Skadden

Privacy & Cybersecurity Update

1 California Attorney General Announces New Regulations to Enhance CCPA Consumer Opt-Out Right

2 California Announces Privacy Protection Agency Board Members

2 Irish Data Protection Commission Releases 2020 Annual Report

4 Seventh Circuit Rules CGL Insurer Has No Duty to Defend Insured in Unlawful Debt Collection Lawsuit

5 Virginia Becomes Second State To Adopt Comprehensive Privacy Law

5 UK Information Commissioner's Office Releases SEC Transfer Analysis

California Attorney General Announces New Regulations to Enhance CCPA Consumer Opt-Out Right

On March 15, 2021, prior to his confirmation as Secretary for Health and Human Services in the Biden administration, then-California Attorney General Xavier Becerra announced a fifth set of new regulations that modify the California Consumer Privacy Act (CCPA). The regulations, which were approved by the Office of Administrative Law, fortify California consumers' rights to opt out of the sale of their personal information by prohibiting the use of so-called "dark patterns."[1] The regulations took effect the same day.

Background

The California Consumer Privacy Act, which was signed into law in June 2018 and became effective as of 2020, gives California consumers the rights to know about businesses' collection of their personal information, to request that it be deleted, and to opt out of its sale. Since its inception, Mr. Becerra had issued regulations to guide businesses in meeting their obligations and consumers in exercising their rights under the CCPA.

Prohibition on Dark Patterns

The newly issued regulations address the concern that so-called dark patterns — interfaces designed to confuse, mislead or frustrate users — would complicate the process of opting out of the sale of personal information and inhibit California consumers' exercise of their CCPA rights.

In particular, the regulations mandate that a business that sells personal information must present its notice of right to opt out by using straightforward language and formatting that is legible on various screen sizes. A press release issued by the attorney general's office added that the regulations also ban a business from placing unnecessary steps in the way of consumers exercising the opt-out right, such as by adding multiple screen click-throughs or by displaying information to encourage users to remain opted in.[2]

[1] The final text of the March 15, 2021, regulations can be found here.

[2] The full text of the press release by the attorney general's office can be found here.

Privacy Options Icon

The regulations additionally provide businesses with the choice to add a specially designed Privacy Options icon (shown below) in addition to posting the notice of right to opt out.[3] Use of the icon is intended to effectively communicate privacy options to consumers but is not mandatory.

Key Takeaways

The March 15, 2021, regulations are the latest of several modifications made to the CCPA since it took effect, though it is possible there will be additional regulations passed to alter the CCPA further into 2021.

Return to Table of Contents

California Announces Privacy Protection Agency Board Members

On March 17, 2021, California Gov. Gavin Newsom, then-Attorney General Xavier Becerra, Senate President Pro Tempore Toni G. Atkins and Assembly Speaker Anthony Rendon announced their five selections for the California Privacy Protection Agency's inaugural board.

Background

The California Consumer Privacy Rights Act (CPRA) established the California Privacy Protection Agency (CPPA), which will direct the rulemaking process to implement the CPRA's provisions. The agency will have full administrative authority to enforce both the CCPA and the CPRA[4] by bringing enforcement actions before an administrative law judge. Civil enforcement of the CCPA and CPRA will remain the responsibility of the California attorney general.

Inaugural Board Members

The CPPA's inaugural board appointees include the following Californians, each of whom has varied amounts of expertise in privacy, technology and consumer rights:

- Jennifer M. Urban (chair of the CPPA), clinical professor of law and director of policy initiatives for the Samuelson Law, Technology and Public Policy Clinic at the University of California, Berkeley School of Law;
- John Christopher Thompson, senior vice president of government relations at LA28, the Los Angeles Olympic and Paralympic Games;
- Angela Sierra, recent chief assistant attorney general of the Division of Public Rights of the State of California;
- Lydia de la Torre, professor at Santa Clara University Law School; and
- Vinhcent Le, technology equity attorney at the Greenlining Institute.[5]

Key Takeaways

The CPPA board is expected to begin the CPRA rulemaking process sometime in the summer of 2021. We will continue to monitor the CPPA's activity in the coming months.

Return to Table of Contents

Irish Data Protection Commission Releases 2020 Annual Report

On February 25, 2021, the Irish Data Protection Commission (DPC) published its annual report for 2020.[6] The Annual Report details the regulatory work completed by the DPC in 2020 in overseeing the application of EU data protection laws, including the General Data Protection Regulation 2016/679 (GDPR) and aims to facilitate compliance and foster accountability.

