter of individual criminal liability looms large since the 2022 conviction of the chief security officer at a leading rideshare company for actions related to his response to data breaches. And now, the SEC has charged the CISO of SolarWinds in his individual capacity with securities fraud related to the company's cybersecurity regime. All companies—especially government contractors—should consider mitigating risk by auditing their cybersecurity protocols and updating their incident response plans.

In October 2021, the DOJ announced the launch of its civil cyber-fraud initiative to combat cyber threats by leveraging the FCA to civilly prosecute government contractors who *knowingly*: (1) provide deficient cybersecurity products or services; (2) misrepresent their cybersecurity practices or protocols; or (3) violate obligations to monitor and report cybersecurity incidents and breaches.

The Defense Federal Acquisition Regulation Supplement (DFARS) is a set of cybersecurity regulations that defense contractors and their suppliers must follow in order to be awarded new contracts from the DoD, any number of which could serve as the basis for a potential FCA enforcement action. These include, among many others, FAR 52.204-21, requiring protection of federal contract information residing on contractor information systems and timely identification of flaws; and DFARS 252.204.7012, requiring safeguard of covered defense information and imposing a 72-hour incident reporting period.

An FCA whistleblower—typically a former employee—would likely allege that a contractor's cybersecurity protocols or responses are out of FAR/DFAR compliance. A whistleblower can show that the company (or an individual) acted *knowingly* by: (1) having actual knowledge of the information; (2) acting in deliberate ignorance of the truth or falsity of the information; or (3) acting with reckless disregard of the truth of the claim.

The FCA does not require specific intent to defraud, but it does require some intent or knowledge of wrongdoing (scienter). Courts have generally held that statements made with reckless disregard, no objectively reasonable interpretation or authoritative guidance (*Proctor v. Safeway Inc.*), or no facts to infer good faith (*McGrath v. Microsemi Corp.*) support such a finding. On June 1, 2023, the U.S. Supreme Court clarified in *Schutte v. Supervalu* that scienter in FCA cases turns on the defendant's knowledge and subjective beliefs at the time the claim was made. Within the Supreme Court's framework, the scienter standard is generally industry-specific.

The default measure of damages under the FCA is the benefit the government received under the contract less the amount paid. In addition to monetary damages (*Feldman v. van Gorp*), a company may be liable for treble or multiplied damages to compensate the government for the costs, delays, and inconveniences caused by the fraudulent claims calculated before deduction fixes entitled to the defrauder (*U.S. v. Bornstein*), thousands of dollars in penalties per claim, adjusted for inflation, and attorneys' fees. An individual or company found liable under the FCA may also face suspension and debarment, preventing the organization or individual from entering into contracts with the government for a time.

In September 2023, the DOJ announced that a large telecommunications company agreed to pay over $4 million to settle FCA allegations regarding the company's failure to satisfy certain cybersecurity controls in connection with an information technology service provided to federal agencies. Of note is the company's proactive approach to the case—including conducting an independent investigation and compliance review and self-reporting—which earned the company cooperation credit with the DOJ, resulting in a reduction in the settlement amount.

The actions of law enforcement and regulators in the past several years show that the U.S. government is focused on cybersecurity—especially when it comes to transparency about security vulnerabilities and breaches—and will continue to use myriad arrows in its quiver to hold companies, government contractors, and individuals accountable.

