California Privacy Protection Agency opens draft regulations for public comment

Changes are expected to consent and opt-out provisions. By **Lindsey Tonsager**, **Claire O'Rourke**, and **Kimberly Railey** of Covington & Burling in the US.

On 8 July 2022, the California Privacy Protection Agency (CPPA) filed the formal 'Notice of Proposed Rulemaking' on regulations that address the amendments made through the California Privacy Rights Act (CPRA). This notice triggered a public comment period that will last until 23 August 2022. The proposed draft regulations, first released with little fanfare on 27 May 2022, are far-reaching and implicate a variety of topics. In addition, the CPPA published an "Initial Statement of Reasons" that offers additional commentary and context for the draft rules. Notably, the CPPA stated this draft is not a comprehensive draft; further regulations related to automated decision-making, privacy impact assessments, and cybersecurity audits will be announced at a later date.

While there are topics remaining, there are many areas in the current draft available for public comment that will be of interest to businesses and consumers. Below is a non-exhaustive summary of key draft regulations.

'Explicit Consent' would be required for unrelated or incompatible processing

The draft rules state that a business must obtain "explicit consent" before collecting, using, retaining, or sharing personal information for purposes that, for the "average" consumer, are "unrelated or incompatible" with the purposes for which the personal information was collected or processed. "Explicit consent" would also be required before a business may collect any new category of personal information. The term "explicit consent" is new to the draft rules; it is not required in the CPRA statutory text.

> If a consumer deletes certain accounts with a business, then the business should automatically delete the consumer's information.

The draft rules include a few examples that suggest the impact on businesses could be significant. One example notes that if a consumer deletes certain accounts with a business, then the business should automatically delete the consumer's information because retention is not reasonably necessary and proportionate.

The draft rules further note some businesses should not use personal information to research and develop unrelated or unexpected new products or services without the consumer's explicit consent.

The rules also state that if a business collects information for a consumer transaction, then the business should obtain explicit consent to use that information to market other products or services. This requirement would appear to be inconsistent with the federal email marketing law (the CAN-SPAM Act), which preempts state law and permits the transfer of email addresses for commercial email marketing as long as the consumer has not opted out.

Opt-out for data sales and sharing for cross-context behavioural advertising

The CPRA statute provides consumers the right to request that their personal information not be sold to third parties or shared for cross-context behavioural advertising. The draft rules would require businesses to honour opt-out preference signals that would apply universally across all businesses and could be offered by the provider of a platform, technology, or mechanism (such as, for example, HTTP header fields for a browser). The rules further clarify that the provider of the opt-out preference signal must make clear to the consumer that the use of the signal will opt the consumer out of the sale and sharing of their personal information. The draft rules would also require businesses to display a consumer's status with respect to the opt-out signal.

Through examples, the regulations also appear intended to address how businesses should handle competing signals. The draft rules discuss a situation where a consumer visits a business's website using a browser with an opt-out preference signal and then visits the business's website with a different browser which does not have the opt-out preference signal enabled. If the business can recognize the consumer across the two browsers, the business should treat the consumer as opted out, despite the consumer appearing to indicate a different choice.

Notably, the Initial Statement of Reasons explains that the draft regulations do not cover opt-in and opt-out expressions for consumers aged 16 and under, partially because "no mechanism currently exists to communicate the expression of these rights."

'Dark patterns' are defined and further clarified

The draft rules also interpret the CPRA's definition of a "dark pattern," or when an "interface has the effect of substantially subverting or impairing user autonomy, decision-making, or choice, regardless of a business's intent." The draft rules require that the number of steps/clicks to opt out may not be more than the number of steps/clicks to provide opt-in consent. The rules would also bar the use of speech that warns consumers of the consequences of their decisions, such as, "No, I don't want to save money" when offering a financial incentive. The draft rules also prohibit bundled consent for "reasonably expected purposes together with purposes that are incompatible to the context in which the personal information was collected."

Provision of advertising and marketing services

The rules cover the kinds of advertising and marketing services that may be offered by service providers and contractors. For instance, pursuant to the draft rules, a company that acts as a service provider or contractor "cannot use a list of [its business customer's] email addresses to identify users on the social media company's platform and serve advertisements to them," apparently regardless of whether that company has agreed to use the information only for the business's benefit and to not use it for its own or others' benefit.

