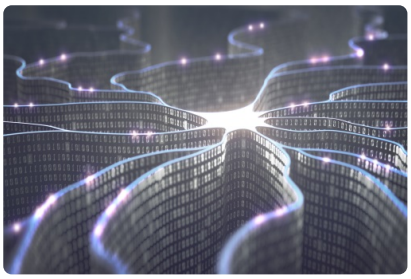
KILPATRICK TOWNSEND

July 1, 2022

Summer 2022 – What Privacy Professionals Need to Know and Do Now – Part II

by John M. Brigagliano , Anthony D. Glosson , Jennie L. Cunningham , Jon Neiditz , Amanda M. Witt



In our second installment of what privacy professionals should know before they start the summer, we provide you with highlights from the draft regulations from the California Privacy Protection Agency ("CPPA") and information about recent guidance on data transfers from China and Hong Kong. It will be interesting to see what major privacy development comes next. Unfortunately it seems that it's almost becoming common place for EU supervisory authorities to declare data transfers using certain analytics tools to be unlawful. Hopefully we'll have more encouraging news before the summer is out.

Highlights from the Draft Regulations from the California Privacy Protection Agency

The CPPA's draft regulations signal an assertive push to police businesses' operations to make the law effective in the agency's image. Below are highlights of several such provisions that commentators have largely overlooked thus far.

- **Deep Link to the Notice at the Point of Collection (§ 7012 (f)).** The draft regulations expressly state that businesses cannot provide the "notice at collection" (this notice includes, in part, the types of personal information to be collected and the purposes for such collection) through a general link to their privacy policy. Instead, businesses must provide a link to the specific section of the relevant privacy policy containing the notice at collection–such that the consumer need not scroll through the privacy policy to find the relevant information. Even if potentially already required under existing regulations, many businesses will need to update their links to comply with the explicit rules for providing this notice under the draft regulations.

- **Persistent Confirmation of Choice (§ 7025 (c)(6); (f)(4)).** A new and seemingly universally applicable requirement (albeit undeveloped) is to persistently display whether the business has honored a consumer's opt out preference signal. According to the draft regulations, the business may, for example, display 'Opt-Out Preference Signal Honored' when a consumer using an opt-out preference signal visits the website. Such a requirement, if retained, would almost certainly require businesses to lean on privacy vendors for launching this new feature that the CPPA has decided is needed on so many US websites.

- **Do not Sell or Share Link Optional for Some (7025(e)).** A business that fully processes opt outs through global privacy controls does need not to post a "Do not Sell or Share" link. Such a choice is ephemeral for businesses that engage in "offline" sharing, however, as such businesses need to collect identifiers (e.g., name or email) to stop such offline sharing—making the opt out not capable of being handled through a global privacy signal.
  What's more, the regulations make it difficult for service providers to assist in online advertising. Providing personal information to certain companies (such as matching providers) that had previously been service providers will now be in scope for CCPA "selling" and "sharing". That such companies may not act as service providers only increases the number of companies than engage in sharing or selling under the CCPA.

- **Are Cookies Related to only the Collection of Information? (§ 7026(a)(4)).** The regulations offer, *sua sponte*, that cookie banners or cookie controls (without any description of such tools' configuration) may not serve as a replacement for "Do not Sell or Share" links, on the basis that cookies concern the collection and not the "sharing" or "sale" personal information. That provision seemingly ignores several cookie-banner realities. For one, the CCPA's continues to have an exception to selling or sharing for a consumer's intentional interaction with third parties, which consumers may arguably establish through an affirmative cookie consent mechanism (so a consent to online tracking through a cookie banner could do away with a business's sharing or selling). Second, the rest of the regulations seems to suggest that disabling online tracking is how many companies should processes "Do not Sell or Share" requests by receiving global privacy signals processed on a device or browser basis, i.e., much in the same way that a cookie banner would disable tracking. Finally, many cookie banners are configurable to receive GPC and DNT signals, so such banners would act as a mechanism for receiving the global privacy signals that the CPPA so strongly favors.

- **No verification for requests to limit sensitive data use or "sharing" opt outs (7027(e)-7060(b)).** The CPPA follows the lead of the California Attorney General ("AG") by prohibiting verification for certain types of opt outs, namely for requests to limit the use of sensitive personal information or opting out of sharing or selling. The agency sees verification as a burden for consumers and unnecessary for receiving requests. For example, the new regulations state that a business requiring a consumer to upload a picture of an ID to facilitate an opt out request is *per se* a regulatory violation.

