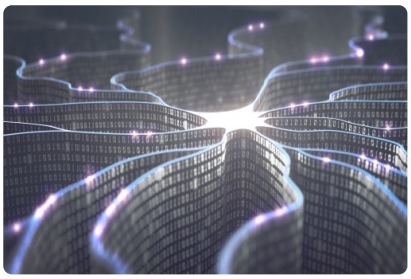
KILPATRICK TOWNSEND

June 27, 2022

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

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



It's been a blazing hot summer and privacy professionals have been sweating to keep up with all of the updates from the last few months. We all knew this was going to be a busy year with updating European data transfer mechanisms and reviewing the long-awaited regulations from the California Privacy Protection Agency ("CPPA"), but I'm not sure if many of us were prepared for a draft bipartisan federal privacy law that has privacy professionals buzzing with excitement and the California Consumer Privacy Act's ("CCPA") impending applicability to California employees. Further abroad, regulators in China and Hong Kong have been busy lately as well, issuing guidance and initiating enforcement actions. Meanwhile, our neighbors to the north are contemplating a major overhaul of PIPEDA, as Canada feels the heat from recent developments in the EU and proposes a set of new bills that would update its current privacy legislation, create specific obligations for AI, and carry significant monetary penalties.

Given the amount of things on your to do list, we have prepared a couple of installments to provide you with an update of things you need to know about the latest developments in privacy. This will helpfully keep you afloat until we see the draft Trans-Atlantic Data Privacy Framework, which is expected in July 2022. Never a dull moment in this field!

In our first installment, we will provide you with information on European data transfers, important developments for organizations with California employees and the highlights of the proposed federal privacy law. Part II will address the 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.

EU & UK Data Transfers

Hopefully your organizations and clients are already well on their way on the project of updating the EU and UK data transfer mechanisms given the impending deadlines. For organizations subject to the European Union's General Data Protection Regulation ("GDPR"), it's imperative to update your Data Processing Agreements ("DPAs") in 2022 if you rely on standard contractual clauses ("SCCs") for the transfer of personal data outside of

the European Economic Area ("EEA"). On June 4, 2021, the European Commission adopted SCCs that businesses may use as a tool to comply with European cross-border data transfer requirements for transferring data outside of the EEA.

Parties currently using the prior version of the SCCs had until ***September 27, 2021*** to start using the new SCCs for all new data arrangements and will have until ***December 27, 2022*** to replace the prior SCCs currently in effect. If the underlying agreement between the parties is re-negotiated or the scope of the data being processed changes during the transition period, the parties must use the new SCCs.

Given the *Schrems II* decision and additional scrutiny on data transfers to the United States, organizations will need to review what supplementary measures are in place, and conduct any necessary transfer impact analyses. The European Commission ("EC") released a set of FAQs on the new SCCs in May 2022; the FAQs are intended to address specific questions and input from parties that adopted the new SCCs. Some of the questions focus on the SCCs' interrelationship with GDPR, a common area of confusion, while others clarify issues related to *Schrems II* obligations, including items that may be considered for transfer impact analyses. The FAQs address a range of other topics, including technical contracting questions. One development to watch for is the EC's announcement that it is developing another set of SCCs for use in situations where data importers are directly subject to the GDPR.

On March 21, 2022, the UK's new International Data Transfer Agreement ("IDTA") and the international data transfer addendum to the EU's Standard Contractual Clauses ("Addendum") came into effect. Organizations must use the IDTA or the Addendum for all new contracts for transfers of personal data from the UK to a third country, by no later than ***September 21, 2022.*** 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***.

CCPA/CPRA Likely to Apply to Employees

California privacy's own Edward Scissorhands, the application of its framework designed for consumers to employee data, is slouching toward California employers to be born on January 1, 2023. Not just state legislators but the bipartisan drafters of the federal bill have failed to stop it, (because the federal bill now would only preempt laws with similar scope and specifically excludes employee privacy). California employers need to start preparing as soon as possible for the applicability of California's comprehensive privacy laws to their employees.