Service provider/ contractor processing

The draft rules largely preserve the processing activities for which service providers and contractors may use personal information. However, there is a proviso on the language authorising internal use of personal information to build or improve the quality of services. That authorisation now "prohibits use [of] the personal information to perform services on behalf of another person." In addition to qualifying the processing activity, the draft rules imply that a business may be liable for violations by their service providers and contractors unless the business, beyond having a compliant written agreement with the vendor, conducts due diligence of the vendor, especially by exercising rights to audit or test such entities' systems.

It is not clear how this will be ultimately reconciled with the plain text of the CPRA, which seems to have a contrary meaning.

The draft rules also elaborate on the terms that written contracts between businesses and service providers/contractors must contain. For example, the agreements would need to specify limited and "specific" purposes for which personal information is sold or disclosed. These purposes may not be described in "generic terms, such as referencing the entire contract generally." Without the required contractual provisions, the relationship between a business and the other entity could be automatically considered a "sale" under the CPRA, regardless of whether or not there is an exchange of personal information for monetary or other valuable consideration. In contrast, the statutory "sale" definition only covers exchanges of personal information for monetary or other valuable consideration.

Third-party liability and contractual requirements

The draft rules further suggest a business may be liable for third-party violations unless the business, in addition to having a compliant written agreement with the vendor, conducts due diligence of the vendor – particularly, by exercising rights to audit or test such entities' systems. As with the service providers and contractors text, this provision appears to be inconsistent with the CPRA's similar plain text language.

The draft rules additionally elaborate on the obligations for written contracts between businesses and third parties to which a business has sold or shared personal information. Pursuant to the draft rules, the relevant contracts must include limited and specific purposes for which personal information is sold or disclosed. There are also further specific terms required, similar to those for the service provider and contractor terms.

'Totality of circumstances' test for correction rights

The draft rules establish a "totality of the circumstances" test for businesses

> First parties must disclose the names, and not solely the categories, of all third parties.

to determine whether personal information is "more likely than not" accurate. Based on this test, the rules state that a business may deny a consumer's correction request if it determines that the contested personal information is more likely than not accurate. The rules also permit a business to delete the disputed personal information as an alternative to correcting the information, as long as the deletion of the personal information does not negatively impact the consumer, or the consumer consents to the deletion.

Further, the rules require businesses to not only correct personal information on existing systems but also to implement measures to ensure personal information "remains correct." A business dealing with a correction request must not only correct personal information but must also give the consumer the name of the source of the contested information in cases where the business itself is not the source of the information.

Greater detail on notice requirements

When a business provides a link to its privacy policy to meet the CPRA's notice requirements, the draft rules could require this link to direct consumers exactly to the section of the privacy policy with the required information, rather than the top of the privacy notice. It is unclear how this provision would work when a business includes disclosures in various sections of the policy, such as sections governing information collection, disclosure, and consumer rights.

Additionally, any third party that controls the collection of a consumer's personal information must provide notice at or before the time it is collected, in addition to or included within the notice at collection provided by the first party.

The draft rules express that first parties must disclose the names, and not solely the categories, of all third parties that control the collection of personal information through the first party's website, online service, or physical location, unless the third party's privacy practices are described in the first party's notice.

Confidentiality, audits and enforcement

The draft rules state that audits, which can be conducted at the broad discretion of the agency, may be "announced or unannounced as determined by the Agency." Additionally, when the agency investigates following a response to a complaint filed through the agency's electronic complaint system, the Enforcement Division "will notify the complainant in writing of the action, if any, the Agency has taken or plans to take on the complaint, together with the reasons for that action or non-action."

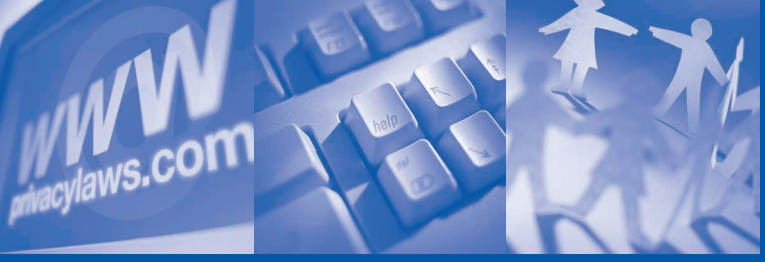
Conclusion

In the accompanying Initial Statement of Reasons, the CPPA states that the regulations as drafted "would not have a significant, statewide adverse economic impact directly affecting business." Public comment on these regulations will continue until 23 August 2022. The CPPA announced that there will also be public hearings the two days immediately following the end of the comment period.

