Skadden

Privacy & Cybersecurity Update

1 Delaware Becomes 13th State To Pass Comprehensive Data Privacy Law

2 Data Protection Authorities From 12 Non-EEA Jurisdictions Issue Joint Statement on Data Scraping and Data Protection

4 D.C. District Court Grants in Part and Denies in Part Health Insurance Provider's Summary Judgment Motion on Plaintiffs' Claims Arising From Data Breach

5 California Privacy Protection Agency Discusses Draft Cybersecurity Audit and Risk Assessment Regulations at Public Board Meeting

Delaware Becomes 13th State To Pass Comprehensive Data Privacy Law

On September 11, 2023, Delaware became the 13th state to pass a comprehensive data privacy law when the Delaware Personal Data Privacy Act (DPDPA) was signed into law. The act, which will go into effect on January 1, 2025, gives consumers privacy rights similar to those provided by other comprehensive state data privacy laws, including Virginia's Consumer Data Protection Act and Connecticut's Data Privacy Act. Nevertheless, there are some key differences between the DPDPA and other state data privacy laws that companies and organizations should note, as discussed below.[1]

Overview of the DPDPA

The DPDPA applies to persons that conduct business in the state of Delaware or produce products or services that target state residents and either (i) control or process the personal data of 35,000 consumers or more (excluding data controlled or processed solely to complete a payment transaction), or (ii) control or process the personal data of 10,000 or more consumers and derives more than 20% of their gross revenue from the sale of personal data. Note that the DPDPA does not exclude nonprofit organizations from its scope unless dedicated exclusively to preventing and addressing insurance crime.

Similarities With Other State Comprehensive Data Privacy Laws

Similar to other comprehensive state data privacy laws, the DPDPA provides consumers with core data rights for personal data such as the right to access, the right to delete and the right to correct. The act also provides consumers with the right to opt out of targeted advertising, as well as the sale of personal data and profiling based on automated decision-making that produces legal or similarly significant effects concerning such consumer. In addition, similar to the California Consumer Privacy Act, the DPDPA grants consumers the right to request information about the categories of third parties to whom the consumer's personal data was disclosed. The DPDPA also invalidates consent that is given by a consumer through the use of "dark patterns," which are website elements that can deliberately obscure, mislead, coerce and/or deceive website visitors into making unintended decisions, such as consent declarations.

[1] The full text of the Delaware Personal Data Privacy Act can be found here.

Moreover, as with most comprehensive state data privacy laws, the DPDPA does not contain a private right of action. Instead, Delaware's Department of Justice (Delaware DOJ) has the exclusive authority to enforce the DPDPA. The Delaware DOJ may seek up to $10,500 per violation and, for the first year of the act's enforcement (until December 31, 2025), must provide businesses with a notice of a violation and 60 days to cure any alleged deficiencies before beginning enforcement proceedings. Beginning on January 1, 2026, the Delaware DOJ shall have discretion to grant any cure periods for alleged DPDPA violations.

Differences Compared to Other Comprehensive Data Privacy Laws

The DPDPA includes certain elements that differ from other comprehensive state data privacy laws, such as:

- The DPDPA does not contain a revenue threshold for the act's scope of applicability, which, combined with a lower threshold volume for the controlling or processing of information compared to other comprehensive state privacy laws, means that more types of business are likely to be subject to the DPDPA.
- The definition of "sensitive data," for which processing requires a consumer's opt-in consent, is more broadly defined than in other state data privacy laws.
- The DPDPA requires controllers to comply with opt-out preference signals, including those sent through a platform, technology or mechanism such as a browser setting, browser extension or global device setting.
- Under the DPDPA, controllers are prohibited from processing the personal data of a consumer for targeted advertising or selling such consumer's personal data without the consumer's consent if the controller has actual knowledge or willfully disregards the fact that the consumer is between the ages of 13 and 18. While most comprehensive state data privacy laws have similar restrictions, they typically only cover consumers between the ages of 13 and 16.

