Skadden

Privacy & Cybersecurity Update

California Attorney General's Office Says Not to Expect CCPA Enforcement Delay Due to COVID-19

An adviser to the California attorney general said that the office expects to proceed with the enforcement of the California Consumer Privacy Act (CCPA) as planned despite recent business disruptions due to the COVID-19 outbreak and the lack of finalized, published regulations.

With many areas of the U.S., including California, under a "shelter-in-place" order due to the COVID-19 pandemic, dozens of businesses are seeking to delay the state's enforcement of the CCPA, which is currently expected to take effect on July 1, 2020. Initially signed primarily by a coalition of industry associations, over 60 businesses have now joined a March 17, 2020, letter[1] to the attorney general requesting a delay due to the substantial strain that the pandemic is placing on their workforce, adding additional difficulty to implementation of the law. In the letter, the businesses say that delaying enforcement until 2021 would allow companies to focus their limited resources on helping their employees through the pandemic, while also giving covered businesses much-needed time to evaluate and carefully operationalize the attorney general's finalized implementing regulations, which have yet to be announced.

Privacy advocates, including Consumer Reports,[2] have responded by characterizing the letter as another in a series of attempts by businesses to delay compliance with a law, which went into effect three months ago. Consumer Reports said the unprecedented number of consumers who are sheltered at home and rely on technology to communicate with others underscores the importance of enforcing CCPA protections as soon as possible. When pressed about the yet-to-be-finalized attorney general regulations and the uncertainty this creates for businesses, privacy advocates pointed to the attorney general's statement last year[3] that the office would "look kindly on those that … demonstrate an effort to comply." The advocates say this statement means perfect compliance is not the base expectation when enforcement begins in July 2020 and that the attorney general's priority, especially initially, will be to prosecute flagrant violations.

[1] The letter can be found here.

[2] Consumer Reports thoughts on the issue can be found here.

[3] The attorney general's comments can be found here.

While the CCPA went into effect on January 1, 2020, the law contains a dual trigger for the start of attorney general enforcement, which may begin: (1) six months after the publication of the final regulations, or (2) July 1, 2020, whichever comes first. In a statement to *Forbes*,[4] the adviser to the attorney general relayed that "right now, we're committed to enforcing the law upon finalizing the rules or July 1, whichever comes first," despite the pandemic.

Key Takeaways

While it is possible the representative may have misspoke in relation to the first prong, the prospect of instant enforcement of (currently) unfinalized rules adds to the anxiety of many business leaders in complying with the law. Either way, considering the CCPA is already in effect, businesses should continue to work toward compliance with the statute and elements of the regulations that have remained relatively consistent across versions of the regulatory drafts promulgated by the attorney general's office. Businesses also must vigilantly monitor regulatory developments, including the release of the finalized regulations, when completed, to ensure they are actively moving toward compliance with the latest CCPA guidance.

Return to Table of Contents

COVID-19, Contact Tracing and Data Protection in the Workplace

Steps taken by the U.K. government in light of the COVID-19 outbreak have raised data protection and General Data Protection Regulation 2016/679 (GDPR) compliance issues.

Like many governments, the U.K. has required individuals who are able to do so to work from home to combat the spread of the COVID-19 virus. In cases where working from home is not possible, employers may wish to use "contact tracing" to contain the spread of the outbreak. Contact tracing involves processing personal data in order to inform individuals that may have come into contact with an infected person. Once informed, those individuals can then take appropriate steps to protect themselves and others, such as by self-isolating. Though the world is in the midst of the pandemic, any processing of personal data as a preventative measure must still be done within the parameters of the GDPR. This has been made clear by a number of data protection authorities and the European Data Protection Board (EDPB).

Contact Tracing and Lawful Processing

Health data, including facts such as whether a person has been diagnosed with COVID-19, is classified as a special category of personal data under the GDPR. This means that its processing is prohibited by GDPR Article 9(1), unless the processing relies (1) on an appropriate GDPR Article 6(1) legal basis and (2) an available condition set out in GDPR Article 9(2) applies.

GDPR Article 6(1)(c) allows for the processing of personal data when it "is necessary for compliance with a legal obligation to which the controller is subject." Employers in the U.K. have a duty pursuant to the Health and Safety at Work etc. Act 1974 to take reasonable care of the health and safety of their workforce, as well as those that may be affected by the employer's business. Consequently, in the context of contact tracing within their own workforce and third parties who may have come into contact with their workforce — for example, through a site visit — GDPR Article 6(1)(c) would likely apply.

