DAVIS GILBERT

Privacy + Data Security

The Top 5 Privacy Issues to Watch for in 2022

The Bottom Line

- While every year brings new complexities to privacy law compliance, 2022 is poised to be a very impactful year.
- With three new U.S. state laws going into effect in 2023 and additional developments in Europe, companies may need to update their privacy programs, policies, and contracts this year in preparation for the various changes ahead.

While we could have listed a dozen or more issues from new laws to regulatory actions to changes by major platforms, below are the top five privacy issues to look out for this year.

Upcoming CPRA Regulations; Preparing for CPRA Compliance

Some parts of the California Privacy Rights Act (CPRA), a/k/a "CCPA 2.0", have already taken effect, including the creation of a new California Privacy Protection Agency (CPPA); the nation's first stand-alone privacy regulatory agency. The CPPA is tasked with drafting and adopting regulations under the CPRA **by July 1, 2022**. The subjects of these new regulations include, but are not limited to:

- Automated decision-making;
- The scope and process for audits by the CPPA;
- Consumer rights to delete and correct personal information;
- Consumer rights to limit the use of sensitive personal information;
- The definition of precise geolocation; and
- Cybersecurity audits and risk assessments to be conducted by businesses.

Most provisions in the text of the CPRA amending the California Consumer Privacy Act (CCPA) will become operative **on January 1, 2023**. Businesses need to pay attention to key changes to the CCPA, some of which include:

- New rules for "sensitive personal information," which include heightened transparency obligations and a requirement to offer consumers the ability to limit the use and disclosure of such data;
- A new definition of "precise geolocation," which includes an area equal to or less than a circle with a radius of 1,850 feet;
- New definitions for "sharing" personal information and "cross-context behavioral advertising," together with new compliance obligations for such activities;
- A new right for consumers to correct inaccurate personal information;
- Eliminating the CCPA's 30-day cure period for violations of the law;
- Requiring certain businesses to submit mandatory "risk assessments" to the CPPA on a "regular basis"; and
- Explicitly requiring businesses to enter into contractual arrangements when sharing personal information with third parties, and to flow down such provisions to any subcontractors that they engage.

These new regulations will be critical for ensuring CPRA compliance. Businesses should prepare for these changes – both from the text of the CPRA and the forthcoming CPRA regulations – and adjust their privacy compliance programs accordingly.

Getting Ready for Compliance With the Virginia CDPA

Virginia's Consumer Data Protection Act (CDPA) goes into effect **on January 1, 2023**, and companies need to begin planning this year to harmonize their privacy programs with the new law.

The CDPA will apply to those that conduct business in Virginia or produce products or services that are targeted to Virginia residents, and that control or process the personal data of at least:

- 100,000 consumers during a calendar year; **or**
- 25,000 consumers and derive over 50% of gross revenue from the "sale" of personal data (defined narrowly as "the exchange of personal data for monetary consideration").

The CDPA provides a range of consumer privacy rights, including rights of access, correction, deletion, portability, and the right to opt out of certain types of processing (including sales of personal data and use of personal data for "targeted advertising").

Similar to the EU's GDPR, it will also require data controllers to enter into contracts with processors that govern their processing activities and flow contractual obligations down to any subprocessors. The CDPA will also require controllers to conduct data protection assessments when engaging in certain processing activities, including targeted advertising, sales of personal data, the processing personal data for profiling that presents high privacy risks, processing sensitive data, and other processing that presents a heightened risk of harm to consumers.

While most privacy laws in the U.S. operate on an opt-out basis, the CDPA introduces an opt-in requirement to process certain sensitive data, such as precise geolocation.

Preparing for Compliance With the Colorado Privacy Act

On the heels of Virginia's new law, the Colorado Privacy Act (CPA) goes into effect **on July 1, 2023**.

The majority of the CPA's requirements will apply to controllers that conduct business in Colorado or produce products or services that are targeted to Colorado residents, and that control or process the personal data of at least:

- 100,000 consumers during a calendar year; **or**
- 25,000 consumers, and derive revenue or receive a discount on the price of goods or services from sales of personal data.

Unlike the California and Virginia privacy laws, there is no revenue threshold for applying the law, which means that business not subject to the CCPA/CPRA or CDPA may be governed by the CPA.

The CPA provides consumers with a set of rights akin to those found in the CDPA, and requires controllers to follow data processing principles such as transparency, purpose specification, and data minimization, similar to the GDPR. The CPA requires controllers to obtain a consumer's opt-in consent to process sensitive data, and, similar to the CDPA, requires companies to conduct and document a "data protection assessment" of activities that present "a heightened risk of harm to a consumer." The Colorado law also provides that an individual's consent is invalid if obtained through "dark patterns," defined as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice."

Implementing the Revised EU SCCs; Awaiting the UK SCCs

In June 2021, the European Commission issued revised Standard Contractual Clauses (SCCs) for use in international data transfers from the European Economic Area (see our prior alert). The new SCCs added many new features, including:

- A customizable design with different modules and optional clauses;
- A "docking clause" that allows for multi-party transfers; and
- More in-depth requirements for data security measures and disclosures concerning local laws that may affect compliance with the SCCs.

While the revised SCCs are already required for new contracts and processing operations going forward, the European Commission has stated that all existing contracts and data transfer agreements must be retrofitted with the new SCCs **by December 22, 2022**.

Additionally, since the United Kingdom is no longer part of the EU, the UK Information Commissioner's Office and Secretary of State are currently endorsing the older versions of the EU SCCs as a stopgap measure. However, the UK is formulating its own UK SCCs, and the UK ICO announced that it intends to publish them in 2022. Accordingly, companies will likely have to incorporate both the new EU and UK SCCs into their international data transfer arrangements by the end of the year.

Uncertainty in the EU Over Cookies and Behavioral Advertising

Last year saw numerous developments that may significantly impact behavioral advertising in the EU going forward. The Irish Council for Civil Liberties, the Belgian Data Protection Authority, and privacy advocate Johnny Ryan all brought legal actions which attack the underpinnings of the behavioral advertising ecosystem in the EU.

For years, the industry has coalesced around the IAB Europe's Transparency and Consent Framework (TCF) to obtain consent from users for the collection of cookie-based data to be used for behavioral advertising. The TCF program relies upon integration into cookie banners and passing consent strings to compliant ad tech companies.

Some regulators have questioned the validity of that consent and who is the controller when collecting such data. Regulators in France have particularly focused on non-compliant cookie banners. Without complying with the GDPR and obtaining proper consent, all such data used in the ad tech ecosystem is tainted. As these various matters unfold, it is possible that the industry will need to alter their practices in order to mollify regulators and ensure that these practices are compliant with the GDPR.

More Beyond the Top Five

These five issues are just the tip of the iceberg when it comes to the outlook for privacy in 2022. We could easily add to this list a more aggressive and newly constructed Federal Trade Commission, more states poised to pass their own privacy laws, major platforms thrusting changes on their users, Congress's seemingly inability to pass a comprehensive consumer privacy law, the rise of ransomware attacks, and an increased focus on sensitive personal information such as biometric data.

For More Information

Please contact the attorneys listed below or the Davis+Gilbert attorney with whom you have regular contact.

Gary Kibel

Partner
212 468 4918
gkibel@dglaw.com

Zachary N. Klein

Associate
212 237 1495
zklein@dglaw.com