Skadden

Privacy & Cybersecurity Update

1 California's Attorney General Announces Draft Regulations To Accompany the California Consumer Privacy Act; Governor Signs Amendments

4 Requirements on the Use of Cookies Clarified by the CJEU

5 FDA Warns of Security Vulnerabilities in Software Widely Used in Medical Devices

6 District Court Holds That Fantasy Sports Company's Email Spoofing Scam Loss is Not Covered by Crime Insurance Policy

California's Attorney General Announces Draft Regulations To Accompany the California Consumer Privacy Act; Governor Signs Amendments

California's attorney general has proposed draft regulations for implementing the California Consumer Privacy Act (CCPA). In a separate development, Gov. Gavin Newsom signed the amendments to the legislation that were passed in September by the state's legislature.

On October 10, 2019, the California Office of the Attorney General published draft regulations to accompany the CCPA. In addition to filling some of the gaps left by the original legislation, the regulations include substantial requirements not found in the statute. The draft regulations focus most heavily on three areas: (1) notice to consumers, (2) business practices for handling consumer requests and (3) verification of requests. The regulations also touch on special requirements regarding minors and practices to prevent discrimination against consumers who opt out of having their personal information sold.

The draft regulations are open for public comment and will likely be revised to some degree before they go into effect. There will be four public hearings for comments throughout California from December 2-5, 2019, and written comments can be submitted by December 6. If substantial changes are made to the regulations, California's rulemaking process requires an additional comment period before they are finalized.

Notice to Consumers

The regulations outline four different types of notice to be provided to consumers:

- initial notice given at the time of collection;
- notice to opt out of the sale of personal information;
- notice of financial incentives; and
- a privacy policy.

Each of these notices must be presented in a way that is understandable to an average consumer, easily visible or accessible, available in the languages in which the business conducts its ordinary business and accessible to consumers with disabilities.

Initial Notice

According to the draft regulations, initial notice must include the categories of personal information to be collected and the business or commercial purposes for which each category will be used. In addition, the notice must include a link to the business's privacy policy.

Notice to Opt Out

Businesses that currently (or may in the future) sell consumers' personal information must provide a notice to opt out, which allows consumers to direct the business to stop selling their personal information and to refrain from doing so in the future. If the business sells personal information, the notice must include a link titled "Do Not Sell My Personal Information" or "Do Not Sell My Info."

If a business does not collect information directly from consumers it does not need to provide a notice. However, if a business receives personal information from third-party sources, before the business may sell that information it must either contact the consumer directly to provide a notice of the right to opt out or contact the source of the personal information to confirm that the source provided a notice to the consumer when it collected the information. The business must obtain signed attestations from the source describing the notice and retain those attestations for at least two years. In addition, the consumer must be able to access the attestations upon request.

Notice of Financial Incentives

Businesses may offer financial incentives to consumers who allow the business to sell their personal information. The proposed regulation makes clear that if a business offers financial incentives, it must provide a notice describing the incentive, including its material terms, instructions on how to opt in to and withdraw from the incentive and sale, and an explanation of why the CCPA permits the incentive.

Privacy Policy

The draft regulations also have expanded the required information that a business must include in its privacy policy.

- The business must post the policy online through a conspicuous link using the word "privacy" on its website homepage or on the landing page of a mobile application.
- The policy must explain consumers' right to know about personal information collected, disclosed or sold. This requirement includes providing a list of the categories of consumers' personal information that the business has collected in the preceding 12 months.
- For each category of personal information collected, the business must provide: the categories of sources from which that information was collected, the commercial purpose(s) for the information collected and the categories of third parties with whom the business shares personal information.
- The policy must include an explanation of how a consumer can designate an authorized agent to make a request under the CCPA on the consumer's behalf. Notably, this requirement goes beyond simply stating that a consumer may use a third-party agent to opt out of the sale of personal information. Instead, it implies that a business must provide a method for facilitating a third-party opt-out as well.
- For businesses that collect personal information of 400,000 or more consumers, the regulations require additional disclosures related to the number of consumer requests and average response times.

Business Practices for Handling Consumer Requests

The CCPA and accompanying draft regulations provide for two explicit rights for consumers: the right to know and the right to deletion. The right to know entitles consumers to request that a business disclose personal information that it has about the consumer. The right to deletion entitles consumers to request that a business delete personal information about the consumer that the business has collected.

