June 2022

Skadden

Privacy & Cybersecurity Update

California Releases Amended Draft Regulations for California Privacy Rights Act

In late May 2022, the California Privacy Protection Agency (CalPPA) issued its first set of draft regulations for the California Privacy Rights Act (CPRA), the law that amended the California Consumer Privacy Act (CCPA). Additional revisions to the draft regulations are anticipated prior to finalizing the regulations. As a result, covered businesses may find it challenging to comply with the CPRA amendments when they take effect, which is currently set for January 1, 2023. In addition to clarifying how covered businesses should comply with certain of the provisions of the CPRA, certain provisions may create burdensome compliance obligations for businesses, possibly signaling a desire to more closely align the California privacy regime with the EU's General Data Protection Regulation (GDPR).

On May 27, 2022, the CalPPA issued draft amended regulations to the CCPA to reflect amendments to the CCPA that are currently set to come into force on January 1, 2023, pursuant to the CPRA. The agency also released a draft Initial Statement of Reasons (ISOR) for discussion at its June 8, 2022, board meeting. These draft regulations seek to clarify how covered businesses should comply with the CPRA's amendments to the CCPA. In addition, the draft regulations appear to introduce new technical and reporting obligations on covered businesses that may require significant resources, some of which do not appear to be required by the CPRA.

We have highlighted certain notable provisions in the draft regulations below:

Consumer Consent: Dark Patterns, Opt-Out Signals and Opt-In Requirements

Several of the revisions in the draft regulations focus on consumer consent and concerns of regulators regarding businesses' use of "dark patterns" to undermine consumers' ability to make informed decisions. The CalPPA also included a requirement for all covered businesses to comply with signals that consumers may send to opt out of the sale/sharing of the consumers' personal information — a requirement that surprised many privacy practitioners given the language in the CPRA that describes the recognition of opt-out signals as optional, as opposed to mandatory. In addition, the draft regulations seem to flip the CCPA from an opt-out regime to an opt-in regime in many scenarios involving the processing of personal information.

Prohibition Against Dark Patterns

The CPRA states that consumer consent obtained through the use of dark patterns does not constitute valid consent. The draft regulations define a "dark pattern" as a user interface that "has the effect of substantially subverting or impairing user autonomy, decisionmaking, or choice, regardless of a business's intent." The draft regulations provide guidance regarding what may constitute a "dark pattern" and offer five principles to help businesses identify and avoid employing dark patterns:

- **Easy to Understand:** The language used when obtaining consent should be easy to read and understand.
- **Symmetry in Choice:** It should be equally as easy for consumers to choose the more privacy-protective option as it is to choose the less privacy-protective option.
- **Avoiding Confusing Options:** Language such as double-negatives or toggles/buttons that don't clearly indicate what they do should not be used.
- **Avoiding Manipulative Elements:** Consent should not be obtained by causing consumers to feel guilt, shame or other emotions, or by bundling consent with other choices.
- **Easy to Execute:** Businesses should not add unnecessary burden or friction to the process by which a consumer submits a CCPA request.

The ISOR notes that the draft regulations are informed by academic scholarship and public comments submitted to the CalPPA, which may indicate that regulations on this topic will continue to evolve. Given the focus on dark patterns by other regulators, including the European Data Protection Board[1] and FTC[2], businesses should consider auditing their current practices with respect to obtaining consumer consent, particularly in light of the fact that a deceptive interface may constitute a "dark pattern" regardless of whether there was any intent to subvert consumer choice.

Mandatory Recognition of Opt-Out Signals

The CPRA provides that businesses are required to give consumers the ability to opt out of the sale/sharing of the consumer's personal information or the use of the consumer's sensitive personal information, such as through a link that is clearly labeled "Do Not Sell or Share My Personal Information." However, the CPRA allows a business to forgo including such a link if the business instead allows consumers to opt out "through an opt-out preference signal sent with the consumer's consent by a platform, technology, or mechanism" — based on technical specifications that the CalPPA has yet to adopt.

Instead of this optional approach to recognizing opt-out preference signals as set forth in the CPRA, the draft regulations require all businesses to abide by opt-out preference signals. The draft regulations introduce a new concept of "frictionless" versus "non-frictionless" processing of such signals — providing that businesses that process opt-out preference signals in a "frictionless" manner are not required to include opt-out links, whereas businesses that process such signals in a "non-frictionless" manner are required to include opt-out links. The draft regulations explain that processing of such signals is "frictionless" if it satisfies all of the following requirements:

- the business does not charge a fee or any other valuable consideration if the consumer uses an opt-out preference signal;
- the consumer's user experience is unaffected by the consumer's use of an opt-out preference signal; and
- no notification, sound or other interstitial content is displayed or otherwise used in response to the opt-out preference signal.