Alternative legal bases under GDPR Article 6(1) state that (1) processing is necessary to protect the vital interests of the data subject or another natural person (which should only be relied on where no other legal basis can be used) or (2) processing is necessary for the legitimate interests of the controller or a third party, except where overridden by the interests of the data subject. The latter legal basis requires a balance between the data subject and the controller's interests, which can be recorded in the form of a legitimate interest assessment. These legal bases are therefore more onerous to fulfill than demonstrating that the processing is necessary to comply with a legal obligation.

Reliance on the consent of the data subject should be avoided in the context of an employment relationship as the imbalance of power between employer and worker will most likely render consent void.

Having established a legal basis on which to rely, a GDPR Article 9(2) condition also must apply. The most relevant of these conditions for an employer seeking to conduct contact tracing is likely to be Article 9(2)(b). For the condition of this article to apply, the processing must be necessary in order for the employer to carry out an obligation in the field of employment or social security and social protection law. Further, this must be authorized by EU or member state law. The authorizing legislation in the U.K. is the Data Protection Act 2018 (DPA), which is the legislation supplementing the GDPR. This sets out that the processing has to be necessary for purposes of performing obligations imposed by law on the employer in connection with employment, social security or social protection. As established above, employers in the U.K. have a duty to take reasonable care of the health and safety of their workforce, as well as those that may be affected by the employer's business. Consequently,

[4] The adviser's statement can be found here.

in the context of contact tracing, GDPR Article 9(2)(b) would likely apply. If this condition is relied upon, the DPA requires the employer to also have an "appropriate policy document in place." This document must set out the employer's procedures for compliance with the core data processing principles listed in GDPR Article 5, which are considered further below.

An alternative to Article 9(2)(b) is Article 9(2)(i), which allows for processing of special category data where necessary for reasons of public interest in the area of public health, which covers "all elements related to health." "Public interest" is not defined in the GDPR, but the U.K.'s data protection authority, the Information Commissioner's Office, has published guidance that (1) public interest needs to point to a benefit of the wider public or society as a whole (rather than an organization's own interests) and (2) this condition may apply where the processing is necessary in responding to new threats to public health, such as a pandemic. The processing also must be on the basis of EU or member state law. In this regard, the DPA sets out that the processing must be carried out: "(i) by or under the responsibility of a health professional, or (ii) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law." An employer therefore would need to be comfortable that they fall within the DPA's second point above in light of the U.K. government's COVID-19 response, unless the processing is being done by, or under the responsibility of, a health professional.

Implementing the Processing and Core Data Protection Principles

Once an employer seeking to conduct contact tracing has ensured that such processing will be carried out lawfully, implementing the processing must be guided by the core data processing principles listed in GDPR Article 5. For instance, the personal data that is processed should be limited to what is required to fulfill the purpose of the processing (the data minimization principle). This generally means that the infected individual does not need to be named. As such, those who came into contact with the infected individual need to be informed that they may have been exposed to the virus, but usually will not need to know the individual's identity.

The GDPR also requires controllers to be accountable for their processing activities and be able to demonstrate that such processing is undertaken at all times in compliance with the regulation's requirements. This means that an employer's records of processing may need to be updated in light of the introduction of contact tracing. This will need to be done with the level of detail required under GDPR Article 30. In addition, when considering the processing of special category personal data, the employer (as controller) must document its decision-making process through the use of a data protection impact assessment as per GDPR Article 35.

Transparency also is important, and workers should be made aware of how their personal data will be used in the context of contact tracing. If an employer's internal privacy notice does not already cover the processing required for contact tracing, it will need to be updated, or, specific privacy notices will need to be issued to individuals whose personal data is to be processed. Such notices will need to fulfill the requirements set down in GDPR Articles 13 and 14, including the requirement to set out the purposes and legal basis for the processing.

If the personal data is to be shared with third parties, such as clients whose staff might have come into contact with the infected worker, the employer must ensure that the third party also complies with data protection law. This may involve conducting diligence on the third party and putting contractual protections in place, if they do not already exist. Employers should take extra care if the intended recipient of the personal data (whether affiliated with the employer or a third party) is located outside of the European Economic Area. As contact tracing inevitably involves special category (health) data, it can be transferred in this way only if one of the derogations in GDPR Article 49 is satisfied. The threshold to meet these derogations (for example, that the transfer is in the public interest, there is a vital interest or with one-off explicit consent) is extremely high and unlikely to be met, especially now that there are limitations on cross-border travel, and the likelihood of individuals outside the jurisdiction coming into contact with the data subject is curtailed. Any such data should therefore be transferred only if aggregated and anonymized, such as for statistical or group reporting purposes.