As the regulatory worlds of California privacy and employment law collide, the action is in the access right; deletion is avoided through employment-related requirements. Access under employment law is to documents, so access to personal information is a new concept for HR, plus the personal information employers hold on

employees is so much more complex and unstructured than information on customers and consumers; employees live most of their lives on employer-provided platforms. Therefore, the new concept under the proposed CPRA regulations of "disproportionate effort" is most critical in connection with employee data, where employers will need to determine reasonable access rules, with no employment-specific guidance yet. Employers will also need to address thorny access issues like the confidentiality of employee and applicant evaluations, sensitive employee resource groups and whistleblower hotlines. Finally, employers will need to operationalize the CPRA exclusion for exercising or defending legal claims as access is used as much for e-discovery in nascent employment disputes as it is under HIPAA for medical malpractice claims.

A Federal Privacy Law with a Chance

Federal privacy legislation optimists received a shot of hope earlier in June when Congress released a draft of the American Data Privacy and Protection Act ("ADPPA"). The bill is bipartisan, and includes a compromise on two of the key areas that have prevented lawmakers from coming to agreement in previous efforts at federal omnibus privacy legislation in the U.S.: ***preemption*** and the ***private right of action***. Legislators have attempted federal privacy law for decades; a recent promising effort in 2019 (bipartisan House bill and partisan Senate versions) stalled in committee.

The privacy substance is a big step beyond notice-and-choice, but the first question is usually the two key compromises. To understand the drivers of the **preemption** compromise, it is useful to distinguish between (a) the old preemption issue of lawsuits under state law and (b) the new preemption issue of the unprecedented operational complexity posed by California law alone and the patchwork of comprehensive state privacy laws spreading gradually across the country. The ADPPA offers just about nothing to businesses on old issue (a), and fairly complete preemption to the benefit of both businesses and people on new issue (b) (with the exception of the Edward Scissorhands discussed above). Thus, for example, a company would not have to administer data subject rights differently in different states, but would get no relief whatsoever from any of the major sources of state privacy lawsuits, including under Illinois's Biometric Information Privacy Act ("BIPA"), state data breach laws and the private right of action for breaches under the CCPA.

As for a federal **private right of action** ("PRA"), the ADPPA puts it off for 4 years, and then it appears to open the door to many types of private actions, but in a way that has worked for federal environmental suits, by first giving the FTC and state AG 60 days to decide to bring suit. What differentiates privacy from environmental violations is that in 60 days you can fix the former, but usually not the latter, which is why this PRA is a good compromise for business. Similarly, injunctive relief demands come with a 45-day cure period for all defendants, and any relief comes with such a cure period for small and medium-sized entities.

Other areas of interest in the draft bill include:

- **Data minimization requirements**. The bill limits collection, processing and transfer to "what is reasonably necessary, proportionate, and limited to [] provide a specific product or service…[or] deliver a communication that is reasonably anticipated…" or carry out certain expressly permitted purposes.
- **Sensitive personal data**. The collection, processing, and transfer of sensitive personal data would require the express consent of individuals.
- **Increased protections for minors**. The bill strengthens requirements for the personal data of children under 17 and bans targeted advertising to the same age group.
- **Algorithmic transparency**. Organizations ("large data holders") would be required to perform and submit annual "algorithm impact assessments" to the FTC.
- **Non-profits in scope**. The bill applies to non-profits as well as for-profit organizations.
- **Privacy by design**. Organizations would need to take certain actions, including establishing "policies, practices, and procedures" to take privacy by design into consideration.
- **Specific practices prohibited**. Particular activities would be barred, including most usages of social security numbers, sharing of passwords, processing internet search or browsing history without express consent, in addition to restrictions on sensitive personal data.

While the compromise bill appears to be carrying some significant momentum, many experts have indicated that the bill still faces substantial obstacles, including a short timeline, committee leadership change after the election, and strong opposition from various interest groups, and 2022 may again see a proposed national privacy law left by the wayside when Congress breaks for is August recess

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.