Businesses that choose to adopt a frictionless method of processing opt-out preference signals in order to avoid displaying opt-out links will likely need to implement new technology, the specifications for which have yet to be specified by the CalPPA.

Opt-In Requirements for Processing

At present, the CCPA requires businesses to disclose the categories of personal information that a business collects and the purposes for which such personal information is collected. The CCPA further requires that processing for any "business purpose" be "reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected." The CPRA amendments take the same approach and add that personal information should not be "further processed in a manner that is incompatible with those purposes."

The draft regulations expand these principles by adopting something akin to a GDPR-like regime requiring a lawful basis for processing, whereby businesses that do not have a legitimate interest for processing are required to obtain explicit consent. The draft regulations do not use GDPR nomenclature; instead, the regulations explain that a business's processing of personal information is "reasonably necessary and proportionate" if such processing is "consistent with what an average consumer would expect when the personal information was collected." The draft regulations thereafter require businesses to obtain the consum-

[1] See our April 2022 *Privacy & Cybersecurity Update* article "European Data Protection Board Invites Feedback in Response to Draft Guidelines on Dark Patterns."

[2] See the FTC's October 28, 2021, release "FTC to Ramp up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions."

er's explicit consent "for any purpose that is unrelated or incompatible with the purpose(s) for which the personal information [is] processed." These requirements would appear to require explicit consent in various situations involving adtech and other technologies that involve the sharing of personal information in a manner that does not comport with the expectations of the "average consumer."

New Requirements for Businesses

The draft regulations clarify certain requirements of businesses and introduce certain new obligations, including identifying with specificity the business purpose for which personal information is processed, as well as certain other provisions that are required to be included in contracts with service providers or contractors, and due diligence requirements. As noted above regarding the opt-in requirements, certain of these changes seem to be intended to align the CCPA more closely with the requirements of the GDPR.

Specifying Business Purposes

Privacy practitioners familiar with the Standard Contractual Clauses mandated by the GDPR will be familiar with the requirement to identify with specificity the purpose for which personal data will be processed. The draft regulations similarly require that contracts between businesses and service providers or contractors identify the "specific business purpose(s)" for the processing of personal information.

New Contractual Requirements

Businesses will need to update their data privacy addenda or other written contracts with service providers and contractors to comply with the CPRA's amendments to the CCPA. Some of these requirements are unique to the CPRA, such as the requirement that a service provider or contractor notifies the business within five business days of determining that it can no longer meet its obligations under the CCPA. Businesses that are contemplating relying on GDPR compliance as equivalent to CCPA compliance should be aware of these gaps and discrepancies when building out or updating their compliance programs.

Due Diligence Requirements

While the draft regulations do not expressly mandate that all businesses conduct due diligence on service providers, contractors and third parties prior to sharing personal information with them, the regulations do indicate that a business that shares personal information without conducting sufficient due diligence may be held responsible for the CCPA violations of such service providers, contractors or third parties.

Other Topics Covered

The draft regulations also address several other topics, including:

- updating requirements of the privacy policies of businesses;
- descriptions of the rights to delete and correct consumers' personal information;
- requests to limit the use or disclosure of sensitive personal information; and
- compliance audits by the CalPPA.

Next Steps

Based on the current timeline, the CalPPA will not be able to finalize the CPRA regulations by the July 1, 2022, deadline. Given that additional draft regulations are forthcoming and that a public comment period of at least 45 days is mandated, the regulations will likely not be finalized until the third or fourth quarter of 2022, which would make compliance from January 1, 2023, very challenging. At the meeting on June 8, 2022, businesses requested at least a six-month extension before enforcement will commence. At present, enforcement of the CPRA is set to begin on July 1, 2023.

Future iterations of the draft regulations are expected to address the following topics:

- technical specifications of the opt-out preference signal;
- opt-out rights with respect to automated decision-making; and
- annual cybersecurity audits and privacy risk assessments for "businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security."

In addition, noticeably absent was any mention of the treatment of personal information of employees, applicants for employment and independent contractors — whose personal information is currently subject to a partial exemption under the CCPA. Absent some sort of extension, this exemption is set to expire on January 1, 2023.

Key Takeaways

The draft regulations for the CPRA provide useful guidance to businesses seeking to prepare for compliance with the CPRA's amendments. However, the regulations also appear to impose additional obligations, compliance with which businesses may find costly and challenging — such as the obligation for all businesses to honor opt-out preference signals, the technical specifications for which do not yet exist. Businesses that are not currently complying or seeking to comply with the GDPR should take heed that compliance with the CPRA's requirements will likely be similarly onerous, including requiring substan-

tial updates to privacy policies and vendor contracts. Adtech companies, as well as their customers, also may need to reassess their practices in light of some of the provisions in these draft regulations due to the mismatch between the adtech industry's methods of processing of personal information and the expectations of the "average consumer."

