Skadden

Privacy & Cybersecurity Update

Five Amendments to the California Consumer Privacy Act on Governor's Desk

The California State Assembly and Senate passed five of the many proposed bills seeking to clarify the California Consumer Privacy Act (CCPA) before it goes into effect on January 1, 2020. Gov. Gavin Newsom has until October 13, 2019, to sign or veto the bills.

As the 2019 California legislative session drew to a close, the legislature passed five amendments to the CCPA that must be signed or vetoed by the governor by October 13, 2019. While the amendments provide some clarity on certain issues, as well as some relief for companies that have only employees and not any consumers who are California residents, many of the more significant amendments that had been proposed by privacy advocates and businesses were not passed.

Exclusion of Certain Employee-Related Information

Under Amendment AB25, many of the CCPA requirements would not apply until January 1, 2021, for job applicants, employees, contractors, medical staff members, owners, officers and directors (the latter five roles also would become newly defined terms), provided their information is used solely in the context of their current or former role with a business. Although the definition of "contractors" is likely meant to include independent contractors working for a business, it is defined broadly as a natural person who provides any service to a business pursuant to a written contract. The amendment also would exclude personal information that qualifies as the emergency contact information of that individual, provided it is collected and used solely in the context of having an emergency contact on file. Finally, the amendment would exclude the personal information of relatives of an individual whose information is collected and retained for the purpose of administering benefits, provided the information is used solely for that purpose. The following CCPA provisions would still go into effect on January 1, 2020, for these individuals:

- the obligation to notify these individuals about the categories of personal information that the business collects and the purposes for which the information is used, at or before the point of collection;
- consent would still be required to collect additional categories of personal information or to use previously collected personal information for new purposes; and

- these individuals could still assert a claim under the CCPA's private right of action for cybersecurity incidents.

Exclusion of Employees of Business Partners and Business Clients

Similar to AB25, under Amendment AB135 many of the CCPA requirements would not apply until January 1, 2021, including when personal information is transmitted in business-to-business written or verbal communications or transactions relating to due diligence, or providing or receiving a product or service to or from the other business, and the personal information concerns an employee, owner, director, officer or contractor of that business. That individual would still be entitled to their right to nondiscrimination and right to opt out of the sale of such personal information. Such individuals could still exercise their private right of action under the law.

Verified Consumer Request (VCR)

While the California attorney general must still release guidance on the meaning of a verified consumer request (VCR), AB25 provides some additional guidance on VCRs, stating that a business, when responding to a VCR, may require authentication of the consumer that is reasonable in light of the nature of the personal information requested. The amendment also prohibits a business from requiring consumers to create a new account with the business in order to submit a VCR. However, if the consumer already maintains an account with the business, then the business may require the consumer to submit a request through that account. This change would be especially beneficial for consumer-facing companies reliant on online contacts.

The amendments also would permit the attorney general to establish rules and procedures on how to process and comply with VCRs for specific pieces of personal information relating to a household in order to address obstacles to implementation and privacy concerns. The current version of the CCPA contains minimal guidance on navigating the complexities of requests related to households as compared to a natural person, so this represents another important area for businesses to track going forward.

Limiting the Catch-All in the Definition of Personal Information

Under the CCPA, information is "personal information" if it is capable of being associated with, or could be reasonably linked, directly or indirectly, to a particular consumer or household. This definition was seen as extremely broad given today's advanced data mining technology. AB874 slightly narrows the definition by stating that the information must be "reasonably capable" of being associated with a particular consumer or household. Additionally, the amendment would specifically exclude de-identified or aggregate consumer information from the definition of personal information. The treatment of such information is somewhat unclear under the CCPA as currently written.

Expanding the Publicly Available Information Exclusion

The CCPA currently excludes "publicly available" information from personal information. However, a business can only rely on that exception if it is using the information "for a purpose that is compatible with the purpose for which the data is maintained and made available in the government records." Amendment AB874 would strike the "compatible purpose" requirement; meaning that a business could rely on that exception even if it used the publicly available information for a different purpose.