- **Content Moderation Becomes Easier for Service Providers. § 7050(b)(5).** Under the new regulations, service providers may now expressly use personal information to prohibit "malicious" or "deceptive" activity (while remaining in their service provider role). Such expanded use rights for service providers more clearly enable such providers to monitor and limit how their services, e.g., to stop hate speech.

- **DPAs more Cumbersome. (7051(a)(2)).** In an apparent effort to make technology licensing more burdensome – the draft regulations prohibits service provider agreements (i.e., data protection addenda) from cross-referencing another contract generally to define the specific business purposes for which the business retained the service provider. That provision misunderstands that the master service agreements to which data protection addenda form a part permit parties to purchase many different types of services over many years. Given that arrangement, many such data protection addenda refer to statements of work or similar ordering documents to define the purposes for which the service provider may receive personal information. This section of the draft regulation therefore adds more steps for drafting and negotiating technology agreements while not offering any apparent advantage to consumers.

China Expands Data Protection Regulations; Hong Kong Issues Model Clauses for Transfers

- **New Chinese Regulatory Guidance for 2022**

  When China's Personal Information Protection Act ("PIPL") came into effect in 2021, it was apparent that further regulatory action would be required to clarify obligations of companies operating in China or processing data about Chinese residents under the new law. The first half of 2022 has seen the issuance new guidance from various regulators responsible for overseeing compliance with the law, along with some early enforcement actions. Regulators also issued guidance based on China's closely-related Cybersecurity Law ("CSL"). These include, among others:

- Cross-border data transfer regulations;
- Vehicle cybersecurity and privacy regulations;
- Cybersecurity regulations for futures and securities; and
- Enforcement actions against apps alleged to have violated data protection laws.

- **Hong Kong Data Transfer Model Clauses**

  At the same time, Hong Kong's chief privacy regulator also issued "recommended" cross-border data transfer model clauses in May. Hong Kong's Personal Data (Privacy) Ordinance ("PDPO") is enforced by the Office of the Privacy Commissioner for Personal Data ("PCPD").

  Section 33 of the PDPO contains detailed restrictions on transferring data out of Hong Kong; however, the local data protection authority, the provision has not yet been brought into effect. Under the provision as drafted, transfers could take place under specific circumstances, including: (i) pursuant to "adequacy" findings similar to the GDPR process; (ii) with the written consent of the data subject; (iii) to avoid adverse action or harm to the data subject. This summer, the PCPD released model clauses (data user to data processor, and data user to data user) similar to the EU transfer mechanism.

  However, unlike the EU model clauses, a transfer mechanism is not expressly required by law due to PDPO Section 33 not yet having the force of law. PDPO nevertheless recommends that businesses use the model clauses as a best practice, and (also unlike the EU) are free to modify them as desired provided that they remain consistent with the PDPO.

Privacy Alphabet Soup:

CPPA: California Privacy Protection Agency

CCPA: California Consumer Privacy Act

GDPR: General Data Protection Regulation

DPAs: Data Processing Agreements

SCCs: standard contractual clauses

EEA: European Economic Area

EC: European Commission

IDTA: International Data Transfer Agreement

ADPPA: American Data Privacy and Protection Act

BIPA: Illinois's Biometric Information Privacy Act (740 ILCS 14)

PIPEDA: Canada's Personal Information Protection and Electronic Documents Act

PRA: private right of action

PIPL: China's Personal Information Protection Act

PDPO: Hong Kong's Personal Data (Privacy) Ordinance

PCPD: Hong Kong's Office of the Privacy Commissioner for Personal Data

Notable Upcoming Deadlines:

- **September 21, 2022**: Addendum for all new contracts for transfers of personal data from the UK to a third country, by no later than September 21, 2022.
- **December 27, 2022**: Parties currently using the prior version of the SCCs will have until December 27, 2022 to replace the prior SCCs currently in effect.
- **January 1, 2023**: California Privacy Rights Act Set to Apply to HR Data Effective January 1, 2023
- **March 21, 2024**: Organizations must replace all old EU SCCs with the IDTA or Addendum for ongoing transfers from the UK to a third country, by no later than March 21, 2024.