Return to Table of Contents

Bipartisan Congressional Group Proposes Comprehensive Federal Privacy Law

A bipartisan group of members of Congress have proposed a comprehensive federal privacy law that would establish federal-level regulation on entities that collect, process or transfer personal data in the United States.

On June 3, 2022, Sen. Roger Wicker and Reps. Frank Pallone and Cathy McMorris Rodgers released a discussion draft of a proposed federal privacy law. The proposed law, the American Data Privacy and Protection Act[3] (ADPPA), would establish the first comprehensive federal data privacy regime, which would largely preempt state-level privacy laws that have recently been passed around the country in several states. The ADPPA's prospects for ultimate passage are not clear, nor is it clear how much of the legislation would change as it goes through the legislative process, but its introduction reflects a significant step in a long-standing effort to develop such a law to provide a uniform, national approach to privacy issues in the United States.

Background

Currently, the United States does not have a uniform law that covers the privacy of all consumer data, though there are privacy laws that address specific types of data or specific industries, such as the Children's Online Privacy Protection Act (for information related to children), the Health Information Portability and Accountability Act (for the health care industry) and the Gramm-Leach-Bliley Act (GLBA) (for the financial services industry). In addition, a number of states have enacted comprehensive data privacy laws (to date, California, Colorado, Connecticut, Virginia and Utah). Efforts to develop a more general federal law have previously stalled, however, over issues such as its effect on state laws, whether individuals would have a private right of action and how burdensome the requirements would be on businesses. In addition, political pressures within Congress have made it difficult to make progress in this area.

Overview of the ADPPA

Below, we describe certain specific elements of the ADPPA, as initially proposed by the bipartisan group of legislators.

Covered Data

The ADPPA regulates "covered data." Similar to many state data privacy laws' definitions of "personal data," the ADPPA defines "covered data" both in terms of information regarding individuals as well as information pertaining to their devices. Specifically, "covered data" is defined as information that is identifiable or is linked or reasonably linkable to either (1) an individual or (2) a device that identifies or is reasonably linkable to one or more individuals, including through derived data and unique identifiers (such as IP addresses or cookies).

However, "covered data" has three important exceptions: "de-identified data," "employee data" and "publicly available information."

The ADPPA defines "de-identified data" as "information that does not identify and is not linked or reasonably linkable to an individual or a device, regardless of whether the information is aggregated." For organizations that hold de-identified data, the ADPPA includes important requirements for how they would have to handle this data. If a covered entity possesses de-identified data, it would have to: (1) take reasonable measures to ensure the data cannot be used to re-identify an individual or device; (2) commit to processing and transferring the data in a de-identified manner and not attempt to reidentify the information; and (3) contractually obligate any recipient of such data to comply with the ADPPA. These requirements are similar to state data privacy laws, but the ADPPA also would cover devices that are not mentioned in the state legislation.

The ADPPA defines "employee data" as (1) information collected during in the course of the hiring process, (2) business contact information for employees, (3) emergency contact information for employees, and (4) information collected and processed by the employer as necessary to administer benefits for an employee.

The ADPPA defines "publicly available information" as information that has been lawfully made available to the general public through (1) federal, state or municipal government records; (2) widely distributed media; (3) website or online services made available to the public, for free or for a fee; or (4) a disclosure that has been made available to the general public as required by federal, state or local law. This language follows the legislation adopted by some of the state data privacy laws, but the ADPPA would go further by expressly stating what some state laws only imply: that website or online services made public are consid-

[3] See the American Data Privacy and Protection Act language.

ered publicly available information regardless of whether the service is free or paid.

Covered Entities

The ADPPA would apply to any entity or person that collects, processes or transfers covered data and is (1) subject to the Federal Trade Commission (FTC) Act; (2) a common carrier subject to Title II of the Communications Act of 1934 as currently enacted or subsequently amended (*e.g.*, telecommunications companies); or (3) an organization not organized to carry on business for its own profit or that of its members (*e.g.*, nonprofit companies). Institutions that are subject to the GLBA — such as banks and other financial institutions — and that are compliant with the information security and data privacy requirements of that law, would be deemed compliant under the ADPPA standards.

