Skadden

Privacy & Cybersecurity Update

California Privacy Protection Agency Seeks Public Comments on Proposed California Privacy Rights Act Rulemaking

The California Privacy Protection Agency (CalPPA) issued an invitation for preliminary written comments from the public under the California Privacy Rights Act of 2020 (CPRA); comments are due November 8, 2021.

On September 23, 2021, CalPPA issued an invitation for preliminary public comments on proposed rulemaking under the CPRA. Under Section 1798.185 of the California Consumer Privacy Act (CCPA), as amended by the CPRA, CalPPA is directed to encourage public participation and develop new regulations to carry out the goals of the CCPA and the CPRA.

Comments are due Monday, November 8, 2021, though CalPPA also is planning to hold informational hearings to obtain further public input, though such hearings have yet to be scheduled.

Background

On November 3, 2020, California voters passed the CPRA, which amended and extended the CCPA of 2018 in certain ways. These amendments included increasing the rights of California residents over personal information, creating new obligations for businesses with respect to the processing and sharing of personal information, and providing additional oversight and record-keeping requirements on businesses whose processing of personal information presents significant risks to consumers' privacy.

The CPRA took effect on December 16, 2020, but most of the provisions won't become enforceable until January 1, 2023. One of the key changes that took effect in 2020 was the establishment and funding of a new state agency, CalPPA, to implement and enforce the CCPA. Under the CPRA, the rulemaking authority previously held by the California Office of the Attorney General transferred to CalPPA, with the new agency's responsibilities including updating existing regulations and adopting new regulations to implement the amendments called for by the CPRA. CalPPA is required to finalize these new regulations by July 1, 2022.

Key Topics for Public Comments

CalPPA is "particularly interested in comments on new and undecided issues not already covered by the existing CCPA regulations." Relatedly, it is primarily seeking comments related to those changes under the CPRA that become enforceable on January 1, 2023, including regarding the following topics:

- **Cybersecurity audits and risk assessments performed by businesses.** The CPRA calls for businesses that process personal information that presents a significant risk to consumers' privacy and security to conduct annual audits and regular risk assessments. CalPPA invites comments on the procedural requirements of the audits and risk assessments, including what they should address, the frequency of the risk assessments, and how to weigh the risks and benefits of processing consumers' personal information. CalPPA also asks to determine which circumstances do businesses' processing of personal information present a significant risk to privacy or security, and when should such processing be restricted or prohibited.
- **Consumers' rights to limit the use and disclosure of sensitive personal information.** Consumers are afforded additional rights under the CPRA limiting the use and disclosure of a new category of "sensitive personal information." CalPPA seeks to determine what rules and processes should be implemented in response to a consumer request to limit the use of their sensitive personal information, such as the technical specifications for the opt-out signal. The agency also is seeking to determine when the collection of sensitive personal information should be exempt from the right to limit use and disclosure because the purpose of such collection is not to infer characteristics about a consumer.
- **Access and opt-out rights with respect to automated decision-making.** The CPRA calls for new regulations governing consumers' rights to access information and opt-out of automated decision-making. CalPPA is asking what activities constitute profiling or automated decision-making technology, what information should be provided in response to an access request and what the scope of consumers' opt-out rights entails. It also seeks input on the processes businesses should follow to facilitate opt-out and access requests.
- **Consumers' right to correct. Under the CPRA, consumers have the right to request the correction of inaccurate personal information.** To facilitate this new right, CalPPA requests comments regarding the frequency and circumstances pursuant to which a consumer may exercise this right, how businesses should respond and exceptions for businesses when a request is disproportionately burdensome.

Key Takeaways

Since the CPRA makes dozens of changes to the existing CCPA and CalPPA is not required to finalize the related regulations until July 1, 2022, businesses must remain adaptable and alert as regulations are clarified in the coming months. CalPPA's invitation to submit feedback during the public comment period presents an opportunity for businesses to potentially influence the ultimate regulations.

Return to Table of Contents

UK Government Launches Public Consultation in Planned GDPR Reform

On September 10, 2021, the U.K. Department for Digital, Culture, Media and Sport (DCMS) announced that the U.K. government has launched a public consultation on the proposed reform of U.K. data protection laws. Reform could prompt the European Commission (EC) to reconsider the adequacy decision it made on June 28, 2021, which allowed the free flow of personal data to continue between the European Economic Area (EEA) and the U.K. following the nation's formal withdrawal from the EU. Organizations could face significant, additional compliance costs if U.K. adequacy is not renewed, suspended or even repealed.

