November 2019

PRIVACY AND DATA SECURITY CLIENT ALERT

SHOOK HARDY & BACON

EU Court Allows Class Action to Proceed, Sets Precedent for Future Data Breach Class Actions

A class action brought against Google will be allowed to move forward after the plaintiff's appeal was permitted, allowing him to continue his claim under section 13 of the Data Protection Act of 1998. The case stems from a workaround that enabled Google to place certain cookies on a user's device without the user's knowledge, allowing the company to secretly track users and collect "browser generated information." The High Court of Justice held that potential members of the plaintiff's proposed class did not have the "same interest" to "justify allowing the claim to proceed as a representative [class] action." However, the Court of Appeal held that the browser generated information is "something of value" that was "taken by Google without [users'] consent during the same period, and are not seeking to rely on any personal circumstances affecting any individual claimant." As such, the Court of Appeal held that the High Court abused its discretion in refusing to allow the case to proceed, and the lawsuit can continue.

On the heels of the *Lloyd* decision, the first data breach class action has been filed against Equifax in the U.K.'s High Court. The lawsuit seeks £100 million ($129.6 million) in damages for the approximately 15 million U.K. customers affected by the 2017 Equifax data breach. In September 2018, the U.K.'s Information Commissioner's Office found that Equifax failed to implement certain safeguards and procedural protections of customers' personal information and issued a fine.

TAKEAWAY

Shook, Hardy & Bacon understands that companies face challenges securing information in an increasingly electronic world.

Shook guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

To learn more about Shook's Privacy and Data Security capabilities, please visit shb.com or contact:

Al Saikali
Chair, Privacy and Data Security Practice
305.358.5171
asaikali@shb.com

This key decision may serve as a basis for allowing data-breach-related class actions to gain traction in the EU, where data breach class actions have historically been unable to gain momentum.

CCPA Sees Amendments and Draft Regulations

California Attorney General Xavier Becerra has released a draft of the highly anticipated proposed regulations to the California Consumer Privacy Act (CCPA). The extensive regulations address numerous topics, such as expanded requirements for notices to consumers, requirements for handling and verifying consumer requests, and calculation of the value of consumer data for purposes of financial incentives. The attorney general's office will accept public comments on the proposed regulations through December 6, 2019. The final regulations are not likely to go into effect before July 1, 2020. Additional information about the proposed regulations and their potential effects can be found in Shook's webinar "The California Consumer Privacy Act: A Conversation on the Draft Regulations." For more information on submitting comments to the attorney general's office, please contact Colman McCarthy, lead attorney of Shook's CCPA Task Force.

In addition, California Governor Gavin Newsom has signed seven bills amending or relating to the CCPA. The bills address issues such as modifying the definition of "personal information," providing limited exemptions for the personal information of employees and business contacts, and correcting numerous drafting errors.

TAKEAWAY

The CCPA regulations could potentially lead to extensive additional compliance obligations, but they won't be final until after the CCPA takes effect. Companies should prioritize baseline compliance for the January 1, 2010, effective date of the CCPA itself.

California Measure Proposes Tougher Privacy Rules for CCPA

Consumer privacy advocate and founding father of the CCPA Alastair Mactaggart has introduced a ballot initiative to strengthen and add to the CCPA. Under the many provisions of the 51-page initiative, entitled the "California Privacy Enforcement Act," the proposed law would:

Colman McCarthy
Associate
816.559.2081
cdmccarthy@shb.com

Kate Paine
Associate
813.202.7151
kpaine@shb.com

Ben Patton
Associate
206.344.7625
bpatton@shb.com

Lischen Reeves
Associate
816.559.2056
lreeves@shb.com

- create new rights around the use and sale of sensitive personal information (e.g., health and financial information, racial or ethnic origin, and geolocation data);
- provide enhanced protection for violations of children's privacy;
- require opt-in consent to collect data from consumers under the age of 16; and
- establish a new state authority to protect these rights, the California Privacy Protection Agency, which will simultaneously enforce the law and provide necessary guidance to industry and consumers.

Approximately 623,000 signatures will be needed to place the initiative on the 2020 ballot in California.

TAKEAWAY

CCPA compliance is not a one-time event. The law will likely continue to develop and expand as advocacy groups continue to push for additional requirements. Companies will need to regularly re-evaluate their CCPA compliance program.

EU Court of Justice Rules on Cookie Compliance

In an important decision involving cookie-consent requirements, the Court of Justice of the European Union (CJEU) issued significant guidance about how consent may be obtained from consumers. The case involved an online-gaming company that prompted a user to enter certain information and included a preselected checkbox that gave permission to the company to install cookies on the user's devices.

The court ultimately found that consent provisions of the ePrivacy Directive and EU GDPR require "some active behavior" from the user for consent to be valid, and it noted Recital 32 of the GDPR, which lists "ticking a box when visiting an internet website" as an example of obtaining valid consent from a user. The CJEU also confirmed that consent requirements under the ePrivacy Directive apply to all information stored or accessed from a device, whether or not it is considered personal data. Lastly, the CJEU held that a service provider must include the durations of cookies that will be installed on a user's device and also detail if third parties will have access to the installed cookies.

TAKEAWAY

Companies operating in the EU can no longer offer preselected options for users in order to obtain consent for the use of cookies.