Tabletop Exercises

A Leading Practice to Strengthen Defenses

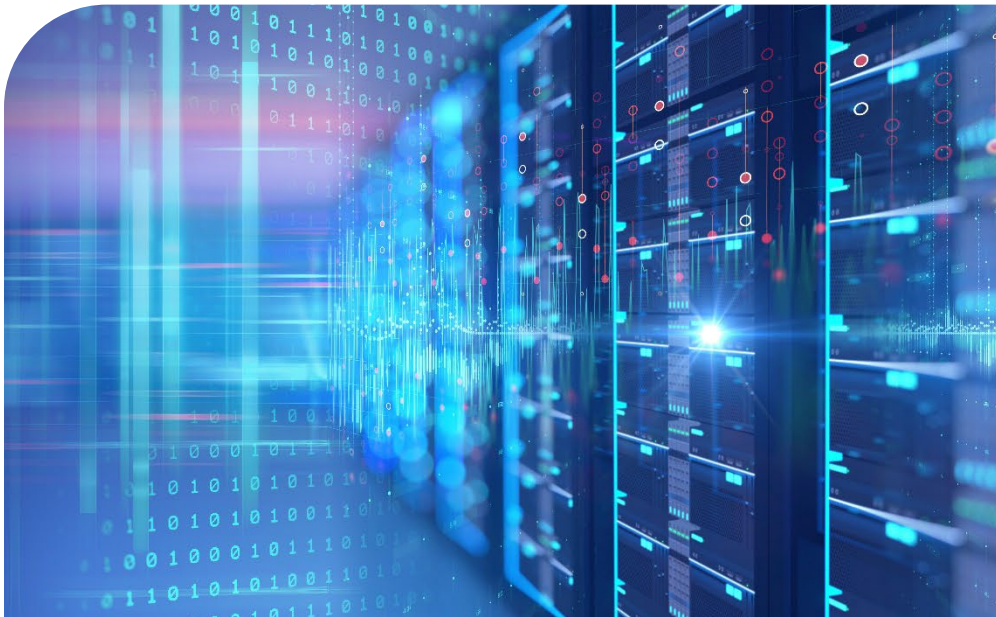
By Matthew B. Welling, Evan Wolff, and Jacob Canter

Every day, organizations face a barrage of attacks from cybercriminals looking to do harm by gaining access to IT systems and sensitive data. Repercussions from these attacks can be significant—lost business data, legal liability, regulatory scrutiny, and a damaged reputation. To prepare for potential attacks, companies need a robust incident response plan that can be quickly and effectively deployed against cyber threats as they arise.

A leading practice to test the robustness of your incident response plan and to prepare for a potential attack is to complete a tabletop exercise. A tabletop exercise simulates real-world scenarios and allows companies to assess their incident response plans in a safe and controlled environment. This helps a company develop "muscle-memory" for their planned response, identify any gaps in existing plans, and recognize additional possibilities for enhancement. Conducting an exercise also creates an important opportunity to gather company stakeholders in a single room to discuss, in practical and concrete ways, how it will respond if a cybersecurity attack ever occurs.

For this reason, in October 2023, Crowell and ArmorText, a leading secure out-of-band communications platform, published a guide titled *Cyber Resilience: Incident Response Tabletop Exercises 2023*. The guide includes three tabletop exercise modules, each consisting of a scenario, a series of facilitator prompts, and, in some cases, follow-up questions or "injects" to further explore participant responses and provide for more dynamic facilitation. The three modules are anchored in cybersecurity incident response, as well as related concerns, such as business continuity questions and post-incident obligations. The modules have roles for all of the relevant stakeholders—from cybersecurity personnel, to legal personnel, to C-suite executives.

As cyber threats continue to evolve and adapt to defenses, tabletop exercises have become an increasingly important component of preparedness. With this guide, you will have a foundation to help your company practice and assess your incident response capabilities and, as a result, improve your overall cyber resilience and preparedness.



Critical Infrastructure

Updating the 2013 NIPP and other Risk Mitigation Actions

By Neda Shaheen, Maida Lerner, Michael Gruden, and Evan Wolff

Protecting critical infrastructure is paramount to today's digital age. Critical infrastructure includes physical and virtual systems essential for the functioning of our society, economy, and national security. Such a definition may include power grids, communication networks, and financial institutions, among other networks that heavily rely on interconnected computer systems. These systems are also considered critical infrastructure, as they are used to protect critical cybersecurity infrastructure.

The Cybersecurity and Infrastructure Security Agency (CISA) has identified 16 critical infrastructure sectors whose assets are so "vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." Cybersecurity is embedded in each of these. The National Infrastructure Protection Plan (NIPP) details how each sector must develop a sector-specific plan through coordinated efforts with public and private partners.

This plan, however, has not been updated since 2013. With the growth of the internet and integration of digital technology, critical infrastructure is more interconnected than ever before. Interconnectivity brings opportunities for efficiency and innovation, but also introduces new vulnerabilities. Since the release of the 2013 NIPP, the threat landscape has evolved significantly, with new and emerging risks posed by cyber threat actors. Thus, updating the 2013 NIPP is an important next step to enhancing the resilience and security of our nation's critical infrastructure.