Finally, an employer only should retain the personal data for as long as needed to fulfill the purpose for which it has been collected. Given that the U.K. government advice states that the incubation period for COVID-19 can be up to 14 days, this provides a guide for how long it is necessary to retain information on employees who have been infected. It will not be necessary to inform those that have potentially been exposed to the virus beyond 14 days after the exposure.

Key Takeaways

Processing personal data must continue to be done in accordance with applicable data protection laws, despite the pandemic. Such laws allow for the personal data necessary to contain the virus to be processed while ensuring there are safeguards in place to protect the individuals whose data is being processed.

Return to Table of Contents

Cybersecurity Challenges and Incident Response Preparedness During the Coronavirus Pandemic

The spread of the novel coronavirus has upended Americans' lives in a matter of months. While life outside has ground to a standstill in many regions of the country, much of corporate America is meeting the unique challenges posed by the current epidemic by adopting remote working technologies and practices. Companies, determined to sustain growth and add value, are adapting long-standing business practices to enable telecommuting and empower a new cyber workforce. For their part, workers are relying to an unprecedented degree on digital tools to keep them connected to coworkers and to do their jobs while staying safe at home.

To read the rest of this Skadden mailing from March 25, 2020, please click here.

Return to Table of Contents

FTC Releases Latest Privacy and Data Security Report

The Federal Trade Commission (FTC) released its 2019 Privacy & Data Security Update, which reviews the previous year and highlights how the agency's approach to cybersecurity has evolved.

On February 25, 2020, the FTC released its 2019 Privacy & Data Security Update (the report)[5], outlining the agency's commitment to enforcing privacy and data security laws. Moreover, the report sends a strong message that the FTC is not shying away from policing large players in the data collection and mining space, and is focused on protecting vulnerable groups of consumers.

Increased Enforcement Actions

The report summarizes the agency's privacy-related enforcement activities from 2019, which included more than 130 spam and spyware cases, more than 70 data protection related cases and more than 80 general privacy lawsuits. The report also highlights numerous matters involving larger and more familiar technology companies, as well as some lesser-known enforcement actions brought over the past year. Of particular interest is the report's discussion of the agency's first-ever action against a developer of stalker apps, which is software that allows purchasers to monitor the mobile devices on which they are installed without users' knowledge, as well as a few other notable actions focused on deceptive practices.

Strengthened Data Security Standard Orders

The report also discusses how the FTC has continued to strengthen its standard orders (the orders imposed by the agency in cybersecurity cases it has settled) in data security cases. The agency has clarified its current seven standard orders by making them more specific. Though they continue to require that a company implement a comprehensive, process-based data security program, they have evolved to also require a company to implement specific safeguards to address problems alleged in a complaint. The standard orders also increase third-party assessor accountability by requiring assessors to identify evidence supporting their conclusions and allowing the FTC to approve and re-approve assessors every two years. Finally, the standard orders now elevate data security considerations to the C-suite and board or director-level by requiring companies to present their board or similar governing body with a written information security program. Accordingly, senior officers must now provide annual certifications of compliance to the FTC.

Other Highlights and Takeaways

The FTC added a few other notable points in the report, including:

- details of 35 cases alleging violations of the Gramm-Leach-Biley (GLB) Act, which requires financial institutions to send customers initial and annual privacy notices, allowing customers to opt out of sharing their information with unaffiliated third parties. The FTC touts its case against Equifax as a prime example in the report;
- a discussion of how the FTC conducts international enforcement with regard to the EU-U.S. Privacy Shield Framework and other cross-border privacy systems;
- a summary of the agency's actions over the past year in enforcing the Children's Online Privacy Protection Act of 1998;
- an outline of the FTC's commitment to protecting consumers and promoting competition by providing examples of some of the comments it has made to courts and government agencies considering data privacy-related cases or policy decisions; and
- details on a number of privacy-related events and workshops hosted by the agency during the course of 2019 that discussed emerging issues in consumer privacy and security.

Return to Table of Contents

[5] The FTC 2019 Privacy and Data Security Update can be found here.

EDPB Adopts Draft Guidelines on Connected Vehicles and Mobility-Related Applications

The EDPB recently drafted guidelines on the processing of personal data in the context of connected vehicles and mobility-related applications.