The ADPPA proposes specific additional requirements for covered entities that are "large data holders" or "third-party collecting entities." These include additional reporting and certification obligations, internal organizational and review measures, and public notice requirements. A "large data holder" is defined as a covered entity that, in the most recent calendar year (1) had annual gross revenues of $250 million or more and (2) collected, processed or transferred (a) the covered data of more than 5 million individuals or devices that identify or are linked or reasonably linkable to one or more individuals, or (b) the "sensitive covered data" of more than 100,000 individuals or devices that are identifiable or reasonably linkable to one or more individuals.

"Sensitive covered data" includes, but is not limited to, Social Security and passport numbers; past, present and future health diagnoses; financial account numbers; biometric information; an individual's private communications, such as voicemails, emails, texts, direct messages or mail; log-in credentials; sexual orientation; race; religion; ethnicity; national origin; union membership status; individuals' online activities across third-party websites or online services; video recording maintained for private use on a device; and information identifying an individual's use of any television, streaming or media services.

"Third-party collecting" entities are defined as covered entities whose principal source of revenue comes from processing or transferring the covered data of individuals that they did not collect directly from the individuals (with an exception for service providers who collect employee data solely for the purpose of providing benefits to the employee).

Unlike some state privacy laws, the ADPPA would not explicitly carve out exceptions for government entities, nonprofits and educational institutions, but would exclude small businesses and organizations that are not under the FTC's jurisdiction. However, entities that are not normally under FTC jurisdiction would be required to register with the FTC if they process covered data for more than 5,000 individuals. This registry would enable individuals to identify third-party collecting entities that process their covered data, allow for requests to delete all covered data related to the individual not directly given to the third-party collecting entity and ensure that any third-party collecting entity no longer collects the data without affirmative consent.

Consumer Rights

The ADPPA would provide consumers with a series of data privacy rights including the rights to:

- **Confirm and access covered personal data.** Individuals would have the right to access their covered data in a human-readable format that is "collected, processed or transferred by the covered entity or any service provider of the covered entity." Additionally, consumers would have the right to access the name of any entity to which their covered data was transferred and to request a description of the purpose for which the data was transferred. In the event that the covered data is no longer in the covered entity's possession, individuals would be able to request a general description of the covered data that the covered entity collected, processed or transferred in a human-readable format.
- **Correct inaccuracies.** Individuals would have the right to "correct any inaccuracy or incomplete information … that is processed by the covered entity and notify any … [entity or provider] to which the covered entity transferred such covered data of the corrected information."
- **Deleted covered data.** Individuals would have the right to require covered entities to "delete covered data of the individual that is processed by the covered entity and notify any … [entity or provider] to which the covered entity transferred such covered data of the individual's deletion request."
- **Data portability.** The ADPPA would afford individuals the right to "export covered data (except for derived data, which is covered data that is created by derivation of information from facts, assumptions or data about an individual or device) of the individual that is processed by the covered entity without licensing restrictions that limit such transfers, in (i) a human-readable format that a reasonable individual can understand and download from the Internet; and (ii) a portable, structured, interoperable and machine readable format." The ADPPA includes exceptions in the data portability requirements for smaller organizations.
- **Opt out of certain data activities.** Under the ADPPA, individuals would be allowed to opt out of data transfers to a third

party and from targeted advertising. Targeted advertising is defined as marketing to an individual based on known or predicted preferences, characteristics or interest derived from covered data collected over time or across third-party websites. Targeted advertising does not include: (1) advertising in response to an individual's specific request for information or feedback; (2) advertising based on an individual's visit into/use of and purchase of a product or service from a store or website; (3) advertising displayed online that is related to the content of the webpage; or (4) processing covered data solely for measuring or reporting advertising performance, reach or frequency.

- **Consent and object to the collection and processing over covered data.** Individuals would have the right to consent to the collection and processing of sensitive covered data, or the transfer of sensitive covered data to a third party. Without the affirmative expressed consent of an individual, a covered entity would not be able to collect, process or transfer the sensitive covered data of the individual. A covered entity would be required to provide an individual with clear and easy-to-execute means to withdraw any affirmative consent with respect to the processing or transfer of the covered data of the individual.

Obligations for Covered Entities

The ADPPA would impose guidelines on how covered entities should collect, process and transfer covered data.

Data Minimization

Under the proposed law, a covered entity could not collect, process or transfer covered data beyond what is reasonably necessary, proportionate and limited to provide or maintain a specific product or communication by the covered entity to the individual.