Should the comment period, public hearings, or agency drafting decisions lead to substantial or major changes to the draft regulations, there must be an additional notice and comment period. However, if the CPPA enacts the rules without such changes, the rules could be finalised as soon as late September.

AUTHORS

Lindsey Tonsager, Partner, Claire O'Rourke, Associate, and Kimberly Railey, Associate of Covington & Burling LLP.
Emails: ltonsager@cov.com
corourke@cov.com
krailey@cov.com



ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Canada introduces three new bills to modernise privacy law

The proposed new law tries to balance privacy of individuals with growing demands for innovative processing for AI purposes, and competitiveness. By **Colin Bennett** of the University of Victoria, Canada.

On 16 June 2022, Canada's federal government tabled Bill C-27 – 'An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act'. They collectively comprise the Digital Charter Implementation Act of 2022.[1] Bill C-27 is a revision of Bill C-11 originally

Continued on p.3

China's Standard Contractual Clauses: Restricted use and complex terms

Welcome clarification on overseas data transfers even if data-heaviest companies will be excluded. By **Graham Greenleaf**.

At the same time as President Xi Jinping stepped briefly into Hong Kong for his "victory lap" after dismantling the "One China, Two Systems" system that it agreed to over 25 years ago, the Cyberspace Administration of China (CAC) issued a consultation draft on 30 June 2022 of its Standard Contract for the Export of Personal

Continued on p.6

Issue 178 **AUGUST 2022**

INTERNATIONAL report

ISSUE NO 178 AUGUST 2022

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Colin Bennett
University of Victoria, Canada
Zuzanna Gulczyńska
Ghent University, Belgium
Souzana Georgopoulou
PL&B Correspondent
Alexandra Guérin-François
CNAM University, France
Joanna Masson
Odoné, France
Lore Leitner, Jack McCarthy and Gabe Maldoff
Goodwin
Lindsey Tonsager, Claire O'Rourke, and Kimberly Railey
Covington & Burling, US
Katharina A. Weimer and Johanna Klingen
Fieldfisher, Germany
Tamar Kaldani
Convention 108 Consultative Committee, France

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

AI is becoming a common theme in new privacy laws

We are pleased to bring you news about Canada's federal level Bill, the Digital Charter Implementation Act, 2022 which includes three pieces of legislation: the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act. The AI Act has been added after a revision and includes provision for a separate AI Commissioner. The new Privacy Commissioner is due to obtain fining powers following advocacy for this change by his predecessors (p.1).

In the UK, AI has been much discussed in the context of the new Data Protection and Digital Information Bill but there will not be – at least for now – a separate AI law, but regulator-led risk assessments and guidance (p.31). The EU is on course to adopt its AI Act. But businesses in the EU already have changes ahead of them in terms of the Digital Services Act and the Digital Markets Act (p.12).

The DPAs in the EU are trying to speed up GDPR enforcement by introducing novelties to their working methods at the European Data Protection Board. The EDPS is an active participant in the discussions for reforms, and other stakeholders are also voicing their opinions (p.9). The EU Commissioner who was responsible for the GDPR, Věra Jourová, has also been demanding operational changes. But most would agree that it is not sensible to start renegotiating a new GDPR text, as this would take years, and the current Commission's mandate ends in two years.

The EU - US data transfer framework is said to be making progress. Our correspondents assess how useful the new agreement will be, and what companies can do in the meantime to secure the legal position of data in international data transfers (p.19). Standard Contractual Clauses, a well-used tool, are also being introduced in China. Even with their limitations, this is welcome news (p.1).

Also in this issue, we bring you an analysis of the draft regulations by the California Privacy Protection Agency implementing the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA) (p.22).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 168+ countries alongside legal analysis, management guidance and corporate case studies.

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 168+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and administrative decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance and reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

3. Electronic Version
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments in Data Protection and related laws.

6. Back Issues
Access all *PL&B International Report* back issues.

7. Events Documentation
Access events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

privacylaws.com/reports

"*PL&B International Report* is obligatory reading for our team members worldwide to keep them up to date on relevant developments in other jurisdictions. Concise but always precise!"

Professor Dr Patrick Van Eecke, Head of European and Vice-chair, global cyber/data/privacy practice, Cooley LLP

UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of data protection legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business strategy.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.