Background

On January 31, 2020, the U.K. left the EU with a transition period ending on December 31 of that year. In order to avoid any immediate disruption to the transfer of personal data between the U.K. and the EU, the EU General Data Protection Regulation (EU) 2016/679 (EU GDPR) was mirrored into U.K. domestic law through amendments to the Data Protection Act 2018 and the passing of the Data Protection, Privacy Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, resulting in the U.K. GDPR. On June 28, 2021, the EC announced that the U.K. satisfied the "adequacy" standard for transborder data flows out of the EU, determining that the U.K. had implemented equivalent and adequate safeguards for the protection of personal data. This enabled the free flow of data to continue between the U.K. and the EEA for four more years (or less if the EC determines that U.K. safeguards are no longer adequate).

In the consultation, the U.K. government made its intention clear to reform the U.K. GDPR and, in the words of then-Digital Secretary Oliver Dowden, "create a new world leading data regime that unleashes the power of data across the economy and society."

Proposed Reforms

In the September 10 consultation, the U.K. government grouped its reforms into five key areas:

1. **Reducing barriers to responsible innovation.** For example, the government proposes to create a limited and exhaustive list of legitimate interests for which organizations can use personal data without applying the balancing test. There are nine legitimate interests specified, which include, *inter alia*, reporting criminal acts, using analytics cookies, anonymizing personal data and improving products or services.
2. **Reducing burdens on businesses and delivering better outcomes for people.** The government proposes replacing the current accountability framework with a risk-based framework based on "privacy management programs." Specific compliance requirements would be replaced by more flexible measures. For instance, the requirement to appoint a data protection officer would be replaced by a requirement to designate a suitable individual, or individuals, to be responsible for an organization's privacy management program and data protection compliance. In addition, the requirement to undertake data protection impact assessments would be replaced by a requirement to develop approaches to identify and minimize data protection risks that reflect an organization's specific circumstances. Furthermore, the requirement to create and maintain records of processing activities would be replaced by a requirement to maintain records in a way that reflects the volume and sensitivity of personal data handled in line with a privacy management program.
3. **Boosting trade and reducing barriers to data flows.** For example, the government proposes to create its own adequacy decisions to facilitate the free transfer of personal data between the U.K. and its trading partners. Some of the government's proposals overlap with questions raised by the U.K. Information Commissioner's Office (ICO) in its consultation on international transfers.[1]
4. **Delivering better public services.** This section covers, *inter alia*, issues regarding the processing of personal data in light of the COVID-19 pandemic (, how private companies and public health authorities interact to share personal data).
5. **Reform of the ICO.** In relation to data breach reporting, the government proposes a new materiality threshold to mitigate the problem of "over-reporting," which currently places a significant burden on the ICO (*i.e.*, a breach would only be reportable where there is a "material risk" to individuals (rather than a "risk" under the GDPR and the current U.K. GDPR)). The requirement to consult the ICO prior to carrying out any high-risk processing, and the related penalties for failing to do so, would also be repealed.

Key Takeaways

Despite the number of proposals, which do include some significant changes to the U.K. GDPR, DCMS remains confident that the U.K. can retain its adequacy decision on the basis that "European adequacy does not mean verbatim equivalence of laws" and "a shared commitment to high standards of data protection is more important than a word-for-word replication of EU Law." It is certainly arguable that many of the underlying principles of the U.K. GDPR are retained in the proposed reforms outlined in the consultation (, the data protection principles, data subject rights and lawful bases of processing have been preserved) and other concepts remain unchanged (, the distinction between processors and controllers and the definition of personal data). However, any form of change to the U.K. GDPR is unlikely to be viewed favorably by the EC, which is under an obligation to continuously monitor the equivalence of the U.K. against EU data protection laws.

If the U.K. adequacy were to not be renewed, suspended or repealed, organizations would face significant, additional compliance costs involving their EEA-based and U.K.-based operations. This would include the obligation to carry out transfer impact assessments and data transfer agreements with additional, supplementary safeguarding measures (, using the EC standard contractual clauses or the binding corporate rules for intra-group data transfers). If the U.K. adequacy were to be retained, any reform to the U.K. GDPR must not hinder the U.K. providing a legal standard of data protection commensurate to that of the GDPR.