The Recall and Warranty Deletion Exception, and the Vehicle and Ownership Information Sale Exception

Under Amendment AB1146, a business could decline a consumer's personal information deletion request where retention of the personal information is required to fulfill the terms of a written warranty or product recall conducted in accordance with federal law. While the remainder of the amendment is directed toward vehicles, this deletion exception is not expressly limited to the vehicle context.

In addition, under this amendment, consumers would not have a right to opt out where vehicle information or ownership information is retained or shared between a new motor vehicle dealer and the vehicle's manufacturer for the purpose of effectuating, or in anticipation of effectuating, a repair covered by a warranty or recall. To remain within this exception, the new motor vehicle dealer and vehicle manufacturer could not sell, share or use the information for any other purpose. As a result, the same information could be subject to CCPA requirements where dealers use the information for other purposes, such as marketing or standard maintenance reminders. Vehicle information is defined as vehicle information number, make, model, year and odometer reading. Ownership information is defined as the name(s) of the registered owner(s) and their respective contact information.

Fair Credit Reporting Act (FCRA) Exception

The amendments clarify that, except for the private right of action for data breaches, the CCPA does not apply to an activity involving the collection, maintenance, disclosure, sale, communication or use of any personal information bearing on

a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living by (1) a consumer reporting agency; (2) a furnisher of information (as set forth in Section 1681s-2 of Title 15 of the United States Code) who provides information for use in a consumer report; and (3) a user of a consumer report. This exception would apply only to the extent that such activity by that agency, furnisher or user is subject to regulation under the FCRA and the information is not otherwise used, communicated, disclosed or sold, except as authorized by the FCRA.

Clarification to Notice Requirement

AB1146 also clarifies matters regarding the notice elements required in any privacy policy or description of California consumers' rights. The amendment confirms that the business need only describe (1) the categories of personal information it has collected about consumers generally (as opposed to the particular consumer viewing the privacy policy or description of rights) and (2) indicate that consumers have a general right to request the specific pieces of personal information that a business has collected about them, as opposed to requiring the actual specific pieces of information to appear in the privacy policy or description of rights.

Exemptions Clarification

AB1146 clarifies that a business is not required to (1) collect personal information that it would not otherwise collect in the ordinary course of its business, (2) retain personal information for longer than it would otherwise retain such information in the ordinary course of business, or (3) re-identify or otherwise link information that is not maintained in a manner that would be considered personal information. Currently, the CCPA only includes the language in (3) above.

Right to Nondiscrimination

AB1146 clarifies that for purposes of deciding whether a business is discriminating against those who exercise their data privacy rights, it is the value provided to the business, and not the value to the consumer, that is taken into account when determining whether differences are reasonably related to the value of consumer's data. As a result, businesses could charge consumers a different price or rate, or provide a different level or quality of goods or services to the consumer, if such differences were reasonably related to the value provided to the business by the consumer's data. Additionally, businesses could offer a different price, rate, level, or quality of goods or services to the consumer if the price or difference were directly related to the value provided to the business by the consumer's data.

Private Right of Action

The amendments clarify that class action lawsuits can be brought only for data breaches pursuant to California's data breach notification law if the personal information was nonencrypted and nonredacted. As currently drafted, the personal information only needs to be nonencrypted or nonredacted.

Consumer Access Requirement Clarifications and Electronic Relationship Exception

Amendment AB1564 would clarify that a business must make available to consumers two or more designated methods for submitting requests relating to the "Right to Request Disclosure of Information Collected" and the "Right to Disclosure of Information Sold," including, at a minimum, a toll-free telephone number. Additionally, if the business maintains a website, it must make the website available to consumers to submit requests for information required to be disclosed. The current wording of the CCPA only requires businesses to make a website address available. In addition, where a business operates (1) exclusively online and (2) has a direct relationship with a consumer from whom it collects personal information, that business only is required to provide an email address for submitting such requests. This amendment could save businesses substantial financial expense and operational complexity if they are not otherwise organized to process consumer contacts via telephone. Notably, businesses that fall into this category would still be required to make their websites available for consumers to submit requests, in addition to providing an email address.