Prohibited Practices

The ADPPA would prohibit and restrict the following practices without affirmative expressed consent:

- collection, processing or transferring of Social Security numbers, except when necessary for extension of credit, authentication or the payment and the collection of taxes;
- transfer of an individual's geolocation information to a third party, except to another device or service of the individual, with the individual's affirmative express consent;
- collection, processing or transferring of biometric information, except for data security, authentication or to comply with a legal obligation;
- transfer of any password, except when the transfer is made to a designated password manager or to a covered entity whose exclusive purpose is to identify passwords that are being reused across sites;
- collection, processing or transferring of known nonconsensual intimate images, except for law enforcement purposes;
- collection, processing or transferring of genetic information, except for purposes of medical diagnosis, medical treatment, medical research or law enforcement investigations, or with the individual's affirmative express consent;
- transfer of an individual's aggregated internet search or browsing history, except with the affirmative express consent; and
- transfer of an individual's physical activity information from a smartphone or wearable device, other than to another device or service of that individual with the individual's affirmative express consent.

Privacy Policies

Covered entities would have to implement reasonable policies, practices and procedures for collecting, processing and transferring covered data. The ADPPA would require that these privacy policies and programs consider federal, state or local laws and be designed to mitigate privacy risks to children and privacy risks related to the products and services of the covered entity. In addition, these policies would have to provide a detailed and accurate representation of the entity's data collection, processing and transfer activities and would be made publicly available. Covered entities also would have to implement reasonable training and safeguards within the covered entity to promote compliance amongst the entity's employees and staff.

Nondiscrimination Based on Privacy Preferences

Covered entities would not be allowed to deny, charge different prices or rates, or condition or effectively condition, the provision of a service or product to an individual on the individual's agreement to waive any privacy rights. This is similar to the "nondiscrimination" obligation under state data privacy laws.

Enforcement

Enforcement by the FTC

The ADPPA would require the FTC to create a new bureau to enforce its requirements. Violations of the ADPPA would be considered an unfair or deceptive act or practice under the FTC Act, meaning the FTC would be able to obtain civil penalties for initial and subsequent violations, amongst other relief. Any relief that the FTC would obtain in enforcing the ADPPA would not be provided directly to harmed individuals. Instead, the penalties paid would be deposited into a relief fund for future victims of entities violating the ADPPA, or the FTC may use the funds for business mentorship programs or to engage in technological research.

Enforcement by State Officials

State attorneys general and chief consumer protection enforcement officers also would be able to bring cases in federal court for injunctive relief; to obtain damages, penalties, restitution or other compensation; and to obtain reasonable attorneys' fees and other litigation costs.

Enforcement by Individuals

Finally, the ADPPA would provide individuals with a private right of action. Four years after the proposed date that the ADPPA would take effect, persons or classes of persons would be able to bring a civil action in federal court seeking compensatory damages, injunctive relief, declaratory relief, and reasonable attorneys' fees and litigation costs. This four-year delay would provide entities and businesses with time to come into compliance the ADPPA's new requirements.

Individuals seeking to utilize this private right of action would be required to provide a 60-day notice to the FTC and their state attorney general before filing a lawsuit, and each entity would determine if it would seek civil actions before the individual would be able to file a lawsuit. If either the FTC or state attorney general decided to seek civil actions, then the individual would be prohibited from taking separate legal action and demanding monetary relief.

If the individual would be able to seek injunctive relief against covered entities, those entities would have a limited right to cure the alleged deficiency. Covered entities would be provided a written notice for 45 days that identified specific alleged violations and to produce a cure. If a cure is achieved, demands for injunctive relief may be dismissed.

Key Takeaways

The ADPPA is, at this point, only a proposed law and could undergo fundamental changes should it proceed through Congress. Nevertheless, the bipartisan effort that went into crafting the bill could be an indicator that a new federal data privacy law is on the horizon. Businesses that collect or process personal information should pay close attention to this legislation and its developments if it continues to move through the legislative process and becomes closer to being signed into law.

Return to Table of Contents

UK Government Announces a Six-Point Digital Strategy

On June 13, 2022, the U.K. government's Department for Digital, Culture, Media and Sport (DCMS) published the latest cross-government Digital Strategy. In an introduction to the strategy, which replaces the last iteration published in 2017, Minister for Tech and the Digital Economy Chris Philp underlined the importance of the U.K.'s success in digital technology as a key driver of economic prosperity, national security and geopolitical strength. The publication highlights that the U.K. already has "many advantages," including superfast internet access and more tech unicorns than France and Germany combined, and sets out six key areas of focus to help ensure that "the UK will be the best place in the world to start and grow a technology business."