Takeaways

The DPDPA will usher in additional compliance requirements for businesses that currently have to adhere to obligations of other comprehensive data privacy laws. Given the low threshold for applicability of the DPDPA, businesses should evaluate whether they may be subject to the act's requirements, though those that comply with other states' laws should have a head start on compliance in Delaware. Nevertheless, businesses that may be subject to the DPDPA should consider how their data privacy practices should be updated to address the differences between Delaware's law and those in other states.

Return to Table of Contents

Data Protection Authorities From 12 Non-EEA Jurisdictions Issue Joint Statement on Data Scraping and Data Protection

On August 24, 2023, 12 non-European Economic Area data protection authorities (DPAs), including the U.K.'s Information Commissioner's Office, the Australian Information Commissioner's Office and the Office of the Privacy Commissioner of Canada,[2] issued a joint statement outlining (i) the key privacy risks associated with data scraping, (ii) some nonbinding recommendations for steps that social media companies (SMCs) and the operators of other websites that host publicly accessible personal data should take to protect any such personal data from data scraping (noting these recommendations may be considered by relevant courts or DPAs when assessing an SMC's compliance with relevant data protection laws) and (iii) steps individual users of SMC sites can take to protect against data scraping of their personal data. Responses from SMCs to the joint statement from SMCs were due on September 24, 2023.

Summary

Data scraping, as the joint statement defines, "involves the automated extraction of data from the web," including, for example, the scraping of data from SMCs' comments sections, chat rooms or public profiles. This data can be utilized in a variety of ways, including for analysis (such as for advertising), intelligence gathering or training AI.

The joint statement is not focused on data scrapers but instead seeks to address privacy-related concerns around the practice by recommending actions to be taken by (i) SMCs and the operators of other websites that host publicly accessible personal data to protect the personal data that they host on their sites and (ii) individuals whose data is hosted on SMC sites. The joint statement also requested responses from SMCs to these recommendations, including providing details on how they currently comply with the recommendations in the joint statement.

Risks of Data Scraping

The nature of data scraping allows for information to be gathered quickly and in large quantities, which has raised significant

[2] Along with the: Office of the Privacy Commissioner for Personal Data (Hong Kong); Federal Data Protection and Information Commissioner (Switzerland); Datatilsynet (Norway); Office of the Privacy Commissioner (New Zealand); Superintendencia de Industria y Comercio (Columbia); Jersey Office of the Information Commissioner; Commission Nationale de contrôle de la protection des Données à caractère Personnel (Morocco); Agency for Access to Public Information (Argentina); and National Institute for Transparency, Access to Information and Personal Data Protection (Mexico).

privacy concerns for data subjects, including in relation to consent, data retention/storage and security. The joint statement notes that DPAs have seen an increase in incidents of privacy breaches resulting from data that has been scraped from SMC sites, either by individuals and companies in the course of their activities or by more nefarious actors seeking to harm the data subjects.

The joint statement notes that data scraping poses risks for users of SMC sites, with scraped data potentially being used to undertake targeted cyberattacks, identity fraud, monitoring, profiling and surveillance, for unauthorized political or intelligence-gathering purposes, and/or to send unwanted spam. The DPAs make clear that all of these potential uses can undermine trust in SMCs and hurt the wider digital economy.

Joint Statement Recommendations for SMCs

The DPAs' statement stops short of imposing binding obligations on SMCs in relation to data scraping. However, the statement sets out certain recommendations for SMCs and makes clear that some of them are already explicit statutory obligations in certain jurisdictions and that compliance may be considered by the relevant DPAs or courts when assessing compliance with data protection laws.