Return to Table of Contents

CJEU Holds That 'Right to be Forgotten' Only Applies to Searches in the EU

The Court of Justice of the European Union (CJEU) has ruled that the requirement for a search engine operator to delist search results as a result of a successful "right to be forgotten" request does not automatically apply outside of the EU.

Background

European Union law provides that data subjects may, in certain circumstances, have their personal data erased under what is known as a "right to be forgotten" request (RTBF). This right has

now been codified by Article 17 of the European Union Regulation (EU) 2016/679 (GDPR).

The CJEU previously held in 2014 that the operator of a search engine is a data controller with regard to the processing of data carried out for an online search.[1] As a result, operators of a search engine are required, following an RTBF request by an individual, to delist links to an individual's personal information where the information is "inadequate, irrelevant or no longer relevant, or excessive."[2]

Following the 2014 ruling, Google only delisted links accessed through Google's EU domains, such as "google.co.uk" or "google.fr." The French data protection authority, the Commission Nationale de l'Informatique et des Libertés (CNIL), adopted the view that following a successful RTBF request, Google should delist applicable search results across all domains worldwide. In light of Google's continued failure to do so, the CNIL imposed a €100,000 fine. Google appealed this decision before the French Conseil d'État (the Council of State acting as the supreme court for administrative claims in France), arguing that the RTBF could not be applied outside of the EU's jurisdiction, and to do so would potentially compel search engine operators to contravene the laws of other jurisdictions. In turn, the Conseil d'Etat referred a number of questions regarding the territorial scope of the RTBF to the CJEU.

The CJEU's Decision

In line with the advocate general's opinion, the CJEU held that, following a successful RTBF request, Google, as the search engine operator, is not required by EU law to delist links to the relevant personal information on all of its domains globally. Rather, EU law only requires that delisting occurs across all EU member states.

The CJEU reached that decision by considering that:

1. the EU seeks to guarantee a high level of protection of personal data within the union.[3] In a globalized world, and with the internet being a global network, the listing of a link to personal information that those outside of the EU have access to could have a substantial effect on an individual within the EU. In light of this, the global delisting of personal information, subject to a successful RTBF request, would be the most effective way for the EU to guarantee a high level of protection of personal data. However, many jurisdictions outside of the EU do not recognize a RTBF or apply such a right differently;
2. the rights to privacy and protection of personal data must be balanced against other fundamental rights, particularly the freedom of information; and
3. the wording of the RTBF legislation[4] and broader data protection legislation does not envision that the RTBF would have a territorial scope beyond the EU. For instance, there are no means of cooperation established between the EU and non-EU states, as there are between EU member state supervisory authorities, to come to a joint decision on the balance of a data subject's right to privacy and protection of personal data against the interest of the public to have access to that information.

While the CJEU made clear that EU law does not require delisting globally, it also does not prohibit it. Consequently, an EU member state supervisory or judicial authority may still decide that it is appropriate to order a search engine operator, such as Google, to carry out a global delisting.

The CJEU also explained that search engine operators must take measures to ensure the effective protection of the data subject's fundamental rights to privacy and the protection of personal data. This means that the measures taken by the search engine operator must have the effect of preventing, or at least "seriously discouraging,"[5] internet users in the EU from gaining access to links connected to a successful RTBF action. The CJEU is likely concerned about the risk of individuals within the EU circumventing the delisting of search results by simply using a search engine domain name outside of the EU, such as by using "google.com" instead of "google.fr." This can be prevented, for example, by using geo-blocking. a technique that limits access to internet content depending on the geographic location of the user, such that a person located in France searching for delisted information on the google.com domain would still not receive the delisted links.

[1] *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos*, C-131/12, 13 May 2014.

[2] Paragraphs 92-94, G*oogle Spain SL, Google Inc. v. Agencia Española de Protección de Datos*, C-131/12.

[3] Article 16 TFEU; recitals 10, 11 and 13 of Regulation 2016/679; and recital 10 Directive 95/46.

[4] Article 17 GDPR and Article 12(b) Directive 95/46/EC.