Background

The strategy, which was announced by ministers attending London Tech Week, builds upon and unifies policy initiatives that were set out in previously published national strategies, including the National Innovation Strategy (published June 2019), the National Data Strategy (published September 2020) and the National Artificial Intelligence Strategy (published September 2021). The new strategy signposts areas for investment and policymaking that the government will undertake in the coming years (including actions that are already underway), to ensure that the country remains an attractive destination for investors and innovators, with a hope of increasing the value of the U.K. tech sector by £41.5 billion by 2025. The strategy[4] focuses on six areas for action:

1. Digital Foundations

At the strategy's core lies the intention to strengthen the foundations of the digital economy. The digital economy is, in turn, based on four "foundational pillars" that the government sees as the critical building blocks for the growth of the tech industry. These foundation pillars are:

- **Robust digital infrastructure.** The strategy details plans to ensure that every part of the U.K. has access to "world-class, secure" digital infrastructure, including gigabit broadband coverage in rural areas and access to 5G coverage by the majority of the population by 2027.
- **Unlocking the power of data.** Noting the key role that data has as a driving force of modern economies, the strategy notes that the government expects to "bring forward" its plans to

[4] The full strategy is available on the government's website.

reform the U.K.'s data protection laws and adopt measures that provide for a more flexible regulatory regime.[5]

- **A light-touch, pro-innovation regulatory framework.** Citing the legislative freedoms available to the U.K. post-Brexit, the government sets out its intention to provide a regulatory environment that is coherent and forward-looking, and that is adapted to the fast-moving nature of digital technologies. To this end, the strategy notes plans for the government to work with key industry stakeholders, including the Confederation of British Industry (CBI) and TechUK (the trade association for the tech industry), to gather practical recommendations for the U.K.'s regulatory regime.
- **A secure digital environment.** The strategy highlights the importance of the government's planned investment of £2.6 billion into the U.K.'s cybersecurity measures, including into research and development, defense and cyber skills training.

2. Ideas and Intellectual Property

Recognizing the important role that new ideas — and the protection of these ideas through intellectual property law — is to securing digital growth, the strategy outlines the government's plan to incentivize and support innovation in both the public and private sectors. In particular, the strategy notes the government's intention to expand tax relief for research and development activity, including through reforms to the Research and Development Expenditure Credit scheme.

3. Digital Skills and Talent

Access to a skilled workforce is essential to ensuring the growth of the U.K. digital economy, with many companies citing lack of available talent as the most significant constraining factor to their growth. The strategy therefore sets out a number of proposals to ensure that the U.K. workforce has access to appropriate training opportunities and that U.K. businesses also are able to attract talent from overseas. The strategy highlights, for example, plans to increase access to visas by skilled individuals, including through the introduction of new visa pathways (the High Potential Individual and Scale-Up visas) and amendments to existing visa programs (*e.g.*, by removing the funding requirement from the Innovator visa by fall 2022).

4. Financing Digital Growth

While the U.K. already enjoys access to deep pools of capital for the tech sector that exceed those anywhere else in Europe (attracting £27.4 billion in private capital inflows in 2021), the strategy identifies areas for further progress. These include incentivizing the U.K.'s institutional investors (including pension funds) to take a more proactive approach to growth technology investing, and through plans to increase IPO activity through review of the listing rules (including the U.K.'s Prospectus Regime).

5. The Whole UK: Spreading Prosperity and Levelling Up

New initiatives and policies must ensure that benefits of digital innovation are available to every region and industry within the U.K., and that these are not limited to those working within tech-focused businesses. The strategy outlines plans to assist businesses across every sector with the adoption of productivity-enhancing digital technologies, including through provision of subsidies and schemes for digital transformation.

6. Enhancing the UK's Place in the World

The strategy notes that, as the internet and digital technologies have an ever-increasing impact on our daily lives, the way the U.K. chooses to govern these technologies will have significant implications for Great Britain's relationships with other global economies. For example, in key areas such as artificial intelligence, the U.K. has the opportunity to contribute to international norms for regulation that may enhance prosperity and democratic values beyond its own borders. The strategy also notes that the U.K. continues to enter into trade agreements that include tech-friendly provisions like tariff-free digital trade and source code protection (*e.g.*, the Digital Economy Agreement that was agreed upon between the U.K. and Singapore earlier this year).

Key Takeaways

While many of the policies and plans published in the strategy will be familiar to those who have kept abreast of the government's earlier strategies on related topics (as noted above), the strategy also represents a welcome step towards a harmonized road map for policy change in the digital sector. The strategy (and particularly the Annex to the Strategy, which includes a comprehensive summary of all the actions the government plans to undertake and their associated timelines) will provide to both U.K. and international businesses an early indicator of the kinds of financial incentives and regulatory advantages that are expected to become available in the coming years. Critics of the strategy (including the government's stakeholder, TechUK), however, note that it lacks a longer-term vision for the role that digital technologies could play in driving systemic change, and also fails to identify targets or metrics to measure the strategy's success going forward.

Return to Table of Contents

[5] We have written about the proposed reforms to the U.K.'s data protection regime in our May 2022 Privacy & Cybersecurity Update. The government published its response to the DCMS consultation on the proposed reforms on June 17, 2022.