While the joint statement notes data security is a dynamic responsibility, it recommends SMCs use a combination of multilayered technical and procedural measures to counter unlawful data scraping, proportionate to the sensitivity of the information, to protect personal data. This includes:

- designating a team to identify data scraping activities;
- monitoring new accounts for strange or suspicious activities;
- limiting visits by users to other users' profiles on a daily or hourly basis, and adding further limits on suspicious accounts;
- deploying techniques to identify "bot" accounts, IP addresses or suspicious activity (including by tracking bot activity and implementing CAPTCHAs);
- for suspicious accounts, implementing IP address blocking and using relevant legal actions to protect users (including by sending cease and desist letters or requiring that scraped information be deleted by the data scrapers);
- having adequate and enforceable terms and conditions of use to prevent data scraping;
- where data scraping may constitute a data breach (depending on the laws of the relevant jurisdiction), notifying affected data subjects and relevant DPAs; and
- supporting website users by engaging proactively to protect data.

While none of the DPAs that issued the joint statement represent EEA countries subject to the General Data Protection Regulation (GDPR), it is interesting to note that many of the recommendations are linked to the SMCs' obligations as data controllers under similar or equivalent data protection laws in the relevant DPA jurisdictions, including obligations relating to accountability, transparency, data minimization and protecting personal data. For example, the recommendations involving identifying, monitoring and limiting potential scraping relate to the data protection principles of controllers maintaining the integrity and security of personal data, while the general obligation to limit the amount of scraped data is reflective of general data minimization principles found in data protection legislation such as the GDPR.

Recommendations for Users

The joint statement provides additional guidance for users of SMC sites, recommending that users review websites' terms of use and policies, pay attention to the type of data inputted into websites used and keep aware of how to, and why they should, change their privacy settings.

Importantly, the statement notes that users of SMC sites should contact the company if they feel their personal data has been scraped unlawfully or improperly and escalate these concerns to DPAs if they feel the SMCs have responded inadequately.

Conclusion

The DPAs' joint statement is a reminder for SMCs to be aware of, and act on, relevant data protection obligations in relation to data scraping and take an active role in protecting their users from unlawful or improper scraping in order to comply with data protection laws. While there has been a wider focus on intellectual property issues surrounding data scraping, the joint statement makes clear that the practice also is a data protection issue and should be considered as part of SMCs' data protection considerations.

Return to Table of Contents

D.C. District Court Grants in Part and Denies in Part Health Insurance Provider's Summary Judgment Motion on Plaintiffs' Claims Arising From Data Breach

The U.S. District Court for the District of Columbia denied CareFirst, Inc.'s motion for summary judgment on plaintiffs' breach of contract claim arising from a data breach that targeted the company, but granted summary judgment regarding its claims that CareFirst violated Maryland and Virginia consumer protection statutes.

The Data Breach and Class Action Litigation

In 2014, defendant CareFirst, Inc., a health insurance provider, suffered a cyberattack through an email-based spear phishing campaign targeted at the company's employees. CareFirst hired a cybersecurity firm to conduct a forensic investigation and found that its systems had been compromised, after which the company notified customers whose data might have been impacted. Soon after, the plaintiffs — Washington, D.C., Maryland and Virginia residents who had health insurance provided by CareFirst, Inc. and received notice letters — brought a class action lawsuit against the company, alleging claims including breach of contract, negligence and violations of consumer protection statutes.

CareFirst's Summary Judgment Motion

On CareFirst's motion for summary judgment, the only claims that remained were for breach of contract and violation of state consumer protection statutes.

The court denied CareFirst's summary judgment motion as to the plaintiffs' breach of contract claim, which had alleged that the company had breached both express and implied promises contained in its privacy statements and Notice of Privacy Practices about its security measures for protecting personal identifying information (PII).

While the court rejected the plaintiffs' argument as to CareFirst's privacy statements, it found the company's Notice of Privacy Practices — which described how CareFirst would "use, disclose … collect, handle and protect" members' PII and stated that the company "maintain[ed] physical, electronic and procedural safeguards . . . to protect [members'] health information" — did support the plaintiffs' argument that the language created a duty. The plaintiffs alleged, and the court agreed, that such statements provided an implicit promise that CareFirst would take reasonable steps to secure the plaintiffs' PII against unauthorized intrusion by third parties.