[5] Paragraph 70, *Google Inc. v Commission Nationale de l'Informatique et des Libertés (CNIL)* Case C-507/17.

Key Takeaways

The CJEU has recognized that the requirement for a search engine operator to de-list search results as a result of a successful RTBF request does not have automatic extraterritorial application. This is mainly because (1) a RTBF is not recognized by all jurisdictions globally, and where it is recognized, jurisdictions may apply it differently, and (2) the EU's data protection legislation does not envisage extraterritorial application of the RTBF. However, there is no prohibition of a global application of the RTBF by a EU member state if appropriate, and search engine operators must at least "seriously discourage" internet users in the EU from gaining access to de-listed search results.

Return to Table of Contents

CJEU Rules on Interpretation of Joint Controller

The CJEU held that a website operator may be a joint controller with the provider of a social media plug-in.

Summary

In *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.*,[6] the CJEU furthered its broad interpretation of the definition of a "controller" as used in EU data protection law. This interpretation is critical since many of the General Data Protection Regulation (GDPR) obligations apply to data controllers. The CJEU held that a website operator that has embedded a social media plug-in on its site could be a "controller," jointly with the provider of the social media plug-in. As a result of the ruling, website operators: (1) are subject to the duties to inform individuals from whom they process personal data pursuant to the GDPR; (2) will require a joint controller arrangement with the provider of the social media plug-in;[7] and (3) are subject to the possibility that a data subject may exercise their privacy rights against either the website operator or the social media plug-in provider (usually by reaching out to the contact point designated by the joint controllers).[8]

Background

Fashion ID, a German online retailer, embedded the Facebook "like" button (the plug-in) on its website. For the plug-in to work, the browser of a visitor to the Fashion ID website had to transmit to Facebook the IP address of the visitor's computer, as well as the browser's technical data. The browser did this automatically and without the visitor's knowledge. It also occurred regardless of whether the visitor was a Facebook member or had clicked on the plug-in.

In light of these facts, a German consumer protection association sought an injunction against Fashion ID arguing that the use of the plug-in resulted in a breach of applicable data protection legislation because of Fashion ID's failure to inform visitors of such processing. The German court then referred a number of questions to the CJEU.

The CJEU's Decision

The CJEU held, in keeping with the court's previous expansive interpretations of the term "controller,"[9] that Fashion ID could be considered a controller jointly with Facebook because they collectively determined the purposes and means of the processing of the personal data. They jointly determined the means that provided the platform on which the plug-in was hosted, as Fashion ID was the website operator. They also determined the purposes of processing in concert with one another as Fashion ID wanted "likes" on Facebook as a way of advertising, while Facebook wanted web traffic from which it could collect data for its own commercial purposes (subject to the limitations set out below).

However, the CJEU did limit the extent of Fashion ID's responsibility to the stages of the processing operation in which the company actually was a controller, namely the collection and subsequent transmission of the personal data. The court ruled that Fashion ID had no control over what data was transmitted by the visitor's browser to Facebook and over what Facebook decided to do with that data.

In its decision, the CJEU made two important points regarding joint controllers. First, Fashion ID's obligation to inform visitors about the processing of their data at the time of collection was limited, in the court's view, to only include the stages of the processing in which it was a controller. It was therefore up to Facebook to inform the site's visitors of any processing of their data beyond the collection and transmission of it by Fashion ID. Second, where data processing is to be based on legitimate interest, it is necessary for the joint controllers to have a legitimate interest that is not overridden by the rights of the data subject.[10]

[6] (Case C-40/17) (July 29 2019). While the case relates to the EU data protection laws in force prior to the introduction of the GDPR, the judgement is still of relevance given that the definitions considered are almost identical to those adopted under the GDPR.

[7] Article 26(1) GDPR.

[8] Article 26(3) GDPR.

[9] *Wirtschaftsakademie Schleswig-Holstein*, C-210/16; and Jehovan todistajat, C-25/17.

[10] The referring court asked whose legitimate interest between the joint controllers should be taken into account, assuming that the "legitimate interest" legal basis applied. The referring court did not request guidance on whether, in the given case, a legitimate interest actually allowed the processing of personal data to occur in the absence of the data subjects' consent.

