Skadden

Privacy & Cybersecurity Update

UK Information Commissioner's Office Publishes Draft Guidance on Employment Monitoring at Work

The recent fines imposed on Meta Platforms Ireland Limited (Meta) by the Irish Data Protection Commission (DPC) have major implications for organizations that rely on contractual necessity as the legal basis for processing individuals' personal data to provide behavioral advertising.

On December 31, 2022, after a lengthy, multi-phase process, the DPC adopted its final decisions in cases against Meta, levying large fines against the company and concluding that the company's Facebook and Instagram operations had violated the General Data Protection Regulation (GDPR) in connection with their processing of personal data for behavioral advertising. The decision has important implications for companies seeking to relying on the GDPR's concept of "contractual necessity" as the legal basis for processing personal data for behavioral advertising.

Nature of the Complaints

Prior to the GDPR's effective date in May 2018, Facebook and Instagram had updated their respective Terms of Use and privacy policies to set out specifically how each platform would now rely on contractual necessity as the basis for lawfully processing users' personal data for the purpose of behavioral advertising, rather than relying on user consent or another appropriate legal basis for such activities. Shortly thereafter, two complaints were lodged with the DPC asserting that Meta (doing business as Facebook at the time) was not relying on contractual necessity, but was in fact relying on users' consent as the legal basis to process personal data for the purpose of behavioral advertising, and that this consent was not valid under the GDPR. The complaints noted that users were required to click the "I accept" button in the Terms of Use to access Facebook and Instagram services. The complainants noted that unless people gave their consent they would only have access to a limited view of Instagram or would be required to delete their Facebook account. Since the use of these services was conditioned on giving consent to these unrelated, bundled advertising activities and users were unable to refuse consent without detriment, the complainants argued that the consent was not freely given, specific, informed and unambiguous, and therefore was invalid under the GDPR.

Meta argued that it entered into a contract with the user at the point at which the user accepted the Terms of Use. The company further argued that as Facebook and Instagram are inherently personalized services, the processing of personal data for the purpose of behavioral advertising was necessary for the performance of its contract with users.

Procedure and Enforcement

The DPC's Initial Findings

On May 14, 2022, the DPC initially concluded two inquiries into the processing activities of Meta, finding that (1) the company had breached the GDPR by failing to process Facebook and Instagram users' personal data in a lawful, fair and transparent manner, but that (2) Meta could lawfully rely on contractual necessity as the appropriate legal basis to process Facebook and Instagram users' personal data for the purpose of behavioral advertising.

The DPC proposed fines of €28-€36 million on Facebook and €23 million on Instagram.

Cooperation With Other European Supervisory Authorities

Since this case involved cross-border data processing, the DPC was required under Article 60 of the GDPR to submit its draft decision to 17 other European supervisory authorities before the draft decision could be finalized.

Ten supervisory authorities raised objections, arguing that Meta's processing of user data for the purpose of behavioral advertising was not necessary to deliver Facebook and Instagram services, and, as a result of Meta not having an appropriate legal basis for such processing, the fines needed to be reconsidered and increased.

The DPC dismissed these objections as not "relevant or reasoned," which triggered the dispute resolution mechanism under Article 65(1)(a) of the GDPR, whereby the European Data Protection Board (EDPB) adopts a binding decision.

EDPB's Binding Decision

On December 5, 2022, the EDPB concurred with the DPC's finding that Meta had breached the GDPR by failing to process Facebook and Instagram users' personal data in a lawful, fair and transparent manner. However, the EDPB rejected the DPC's finding that Meta could continue to lawfully rely on contractual necessity as the appropriate legal basis to process users' personal data for the purpose of behavioral advertising. As a result, the EDPB directed the DPC to reconsider the amount of fines issued against Meta and to conduct a new investigation into Facebook's and Instagram's processing activities.

