Comparison of the proposed 2020 Washington Privacy Act (SSB-6281) to: GDPR, CCPA, California Ballot Initiative, and the 2019 WA Proposal

By Stacey Gray, Pollyanna Sanderson, and Katelyn Ringrose
February 12, 2020

As Congress continues to work toward drafting and passing a comprehensive national privacy law, state legislators are not slowing down. In Washington State, a new comprehensive privacy law is moving quickly: last week, the Washington Privacy Act (SSB 6281) was voted out of the Washington Senate Ways & Means Committee, and appears likely to be voted on by the Senate. If approved, it will reach the House, which is currently considering (and amending) an almost identical companion bill. The deadline for the bill to be voted on by both Senate and House (including, if applicable, resolving any differences) is March 12, 2020.

FPF commented at a recent public hearing that, if passed into law, the Washington Privacy Act (as represented by Senator Carlyle's SSB-6281) would be a significant achievement for US privacy legislation. We have previously noted that the WPA would incorporate protections that go beyond those in the California Consumer Privacy Act, the only existing comprehensive consumer privacy law in the United States.

Is the Washington Privacy Act a good model for U.S. legislation? Lawmakers should consider:

- How well does it align with the EU's General Data Protection Regulation (GDPR), the current "gold standard" for global privacy law?
- How well does it align with, or go beyond, the California Consumer Privacy Act (CCPA)?
- How well does it align with this year's new California Ballot Initiative? The upcoming California Privacy Rights Act of 2020, if certified for the 2020 ballot in California, would significantly raise the bar for federal and state privacy protections.
- Finally, how strong are the provisions of the 2020 Washington Privacy Act compared to ***last year's version*** that narrowly failed to pass? Lawmakers should consider the extent to which this year's bill addresses (or does not address) significant weaknesses in the 2019 bill (including in the scope of rights, protections for sensitive data, and facial recognition provisions).

FPF has created the following charts to compare the EU General Data Protection Regulation (GDPR); the California Consumer Privacy Act (CCPA); the upcoming 2020 California Ballot Initiative; the WPA of 2019 (Senate Bill 5376); and the WPA of 2020 (Substitute Senate Bill 6281). These charts take into account the following key features of all five current, proposed, or past laws: (1) jurisdictional scope; (2) definitions and structure; (3) pseudonymous data; (4) individual rights; (5) obligations on companies; (6) facial recognition provisions; and (7) preemption and enforcement.

- Read the ***current*** EU General Data Protection Regulation (and FPF's guide to GDPR vs. CCPA)
- Read the ***current*** California Consumer Privacy Act
- Read the ***upcoming*** 2020 CA Ballot Initiative
- Read ***last year's*** 2019 WPA: SB 5376 **(did not pass in WA House)**
- Read the ***most recent*** 2020 WPA: SSB 6281 **(being considered by Washington legislators)**

1. JURISDICTIONAL SCOPE //

The 2020 Washington Privacy Act (SSB-6281) would govern legal entities in Washington that collect data from Washington residents. Although narrower in scope than the GDPR, the WPA contains a significantly broader scope and territorial reach than the CCPA. Unlike the CCPA (which governs for-profit businesses), the WPA would also govern non-profit organizations, including public charities and foundations. In some cases, the WPA would even govern entities that do not "conduct business" in Washington, if they produce products or services "targeted to" residents of Washington.