Key Takeaways

The court's ruling shows that: (1) the CJEU continues to adopt a broad interpretation of "joint controller"; (2) website operators will have to ensure that they enter into a joint controller arrangement with plug-in service providers to address responsibility and liability issues in relation to the joint processing of personal data; and (3) website operators will have to ensure that they provide visitors with appropriate notice of processing relating to plug-ins. In light of this decision, website operators may need to update their privacy notices.

Return to Table of Contents

UK Court Decides on the Use of Facial Recognition Technology

In *Bridges v. South Wales Police* a Welsh court set a precedent for use of Automated Facial Recognition (AFR) technology by law enforcement.

On September 4, 2019, the Divisional Court in Cardiff, Wales, dismissed an application for judicial review brought by a civil liberties campaigner against the use of AFR technology by the South Wales Police (SWP). The SWP has taken the national lead on testing and conducting trials of AFR use in the U.K., with the trials funded by grants from the U.K. government. This is the first time that the legal implications of facial recognition technology have been considered in any court in the world, and sets a potentially important precedent for the use of AFR by law enforcement bodies.

Background

Edward Bridges, a member of the public supported by Liberty, a civil liberties organization, challenged the lawfulness of the SWP's overall use of AFR technology, in addition to two separate occasions where AFR technology was used while he was present. Both instances involved the SWP's use of its pilot AFR Locate technology during its trial phase. Bridges' claims fell under a range of both European and British human rights and data protection laws, including the European Convention on Human Rights (ECHR), the U.K. Data Protection Act (DPA) (both under the 1998 act and the current act of 2018) and the Equality Act of 2010.

The Technology

Over the past several years there have been many technological advancements in the field of forensic policing, with each advancement triggering new civil liberties concerns, resulting in the implementation of specific legislative measures to balance the line between effective policing tools and the protection of privacy and civil liberties. The U.K. courts have historically taken the position that "law enforcement agencies should take full advantage of the available modern technology and forensic science."[11]

AFR is a new technology that allows images to be taken and processed to extract facial biometric data, which is then compared with images stored on a database for a specific purpose. AFR Locate specifically is intended to identify persons who are on a watchlist created by police forces across the country to help detect and prevent crime. The SWP has deployed the technology in public spaces to pinpoint individuals who could be connected with criminal activities.

Currently, the use of AFR technology is controversial from a data protection standpoint. The U.K.'s data protection authority, the Information Commissioner's Office (the ICO), is currently conducting an investigation into the trial use of such technology by the police, and Information Commissioner Elizabeth Denham has publicly expressed concerns regarding the rollout of AFR. Specifically, the ICO notes that police forces have not fully demonstrated their compliance with applicable data protection laws, including the processes by which watchlists are collated and by which images are utilized.

The Court's Ruling

Bridges was concerned that his photo may have been taken by AFR from a police van while he was Christmas shopping. His primary arguments claimed that there is no legal basis for the use of AFR Locate, and that there is not currently any sufficient legal framework that outlines the safeguards in place for the use of AFR. In response to the first submission, the court noted that the SWP and the U.K. government rely on the police's common law powers as sufficient authority to use these new technologies. Those common law principles enforce a duty on police constables to detect and prevent crime, which includes the power to use, retain and disclose imagery of individuals for the purposes of detecting crime. In this case, the court concluded that the police's common law powers were a sufficient legal basis for the use of AFR Locate.

As for Bridges' submission in relation to the legal framework, the court concluded that there was a clear and sufficient legal framework in place governing when, and how, AFR Locate may be used. The fact that the technology is new does not mean it automatically falls outside the scope of the existing regulations or that it is necessary to create a bespoke legal framework for its use.

[11] *R(S) v. Chief Constable of the South Yorkshire Police* [2014] 1 WLR 2196.

The legal framework comprises primary legislation (*e.g.* the DPA 1998 and its successor, the DPA 2018) and secondary legislation (in the form of codes of practice issued under primary legislation) and the SWP's own policing policies. According to the court, the cumulative effect of each of these different sources is sufficient to satisfy that the use of AFR is in "accordance with the law."