Introduction

As connected vehicles move into the mainstream, expanding from luxury cars to midmarket models, they are fast becoming massive data hubs with associated data processing taking place in a complex ecosystem featuring a multitude of actors. This heightens stakeholders' challenge of incorporating a "protection of personal data" dimension that ensures connected car users enjoy transparency and control regarding their data. The guidelines will have extensive ramifications for industry participants, but will remain open for public feedback until May 1, 2020.

Scope of the Guidelines

The guidelines focus on the processing of personal data in relation to the nonprofessional use of connected vehicles by data subjects. More explicitly, it covers personal data (1) processed inside the vehicle, (2) exchanged between the vehicle and personal devices connected to it (*e.g.*, the user's smartphone), or (3) collected within the vehicle and exported to external entities (*e.g.*, vehicle manufacturers, infrastructure managers, insurance companies, car repairers) for further processing.

The Role of Consent

One of the key points outlined in the guidelines is the interplay between the GDPR[7] and the ePrivacy Directive[8] as currently implemented in national laws across the EU. The EDPB states that connected vehicles qualify as "terminal equipment" (as with a computer or a smartphone) under the ePrivacy Directive and are therefore subject to requirements that mandate consent to store or access information (including personal data) on an end-user's terminal equipment (*i.e.*, EU cookie rules). Reinforcing its opinion from May 2019,[9] the EDPB noted that although the GDPR and the ePrivacy Directive both will apply, where information stored in the end-user's device constitutes personal data, Article 5(3) of the ePrivacy Directive shall take precedence over Article 6 of the GDPR.

This finding means that granular consent always will be required to store and access any information within a connected vehicle. Any subsequent processing of such information (*i.e.*, processing of information outside of the vehicle) will require separate and additional consent. The EDPB clarifies that the initial consent (*i.e.*, "cookie consent") given in relation to the processing of information within the vehicle cannot be used to subsequently process information (*e.g.*, by the vehicle's manufacturer later on for its marketing purposes). This applies irrespective of whether the subsequent processing is for a compatible purpose for which the initial consent was given or for a wholly new purpose. Any subsequent processing of personal data remains subject to the GDPR. In sum, the EDPB's classification of connected vehicles as terminal equipment makes user consent a cornerstone of compliance regarding connected vehicle data processing.

The guidelines' case study of "Pay As You Drive (PAYD) Insurance" shows how this works in practice. An insurance company providing a PAYD insurance policy will require information such as the miles covered by the vehicle and the driving behavior (braking patterns, instances of rapid acceleration, etc.) of the policyholder, which may be contained in the SIM card of a telematics service incorporated into the vehicle. Regarding the EU cookie rules: (1) consent will be required to store and access such information within the vehicle and (2) separate consent also will also be needed to subsequently process the information by the insurance company outside of the vehicle. For any subsequent processing of personal data that takes place outside of the vehicle, the insurance company will need to comply with the GDPR and, among other actions, establish a lawful basis for processing the relevant personal data under GDPR Article 6.

There are two exceptions where the consent under ePrivacy Directive Article 5(3) may not be required initially: (1) for the sole purpose of carrying out the transmission of a communication over an electronic communications network and (2) when it is strictly necessary for the provider of an information society service explicitly requested by the subscriber or user to provide the service. In these limited scenarios, the EDPB acknowledges that the processing of personal data by accessing information within the vehicle can be solely based on one of the appropriate legal bases under GDPR Article 6.

Data Privacy Concerns and High-Risk Data

The EDPB guidelines also note that connected vehicles raise significant data protection concerns, emphasizing the following:

Lack of Control and Information Asymmetry: Drivers and passengers may not always be adequately informed about the processing of data taking place via a connected vehicle. This is

[6] Please see here for the guidelines.

[7] General Data Protection Regulation (2016/679).

[8] "ePrivacy" directive (2002/58/EC, as revised by 2009/136/EC).

[9] Please see here for the EDPB's May 2019 opinion.

particularly true because information only may be given to the owner of the vehicles, creating risk that affected individuals do not have the necessary control to avail themselves of their data protection and privacy rights.

Quality of User Consent: The consent obtained by individuals whose data is processed may not be high-quality consent. Where data processing is based on consent, all elements of a valid consent have to be met, meaning that for a given purpose consent shall be free, specific and informed; constitute an unambiguous indication of the data subject's wishes; and may not be bundled under the GDPR and further interpreted in the EDPB guidelines on consent.[10] The guidelines further specify that careful attention must be paid when obtaining valid consent from the various participants, such as car owners or car users.