DPC's Final Decision

On December 31, 2022, the DPC adopted its final decisions, finding that Meta could not rely on the contractual necessity legal ground to process its users' data for the purpose of behavioral advertising, and imposed increased fines of approximately €210 million on Facebook and €180 million on Instagram, or roughly $420 million in total. The DPC further ordered Meta to bring its processing activities into compliance with the GDPR within three months.

However, the DPC did not indicate in its final decision any intention to conduct new investigations into Facebook and Instagram as directed by the EDPB, on the basis that such direction may involve an overreach on the part of the EDPB. The DPC has further stated on its website that "it considers it appropriate that it would bring an action for annulment before the Court of Justice of the EU in order to seek the setting aside of the EDPB's directions."

Separately, Meta announced its intention to appeal both decisions and the related fines.

Key Takeaways

As Meta's appeal of these decisions works its way through the Irish appellate system, organizations should review how their data collection and processing activities compare with those at issue in the case, and be mindful that — at least for now — data protection authorities may not view contractual necessity as an appropriate legal ground for processing users' data for the purpose of behavioral advertising.

When conducting processing activities for the purpose of behavioral advertising, organizations will need to carefully consider which legal basis will be appropriate depending on the industry in which they operate. In a business-to-business context, organizations may be able to rely on legitimate interests, whereas, in a business-to-consumer context, organizations may need to obtain valid consent from their users prior to engaging in such activities.

Return to Table of Contents

Final CPRA Regulations Anticipated To Take Effect in April 2023

The California Privacy Protection Agency (CPPA) has indicated that it will not issue final regulations implementing the California Privacy Rights Act (CPRA) until late January or early February 2023, meaning the final regulations likely will not take effect until at least April 2023.

On January 23, 2023, the CPPA announced that the agency will hold a public meeting on February 3, 2023, to discuss the status of its rulemaking process for the CPRA, setting off a timeline that seems likely to result in final regulations that will be enforceable in April 2023.

As described in greater detail in our November 2022 *Privacy & Cybersecurity Update*, although the CPRA became enforceable on January 1, 2023, the CPPA was unable to develop and approve final regulations before that date. If, as expected, the CPPA submits final regulations to its board in early February and the board approves the draft, the agency can submit the final rulemaking package to the California Office of Administrative Law (OAL) in mid-February. The OAL would then have 30 working days to approve or disapprove the regulations, and upon their approval, the draft regulations will become final. Thus, board members have stated that the soonest the regulations could take effect is in April.

Civil and administrative enforcement of the CPRA was originally set to commence on July 1, 2023. However, the CPPA board has discussed the need to act as a "reasonable enforcer" and provide leniency to businesses that have made good-faith efforts to comply with the regulations given the uncertainty regarding when the regulations will be finalized and the limited time remaining for businesses to adjust their compliance posture. Furthermore, the most recent proposed CPRA regulations indicate that enforcement may be further delayed on a case-by-case basis. Specifically, the proposed regulations stated that the CPPA "may consider all facts it determines to be relevant, including the amount of time between the effective date of the statutory or regulatory requirement(s) and the possible or alleged violation(s) of those requirements, and good faith efforts to comply with those requirements."

Once the current rulemaking package, which is only a partial set of regulations, is finalized, we expect additional regulations related to automated decision-making, cybersecurity audits and privacy risk assessments in the near future.

Key Takeaways

Until the new regulations are finalized, companies should ensure that they comply with existing California Consumer Privacy Act regulations. However, as some CPPA board members have indicated that they do not expect major revisions to the most recent CPRA draft regulations and that the enforcers may provide leniency to businesses that have made good-faith efforts to comply with the regulations, companies should be preparing to comply with the CPRA's regulations as well.

Return to Table of Contents

UK Information Commissioner's Office Publishes Names of Organizations Subject to Data Breaches, Complaints and Investigations

The U.K.'s Information Commissioner's Office (ICO) has published a range of data sets on its website that identify organizations that have self-reported personal data breaches, that were the subject of data protection complaints, and that were under investigation by the ICO.