Interplay Between Data Protection Legislation and AFR Technology

Bridges contended that the use of AFR was contrary to the DPA 1998 and the DPA 2018. Despite the facts of the case occurring prior to the implementation of the DPA 2018, the court assessed the use of AFR as if the DPA 2018 had been in full force and effect at the time. Data protection rules apply to all operations which involve the retention or use of personal data.

The court concluded that the use of AFR Locate met the requirements of the first data protection principle (DPA 2018 Section 4(4)) on the basis that the information was processed for the SWP's legitimate interests to prevent and detect crime, as set out above. The court held that the processing of biometric data was necessary for the SWP to successfully identify persons on its criminal watchlist.

The court also considered obligations placed on the SWP under Schedule 3 of the DPA 2018 regarding the processing of personal data by law enforcement. Specifically, they considered whether the biometric data obtained was subject to "sensitive processing" and whether the processing was "strictly necessary" for law enforcement purposes. The court confirmed that the "processing … of biometric data for the purposes of uniquely identifying an individual" would be subject to specific conditions for "sensitive processing" under the DPA 2018. The court was satisfied that the operation of AFR Locate involved sensitive processing of the biometric data of members of the public, and that the processing of such data was lawful, non-arbitrary and fair. Furthermore, the court evaluated the SWP's data protection impact assessment and concluded that the SWP took into account appropriate technical and organizational safeguards to protect against personal data breaches. In essence, the court found that the existing legal and regulatory regime was sufficient for governing the lawful use of AFR technology.

Key Takeaways

The existing legal framework seeks to strike a balance between the protection of individual privacy rights and the prevention of crime. Whilst the police powers granted under common law empower the SWP to legally use AFR, the decision in *Bridges v. South Wales Police* further confirms that AFR can be integrated into law enforcement activities without any need for the establishment of a new, separate legal framework. However, the ICO, which continues to remain skeptical of AFR technology, is expected to provide further regulatory guidance in this area.

Return to Table of Contents

Federal Judge Puts Dispute Involving Multimillion-Dollar Phishing Scam Coverage on Hold

A Texas federal judge recently issued an order temporarily staying a property management company's coverage action against its primary and excess crime insurers relating to a $10 million loss stemming from a phishing scam.

On August 1, 2019, the U.S. District Court for the Northern District of Texas issued an order, on the parties' joint motion, temporarily halting property management company RealPage, Inc.'s (RealPage) coverage dispute against its primary and excess crime insurers, National Union Fire Insurance Company of Pittsburgh, Pennsylvania, (a subsidiary of AIG) and Beazley Insurance Company (Beazley), relating to a $10 million loss sustained by RealPage as a result of a phishing scam.[12]

The Phishing Scam and Fraudulent Funds Transfer

According to RealPage's complaint, the company provides software and data analytics, as well as back office management services, to real estate owners and managers. One of the management services that RealPage provides is the collection of rental payments from residents of the company's property manager clients and the subsequent transfer of those payments to the clients through a web portal. RealPage allegedly uses a third-party software application to allocate and direct the resident payments received through the web portal. Once the residents make a payment through the web portal, further transfer of funds is controlled entirely by RealPage, the complaint alleges.

In May 2018, one or more unauthorized parties allegedly used a targeted phishing scheme to obtain a RealPage employee's account credentials. The perpetrator(s) then allegedly used those credentials to access the third-party software application and

[12] *RealPage, Inc. v. Nat'l Union Fire Ins. Co of Pittsburgh, Pa.*, No. 3:19-cv-01350 (N.D. Tex.).

change RealPage's bank account disbursement instructions, allowing the perpetrator(s) to fraudulently divert more than $10 million in funds that the company had collected for its clients. The complaint further alleges that while some of the stolen funds were recovered, RealPage ultimately had a net loss of more than $6 million.