Further Processing of Personal Data: In the same vein as set out above, when data is collected on the basis of consent as required by ePrivacy Directive Article 5(3), there is a risk that the data will be further processed on the basis of that initial consent. The guidelines underline that data only can be further processed if there is an additional lawful basis for processing, noting also that the initial consent will not legitimize further processing, as consent needs to be informed and specific to be valid.

Excessive Data Collection: The increasing number of sensors being deployed in connected vehicles naturally heighten the risk of excessive data collection compared to what is necessary to achieve the purpose for the collection.

Security of Personal Data: Multiple functionalities, services and interfaces (*e.g.*, internet, USB, RFID, Wi-Fi) offered by connected vehicles increase the amount of potential attack surfaces and therefore the number of potential vulnerabilities through which personal data could be compromised.

The guidelines further highlight three categories of "high-risk" personal data that warrant special attention:

Geolocation Data: Collecting geolocation data makes it difficult for data subjects to remain anonymous and may reveal sensitive information. The guidelines emphasize how controllers may "infer the place of work … residence and possibly reveal sensitive information such as religion through the place of worship, or sexual orientation through the places visited" by collecting geolocation data. Data controllers should therefore be vigilant and not collect location data except where absolutely necessary.

Biometric Data: When collecting biometric data it is crucial that the data subject is granted full control over their data, and that nonbiometric alternatives (*e.g.*, physical keys or codes) are available without additional constraints (*i.e.*, the use of biometrics should not be mandatory). Therefore, when storing and comparing biometric data, the EDPB stresses that this must be done so in encrypted form and only on a local basis.

Criminal Data: Certain personal data could reveal criminal offenses (offense-related data), such as for example, speed data combined with geolocation data that discloses a speeding offense. However, such data can only be processed under the control of official authority or when the processing is authorized by EU or member state law and provides for appropriate safeguards for the rights and freedoms of data subjects as stated in GDPR Article 10. As a result, the EDPB recommends the local processing of such data to ensure data subjects remain in control of such highly sensitive information and to protect against illegitimate access.

EDPB Mitigation Recommendations

To mitigate against the aforementioned risks the EDPB sets out, the guidelines include recommendations outlining how to handle and process the data, of which the key takeaways include:

Relevance and Data Minimization: Data controllers should pay special attention to the categories of data they need from a connected vehicle and only should collect personal data that is relevant and necessary for processing.

Data Protection by Design and by Default: Developing connected vehicles to enhance privacy is crucial in the connected car environment. As such, technology should be designed to keep personal data collection to a minimum and implement strict privacy protection settings. The EDPB stresses the importance of processing personal data locally and recommends using technology that does not involve the external transfer of personal data. Where personal data is transferred outside the vehicle, the EDPB recommends anonymization, or at least pseudonymization, of the data.

Information: Prior to processing, data subjects should be provided with information, such as the identity of the data controller, the purpose of processing and the data recipients, in clear and easily-accessible terms. The guidelines allow for information to be provided to data subjects in layers, based on two levels: (1) first-level information, which is information most important for data subjects (*e.g.*, identity of the data controller, purpose of processing, all recipients of the data), and (2) second-level information, which is information that is of interest at a later stage.

[10] Please see here for guidelines on consent.

Data Subject Rights: Data controllers should ensure that data subjects have control over their data during the entire processing period. The guidelines encourage companies to implement tools providing data subjects with an effective way to exercise their rights under the GDPR, recommending the use of a profile management system that allows data settings to be centralized and data subjects to record their preferences to exercise their rights.

Security: Data controllers should ensure that connected vehicles have measures that guarantee the security and confidentiality of processed personal data, such as by using encryption-key management systems that are unique to vehicles or by making access to personal data subject to reliable user authentication techniques (*e.g.*, passwords, electronic certificates).

Key Takeaways

The guidelines set out a detailed compliance regime for connected vehicles based on an interplay between the ePrivacy Directive and the GDPR. The EDPB's position that connected vehicles are terminal equipment for the purposes of the ePrivacy Directive — and therefore are subject to its rules mandating consent to store or access information — makes user consent a central tenant of the compliance regime for processing data in the connected vehicle ecosystem. It will be interesting to see the final guidance following the May 1, 2020, public comment deadline, given the significant potential consequences for industry participants.

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
213.687.5010
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

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

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
One Manhattan West
New York, NY 10001
212.735.3000