	EU GDPR	**CCPA**	**CA Ballot Initiative**	**WPA 2019**	**WPA 2020**
Who can exercise rights?	Natural persons ("data subjects")	California residents	California residents	Washington residents	Washington residents
Who has obligations?	All govt and non-govt legal entities and individuals established in the EU or offering goods or services to EU residents	For-profit businesses that "[do] business in the State of California" and meet thresholds (below)	For-profit businesses that "[do] business in the State of California" and meet thresholds (below)	Non-govt legal entities that "conduct business in Washington or produce products or services that are **intentionally** targeted to residents of Washington."	Non-gov't legal entities that "conduct business in Washington or produce products or services that are targeted to residents of Washington."
Thresholds	None. However, there is a limited small-business exemption for certain obligations (see e.g. Art. 30(5))	$25 million annual revenue; **or** **50,000+** consumers; **or** 50% of annual revenue derived from selling consumers personal data	$25 million annual revenue; **or** **100,000+** consumers; or 50% of annual revenue derived from selling **or** **sharing** consumers' personal data	100,000+ consumers; or derives 50%+ annual revenue from the sale of personal data **and** processes or controls personal data of 25,000+ consumers	**100,000+** consumers **during a calendar year**; or derives 50%+ annual revenue from the sale of personal data **and** processes or controls personal data of 25,000+ consumers

2. DEFINITIONS AND STRUCTURE //

The 2020 Washington Privacy Act (SSB-6281) contains key terms and an overall structure that closely aligns with the GDPR. It would define personal data broadly as "any information that is linked or reasonably linkable to an identified or identifiable natural person." This definition is in line with long-standing global norms; for example, personal data was defined similarly as early as 1981 in the text of Convention 108, the first binding international data protection agreement. The 2020 WPA also contains different obligations for "controllers" and "processors," with narrow CCPA-like exemptions for "de-identified" data and "publicly available information."

	EU GDPR	CCPA	CA Ballot Initiative	WPA 2019	WPA 2020
Broad definition of covered data	Y	Y	Y	Y	Y
"Controllers" & "Processors"	Y	Y ("businesses" and "service providers")	Y ("businesses" and "service providers")	Y	Y
Excludes "de-identified" data	Y *	Y	Y	Y	Y
Excludes "publicly available information"	N	Y	Y	Y	Y
** The GDPR defines personal data very broadly. (Art. 4(1)). Its provisions do not apply to data which does not relate to an "identified or identifiable person" or to personal data "rendered anonymous in such a manner that the data subject is no longer identifiable."* (Recital 26).					

3. PSEUDONYMOUS DATA //

The 2020 Washington Privacy Act treats "pseudonymous data" differently than other covered data. Under the WPA, pseudonymous data – data that "cannot be attributed to a specific consumer without the use of additional information" – is exempted from access, deletion, and correction rights, but not from opt-outs of sale, profiling, or targeted advertising. This provides flexibility for companies processing data that is less identifiable (and therefore harder to associate with individuals in order to fulfill their requests) but still carries some risks to privacy or autonomy. For example, pseudonyms are frequently used in large datasets to conduct scientific research (e.g., in a HIPAA Limited Dataset, John Doe = 5L7T LX619Z).

In contrast, other U.S. laws do not explicitly codify different obligations for pseudonymous data. In practice, however, there is a growing consensus that U.S. privacy law will need to reflect the practical challenges of dealing with data that falls along a spectrum of identifiability. For example, in practice under the CCPA, individual rights to access, delete, or correct their data are almost always more limited for pseudonymous data due to the challenges with (1) linking the request to the data the company holds; and (2) verifying that the request is authentic and that disclosure or deletion is being conducted on behalf of the right person. (See the California Attorney General's ongoing CCPA rulemaking efforts).

In the EU, the GDPR explicitly recognizes that pseudonymization of personal data decreases risks to the rights and freedoms of individuals (see Recital 28). The GDPR also exempts controllers from complying with individual requests to exercise rights of access and deletion (erasure) when identification in a dataset would require the controller to acquire additional information, unless the individuals themselves provide additional information to help re-identification (see Article 11). Pseudonymization is also considered an important safeguard for the GDPR's "privacy by design" requirements in Article 25 and for data security measures in Article 32.