Under the draft regulations, a business must provide at least two designated methods for submitting these requests. Acceptable methods include a toll-free phone number, a link or form available through the business's website, a designated email address, a form submitted in person or a form submitted through the mail. However, one of the methods chosen must reflect the manner in which the business primarily interacts with the consumer. In addition, the business must maintain records of consumer requests and how it responded to those requests for at least 24 months.

Upon receiving a request to know or a request to delete, the business must confirm receipt within 10 days and provide information about how the request will be processed. The information provided must describe the business's verification process and state when the consumer should expect a response. If the business is unable to verify the identity of the requestor, it cannot disclose any personal information and may deny the request. The business has 45 days to respond to the request, which includes the time taken to complete consumer verification. Note that unlike a request to know or delete, a request to opt out need not be a verifiable consumer request.

The Right To Know

When responding to a request to know, the business must provide an individualized response to the consumer detailing:

- the categories of sources from which it collected the personal information;
- the business or commercial purpose for which it collected the personal information;
- the categories of third parties to whom the business sold or disclosed the category of personal information for a business purpose; and
- the business or commercial purpose for which it sold or disclosed the category of personal information.

This disclosure must provide consumers with a meaningful understanding of the categories listed.

The Right To Request Deletion

Businesses must comply with a consumer's request to delete their personal information by de-identifying personal information, aggregating the personal information, or permanently and completely erasing the personal information on its existing systems with the exception of archived or backup systems (in which case deletion may be delayed until the archived or backup system is next accessed or used). In its response to a consumer's request to delete, the business must specify the manner in which it has deleted the personal information. In the event that a business denies a consumer's request to delete, it must inform the consumer that it will not comply with the consumer's request and describe the basis for the denial, including any statutory and regulatory exceptions; delete the consumer's personal information that is not subject to the exception; and not use the consumer's retained personal information for any other purpose than provided for by that exception.

Verification of Requests

Businesses must use reasonable methods to verify that the person making a request to know or delete is the consumer about whom the business has collected information. The draft regulations suggest that the more sensitive the information, the more rigorous the verification process will be. In other words, businesses should not release sensitive information without being very certain of the identity of the individual requesting the information. If a business cannot verify the identity of a person making a request for access, the business may proceed as if the consumer requested disclosure of only the categories of personal information, as opposed to the content of such personal information. If a business cannot verify a request for deletion, the business should treat the request as one to opt out of the sale of personal information.

Password-Protected Accounts

If the consumer making a request has a password-protected account with the business, the business can verify the consumer's identity by having the individual re-authenticate themselves. For this purpose, the business can utilize its existing re-authentication procedures. However, should the business suspect malicious or fraudulent activity, further verification is required.

Non-Account Holders

For requests from consumers without an account with the business, the regulation sets out three categories of required verification.

- For requests for categories of personal information, businesses need to verify identity "to a reasonable degree of certainty." This requires at least two matching data points provided by the consumer with reliable data held by the business.
- For requests to obtain actual data held, businesses need to verify identity "to a reasonably high degree of certainty." This requires matching at least three data points and obtaining a signed declaration under penalty of perjury.
- For requests for deletion, the degree of verification varies based upon the sensitivity of the personal data and the risk of harm posed by unauthorized deletion (for example, deletion of sentimental family photographs versus browsing history). Prior to deleting personal information, the business must provide a double opt-in process to confirm the deletion request.

Special Regulations Regarding Minors and 'Non-Discrimination'

Minors

The regulations set special requirements for selling the personal information of minors and distinguish between two categories of minors: those under 13 years of age and those between 13 and 16 years of age.

Businesses that knowingly collect or maintain the personal information of children under 13 must determine that the person authorizing the sale of the information is the child's parent or guardian. The draft regulations provide several methods for doing so, including providing a consent form to be signed by the parent or guardian under penalty of perjury, having a parent or guardian call a toll-free number and verifying a parent or guardian's identity by checking a government-issued ID.

Alternatively, minors between the ages of 13 and 16 need only be made aware of their ability to opt in to the sale of their personal information. When a business receives a request to opt in from such a minor, the business must inform the minor of the right to opt out at a later date and the process for doing so.

Non-Discrimination

Although the draft regulations prohibit different treatment of consumers who allow their personal information to be sold than those who opt out under the CCPA, the regulations allow businesses to offer a price or service difference if it is reasonably related to the value of the consumer's data (and provide an outline for calculating the value of consumer data for this purpose).