The court next assessed the parties' competing expert opinions about whether CareFirst breached this duty. The court found no evidence that CareFirst failed to engage a full-scale incident response plan or failed to properly train employees to recognize spear phishing attempts, as the plaintiffs alleged. However, the court did credit evidence in the record showing that CareFirst's IT team did not look for lateral movement when investigating the incident and did not have a database access monitoring system — actions and programs that the plaintiffs argued would have helped the company identify and prevent the unauthorized access. Since the court also found sufficient evidence in the record supporting the existence of causation and damages, CareFirst's motion for summary judgment on plaintiffs' breach of contract claim was denied.

The court also addressed CareFirst's summary judgment motion on the plaintiffs' consumer protection claims under Maryland's consumer protection statutes, which it ultimately granted.

Regarding the Maryland Consumer Protection Act, the plaintiffs alleged that CareFirst's Notice of Privacy Practices contained an actionable misrepresentation because it stated that the company "maintained data-security safeguards according to federal and state standards." The court disputed that the statement was a misrepresentation and stated that, even if it was, none of the evidence showed the named plaintiffs relied on the Notice or were aware of it when they chose CareFirst as their provider. The court also found no evidence to support that CareFirst violated the Maryland Personal Information Protection Act (MPIPA) because the data at issue in the breach did not involve Social Security numbers or any other data categories covered by the MPIPA.

Takeaways

The CareFirst decision sheds light on how courts approach typical claims in data breach cases and underscores that the language of privacy statements and policies provided to customers may be critical to questions of liability following an incident. The promises contained in those statements — express or implied — may be interpreted to create an affirmative duty to safeguard customers' personal information, and may require a company to implement certain monitoring systems, training programs or other protocols to effectively demonstrate it has taken reasonable steps to protect that data. Therefore, companies should ensure that the language of privacy practices and statements are thoughtfully considered and consistent with their practices.

Return to Table of Contents

California Privacy Protection Agency Discusses Draft Cybersecurity Audit and Risk Assessment Regulations at Public Board Meeting

On September 8, 2023, the five-member board of the California Privacy Protection Agency (CPPA) held a public meeting to discuss topics concerning the implementation of the California Privacy Rights Act of 2020 (CPRA), which amended the California Consumer Privacy Act of 2018. Most notably, the board discussed the CPPA rulemaking subcommittee's draft regulations on cybersecurity audits and risk assessments, issued on August 29, 2023, and the scope of their applicability to businesses subject to the CPRA prior to initiation of the formal rulemaking process for these regulations.[3]

Background

The CPRA requires that "businesses whose processing of consumers' personal information presents a significant risk to consumers' privacy or security" (i) perform an annual cybersecurity audit documenting and assessing the businesses' implementation of various safeguards and (ii) submit periodic risk assessments concerning their processing activities to the CPPA.[4] At the September 8 meeting, the CPPA board provided feedback on specific provisions of the draft regulations identified for the board's consideration and discussion, focusing on the applicability and scope of the cybersecurity audit and risk assessment requirements.

Cybersecurity Audit Regulations

The draft regulations require that businesses undergo a cybersecurity audit when at least 50% of their annual revenues derive from the sale or sharing of personal information. The draft regulations propose additional threshold options that would trigger the cybersecurity audit requirement, including:

- revenue and personal information processing thresholds (*e.g.*, a business that has a specified gross revenue and processed the personal information of a set number and type of consumers in the preceding calendar year);
- a flat annual gross revenue threshold; and/or
- a flat number of employees threshold.

The board focused on applicability of the cybersecurity audit requirement to entities that are not data brokers (*i.e.*, do not derive at least half their annual revenues from the sale or sharing of personal information), emphasizing that defining appropriate thresholds is critical, especially given the burdens the audit requirements would impose on businesses.