Following the influx of Big Tech companies to Dublin's "Silicon Docks" over the past two decades, the DPC has become one of the most influential data protection regulators in Europe. Its appointment as "lead supervisory authority" (*i.e.*, the supervisory authority in an EU member state with primary responsibility for dealing with a company's cross-border data processing activities) for many of the largest tech companies means that much of the most significant GDPR enforcement action can be expected to come from Ireland, subject to the cooperation mechanism in place (as further detailed below) under the GDPR between data protection authorities, the lead supervisory authority and the European Data Protection Board. As just one example of its influence, the case of *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems* (Case C-311/1), which has had numerous implications in recent matters, began with a complaint to the DPC. The data protection world should therefore keep a close eye on developments in Ireland, with the 2020 Annual Report helping to provide an analysis of the areas in which the DPC has been most active over the past year.

[3] A PNG file of the approved optional icon can be found here.

[4] Enforcement of the CPRA will begin July 1, 2023.

[5] More detailed biographies of each board appointee can be found here.

[6] The full text of the DPC's 2020 Annual Report can be found here.

2020 in Review

The 2020 Annual Report includes a number of notable statistics, particularly in relation to investigation and enforcement under the GDPR:

- **Cases and Staff.** The DPC handled a total of 10,151 cases in 2020, a 9% increase from 2019 figures (9,337 cases), a growth the agency attributes to an unwelcome trend: noncompliance with the GDPR by both organizations and individuals. Such misuse is the result of both genuine confusion over how the GDPR operates and is applied, as well as clear attempts to obfuscate the data protection requirements imposed by the GDPR. In order to combat this increase in cases, the DPC hired an additional five employees in 2020 (bringing its number of staff members to 145 at year end) and the government increased funding to the DPC year-on-year from €1.7 million in 2013 to €16.9 million in 2020.
- **Large-scale Inquiries.** As of December 31, 2020, the DPC had 83 statutory inquires on hand, including 27 cross-border inquiries, many of which are due to be finalized in 2021 and are diverse in topic matter. However, a number of the investigations are focusing on ensuring companies have discharged their GDPR obligations to only process personal data where they have a lawful basis, and provide adequate prior information in their privacy notices.
- **Fines.** The DPC issued a total of six administrative fines in 2020, one of which was in a €450,000 fine to Twitter International Company in December 2020, the regulator's first cross-border case. This fine was the first decision to go through the GDPR's Article 60 cooperation mechanism, under which supervisory authorities in other member states in the EU can object to the decision of the lead supervisory authority. In this case, the objections of the other member states included concerns about the calculation of the fine.
- **Complaints.** The DPC employs a dedicated team of individuals who solely focus on the receipt and handling of complaints under data protection laws and regulations. In 2020, 4,476 complaints against organizations from individuals were resolved by the DPC. Excessive personal data collection, employment law disputes and securing access to personal data were identifiable trends in complaints received, as noted in the report.
- **Breaches.** In 2020, there were 6,673 data security breaches recorded by the DPC, representing a 10% increase on numbers reported in 2019. The majority of breaches occurred in the private sector, and 87% of all data breach notifications received were classified as Unauthorized Disclosures. Notably, the use of social engineering and phishing attacks has increased since the beginning of the COVID-19 pandemic, demonstrating more than ever the need for organizations to take proactive steps to implement and test their IT security measures.
- **Data Protection Governance.** The DPC received 570 new data protection officer notifications over the past 12 months, bringing the total number at year end to 2,166. Though the majority of these notifications came from within the private sector, the compliance rate in the public sector rose substantially from 69% to 96%.

Key Takeaways

- The 2020 Annual Report (coupled with the DPC's Two-Year Regulatory Activity Report 2018-2020[7]) identifies general thematic patterns and issues which will feature heavily in the DPC's strategic plan going forward, specifically regarding supporting individuals, compliance, regulation and enforcement.
- The DPC's enforcement priorities acknowledge the central role of data protection compliance programs within organizations, stating that "[w]hilst ex-post enforcement by the DPC will always play a central role in the discharge of its regulatory functions, the DPC is also mindful of the importance of encouraging compliance at source." The DPC also noted in passing that enforcement efforts would continue, with cookies being a key focus of their activities in 2021. This was reflected in a speech by Irish Data Protection Commissioner Helen Dixon at a conference in late 2020, in which she was hesitant to list the DPC's enforcement priorities because enforcement is often more reactive than proactive.
- While the DPC has not issued fines as large as the French supervisory authority (the Commission nationale de l'informatique et des libertés), or as numerous as the Spanish supervisory authority (the Agencia Española de Protección de Datos), the 2020 Annual Report reveals that there are a large number of ongoing investigations that are due to be finalized in 2021. Many of these investigations involve Big Tech companies and therefore will undoubtedly attract media attention. We will continue to monitor the DPC's enforcement action and provide updates when we receive them.

Return to Table of Contents

[7] The full text of the DPC's Two-Year Regulatory Activity Report (2018 – 2010) is available here.