In December 2022, in a change of policy, the ICO published numerous data sets relating to self-reported personal data breaches, data protection complaints from members of the public and investigations by the ICO for breaches of U.K. data protection laws (including the U.K. GDPR, the U.K. Data Protection Act 2018, and the Privacy and Electronic Communications Regulations 2003 (PECR)).[1] Published under the umbrella label "Complaints and concerns," the data sets include the names of organizations that were the subject of such reports, complaints and investigations, even if no enforcement action was taken against them by the ICO. While the ICO regularly publishes the names of organizations that are the subject of a major audit or enforcement action (*e.g.*, penalty notice), the office has not previously published information about organizations in relation to routine complaint handling, investigations or personal data breach notifications.

The change of policy appears to be inspired by the ICO's "new" approach to enforcement action, which places a greater emphasis on transparency. At the National Association of Data Protection Officers on November 22, 2022, U.K. Information Commissioner John Edwards noted[2] that "members of the public, and those affected by a breach or infringement are entitled to know that we've held the business or organization to account, and that they've changed their practices as a result."

Overview of the Data Sets

The ICO published various data sets, including:

- **Data protection complaints:** Data sets of complaints the ICO has handled from members of the public about organizations' personal data practices.
- **Self-reported personal data breaches:** Data sets of instances where organizations have self-reported potential personal data breaches to the ICO.

[1] The data sets can be found here.

[2] Read John Edwards' keynote speech here.

- **Cyber investigations:** Data sets of investigations by the ICO of potentially serious breaches of personal data resulting from cyber-related attacks.
- **Civil investigations:** Data sets of investigations by the ICO of potentially serious breaches of personal data resulting from causes other than cyber-related attacks.
- **Investigations under PECR:** Data sets of investigations of potentially serious breaches of privacy rights in relation to electronic communications under PECR (*e.g.*, cookies, marketing calls, texts and emails).

The data sets include a range of high-level information, including the:

- applicable legislation (*e.g.*, U.K. GDPR, PECR);
- name of the organization responsible for the processing of personal data;
- sector the organization operates in;
- nature of the issues involved (*e.g.*, the article of the U.K. GDPR that the organization is alleged to have breached); and
- outcome of the ICO's evaluation of the issues (*e.g.*, "insufficient information to proceed," "no further action," "advice given" or "fine – lower tier").

To date, the ICO has published quarterly data sets for the period from January 2021 to June 2022. These data sets contain information about matters that the ICO has already evaluated (*i.e.*, not matters that are still under consideration). It remains to be seen whether the ICO will continue to publish these data sets on a quarterly basis and whether it will publish more granular information (*e.g.*, the amount of any fine imposed on an organization).

Publication of Reprimands

The publication of the data sets follows the decision by the ICO to publish all reprimands issued from January 2022 onward, unless there is a justified reason not to (*e.g.*, matters of national security). A reprimand is a nonbinding enforcement action that the ICO can exercise under the U.K. GDPR following an investigation or a dialogue with an organization about any area of noncompliance. While a reprimand cannot compel an organization to take action, it usually includes a set of recommendations that the ICO expects an organization to implement. Announcing the publication of the reprimands, the ICO's Director of Investigations Stephen Eckersley highlighted the ICO's increased emphasis on transparency, stating "ultimately, we want to be transparent with the public when we hold a business or organization to account."[3]

Key Takeaways

While some organizations may be concerned about potential reputational damage arising from the publication of the data sets, they should take comfort in the fact that the vast majority of entries in the data sets do not involve enforcement action being taken against the organizations concerned. As such, organizations that implement robust data protection and cybersecurity policies, plans and procedures are unlikely to suffer reputational damage from the publication of these data sets or any future plans by the ICO to increase transparency.