Federal Employee and Applicant Data Breach Results in $63 Million Settlement

A federal court has preliminarily approved a $63 million settlement of claims arising from a massive data breach affecting federal employees and applicants.

On June 7, 2022, Judge Amy Berman Jackson of the U.S. District Court for the District of Columbia gave preliminary approval for a $63 million settlement of claims arising out of a series of data breaches involving information about current and former federal employees and applicants. In its ruling, the court stated that recoverable claims would be limited to redressing economic harms (including potentially time spent attempting to mitigate these harms), but would not include compensation solely for increased risk of harm.

Background

From 2013-15, the Office of Personnel Management (OPM) and its background check services contractor Peraton Risk Decision Inc. (Peraton) experienced a series of data breaches affecting the personal information of nearly 22 million former, current and prospective federal employees. These affected records included Social Security numbers, mental health records, financial histories and other information, and in some cases included fingerprints. The OPM announced the breaches in 2015, and class action suits quickly followed that sought damages for the affected data subjects.

The case had originally been dismissed in 2017 on the grounds that mere increased risk of harm was insufficient to establish Article III standing for the class, but was revived in part by the D.C. Circuit Court in June 2019, when it ruled the increased risk was enough to clear the "low bar" for moving cases forward at the pleading stage.

The Settlement

Despite the Circuit Court's decision that implied that increased risk of harm can be the basis for pursuing a claim, under the proposed settlement only those who suffered actual out-of-pocket harms (which can include time spent attempting to mitigate risks) are eligible to recover damages. Specifically, eligible class members include individuals who had their personal information exposed as a result of the OPM and/or Peraton breaches, and who, after May 7, 2014, incurred out-of-pocket expenses related to (1) losses from identity theft (2) implementing or eliminating a credit freeze on a class member's credit file and (3) credit monitoring and identity theft service costs. The time associated with these expenses also falls within the settlement as a potentially valid claim.

The minimum claim award under the settlement is $700 and the maximum is $10,000. In awarding damages, a claims administrator will consider factors such as the date the out-of-pocket costs were incurred, the type of information misappropriated, the class member's description of how the costs relate to the breach and the class member's actions, to determine whether the claim is reasonably due to the data breaches. All claims must be submitted by December 23, 2022, to be eligible for payment. There is a possibility that claims can be reduced equally if there are not enough available funds to settle each claim.

A fairness hearing is scheduled for October 14, 2022, where the court will issue a final ruling on whether the affected class is certifiable under the Federal Rules of Civil Procedure, and whether the settlement is fair and reasonable. Individuals who are part of the class subject to claim payment will have the opportunity to voice any concerns with the potential settlement and contest its approval, provided they submit their opposition by September 9, 2022.

Key Takeaways

The settlement is the latest in a long series of expensive damages awards arising out of data breaches, and follows the lead of many circuit courts (including the Second, Third, Fourth, Eighth and Eleventh Circuits) in limiting recoverable harms to actual damages, rather than speculative damages based on increased risk of harm. Nevertheless, the size of the award reaffirms that companies experiencing large data breaches may have to pay significant damages as compensation to affected data subjects.

Return to Table of Contents

US Department of Energy Releases New National Cyber-Informed Engineering Strategy

The U.S. Department of Energy (DOE) released a cybersecurity-focused framework for the energy sector, with a focus on providing a proactive approach to building cyber-resilient clean energy systems.

On June 15, 2022, the DOE published a new strategy focused on preemptively engineering cyber-resilient clean energy systems. The DOE's release, called the National Cyber-Informed Engineering (CIE) Strategy, aims to "engineer out" cyber risk at the outset through the integration of cybersecurity considerations

into the conception, design, development and operation of any digitally driven physical system. In short, the purpose of the CIE strategy is to diminish or eliminate the effects of a cyberattack.

Background: Identifying the Security Gap

In today's digital world, all industries are faced with a level of cybersecurity risk. Given the increasing frequency of sophisticated technological cyberattacks, the DOE developed a coordinated and collaborative CIE strategy that enables the nation's critical energy infrastructure to withstand intentional cyber events.

Traditionally, most critical infrastructure control systems have addressed cybersecurity and engineering matters separately. Engineers have been trained to build energy systems with safety, reliability and functionality in mind rather than to protect against informed and capable hackers. As a result, engineers tend to rely on specialized practitioners' responsive cybersecurity measures once systems are compromised. This separation between cybersecurity and engineering has created gaps in cyber protection, which has increased system vulnerabilities and reactive security spending. As stated in the strategy, the DOE sees an opportunity for proactive protection and mitigation against compromising cyberattacks in the nation's energy control systems.