The U.K. government has asked interested parties to submit their responses to the consultation by November 19, 2021. Responses can be submitted via DCMS' online survey platform, by email to DataReformConsultation@dcms.gov.uk or by writing to Domestic Data Protection team, DCMS, 100 Parliament Street, London SW1A 2BQ.[2]

Return to Table of Contents

[1] This was covered in our August 2021 *Privacy & Cybersecurity Update*.

[2] The consultation and further information can be found on the government website.

Seventh Circuit Rules No Fourth Amendment Violation in Case Involving Warrantless Surveillance of IP Address Data

On September 8, 2021, the U.S. Court of Appeals for the Seventh Circuit ruled in *United States v. Soybel*[3] that using a pen register to identify IP addresses visited by a criminal suspect's own IP address does not constitute a Fourth Amendment search requiring a warrant. The suspect's IP address was routed through a third-party internet service provider, destroying any expectation of privacy in the routing information that the pen register captured. The court likened the use of IP address pen registers to telephone pen registers, the warrantless use of which to capture phone numbers dialed by a criminal suspect was upheld by the Supreme Court in *Smith v. Maryland*.[4]

Background

Industrial-supply company W.W. Grainger experienced several cyberattacks on its computer systems in 2016. Grainger identified the single extra-network IP address associated with each intrusion and reported the cyberattacks to the FBI, which determined that the IP address originated from the apartment building of Edward Soybel, a disgruntled former Grainger employee. To confirm whether the attacks were attributable to Mr. Soybel (and not to another apartment in his building), the government applied for an order under the Pen Register Act[5] to install IP pen registers — which can detect the IP addresses reached from a specific computer — and collect information regarding solely whether and when he accessed Grainger's systems. The Illinois federal court district judge granted the pen register application upon a showing of relevance (as required under the Pen Register Act), and without a finding of probable cause.

The apartment building's internet service provider installed the pen registers in the building without entering Mr. Soybel's unit, with the pen registers showing that only his private IP address attempted to connect to Grainger's system at the same times that the building's IP address tried to breach the company's firewall. Mr. Soybel was subsequently indicted for violations of the Computer Fraud and Abuse Act.[6]

Mr. Soybel moved to suppress the pen register evidence and its fruits at trial. His motion was denied, and a jury convicted him of violating the Computer Fraud and Abuse Act. He appealed, arguing that the warrantless use of pen registers constituted an unreasonable search under the Fourth Amendment. The Seventh Circuit affirmed the district court's decision and held that the use of a pen register to identify IP addresses is not a Fourth Amendment search requiring a warrant.

No Fourth Amendment Violation

The court noted that not every law enforcement investigation is a Fourth Amendment search requiring a warrant premised on probable cause; a Fourth Amendment search only occurs when an individual has a reasonable expectation of privacy in the object of the challenged search. In *Smith*, the Supreme Court decided that an individual generally "has no legitimate expectation of privacy in information he voluntarily turns over to third parties,"[7] and the government may generally acquire such information without creating a Fourth Amendment search. The Supreme Court also held that the government's use of pen registers to capture the numbers a criminal suspect dials from a landline phone is not a Fourth Amendment search requiring a warrant, where the numbers dialed were routed through and recorded by the phone company. Similarly, the Seventh Circuit here found that Mr. Soybel had no reasonable expectation of privacy in the IP address routing information captured, as it was routed through his internet service provider.

Mr. Soybel argued that his case was more similar to *Carpenter v. United States*[8] than *Smith*. In *Carpenter*, the Supreme Court ruled that the government obtaining historical cell-site location information without a warrant constituted an unconstitutional search. The Seventh Circuit rejected this argument, stating that the warrantless collection of historical cell-site information poses significant privacy concerns not applicable here, as such cell data provides a detailed record of a person's location. IP pen registers, on the other hand, cannot track a person's past movements.

Return to Table of Contents

[3] *United States v. Edward Soybel*, No. 19-1936, U.S. Ct. App. (7th Cir. 2021).

[4] *Smith v. Maryland*, 442 U.S. 735 (1979).