RealPage Seeks Coverage From its Crime Insurers; the Insurers Deny Coverage

According to the complaint, at the time of the loss, RealPage had primary and excess crime policies issued by AIG and Beazley, respectively, which provide coverage for losses arising out of various financial crimes, including computer fraud. The AIG primary policy allegedly covered loss to property that RealPage "own[s]" and "hold[s] for others whether or not [RealPage is] legally liable for the loss of such property."

RealPage tendered the loss to AIG and Beazley. In response, AIG acknowledged that the loss triggered its policy's computer fraud insuring agreement, but only agreed to pay a limited portion of RealPage's losses consisting of diverted funds that AIG calculated as representing transactional fees owed to the company by its clients. According to RealPage, AIG wrongfully disclaimed coverage for the majority of the company's losses consisting of diverted funds that would have been sent to client bank accounts, claiming that RealPage did not "own" the funds or "hold the funds for others." In response to the partial disclaimer, the company allegedly provided AIG with "clear and undisputed information" demonstrating that "RealPage was holding th[e] funds for clients … when the funds were diverted, which information demonstrated RealPage's right to coverage." AIG allegedly declined to withdraw its disclaimer.

The complaint further alleges that Beazley also failed to provide coverage for the loss under its excess crime policy, despite the fact that RealPage's loss exceeded the limits of the AIG primary policy.

RealPage's Coverage Action and the Parties' Joint Motion to Stay

On June 5, 2019, RealPage commenced a coverage action against AIG and Beazley in the Northern District of Texas seeking a declaration that RealPage's loss resulting from the fraud incident is covered under AIG and Beazley's crime policies. RealPage also brought claims for breach of contract, anticipatory breach of contracts and violations of the Texas Insurance Code.

On August 1, 2019, the parties filed a joint motion to stay the proceedings for 120 days to allow time for RealPage to investigate new developments related to its damages and afford the parties an opportunity to potentially resolve at least a portion of the dispute without further litigation. Specifically, according to the motion, RealPage learned after the filing of its lawsuit that a portion of its claimed damages may be recouped from "a previously unknown source," which "may materially affect RealPage's claims against Defendants, as well as the amount of its damages." On August 1, 2019, the court issued an electronic order granting the parties' motion to stay. The case is currently stayed until December 2, 2019, at which point the stay will be automatically lifted.

Key Takeaways

It remains to be seen whether the parties will be able to resolve their dispute during the stay. Regardless, this case is a reminder that traditional crime policies may seem comprehensive, but nevertheless may fall short in the event of a cyber loss. While there are a number of non-insurance measures that a company can take to protect against the risk of cybercrime, such as information security training and protocols, insurance coverage nevertheless remains a key risk management tool. Thus, businesses should seek to tailor their crime and/or cyber policies to best fit their needs in order to increase the likelihood that coverage will be available in the event of a cyber loss. Similarly, insurers should carefully craft and review their policy forms to ensure that they are comfortable with the coverage being provided.

Return to Table of Contents

Marriott Ordered to Publicly Release Forensic Report in Cybersecurity Class Action Lawsuit

A Maryland federal judge's recent decree ordering the Marriott hotel chain to produce a report revealing key details about how a data breach occurred may signal a trend towards more transparency in cybersecurity litigation.

On August 30, 2019, a federal judge in Maryland ordered Marriott to make public a Payment Card Industry Forensic Investigative report (PFI report), thereby revealing potentially sensitive and inculpatory information about the company's cybersecurity.

A PFI report is the product of a forensic investigation initiated by credit card companies in the aftermath of a cybersecurity incident to assess a merchant's compliance with industry standards for security. The judge rejected Marriott's arguments that public release of the report would facilitate future cyberattacks, compromise its ongoing investigation and reveal confidential aspects of Marriott's business to competitors, concluding that the First Amendment requires Marriott to produce the report.

Attacks on Marriott's Starwood Database and Resulting Class Action Lawsuit

The litigation stems from a data breach that Marriott announced on November 30, 2018, involving unauthorized access to its Starwood brand's guest reservation database. Marriott claims the attackers stole personal data from up to 383 million guests, beginning as early as 2014.