Return to Table of Contents

CJEU Rules That Organizations Must Disclose Individual Recipients of Personal Data in Data Subject Access Requests

The Court of Justice of the European Union (CJEU) has delivered a preliminary ruling stating that the GDPR requires data controllers to provide data subjects with a list of the specific recipients of their personal data when responding to data subject access requests.

On January 12, 2023, the CJEU delivered a preliminary ruling in the *RW v Österreichische Post AG* (Post AG) case.[4] The CJEU ruled that the GDPR permits data subjects to decide whether they want to obtain the categories of recipients, or a list of the specific recipients of their personal data. The CJEU also clarified that a data controller may only refuse to provide such information according to certain limited exceptions.

Background

On January 15, 2019, a data subject identified in the ruling as "RW" asked Post AG, an Austrian postal service provider, (1) whether his data was shared with any third parties and (2) if it was, the identity of those third parties. In response, Post AG stated that, generally, it used personal data to the extent permissible by law in the course of its activities and provided data to business customers for marketing purposes. The service also directed RW to websites containing general data protection notices and general information regarding the categories of recipients to whom Post AG disclosed personal data. However, Post AG did not reveal the specific recipients of RW's personal data.

RW initiated proceedings against Post AG, seeking an order requiring the service to disclose a list of the specific recipients of his personal data. In response, Post AG provided RW with a list of the categories of recipients of his personal data, including IT organizations, advertisers and nongovernmental organizations.

[3] Read Stephen Eckersley's comments here.

[4] The decision is available here.

The Language of the GDPR and Lower Court Rulings

Article 15(1)(c) of the GDPR provides that data subjects have the right to obtain from data controllers "the recipients or categories of recipient to whom their personal data have been or will be disclosed." The GDPR does not expressly state whether the data subject or the data controller has the power to choose between providing a list of specific recipients or categories of recipients.

RW's case was dismissed at first instance and on appeal on the grounds that, according to the courts, the GDPR gave the data controller the choice as to what information to provide.

On referral to the Austrian Supreme Court, the court disagreed with the lower courts and found that the GDPR supported the position that it is up to data subjects to decide the level of details they wish to receive, noting that if data controllers had the choice, they would never provide lists of specific recipients. However, as this required an interpretation of GDPR, the Austrian Supreme Court referred this question to the CJEU, which provides preliminary rulings in situations such as the one at hand when the national court of an EU member state requires an interpretation of EU law before it can pass judgment.

Scope of Data Subjects' Right To Be Informed

The CJEU found that since the terms "recipients" and "categories of recipients" were used in succession, it was difficult to determine if the GDPR expressed a preference for the type of information that should be provided to data subjects. However, the CJEU concluded that the overall intent of the GDPR is to give data subjects the ability to receive more than mere categories of recipients of their personal information. The CJEU noted that:

- Recital 63 of the GDPR gives data subjects the right to know and obtain information from a data controller with respect to the specific recipients of their personal data, without reference to categories of recipients;
- The right of access is intended, in part, to enable data subjects to verify that the data controllers are complying with the GDPR's data processing principles under Article 5, including the principle of transparency; and
- This data subject access right is different from certain obligations in Articles 13 and 14 for data controllers to provide information to data subjects, which also allows for providing information on recipients or categories of recipients.

The CJEU ruled accordingly that for data subjects to be able to effectively exercise their GDPR rights, they must have the right to be informed of the specific recipients of their personal data.

The Limited and Narrowly Tailored Exceptions

The CJEU notes that Article 12(5) of the GDPR offers data controllers certain narrow exceptions to their obligations to respond to data subject requests. As the GDPR safeguards the freedoms of data subjects to exercise their rights, the exceptions to these requests are limited and narrowly tailored. Accordingly, the CJEU found that a data controller is obliged to provide a data subject with a list of the specific recipients of their personal data unless it is (1) impossible, or (2) the controller can show that the request is manifestly unfounded or excessive.

The CJEU noted that the impossibility exception will only apply in very limited circumstances. For example, it could arise where a data subject submits a data subject access request without providing the data controller with any means of identifying and contacting the data subject (*e.g.*, a letter containing only the data subject's first name and no other contact details).