In November 2023, the Biden Administration announced its plans to review and revise Presidential Policy Directive 21, which established how federal agencies would steer protection of critical infrastructure and called for them to work together to create the 2013 NIPP. In the announcement, the White House acknowledged that an "updated policy would strengthen the public-private partnership and provide clear guidance to executive departments and agencies on designating certain critical infrastructure as systemically important." An updated NIPP would also complement the National Cybersecurity Strategy, released in March 2023 as part of the Biden Administration's efforts to protect critical infrastructure through comprehensive cybersecurity measures, public-private partnerships, and information-sharing practices.

In February 2023, the Government Accountability Office (GAO) released a report on Critical Infrastructure Protection, calling on CISA to update the 2013 NIPP and provide templates for revising sector-specific guidance documents. On Oct. 25, 2023, the U.S. House of Representatives, Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection held a hearing on federal cybersecurity governance, focusing on plans to raise the level of federal cybersecurity resilience across the government as a whole.

Protecting critical infrastructure is a complex and ongoing challenge requiring a collaborative, comprehensive, and proactive approach that enhances overall resilience. As we wait for an update to the NIPP, there are actions that CISA suggests government contractors take to help protect the nation's security, such as setting specific goals and objectives, identifying infrastructure, implementing risk management activity, and measuring effectiveness. It is important to identify assets, systems, and networks that contribute to critical functionality and collect information pertinent to risk management, as well as to evaluate risk and consider potential direct and indirect consequences of an incident. Implementing a risk management approach, founded on prevention, protection, mitigation, response, and recovery activities, as well technical solutions, is an important step that companies may take to help protect the nation's critical infrastructure and therefore promote the resilience of our vital systems.

EU Cybersecurity

Legislative Developments for the Region

By Yung Shin Van Der Sype

Cybersecurity plays a key role in various legal instruments of the European Union. It frequently appears as a specific duty or as a necessary element for establishing trust with the public.

At the center of cybersecurity in the EU is Directive (EU) 2022/2555 (NIS 2). The NIS 2 entered into force on January 16, 2023, replacing the former NIS Directive. NIS 2's goal is to strengthen cybersecurity by laying down measures that establish a high common level of cybersecurity across the EU. NIS 2 expands the scope of cybersecurity requirements to include both "essential" and "important" entities across various sectors, including energy, transportation, banking, health, digital infrastructure, and others. It sets thresholds based on the size of the entity, and noncompliance can result in significant penalties. EU member states have until October 2024 to implement NIS 2 in their respective jurisdictions.

In a similar vein, the Directive on the resilience of critical entities (Critical Entities Directive) and the Regulation on digital resilience for the financial sector (DORA) also entered into force in 2023. The Critical Entities Directive requires EU Member States to take specific measures to ensure that services essential for the maintenance of vital societal functions or economic activities are provided in an unobstructed manner and to enhance the resilience of critical entities providing such services. The law also requires Member States to identify critical entities and to support those entities in meeting the new cybersecurity obligations. DORA establishes uniform requirements concerning the security of network and information systems supporting the business processes of financial entities.

Also in 2023, the European Union has made significant advancements in cybersecurity legislation, focusing on enhancing security across various sectors and reinforcing the resilience of digital products and services. Key developments include the proposed amendment to the Cybersecurity Act, the proposal for a Cyber Solidarity Act, and the agreement on the text of the Cyber Resilience Act.

The European Union Agency for Cybersecurity (ENISA) plays a crucial role in establishing and maintaining the EU cybersecurity certification framework. Currently, this framework includes certification schemes for ICT products, services, and processes. A targeted amendment to the EU Cybersecurity Act proposed in April 2023 will further enable the adoption of EU certification schemes for managed security services, covering areas like incident response and security audits.

In April 2023, the European Commission proposed the Cyber Solidarity Act, which seeks to further improve the response to cyber threats across the EU. The proposal includes a European Cybersecurity Shield and a comprehensive Cyber Emergency Mechanism to create a better cyber defense method.