The many lawsuits that resulted were consolidated into one multidistrict class action and divided into five tracks: government, financial institution, consumer, securities and derivative. While Marriott's motion to dismiss in the securities and derivative tracks was pending, the judge stayed discovery in all other tracks and provisionally sealed Marriott's motion to dismiss in the government track action, which included a copy of Marriott's PFI report.

The Plaintiffs Seek Production of Marriott's PFI Report

Before the deadline for amending their complaint, the plaintiffs in the securities and derivative track class actions moved to unseal Marriott's PFI report. The plaintiffs argued that the First Amendment right to access judicial records mandated the unsealing of the PFI report, which had been filed with the court as an attachment to Marriott's motion to dismiss in the government track action.

Marriott responded, arguing that three compelling interests outweighed plaintiffs' right of access. First, the company claimed that releasing the PFI report would allow criminals to use it to hone their strategies and perpetrate future attacks. Second, Marriott argued it needed to protect the integrity of ongoing investigations into the breach, which could be compromised by the release of the PFI report. Finally, the company sought to prevent competitors from gaining insight into commercially sensitive information about its business practices contained in the PFI report.

The Court Orders Unsealing of the PFI Report

On August 30, 2019, the court upheld the plaintiffs' arguments and ordered the unsealing of Marriott's PFI report, ruling the company must produce the PFI report in its entirety, subject to any narrowly tailored redactions proposed by Marriott and upheld by a magistrate judge.

The court held that the PFI report was a judicial record subject to the First Amendment right to access, not simply because it was filed in connection with Marriott's motion to dismiss, but because the report was relied on by the parties in their pleadings and "will play a significant role in the adjudicative process by helping [him] decide whether the complaint is facially sufficient."

The court found Marriott's arguments insufficient to raise a compelling interest that outweighed the plaintiffs' First Amendment right to access the PFI report. First, the court considered Marriott's argument about preventing future attacks to be "speculative and generalized," observing that "[u]nder this reasoning, none the details of how the Starwood database was compromised could ever be revealed, which would prevent the public from understanding how the data breach occurred in the first place …" He also rejected Marriott's arguments that unsealing the PFI report would compromise ongoing investigations and place commercially sensitive data in the hands of Marriott's competitors, because the company did not specify how such investigations would be compromised or why sealing the entire report was necessary to prevent competitors from accessing confidential information.[13]

Emphasis on Transparency

Underpinning the court's order is an emphasis on the perceived need for transparency early in cybersecurity litigation. Granting plaintiffs access to PFI reports prior to discovery facilitates the efficient administration of class actions because it allows courts to make better-informed decisions about the validity of the claims and defenses at issue earlier in the life of the litigation. Nevertheless, such prompt and early access to PFI reports could curtail defendants' hopes of winning early pretrial dispositive motions, while providing class action plaintiffs with a powerful evidentiary tool. PFI reports are aimed at determining whether, and to what extent, a retailer is to blame for a security incident. Thus, the report can contain inculpatory and, at best, unflattering information about the defendant that plaintiffs can use to bolster their existing claims and raise novel ones.

[13] The full text of the court's ruling can be read here.

Key Takeaways

Companies involved in cybersecurity litigation should avoid filing their PFI report as part of any pleadings, even under seal. Marriott opened the door to the plaintiffs' First Amendment argument when it filed its PFI report as part of a motion to compel.

Nevertheless, the court's order suggests that even if a PFI report is not filed as part of a pleading, it may still be subject to early production if the parties rely on it in their pleadings and the judge considers it useful in deciding a motion to dismiss. Given this, additional steps should be considered to mitigate the consequences of a publicly released PFI report. For example, companies may consider hiring their own forensic vendor to undertake an investigation, which may counter the PFI report produced by the merchant's vendor. Companies also should hone their PR strategies to respond to negative press arising from the pubic release of a PFI report.

Finally, before an incident arises, companies may consider hiring a forensic vendor to produce a mock PFI report to help alert a company of potential shortcomings in its cybersecurity prior to an incident or related litigation.

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

Donald L. Vieira
Partner / Washington, D.C.
202.371.7124
donald.vieira@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