For example, suppose a video streaming business offers a free service and a premium service that costs $10 a month. If only the consumers who pay for the premium service are able to opt out of the sale of their personal information, the practice is discriminatory, unless the monthly payment is reasonably related to the value of the consumer's data to the business. This scheme prevents consumers from being penalized for choosing to opt out of the sale of their personal information.

Amendments Signed by Governor

On October 11, 2019, Gov. Newsom signed several amendments described in our September 2019 *Privacy and Cybersecurity Update*.[1] The amendments sought to clarify elements of the CCPA regarding excluding certain employee-related information, excluding employees of business partners and business clients, verifying consumer requests, limiting the catch-all in the definition of personal information and expanding the publicly available information exclusion, among others.

Key Takeaways

With the CCPA taking effect on January 1, 2020, many businesses eagerly have awaited the attorney general's regulations. While the draft regulations provide some clarity to the act, they also add some additional hurdles for CCPA compliance. Moving forward, businesses should begin to draft requisite notices, update their privacy policies, and put in place procedures for handling and verifying consumer requests. However, it is important to note that these regulations are subject to public comment and are likely to be updated or amended before becoming law.

Return to Table of Contents

[1] See September 2019 *Privacy and Cybersecurity Update* here.

Requirements on the Use of Cookies Clarified by the CJEU

The Court of Justice of the European Union (CJEU) has clarified requirements regarding the use of cookies, stating that consent cannot be obtained by using preselected check boxes.

Background

In the process of entering an online lottery run by Planet49 GmbH (Planet49), internet users were provided with two consent declarations, each accompanied by a check box. The first consent declaration check box was not preselected and involved agreeing to receive third-party advertising. The second consent declaration check box was preselected and concerned agreeing to the installation and use of cookies on the internet user's device. Participation in the lottery required the first consent declaration to be checked off, but not the second.

A claim was brought in German court against Planet49, arguing that the check box consent methods used by the company did not satisfy the necessary requirements under applicable e-privacy and data protection laws. Questions were subsequently referred by the German court to the CJEU regarding the validity of consent to use cookies and to determine what information needed to be given to internet users about cookies. The CJEU handed down its judgement in the case[2] on October 1, 2019.

CJEU Decision

Preselected Check Boxes are Not Valid Consent

The CJEU concluded that the consent requirements laid out in the EU's e-Privacy Directive, read in conjunction with the EU's Data Protection Directive and subsequently the General Data Protection Regulation (GDPR), are not fulfilled by preselected check boxes.

The CJEU noted that while the e-Privacy Directive states that the user must give their consent to use cookies, it does not indicate how that is to be done. The CJEU, therefore, considered the meaning of consent, including examining how it is defined under the Data Protection Directive and GDPR (under which the court noted that active consent is now expressly required), and concluded that consent requires an action to be taken by the user. Hence, a preselected check box does not provide valid consent. The CJEU further clarified that the action taken by the user must

[2] *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH.*

relate specifically to the use of cookies and cannot include other purposes. Consequently, clicking the button agreeing to participate in the lottery was not a valid action for giving consent.

Consent Requirements for Cookies Apply to Both Non-Personal and Personal Data

The CJEU agreed with the advocate-general's conclusion that the e-Privacy Directive does not differentiate between personal data (as defined under the Data Protection Directive and the GDPR) and other forms of data. This is because the e-Privacy Directive refers to storing and gaining access to "information" rather than specifying "personal data." Furthermore, the court adopted the advocate-general's wording that the e-Privacy Directive "aims to protect the user from interference with his or her private sphere, regardless of whether or not that interference involves personal data." Consequently, the consent requirements for cookies apply to both non-personal and personal data equally, according to the CJEU's ruling.

The User Must Be Informed of Cookie Duration and Third-Party Access to Cookies

The CJEU held that a user must be informed of both the duration that cookies operate and of third-party access to the cookies. The e-Privacy Directive requires users to be provided with "clear and comprehensive information" prior to giving their consent. The court once again looked to the information requirements in the Data Protection Directive and the GDPR to clarify whether or not "clear and comprehensive information" included cookie duration and third-party access.

The CJEU noted that while the Data Protection Directive did not explicitly state that the duration of the data processing must be provided to a user, such information should be provided to meet the requirement of fair data processing. That interpretation is supported by the GDPR's requirement that users be provided with information relating to the period for which personal data will be stored, or, if that is not possible, the criteria used to determine such period.

Regarding third-party access, the CJEU stated that both the Data Protection Directive and the GDPR require users to be informed of the recipients or categories of recipients of their data.