The manifestly unfounded exception only applies if the data subject has no clear intention to access their data or is using the request to harass an organization with no purpose other than to cause disruption. For example, this could arise in a case in which a data subject decides that information that a data controller holds about them is inaccurate, so they decide to make unsubstantiated claims against the data controller coupled with numerous vexatious access requests.

According to EDPB guidance, the exception for excessive requests would apply if, for example, (1) the data subject access request repeats the substance of previous requests, (2) the request overlaps with previous requests or (3) a reasonable period of time has not elapsed between the requests.

Key Takeaways

The obligation on data controllers to provide data subjects with a list of the specific recipients of their personal data will pose practical challenges for all organizations.

In light of the CJEU's ruling and the narrow interpretation of the impossibility and manifestly unfounded and excessive exceptions, organizations will have to ensure that they have sufficient internal processes in place to identify the third parties with whom they share data subjects' personal data and can access that information to ensure their continued compliance with GDPR. In particular, organizations should maintain an up-to-date repository of their data protection agreements with third parties, which should contain a list of the processors and subprocessors used.

Return to Table of Contents

FCC Issues Proposed Changes to Customer Data Breach Reporting Requirements

The Federal Communications Commission (FCC) recently proposed changes to the data breach reporting requirements for customer proprietary network information (CPNI) that apply to U.S. telecommunications carriers.

On January 6, 2023, the FCC released a notice of proposed rulemaking (NPRM) to update and strengthen its data breach reporting requirements for U.S. telecommunications carriers with respect to consumer data. The FCC seeks to align the requirements with the Cybersecurity and Infrastructure Security Agency's (CISA) new incident reporting system. The proposed rulemaking is open for comment until February 22, 2023, and reply comments are due by March 24, 2023.[5]

Key Proposed Changes

The key changes in the NPRM include the following:

- **An expansion of the definition of "breach."** The proposed rule would expand the definition of "breach" to include *inadvertent access*, use or disclosures of customer information. The current rule defines a breach as an instance "when a person, without authorization or exceeding authorization, has *intentionally* gained access to, used, or disclosed CPNI" (emphasis added).
- **Notifying the FCC and other federal law enforcement agencies of data breaches.** The proposed rule would require carriers to notify the FCC of any data breaches as soon as practicably possible. Under the current rule, carriers are required to notify the FBI and the Secret Service, but not the FCC itself. The FCC stated that this proposal would align the commission's data breach requirements with other federal sector-specific laws that require prompt notification to the relevant subject-matter agency.
- **Notifying customers.** The proposed rule would require carriers to notify customers of CPNI breaches "without unreasonable delay" after discovery of a breach and notification to law enforcement, unless a law enforcement agency requests a delay. The current rule prohibits carriers from notifying customers or disclosing the breach to the public until at least seven full business days after notification to the Secret Service and FBI.
- **Implementing equivalent measures to telephone and video relay service providers.** The proposed rule would amend the data breach requirements for Telephone Relay Service (TRS) and Video Relay Service (VRS) providers to include identical requirements as those proposed for carriers. This expansion would ensure equivalent privacy protection for TRS and VRS users.

Other Proposed Changes and Comments

The FCC also is seeking comment on whether to adopt a harm-based notification trigger that would allow carriers to refrain from sending a notification to customers or law enforcement of a breach for instances where a carrier can reasonably determine that no harm to customers is reasonably likely to occur. The current rule requires a notification in any instance where there is a breach of a carrier's customers' CPNI. The FCC noted that many states already use such a harm-based trigger.

Finally, the FCC is asking for comments on whether to set a threshold on the number of subscribers affected to require notification to the commission and law enforcement, whether there should be a requirement for breach notifications to include disclosures of specific types of information and whether to address breaches of sensitive information beyond CPNI.