Lastly, most recently on November 30, 2023, the European Commission, Council, and Parliament reached an agreement on the text of the Cyber Resilience Act (original proposal), which is considered a major step toward ensuring the security of products with digital elements. The European Parliament approved the Cyber Resilience Act on March 12, 2024. Once formally adopted by the Council, the text will be published in the Official Journal of the European Union. The Regulation is expected to enter into force in early 2024 and to become applicable within 21 months (for reporting certain incidents and vulnerabilities) to 36 months after its entry into force.

Global Developments

New Actions in the Asia-Pacific

By Akanksha Sinha and Kate Growley, Crowell & Moring International

Across the Asia-Pacific (APAC), the past year has brought defining developments for privacy and cybersecurity regulations in the region. A number of countries have implemented new or updated existing policy instruments—a testament to the growing relevance of a strong privacy and cybersecurity framework in the face of rapid global digital transformation. Topline 2023 changes and actions across APAC have included Vietnam's Decree on Personal Data Protection; Bangladesh's Cyber Security Act and draft Data Protection Act; amendments to Taiwan's Cyber Security Management Act; and Indonesia's Presidential Regulation Number 47 of 2023 on Cyber Crisis Management and National Cyber Security Strategy.

Australia and India stood out for their pivotal moves on privacy and cybersecurity with the potential to set important precedents for the region. Prompted in part by a spate of significant cybersecurity incidents, the new Australian Cyber Security Strategy 2023-2030 signifies the country's intent to become a world leader in cybersecurity by 2030. Its "all of country" approach ambitiously tackles a range of issues, from critical infrastructure protection to cyber workforce skilling and international cooperation. Central to these efforts is the expectation that the strategy will usher in landmark legislation on cybersecurity standards and incident reporting, to be significantly informed by industry input. The government began implementation efforts on this Strategy in early 2024, by opening a round of public consultation to revise the Security of Critical Infrastructure Act 2018. This step aims to improve the country's security and resilience, with cyber response and prevention at the forefront. On the privacy end, the Australian government is negotiating revisions to its Privacy Act, which is poised for legislative amendments in 2024 after the latest round of public consultation closed in March 2024. Chief among those amendments could be a new standard where—regardless of the terms of any consent—the collection, use, and disclosure of personal information would need to be "fair and reasonable," rather than the current standard of "reasonably necessary."

Meanwhile, stronger legislation on data protection has been a key theme for India, with what is now the world's most populous country finally passing its Digital Personal Data Protection Bill in 2023. This long-awaited bill had been in the making for five years, drawing on fundamental concepts found in the EU's General Data Protection Regulation but with key distinctions in its applicability. Still, questions remain about the new law's resources and enforcement, especially after a contentious path through the country's Parliament. In 2024, we should learn the answers to many of these questions, in part due to the Central Government's publication of implementing rules and the establishment of the Data Protection Board of India, which will be charged with enforcement. However, the publication of these rules is likely to be delayed until after the country's general elections conclude in June 2024.

Singapore is another country often benchmarked for keeping good pace with evolving technology through its policy and regulatory landscape. In December 2023, it released the first draft of amendments to its Cybersecurity Act 2018, containing novel provisions to enhance the cyber resilience of not only its critical infrastructure, but also other entities with implications for the country's national interests. Public consultation on these amendments concluded in January 2024, followed by the first reading of the Bill in the Parliament in early April, and now expected to be passed later this year. Overall, Singapore continues to establish a robust regulatory ecosystem for privacy and cybersecurity, particularly where those issues intersect with today's buzz word – artificial intelligence. The summer of 2023 saw the Personal Data Protection Commission publishing proposed guidelines on the use of personal data in AI systems, which

received substantial private sector feedback on how personal information is used in AI's development and deployment. And in December 2023, the Prime Minister's Office released the National Artificial Intelligence Strategy (NAIS) 2.0, aiming to set regional standards for AI's use in detecting and mitigating cyberattacks, among other goals. In 2024, we will likely see AI increasingly interwoven into privacy regulations and cybersecurity infrastructure by both APAC governments and businesses to support the region's growing digital economy.