[5] 18 U.S.C. §§ 3121 *et seq.*

[6] 18 U.S.C. § 1030.

[7] 442 U.S. at 743–44.

[8] *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

Court Rejects Policyholders' Bid for Certain Third-Party Discovery in Coverage Battle Over Hacking Incident

A federal district court denied policyholders' attempt to seek certain discovery from its nonparty insurance broker in an action seeking coverage for a hacking incident.

On September 20, 2021, a U.S. District Court for the Southern District of New York judge ruled that plaintiffs Virtu Financial Inc. and Virtu Americas LLC (Virtu), financial services providers, were not entitled to discovery from their nonparty insurance broker. The plaintiffs were seeking certain documents that the court had already ruled were not relevant to Virtu's insurance coverage action alleging that its insurer, Axis Insurance Company (Axis), wrongfully denied coverage for a nearly $11 million loss stemming from a hacking incident.[9]

The Hacking Incident

According to Virtu's complaint, in May 2020 the company's computer systems were breached by hackers, who gained access to the email account of a Virtu executive. Posing as the executive, the hackers allegedly sent a series of emails from the executive's account to Virtu's accounting department directing them to issue two wire transfers totaling nearly $11 million to Chinese banks. The accounting department, believing the requests to be legitimate, executed the wire transfers, after which the company investigated and found to be fraudulent. While Virtu was able to recover a portion of the funds, according to the complaint approximately $6.9 million remains outstanding, in addition to the significant forensic and legal costs incurred to address the hacking incident.

Virtu's Insurance Claim and the Coverage Action

Virtu noticed the incident to Axis, which issued a financial institution bond insurance policy to the company, which provided "Computer Systems Fraud" coverage, with a limit of $10 million, and "Social Engineering Fraud" coverage, with a limit of $500,000.

As stated in the policy, the Computer Systems Fraud aspect covered "[l]oss resulting directly from a fraudulent (1) entry of Electronic Data or Computer Program into, or (2) change of Electronic Data or Computer Program within any Computer System operated by the Insured, . . . provided that the entry or changes causes (i) Property to be transferred, paid or delivered, (ii) an account of the Insured … to be added, deleted, debited or credited, or (iii) an unauthorized account or a fictitious account to be debited or credited." The Social Engineering Fraud aspect covered "[l]oss resulting directly from an Employee having, in good faith, transferred … money … from the Insured's account to a person or account outside of the Insured's control, in reliance upon a Social Engineering Fraud Instruction directing such transfer[.]"

Axis accepted coverage under the Social Engineering Fraud policy but denied coverage under the Computer Systems Fraud policy on the basis that the loss was not directly caused by the hacking itself, but rather by the Virtu accounting department employees who issued fraudulent transfers.

On August 10, 2020, Virtu filed suit in the U.S. District Court for the Southern District of New York against Axis seeking coverage under the Computer Systems Fraud policy for the hacking incident.

Court Rejects Virtu's Attempt to Seek Certain Discovery From Third-Party Broker

On September 20, 2021, the court ruled that Virtu could not obtain documents from a third party that the court previously held were not relevant to the parties' dispute. Virtu had served a subpoena on its broker, party Marsh & McLennan Companies (Marsh) seeking, among other things, (1) Axis' Computer Systems Fraud and Social Engineering Fraud policy forms for policies issued after Virtu noticed the hacking incident to Axis and (2) documents concerning any actual or proposed changes to Axis' Computer Systems Fraud and Social Engineering Fraud policy forms after Virtu noticed the hacking incident to Axis. A prior discovery order, issued August 30, 2021, denied Virtu's motion to compel production of similar categories of documents from Axis, reasoning that (1) evidence of policy form changes imposed after Virtu filed its insurance claim had no bearing on the parties' intent with respect to the meaning of the policy terms; (2) evidence showing later changes to the policy language for use with other customers had no bearing on whether Axis acted in bad faith in selling and administering the policy vis-a-via Virtu; and (3) the cases relied on by Virtu in support of its request are inapposite because they do not involve similar facts or require production of post-claim changes to a policy.[10] "Virtu may not circumvent this Court's prior ruling on its motion to compel by demanding those same irrelevant documents from a third party," the court explained.