Key Takeaways

The FCC's proposed rulemaking and request for comment signals some potentially significant changes to the commission's cybersecurity breaches requirements. These changes would bring the commission's rules in closer alignment with other federal and state breach notification standards. Carriers and TRS and VRS providers within the FCCs jurisdiction should consider submitting comments to the FCC and should closely monitor the commission's actions in this area.

Return to Table of Contents

District Court Approves $11 Million Settlement to End Data Breach Class Action

The U.S. District Court for the Northern District of Texas approved an $11 million settlement resolving claims against insurance technology provider Zywave Inc. (Zywave) and its subsidiary Insurance Technology Corp (ITC) stemming from a data breach that allegedly exposed personal information of over 4 million individuals.[6]

The Data Breach

In February 2021, ITC suffered a data breach in which hackers allegedly unlawfully gained access to the names, Social Security numbers, driver's license numbers, dates of birth and other sensitive information belonging to over 4 million individuals who were customers of insurance brokers who were, in turn, customers of Zywave and ITC. In May 2021, Zywave and ITC began notifying customers of the data breach.

[5] The FCC's announcement and proposal can be found here.

[6] The case is *Heath, et al. v. Insurance Tech. Corp., et al.*, No. 21-cv-01444-N (N.D. Tex. Jan. 4, 2023) (ECF No. 554).

The Class Action and Settlement

Shortly thereafter, in June 2021, a group of individuals allegedly affected by the data breach filed a putative class action against Zywave and ITC in the Northern District of Texas individually and on behalf of a class of all persons whose personally identifiable information (PII) allegedly was compromised as a result of the data breach. The lawsuit alleged that the PII of plaintiffs and the putative class members was compromised due to Zywave and ITC's negligent and/or careless acts and omissions and their failure to adequately protect the class members' PII.

In February 2022, the named plaintiffs reached a proposed settlement with Zywave and ITC and sought preliminary approval of the settlement from the court, which was granted in March 2021.

The proposed settlement provided that the court should certify, for settlement purposes only, a nationwide class of all individuals whose PII was potentially subjected to the data breach and a California subclass of all California residents at the time of the data breach whose PII was potentially subjected to the data breach (collectively, settlement class). It also created an $11 million settlement fund and provided for three separate categories of relief: (1) cash payments in the amount of $100 to $300 to eligible settlement class members residing in California; (2) reimbursement of up to $5,000 in out-of-pocket expenses incurred as a result of the data breach per settlement class member; and (3) 12 months of an identity theft protection service. As part of the proposed settlement, the parties agreed that the plaintiffs would ask the court to approve a $2,000 service award to each named plaintiff and an award of attorneys' fees of up to one-third of the settlement amount (*i.e.*, approximately $3.7 million) plus costs and expenses not to exceed $30,000, all of which would be paid from the $11 million settlement fund.

On January 4, 2023, the district court granted final approval of the settlement, concluding that it was "fair, reasonable, and adequate, and in the best interest of the Settlement Class," certifying that the prerequisites under Rule 23 of the Federal Rules of Civil Procedure had been met. The court also approved the requested $2,000 service award for each named plaintiff and the requested $8,666.63 in costs and expenses to the plaintiffs' counsel, but awarded $3 million in plaintiffs' attorneys' fees (slightly lower than the requested $3.7 million).

Key Takeaways

The Zywave settlement underscores the importance of businesses to ensure that they have adequate safeguards in place to protect against data breaches and other cybersecurity threats. It also provides an important reminder for businesses to consider whether and how their insurance programs may respond to such incidents.

Return to Table of Contents

Beyond the CCPA: Additional Privacy Laws for Specific Groups Take Effect in California

Against the backdrop of the broader CCPA and its amendments in the CPRA, new privacy laws protecting certain specific groups took effect in California, demonstrating that even after states enact sweeping privacy legislation, there remains room for additional, more targeted privacy protections.