Seventh Circuit Rules CGL Insurer Has No Duty to Defend Insured in Unlawful Debt Collection Lawsuit

On March 12, 2021, the U.S. Court of Appeals for the Seventh Circuit affirmed a district court's ruling that Zurich American Insurance Company (Zurich) does not have a duty to defend debt collection company Ocwen Financial Corporation (Ocwen) under a commercial general liability (CGL) insurance policy, following accusations that Ocwen's debt collection practices violated the Telephone Consumer Protection Act (TCPA), the Fair Debt Collection Practices Act (FDCPA) and constituted an invasion of privacy.[8]

The Underlying Action

Plaintiff Tracey Beecroft sued Ocwen, alleging that it aggressively pursued her for collection of a debt that she had previously discharged in bankruptcy. According to Ms. Beecroft's complaint, Ocwen made 58 phone calls to her cell phone using an automatic dialer, and on two occasions she picked up the phone and asked Ocwen to stop calling. Ms. Beecroft allegedly suffered emotional and physical distress as a result of Ocwen's alleged harassing conduct and was allegedly denied a mortgage after Ocwen wrongfully reported the alleged default to credit agencies. The complaint alleged that Ocwen's conduct violated the TCPA, the FDCPA and the plaintiff's common law right to privacy.

The Coverage Dispute

Ocwen then tendered the lawsuit to its CGL insurer, Zurich. The insurer denied coverage in reliance on policy exclusions barring coverage for, among other things, bodily injury and personal and advertising injury directly or indirectly arising out of or based upon any act or omission that actually or allegedly violates the TCPA or any other statute or common law that addresses, prohibits or limits the printing, dissemination, disposal, monitoring, collecting, recording, use of, sending, transmitting, communicating or distribution of material or information.

Zurich then filed suit against Ocwen in the U.S. District Court for the Northern District of Illinois seeking a declaration that Zurich had no duty to defend or indemnify Ocwen for the underlying *Beecroft* lawsuit. On Zurich's motion for judgment on the pleadings, the district court ruled in the insurer's favor, concluding that Zurich had no duty to defend Ocwen because all of the factual allegations in the complaint fell within the scope of the policy exclusions. Following the ruling, Ocwen appealed to the Seventh Circuit.

Ocwen's Appeal to the Seventh Circuit

On appeal, Ocwen only challenged the district court's holding that the policy exclusions barred coverage for the common law invasion of privacy claim. According to Ocwen, the potential for coverage existed because the *Beecroft* lawsuit contains the following factual allegations that do not fall within the policy exclusions: (1) some calls were made to Ms. Beecroft's home phone using a live operator (thereby precluding TCPA liability because the statute prohibits calls to landlines only if artificial or prerecorded voices are used) and (2) some calls were not made with the intent to annoy, abuse or harass (thereby precluding FDCPA liability because that statute does not cover calls that were made negligently). According to Ocwen, this alleged conduct did not fall within the policy exclusions because it is not prohibited by the TCPA or the FDCPA and did not arise out of conduct that violates either statute.

A three-judge panel for the Seventh Circuit disagreed. While acknowledging the broad scope of the duty to defend under Illinois law, the panel explained that the "arising out of" language in Zurich's policy exclusion "excludes the underlying *conduct* that forms the basis of the violation of an enumerated law, even if liability for that underlying conduct might exist under a legal theory that is not expressly mentioned in the policy exclusion (*e.g.*, common-law invasion of privacy)."

The panel then proceeded to reject Ocwen's characterization of the allegations in the *Beecroft* complaint. Although the court acknowledged that the complaint alleges both that Ms. Beecroft answered two phone calls with a live operator and that Ocwen called her home phone, the court nevertheless concluded that "the natural reading of the complaint" precludes linking those two allegations together as Ocwen urged. In any event, even if the calls to Ms. Beecroft did not violate the TCPA, Ocwen could not escape the FDCPA, the court concluded, reasoning that the district court did not err in inferring that Ocwen intended to annoy or harass the plaintiff by continuing to call her after she requested that the company stop, which constituted a FDCPA violation.

Key Takeaways

This case serves as an important reminder for policyholders and insurers alike to closely review and understand the scope and import of policy exclusions, including lead-in and prefatory language, which can be outcome determinative. While many commercial general liability insurance policies contain exclusions for violations of the TCPA and similar laws such as the FDCPA, as the *Beecroft* court noted, an "arising out of" lead-in to exclusions can significantly broaden their scope and bar coverage for common law claims, such as invasion of privacy, that are based on the same underlying conduct.

Return to Table of Contents

[8] *Zurich Am. Ins. Co. v. Ocwen Fin. Corp.*, No. 19-3052, 2021 WL 939205 (7th Cir. Mar. 12, 2021).