[9] *Virtu Financial, Inc., et ano v. Axis Insurance Co.*, No. 1:20-cv-06293 (S.D.N.Y.), ECF No. 93.

[10] The prior discovery order also found certain portions of Axis' underwriting file for the policy at issue discoverable. Therefore, consistent with that order and the September 20 order, the same portions of Marsh's underwriting file for the policy – which Virtu sought in the subpoena – should be discoverable by Virtu.

Key Takeaways

As this decision demonstrates, courts in coverage disputes may be hesitant to permit broad discovery into the meaning of disputed policy provisions. Therefore, it is imperative that insurers and policyholders have a clear and mutual understanding of the scope of cyber, computer fraud and/or social engineering coverage provided under a policy before a loss arises in order to avoid battles over policy language.

Return to Table of Contents

Recent US Government Actions Remind Companies of Possible US Sanctions Risks Related to Facilitating Ransomware Payments

As part of its "whole-of-government" approach to confronting the ransomware threat, the U.S. government has in recent years leveraged economic sanctions enforced by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) as a tool to disrupt and dissuade ransomware threat actors. To confront the growing threat from malign cyber activities targeting U.S. interests, in April 2015 and December 2016, the U.S. president issued two executive orders giving the U.S. secretary of the Treasury, through OFAC, the authority to impose sanctions on persons engaging in malicious cyber activities, including ransomware.[11]

Most recently, on September 21, 2021, OFAC designated SUEX OTC, S.R.O (SUEX), a cryptocurrency exchange, under its cyber-related authorities.[12] OFAC alleged that SUEX facilitated financial transactions for ransomware actors, including transactions involving illicit proceeds from at least eight ransomware variants.[13] This was the first such designation by OFAC of a cryptocurrency exchange, and OFAC identified numerous bitcoin addresses associated with the company. The designation of SUEX means that U.S. Persons[14] are prohibited from dealing with SUEX, or any person owned, directly or indirectly, in the aggregate, 50% or more by SUEX.[15] Any assets of SUEX that come into the control or possession of a U.S. Person must be blocked (*i.e.*, frozen) and cannot be transferred without authorization from OFAC.[16] Other transactions involving a U.S. nexus and SUEX are also generally prohibited.

On the same day as SUEX's designation, OFAC issued updated guidance to ransomware victims and third parties that may be involved in ransomware payments, such as exchanges, banks and insurers, regarding the potential sanctions risks of facilitating ransomware payments (the OFAC Advisory).[17] The OFAC Advisory strongly discourages ransomware payments, encourages companies to strengthen defensive and resilience measures to prevent and protect against ransomware attacks, and encourages the timely reporting of ransomware incidents to law enforcement and other relevant U.S. government agencies.[18] In designating SUEX, the U.S. Department of Treasury put exchanges and other third parties on alert that the U.S. will continue to seek to disrupt and hold accountable persons that facilitate ransomware activities.[19] Consistent with the OFAC Advisory and other applicable requirements, companies should put in place policies and procedures, including anti-money laundering and sanctions controls, to prevent sanctioned persons and illicit actors from exploiting their platforms.

Return to Table of Contents

[11] Exec. Order No. 13694, 80 Fed. Reg. 18,077, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" (April 1, 2015); Exec. Order No. 13757, 82 Fed. Reg. 1, "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities" (Dec. 28, 2016).

[12] OFAC, "Publication of Updated Ransomware Advisory; Cyber-Related Designation," U.S. Department of the Treasury (Sept. 21, 2021).

[13] Press Release, U.S. Department of the Treasury, "Treasury Takes Robust Actions To Counter Ransomware," (Sept. 21, 2021), (Treasury Press Release).

[14] A U.S. Person is any U.S. citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States. *See, e.g.*, 31 C.F.R. § 560.314.

[15] OFAC, "Revised Guidance on Entities Owned by Persons Whose Property and Interests in Property Are Blocked," U.S. Department of the Treasury (Aug. 13, 2014).

[16] Title to the blocked property remains with the target, but the exercise of powers and privileges normally associated with ownership is prohibited without authorization from OFAC.

[17] OFAC, "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," U.S. Department of the Treasury (Sept. 21, 2020).

[18] *See id.*, at 1, 4-5.

[19] *See* Treasury Press Release, supra note 3.

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

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

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@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