Data Protection Law Takes Effect in Cayman Islands

Coming into force on September 20, 2019, the Data Protection Law (DPL) is meant to align privacy law in the Cayman Islands with other major jurisdictions around the world, most notably the EU. Modeled after the GDPR, the DPL gives individuals a right of access to personal data, a right to request that a data controller stop processing their personal data for direct-marketing purposes, and rights in relation to automated decision-making. The Office of the Ombudsman issued guidance and will act as the supervisory authority for data protection. It will also look to interpretations and court decisions from the EU as persuasive authority.

TAKEAWAY

Companies operating in the Cayman Islands need to assess the applicability of the DPL. While it seems the ombudsman will apply EU law standards, there may be subtle differences that should be accounted for when developing a compliance program.

European Data Protection Board Adopts New Guidance on GDPR Issues

The European Data Protection Board (EDPB) met for two days in November to complete the annual review of the EU-US Privacy Shield and discuss various GDPR topics such as guidelines on territorial scope and data protection by design and default. Following a public comment period, the EDPB embraced the final version of its own Guidelines on Territorial Scope, which "aim to provide a common interpretation of the GDPR for EEA Data Protection Authorities when assessing whether a particular processing by a controller or a processor falls within the territorial scope of the legal framework." Additionally, the EDPB adopted its own report regarding the efforts of U.S. authorities to implement the Privacy Shield and concluded that the U.S. Ombudsperson currently does not have the power to remedy noncompliance. Lastly, the EDPB initially approved guidelines regarding data protection by design and default that requires controllers to implement appropriate technical and organizational measures as well as safeguards to protect the rights and freedoms of data subjects. The guidelines will be submitted after a public comment period.

TAKEAWAY

Controllers and processors under the GDPR should carefully review the issued guidance to determine whether their processing activities are within the scope of the GDPR. Additionally, companies should evaluate whether their privacy programs need updates based on the guidelines on data protection by default and design.

HHS Fines Major Florida Healthcare Network

The Office for Civil Rights (OCR) has fined Jackson Health System (JHS) $2.15 million for myriad HIPAA violations including: failing to detect and stop an employee who stole and sold thousands of patient records; losing patient files without notifying OCR as required by law; and failing to properly secure protected health information (PHI) that was leaked to the media. OCR initiated an investigation and found that "JHS failed to provide timely and accurate breach notification to the Secretary of HHS, conduct enterprise-wide risk analyses, manage identified risks to a reasonable and appropriate level, regularly review information system activity records, and restrict authorization of its workforce members' access to patient ePHI to the minimum necessary to accomplish their job duties."

TAKEAWAY

Always notify the proper authorities and individuals of a data breach within a timely manner and conduct periodic risk assessments to alleviate any identified risks. Applying data minimization principles can detour improper handling of customer data by unauthorized employees.

Irish Data Protection Commission Releases Guidance on Data Breach Notification Requirements under GDPR

Ireland's Data Protection Commission (DPC) released practical advice for data controllers on how to handle data breaches and navigate the mandatory data-breach-notification regime of the GDPR. The guidance lists specific information that should be provided when notifying authorities of a breach and as well as several criteria for determining the risk to the rights and freedoms of affected data subjects, including the nature of the breach, the volume of personal data involved and the potential damage to data subjects. The guidance also encourages data controllers to utilize standard operating procedures so they can be prepared to handle a security incident.

TAKEAWAY

Companies in Ireland affected by a data breach should notify individuals and authorities within the proper time period and include all the detailed information listed in the DPC's report. Establishing and maintaining internal policies and procedures for addressing a data breach are essential to timely responding to an incident.

EDPB Publishes Guidelines for Processing in Connection with Contracts

The European Data Protection Board (EDPB) has provided guidance on the processing of personal data necessary for the performance of a contract for online services under Article 6(1)(b) of the GDPR. Specifically, the guidelines address how the GDPR applies to processing for service improvement, fraud prevention, online behavioral advertising and personalization of content. Importantly, the guidance provides that merely referencing or mentioning data processing in a contract is not enough to bring the processing within Article 6(1)(b). Rather, determining the substance and fundamental objective of a contract is a prerequisite for determining whether data processing is necessary for its performance.

TAKEAWAY

Companies cannot simply rely on contractual language stating that processing is necessary to perform the contract. Only process personal data necessary to achieve the goals and objectives of the contract.

Sri Lanka Close to Enacting a New Privacy Law

The Sri Lankan Ministry of Digital Infrastructure and Information Technology (MDIIT) announced the final draft of its proposed data-protection bill. Similar to the GDPR and CCPA, the proposed legislation aims to regulate the processing of personal data by companies and strengthen the rights of data subjects. Under the bill, controllers would implement internal controls and procedures, appoint a data protection officer and perform privacy impact assessments prior to processing personal data that is "likely to result in a high risk to the rights and freedoms of data subjects." The final draft also details that penalties shall not exceed a sum of ten million rupees (approximately $140,000) in any case. If certified, the law will be implemented in stages and take effect within three years from the date of certification.

TAKEAWAY

Companies with a presence in Sri Lanka should assess the impact of this law and developing privacy programs to successfully implement the law's provisions.

The choice of a lawyer is an important decision and should not be based solely upon advertisements.