Freely Given Consent

The GDPR makes clear that a user's consent is presumed not to be freely given if the performance of a contract is dependent on consent being given, despite it not being necessary for the performance of the contract. That may have been the case on the *Planet49* facts, as participation in the lottery required the consent declaration for the first check box — agreeing to receive third-party advertising — to be selected. The CJEU did not, however, rule on this issue, as it had not been referred the question, thus leaving it to the referring court to decide. The advocate-general did, however, note that in his view processing the personal data for the purposes of third-party advertising was necessary because the lottery was based on the collection of personal data for advertising purposes.

Key Takeaways

Website operators will need to revisit their cookie notice and methods for receiving consent to ensure that they are (1) not using preselected check boxes and (2) getting consent for the use of cookies with regard collecting both personal and non-personal data for a clearly established purpose. They also will have to ensure that users are informed of the duration that cookies will operate for and the third parties with which they will be shared. Finally, it is worth noting that the e-Privacy Directive is due to be replaced by the e-Privacy Regulation (expected in 2020), which may bring further changes regarding the use of cookies.

Return to Table of Contents

FDA Warns of Security Vulnerabilities in Software Widely Used in Medical Devices

After researchers identified security vulnerabilities in commonly used software for connecting devices to networks, the U.S. Food and Drug Administration (FDA) issued a warning on the security of medical devices.

On October 1, 2019, the FDA issued a warning about security issues present in a decades-old piece of software that is heavily used in medical devices. If exploited, the vulnerability, called "URGENT/11," could be used by remote attackers to compromise the safety and security of network-connected medical devices or hospital networks.

Vulnerabilities in Software

Researchers for Armis Labs originally identified 11 software vulnerabilities in software called IPnet, which originally was developed decades ago. The IPnet software falls into a category of code called a "TCP/IP stack," which allows a given device to connect to a network, such as the internet or a local LAN network. Since its original development, IPnet reportedly has been incorporated into a wide range of operating systems commonly used on "always on" devices, such as medical devices.

Some researchers think that these vulnerabilities could affect more than 200 million devices, including industrial controllers, infusion pumps, patient monitors, firewalls, MRI machines and printers. Partly because this code is so foundational, it has gone unchanged for many years, and software has evolved to fit the myriad applications and products in which it is used.

The Cybersecurity and Infrastructure Security Agency (CISA), operating within the Department of Homeland Security, released an advisory about the URGENT/11 vulnerabilities in July 2019. Following that initial advisory, the FDA became aware that the vulnerabilities affect operating systems in a number of medical devices and issued its warning.

FDA Warning

The FDA's warning describes the vulnerability, identifies a number of operating systems in which the software is known to be embedded and makes certain recommendations for device manufacturers, health care providers, and their staff and patients.[3] The recommendations include:

For device manufacturers:

- assessing the vulnerability of their products;
- working with operating system vendors to obtain any available software patches to address the issue;
- working with health care providers to identify affected devices already in use and developing ways to reduce risk to acceptable levels; and
- reporting affected devices to CISA.

For health care providers:

- advising patients who use medical devices that may be affected and reminding them to seek medical help immediately if the device seems to be operating improperly; and
- working with device manufacturers to determine which devices are affected and develop risk mitigation plans.

For health care staff:

- monitoring their network traffic for indications that an attack is taking place; and
- using firewalls, virtual private networks and/or other measures to minimize exposure to attacks exploiting the vulnerability.

For patients:

- talking to their health care providers to determine if their devices are affected; and
- seeking medical help immediately if they think the operations or functions of their medical devices change unexpectedly.

At this time, the FDA says that it has not received any reports of actual data breaches related to these vulnerabilities.

Key Takeaways

Medical devices represent a growing segment of the internet-of-things market, and the FDA's announcement signals that the regulator is active in the cybersecurity space. The agency is monitoring security developments as they relate to medical devices, and health care providers and manufacturers should remain mindful of cybersecurity involving their devices, including potential URGENT/11 vulnerabilities. Failure to do so — especially after warnings from the FDA — could create liability if devices are attacked by exploiting these vulnerabilities.

Return to Table of Contents

District Court Holds That Fantasy Sports Company's Email Spoofing Scam Loss is Not Covered by Crime Insurance Policy

A Nevada federal judge recently held that an insurer does not owe coverage under its crime policy for a roughly $180,000 loss suffered by its policyholder as a result of an email spoofing scam.