Class Actions

Case Study: The California Invasion of Privacy Act

By Jacob Canter

In 1967, California passed the California Invasion of Privacy Act (CIPA) to protect its citizens from attempted eavesdropping on their private conversations. Now, California plaintiffs are wielding CIPA to challenge whether websites may use marketing technology that tracks website usage absent prior explicit consent. Dozens of class action cases based on this theory of liability have been filed in federal and state courts in California. Hundreds of demand letters based on this same theory have been sent to companies. Crowell has been closely monitoring the wave of website-based wiretap class actions cropping up.

This new surge of privacy class action litigation is significant because it puts all website tracking technology at risk. Many publicly available software tools give website owners the ability to understand their users' online preferences. And user preference data has become an important tool for companies when making marketing and sales decisions. Now, as the software that facilitates user-tracking is being challenged, website owners may have to obtain prior consent from website visitors to employ this technology, or owners may have to rethink their marketing and sales practices. Both alternatives bear risk, though—the former may not be technologically practicable, and it may discourage website visitors; the latter may impact how the company researches its market and develops business strategy.

Liability under CIPA bears risk, too: a private litigant is entitled to the greater of $5,000 per violation or treble damages. And while these are novel theories of injury that have not received a stamp of approval from California appellate courts, they have not been rejected by the appellate courts either. The legal uncertainty creates its own risk as well.

In 2024, Crowell is closely monitoring the California legal system to see if we receive further guidance on the viability of a CIPA claim against the use of website tracking tools. For now, companies should strongly consider auditing their own use of tracking technology—do the tools provide business value, and what protections, if any, are available under your contracts with the software vendors? While we don't have a crystal ball, we think it is likely that the wave of CIPA class action litigation will continue.

About Crowell & Moring LLP and the Privacy and Cybersecurity Group

Crowell & Moring LLP is an international law firm with offices in the United States, Europe, MENA, and Asia. Drawing on significant government, business, industry and legal experience, the firm helps clients capitalize on opportunities and provides creative solutions to complex litigation and arbitration, regulatory and policy, and corporate and transactional issues. The firm is consistently recognized for its commitment to pro bono service as well as its programs and initiatives to advance diversity, equity and inclusion.

Crowell's Privacy and Cybersecurity group offers companies an integrated approach to managing privacy and cybersecurity risks combining legal, technical, and regulatory experience in a single seamless team across global markets. Our team includes lawyers with extensive government, in-house, consulting, and technical experience across multiple industries. Where necessary, we integrate Crowell's intellectual property, corporate, insurance, white collar, trade secrets, health care, energy, transportation, and government contracts capabilities to address the privacy and cybersecurity risks faced by our clients. Our team also regularly works with forensic professionals and coordinate with law enforcement.

Contacts

H. Bryan Brewer III
Partner
+1 202.624.2605
bbrewer@crowell.com

Jacob Canter
Counsel
+1.415.365.7210
jcanter@crowell.com

Jodi Daniel
Partner & CHS Managing Director
+1.202.624.2908
jdaniel@crowell.com

Laura A. Foggan
Partner
+1.202.624.2774
lfoggan@crowell.com

Brandon Ge
Counsel &
CHS Director
+1.202.624.2531
bge@crowell.com

Kate Growley
C&M International Director
kgrowley@crowellmoring.asia

Michael Gruden
Counsel
+1.202.624.2545
mgruden@crowell.com

Gage Javier
Associate
+1.202.654.6743
gjavier@crowell.com

Maida Lerner
Senior Counsel
+1.202.624.2596
mlerner@crowell.com

Sarah Rippy
Associate
+1.303.524.8634
srippy@crowell.com

Neda Shaheen
Associate
+1.202.624.2642
nshaheen@crowell.com

Adam J. Singer
Counsel
+1.202.688.3508
asinger@crowell.com

Akanksha Sinha
C&M International Consultant
+65.8622.9428
asinha@crowell.com

Maarten Stassen
Partner
+32.2.214.2837
mstassen@crowell.com

Yung Shin Van Der Sype
Counsel
+32.2.897.0872
yvandersype@crowell.com

Jennie Wang VonCannon
Partner
+1.213.310.7984
jvoncannon@crowell.com

Matthew B. Welling
Partner
+1.202.624.2588
mwelling@crowell.com

Evan D. Wolff
Partner
+1.202.624.2615
ewolff@crowell.com

crowell.com