The draft regulations also propose options for the scope of the cybersecurity audits. One option requires an assessment of how a business's cybersecurity program considers and protects against various enumerated negative impacts to consumers' safety (*e.g.*, unauthorized access to personal information, impairing consumers' control over personal information, or economic, physical, psychological or reputational harm to consumers associated with unauthorized access to or use of such information). The other option requires an assessment of "any risks from cybersecurity threats, including as a result of any cybersecurity incidents, that have materially affected or are reasonably likely to materially affect consumers." Board members encouraged shifting to a standard that does not require businesses to opine on what may be damaging to consumers, instead suggesting a bright-line option or a combination of the proposed options (*e.g.*, requiring assessment of risks from cybersecurity threats that have materially affected or are reasonably likely to materially affect consumers, and using the categories of harms from the first proposed option as illustrative examples).

Risk Assessment Regulations

The risk assessment requirement mandates that a business assess and report on whether the negative impacts to consumers' privacy from a processing activity are outweighed by the benefits to the consumer, the business, other stakeholders and the public. If not, the business must cease the processing activity.

The draft regulations propose subjecting businesses to the risk assessment requirement where they meet certain criteria, including:

- selling or sharing personal information;
- processing sensitive personal information;
- using automated decision-making technology in furtherance of enumerated decisions;
- processing personal information of individuals aged under 16;
- processing the personal information of consumers who are employees, contractors, job applicants or students by using technology to monitor such consumers;
- processing personal information of consumers in publicly accessible places; or
- processing personal information to train artificial intelligence or automated decision-making technology (with proposed definitions of "artificial intelligence" and "automated decision-making technology" included in the draft regulations).

[3] The full text of the draft regulations are available here.

[4] Cal. Civ. Code § 1798.185(a)(15). The CPRA charges the CPPA with issuing regulations on such audits and assessments.

The draft regulations suggest various requirements for complying with risk assessments and identify topics that businesses must consider and include additional requirements for businesses that (i) use automated decision-making technology for purposes to be set forth in the yet-to-be published draft regulations for processing, subject to automated decision-making technology access and opt-out rights, or (ii) process personal information to train artificial intelligence or automated decision-making technology. The board discussed the definitions of "artificial intelligence" and "automated decision-making technology" included in the draft regulations, noting that though they appear quite broad, their language has been drawn from sources including the National Institute for Standards and Technology and is limited by other provisions within the text.

Among other requirements, the draft regulations state that the subject business identify the benefits and negative impacts associated with a processing activity. The board suggested that language be included to require more specific descriptions of the financial benefits that businesses derive from selling or sharing personal information.

Despite certain synergies with other regulations and state laws' data privacy impact assessment requirements (including the GDPR and the Colorado Privacy Act), board members expressed concern that certain granular requirements of the proposed CPRA risk assessments could impose undue burdens on businesses attempting to comply with the various laws' obligations.

Takeaways

The CPPA has not yet initiated the formal rulemaking process for cybersecurity audits or risk assessments (at which point public comments will be requested), and the draft regulations remain subject to change through board discussion and public participation. The CPPA board's feedback from the September 8 meeting will guide the rules subcommittee in revising the draft regulations for further discussion at the next board meeting (scheduled for November or December 2023) as the informal rulemaking process continues. Though the September 8 meeting concerned cybersecurity audit and risk assessment regulations, the Rules Subcommittee also continues to develop regulations on automated decision-making technology, and the different draft regulations could be approved for formal rulemaking on separate timelines.

Return to Table of Contents

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

Avia M. Dunn
Partner / Washington, D.C.
202.371.7174
avia.dunn@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

Maya P. Florence
Partner / Boston
617.573.4805
maya.florence@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

Richard J. 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

David Simon
Partner / Washington, D.C.
202.371.7120
david.simon@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

Nicole L. Grimm
Counsel / Washington, D.C.
202.371.7834
nicole.grimm@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