On September 11, 2019, the U.S. District Court for the District of Nevada held that fantasy sports company Sanderina LLC and Sanderina II, LLC (Sanderina) was not entitled to coverage under its crime policy issued by Great American Insurance Company (Great American) for an approximately $180,000 loss sustained as a result of an email spoofing scam.[4]

[3] The text of the warning is available here.

[4] *Sanderina, LLC v. Great Am. Ins. Co.*, No. 2:18-cv-00772-JAD-DJA, 2019 WL 4307854 (D. Nev. Sept. 11, 2019).

Email Spoofing Scam Loss and Sanderina's Insurance Claim

In 2017, Sanderina's controller received a series of fraudulent emails from an unknown third party posing as the company's majority owner by using an email address nearly identical to that of the majority owner. Over the course of eight days, the imposter sent emails requesting that the controller make six wire transfers to the fraudster's bank account. The controller, believing that the fraudulent instructions were legitimate, wired $260,000 in Sanderina funds to a bank account under the fraudster's control. The company eventually discovered that it had fallen victim to a scam and was able to recover approximately $82,000 of the stolen funds. Sanderina then hired a cybersecurity firm to investigate the incident, but the firm could not find any instance of unauthorized access to the company's computer system.

Shortly after discovering the fraud, Sanderina made a claim for the loss under its crime policy issued by Great American. As relevant here, the crime policy provides the following coverages: (1) computer fraud coverage for losses "resulting directly from the use of any computer to impersonate you, or your authorized officer or employee, to gain direct access to your computer system, or to the computer system of your financial institution, and thereby fraudulently cause the transfer of money;" (2) forgery or alteration coverage for losses "resulting directly from forgery or alteration of checks, drafts, promissory notes, or similar written promises, orders, or directions to pay a sum certain in money;" and (3) funds transfer fraud coverage for losses "resulting directly from a fraudulent instruction directing a financial institution to transfer, pay or deliver funds from your transfer account." Great American denied coverage on the basis that the email spoofing loss did not fall within the terms of the policy.

Sanderina's Coverage Action and Great American's Motion for Summary Judgment

Sanderina filed suit against Great American in Nevada state court seeking coverage under the policy for the email spoofing loss. After removing the case to federal court, Great American moved for summary judgment. The court granted Great American's motion, holding that the plain language of the policy does not cover a loss resulting from email spoofing scam incidents.

The court concluded that the policy's Computer Fraud coverage did not apply because the fraudster did not "gain direct access" to Sanderina's computer system, citing the testimony of the company's Federal Rule of Civil Procedure 30(b)(6) representative witness that neither Sanderina nor the cybersecurity firm it hired to investigate the incident found any evidence that the fraudster gained access to the company's computer system.

Sanderina argued that the forgery or alteration coverage nonetheless applied because the fraudulent emails contained directions to pay money. However, the court rejected that argument because the policy "unambiguously requires 'directions to pay a sum certain in money' to be 'similar' to 'checks, drafts [and] promissory notes,'" while also considering similar facts in another case in the Ninth Circuit, which previously concluded that emails containing directions to pay money were not similar to checks.

The court similarly concluded that the policy's funds transfer fraud coverage did not apply because (1) Sanderina is not a financial institution so the fraudulent instructions were not "sent or transmitted to a financial institution" as required by the policy's definition of "fraudulent instructions" and (2) the controller requested and knew about the transfers, so the fraudulent instructions were not "issued, forged or altered without [Sanderina's] knowledge or consent," as also required by the "fraudulent instructions" definition.

Key Takeaways

The issue of coverage under crime policies for loss resulting from email spoofing and other social engineering scams continues to be litigated with increasing frequency. While some courts have determined that such losses are covered, other courts have concluded that spoofing scams do not trigger coverage, with the court's decision in *Sanderina v. Great American* adding to this body of law. *Sanderina* may be valuable for insurers in future coverage disputes regarding losses arising from spoofing scams and other forms of social engineering fraud. The decision also may cause policyholders to revisit and attempt to clarify the scope of coverage intended for such incidents under their policies.

Return to Table of Contents

Privacy & Cybersecurity Update

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
213.687.5381
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

Amy Park
Partner / Palo Alto
650.470.4511
amy.park@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

Ivan Schlager
Partner / Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

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

Jen Spaziano
Partner / Washington, D.C.
202.371.7872
jen.spaziano@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
Four Times Square
New York, NY 10036
212.735.3000