On January 1, 2023, several targeted privacy laws took effect in the state of California that provide protections to student test takers, users of mental health applications, victims of a crime or an alleged crime, and fleet and commercial vehicle drivers. These new privacy laws demonstrate that, even after passing broad privacy laws like the CCPA and CPRA, state legislatures can find gaps that can be addressed through additional legislation.

The CCPA, which was signed into law in June 2018 and went into effect on January 1, 2020, created new privacy-related rights for California consumers and imposed substantial new data protection obligations on businesses that collect or store data about California consumers. While the CCPA provides broad protections, the legislature quickly amended it by passing the CPRA, which took effect on January 1, 2023, and will provide expanded privacy protections for California consumers once final draft regulations are approved.

On the same day, these four other laws with privacy implications took effect in California:

- The Student Test Taker Privacy Protection Act (protecting information about students taking proctored tests);
- Assembly Bill 2089 (expanding medical privacy to additional types of information);
- Senate Bill 1228 (creating procedures around the use of DNA information to prevent misuse by law enforcement); and
- Assembly Bill 984 (prohibiting the use of tracking devices in certain types of new alternatives to vehicle license plates).

New Privacy Legislation

The Student Test Taker Privacy Protection Act prohibits businesses that provide proctoring services in educational settings from collecting, retaining, using or disclosing personal information that is not strictly necessary to providing those proctoring services.[7] However, this prohibition does not apply in every circumstance. For example, the law allows a business to collect, use, retain or disclose personal information when it is necessary to comply with federal, state or local law.

[7] The full text of the law can be found here.

Assembly Bill 2089 amends California's Confidentiality of Medical Information Act (CMIA), which prohibits certain businesses from using medical information for any purpose that is not necessary to the provision of health care services, by expanding its definition of medical information.[8] The revised definition includes mental health application information, which, generally is defined as information related to a consumer's mental health or substance use disorder collected by a mental health digital service. Further, the law adds businesses that offer certain mental health digital services to within the purview of the CMIA.

Senate Bill 1228 creates procedures surrounding reference samples of DNA, and profiles developed from these samples, provided by victims of a crime or an alleged crime and individual volunteers for the purpose of exclusion.[9] These procedures, among other things, require law enforcement to use these DNA samples only for purposes directly related to the incident being investigated, prohibit law enforcement from comparing these DNA samples to other samples that are unrelated to the incident being investigated and prohibit law enforcement from including these DNA profiles in databases that allow comparison or matching with profiles derived from DNA from crime scenes.

Finally, Assembly Bill 984 paves the way for California to begin using alternatives to existing vehicle identification systems such as stickers, tabs, license plates and registration cards.[10] These alternatives could include, for example, electronic devices such as digital license plates. Generally, the law prohibits these alternatives from being equipped with GPS or location tracking technologies when used on private vehicles. However, it allows such technology to be incorporated into these alternative devices for fleet and commercial vehicles, but imposes certain restrictions and notification requirements on the use of such technology. Specifically, while the law generally prohibits employers from using alternative devices with tracking technology to monitor employees, it does allow employers to use such devices to surveil employees during work hours if such surveillance is strictly necessary to an employee's performance of duties. Under the law, employers must first notify employees that they will be monitored and allow them to deactivate the device's monitoring capabilities outside of work hours. Notice to employees must include specific information such as what activities will be monitored, what employee data will be collected and where data will be stored.

Key Takeaways

While the CCPA and CPRA provide broad protections for California residents, these four additional laws demonstrate that legislatures may still find a range of other, more focused privacy issues on which to take action. Organizations should therefore continue to be on alert for small-profile laws that may affect their operations.

[8] The full text of the law can be found here.

[9] The full text of the law can be found here.

[10] The full text of the law can be found here.

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

Ken D. Kumayama
Partner / Palo Alto
650.470.4553
ken.kumayama@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Jason D. Russell
Partner / Los Angeles
213.687.5328
jason.russell@skadden.com

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

Ingrid Vandenborre
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

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