The CIE Solution

The CIE strategy places cybersecurity at the center of the energy sector, making it a foundational element of engineering risk management for all cyber-physical infrastructures. The CIE strategy focuses on building cybersecurity into energy systems at the earliest possible stages to avoid responding to vulnerabilities that are typically only identified after a system has been compromised. In doing so, CIE builds upon existing software security strategies, such as "secure-by-design" software development and "zero-trust" architecture.

The "secure-by-design" methodology focuses on eliminating design flaws in the architecture of software systems. Secure-by-design software development builds cybersecurity into control systems early on in the process and ensures all phases of control systems are secure and can quickly recover from cyberattacks. CIE expands on this concept by building secure architectures into digitally accessible physical infrastructures. The DOE proposes to bring the energy sector up to date by employing this existing secure-by-design approach.

The "zero-trust" approach removes implicit trust from devices, which entails shifting away from expecting that a secure perimeter will defend against hackers. CIE extends this concept by assuming cyberattacks will occur and by deploying defenses to mitigate possible consequences. By tying together cybersecurity and engineering, the CIE strategy incorporates cyber risk management early into the design process to reduce or eliminate previous cyber vulnerabilities.

The CIE strategy is anchored in five integrated pillars: awareness, education, development, current infrastructure and future infrastructure. Taken together, these pillars provide the body of knowledge, diverse workforce and engineering capabilities for CIE to effectively curb against cyberattacks. These pillars are outlined below:

- **Awareness:** Centers on promulgating a universal understanding of CIE through targeting the network of energy industry practitioners, formulating technical requirements for CIE implementation, developing policy initiatives and partnerships, and constructing case studies that illustrate CIE's benefits.
- **Education:** Focuses on cultivating CIE practitioners through training and credentialing programs, partnering with academic institutions to incorporate CIE principles into appropriate courses, connecting with industry employers to ensure CIE certification and continuing education programs, and partnering with federal programs to support educating the engineering workforce on CIE principles.
- **Development:** Emphasizes building a repository of tools and methods that practitioners can look to when applying CIE to current and future infrastructures. Building this toolkit involves leveraging knowledge from various energy institutions and developing a CIE center and database.
- **Current Infrastructure:** Uses a consequence-driven approach to employ CIE principles to existing critical infrastructure by identifying needed upgrades, triaging the most important applications for CIE and developing a framework that assesses the efficacy of upgrade and mitigation strategies for existing infrastructure systems.
- **Future Infrastructure:** Stresses conducting research and development for building a novel and incentivized design standard for CIE energy infrastructure systems in the private and public sectors.

These pillars provide the foundation for a cybersecurity-focused energy sector. Still, the DOE recognizes that a broad set of stakeholders will need to develop an implementation plan for each pillar to ensure the effective execution of the CIE strategy. When fully implemented, a CIE energy sector is one where engineers learn about cybersecurity, incorporate cybersecurity practices into their system and process designs, and evaluate the potential for disruption and harm from cyberattacks when developing control systems. As such, engineers can integrate cyber risk management early in a system's life cycle, allowing future systems to be cyber-resilient at their core.

DOE's Expected Benefits of the CIE Strategy

The CIE strategy provides a framework for incorporating cybersecurity into energy infrastructures at the earliest opportunity and maintaining cyber resiliency throughout a control system's life cycle. This strategy signals what the DOE hopes is a cultural shift in the energy sector toward prioritizing cybersecurity in tandem with safety. To that end, applying CIE may prove advantageous for companies in the long term since integrating cybersecurity protection into the early stages of control system development is cost-effective. These savings are evident as utilizing early cybersecurity incorporation can mitigate or eliminate potential avenues for cyberattacks and reduce their possible consequences. Accordingly, companies can reduce costs by applying foresight to cybersecurity problems rather than having to spend money to fix matters post-attack.

Key Takeaways

Although the DOE created the CIE strategy for the energy sector, the concepts and principles can act as a leverageable model across industries. Embedding CIE methods into the education and credentialing of all engineers creates a cyber-aware workforce that is able to design resilient infrastructure systems no matter the sector. Given this broad applicability, the CIE strategy can serve as a guide for other critical infrastructure sectors. Additionally, since energy companies may face increased regulatory scrutiny concerning their business operations once a CIE implementation plan is finalized, companies may want to proactively begin reviewing their cybersecurity systems before the new standards are released.

Contacts

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5010
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Ken D. Kumayama
Partner / Palo Alto
650.470.4553
ken.kumayama@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Jason D. Russell
Partner / Los Angeles
213.687.5328
jason.russell@skadden.com

David Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

Ingrid Vandenborre
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
One Manhattan West
New York, NY 10001
212.735.3000