Virginia Becomes Second State To Adopt Comprehensive Privacy Law

On March 2, 2021, Virginia Gov. Ralph Northam signed into law the Virginia Consumer Data Protection Act (CDPA), making Virginia the second state after California to enact comprehensive privacy legislation. The CDPA will become effective on January 1, 2023, the same day the California Privacy Rights Act (CPRA) comes into effect, replacing the current California Consumer Privacy Act (CCPA), which went into effect in 2020.

The new Virginia law draws on concepts from the European Union's General Data Protection Regulation (GDPR) (such as the use of "controllers" and "processors") and from California's laws (such as the rights of consumers). The net result will be a more complicated privacy compliance environment for companies that will be further exacerbated if additional states enact their own "similar but different" approaches to privacy law.

You may view this complete article, which was published as a stand-alone Skadden client alert on March 10, 2021.

Return to Table of Contents

UK Information Commissioner's Office Releases SEC Transfer Analysis

On September 11, 2020, the U.K. Information Commissioner's Office (ICO) issued a letter on the application of GDPR transfer provisions to U.K.-based firms seeking to comply with regulatory obligations to the Securities and Exchange Commission (SEC).[9] The ICO's letter concludes that U.K.-regulated firms can now rely on the "public interest" derogation to transfer U.K. personal data to the SEC during the course of an investigation. The letter was made public on January 19, 2021.

Following the European Court of Justice's decision in *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (*Schrems II*), the EU-U.S. Privacy Shield is no longer a legitimate mechanism for transferring personal data from the EEA/U.K. to the U.S. This decision has presented a significant challenge to EEA- and UK-based organizations, particularly as the derogations set forth in Article 49 of the GDPR are often unavailable as an alternative means of data transfer. These derogations are limited in scope, are applied only on an exceptional basis and, in strict compliance with the GDPR's accountability principle, must be well documented and subject to appropriate safeguards. The ICO's letter provides clarity on the application of the public interest derogation in the context of responding to mandatory information requests from the SEC, though some questions remain unanswered.

Background

The SEC requests and examines information in the course of its activities, which includes the administration of SEC-regulated U.K. entities. The information requested includes personal (and sometimes special category) data. The transfer of such data from U.K.-based companies to the SEC must comply with Article 44 of the GDPR, which provides that the level of protection guaranteed to natural persons must not be undermined by an international transfer. The U.S. has not received an adequacy decision from the European Commission and, following the *Schrems II* decision, the safeguards outlined in Article 46 of the GDPR cannot be easily guaranteed when transferring data to the U.S. As such, U.K.-based companies instead have to look to the limited derogations contained in Article 49 of the GDPR when responding to such regulatory requests.

The ICO's letter outlines how transfers to the SEC from the U.K. will meet the threshold for the Article 49.1(d) derogation, defined as the transfer being necessary for important reasons of public interest.

This decision is based on three key considerations:

- **U.K. Law.** The U.K. is a signatory to the Financial Stability Board, which lists "Objections and Principles of Securities Regulations" that are considered "materially relevant for fostering sound financial systems" and are consistent with the SEC's own rules and regulations. Additionally, the Financial Conduct Authority's handbook encourages cooperation with regulators (including overseas regulators).
- **Strict Necessity.** In the letter, the ICO also reiterated the importance of being able to identify the exact basis in EU/U.K. law for the relevant public interest, taking into consideration the principle of "strict necessity." It considered the bases under U.K. law to be sufficient for this purpose. It also noted that proportionality — "finding the balance between competing human rights" — should be considered in view of the EU Charter of Fundamental Rights and the European Convention of Human Rights.

[9] The full text of the ICO's letter can be found here.

- **Scope of Proportionality.** As indicated, linking to the "strict necessity" test is the requirement for proportionality, which aligns with the GDPR's core principles of data minimization and accountability. The ICO's letter concluded that SEC requests "are never regular and predictable" and "should not be large scale and systematic," reminding U.K.-based entities that they should document their considerations to maintain evidence that SEC requests are within the scope of their regulatory power and requirements, "as part of a fully auditable governance process."

Key Takeaways

U.K. companies likely will take comfort knowing that reliance on the public interest derogation for transfers of U.K. personal data to the SEC has been considered and authorized by the ICO. They should, however, still remain mindful of their obligations under the GDPR, including establishing a lawful basis for processing and complying with transparency obligations, as well as the data minimization and the accountability principles (such as by keeping up to date and detailed records of processing and transfers).

The ICO's letter confirmed that this decision would likely remain applicable given the U.K.'s exit from the EU in January 2021, and the subsequent implementation of the U.K. version of the GDPR.

However, it remains to be seen whether the public interest derogation is or will be applicable to data transfers to other U.S. regulators. The letter indicated that a discussion had or would at some point take place between the SEC and the ICO, a helpful indicator that other regulators have or may be considering entering into similar discussions.

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

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

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