	EU GDPR	**CCPA**	**CA Ballot Initiative**	**WPA 2019**	**WPA 2020**
Recognizes pseudonymous data	Y *	Indirect **	Indirect **	N	Y
** More precisely, the GDPR recognizes "pseudonymization" as a method to decrease privacy risks and comply with certain obligations (see description above). ** Indirectly, individual rights to access and delete pseudonymous data in California may be limited in practice due to challenges with verifying consumer requests (see description above).*					

4. INDIVIDUAL RIGHTS //

The WPA would codify individual rights for residents of Washington that go beyond both CCPA and the bill introduced in Washington in 2019. For instance, it would offer consumers a right to correct inaccurate data and to exercise broader rights to opt out of not only "sale" but also "profiling" and "targeted advertising." In comparison, the CCPA does not require an opt out of certain targeted advertising practices if they can be conducted without "selling" data (a limitation that would be eliminated in the Ballot Initiative). Last year's Washington bill contained a right to object to processing for targeted advertising, but would have allowed other kinds of data processing if outweighed by the interests of the company. The WPA would also grant consumers additional protections by requiring companies to establish internal appeals processes, paralleling certain procedural elements of the GDPR.

Finally, the WPA would require opt-in consent for collection of "sensitive information." This includes, for example, racial or ethnic origin, biometric data, sexual orientation, or mental or physical health condition or diagnosis. Heightened protection for sensitive data largely aligns with the Ballot Initiative and the GDPR, which requires either "explicit consent" or a very narrow and specifically prescribed

justification to process "special categories of data" (see Article 9). Notably, the 2020 WPA also includes "specific geolocation" as a type of sensitive data that requires opt-in consent. This aligns with the Ballot Initiative, but in comparison, under the GDPR, geolocation data can be processed in some situations without consent where other strong safeguards apply (see e.g. guidance on location data collected through Wi-Fi Analytics). In other cases, EU privacy laws like the ePrivacy Directive may apply.

<table>
<tr><th></th><th>EU GDPR</th><th>CCPA</th><th>CA Ballot Initiative</th><th>WPA 2019</th><th>WPA 2020</th></tr>
<tr><td>Right to Access</td><td>Y</td><td>Y</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>Right to Correct</td><td>Y</td><td>N</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>Right to Delete</td><td>Y</td><td>Y</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>Right to Portability</td><td>Y</td><td>Y</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>Internal Appeals Processes</td><td>Y *</td><td>N</td><td>N</td><td>N</td><td>Y</td></tr>
<tr><td>Opt out of "Sale"</td><td rowspan="3">Y **</td><td>Y</td><td>Y</td><td>N</td><td>Y</td></tr>
<tr><td>Out Out for "Targeted Advertising"</td><td>N ***</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>Opt Out of "Profiling"</td><td>N</td><td>N</td><td>N</td><td>Y</td></tr>
<tr><td>Opt In Consent for Sensitive Data</td><td>Y</td><td>N</td><td>Y</td><td>N ****</td><td>Y</td></tr>
<tr><td colspan="6">* Companies engaged in high-volume or high-risk processing must appoint a Data Protection Officer (DPO) who handles requests, communications, and appeals (Article 37, Article 38, and Article 39). ** An individual can object to any processing of their personal data conducted pursuant to certain lawful bases, at which point the controller may no longer process the data unless it demonstrates "compelling legitimate grounds" to override that person's interests, rights, and freedoms (Article 21). If such processing is conducted with consent, the consent must be easy to withdraw at any time (Article 7.3). Finally, the GDPR includes an absolute right to object to "direct marketing." (Article 21.2). *** The CCPA does not restrict targeted advertising if it can be conducted without "selling" data. In contrast, the Ballot Initiative contains a broader opt-out provision (of both "sale" and "sharing") and specifically limits service providers from engaging in any "cross-context behavioral advertising." **** Except where consent could be used as a way for a company to engage in "high risk" processing, as determined by risk assessments. (s8(3)).</td></tr>
</table>

5. OBLIGATIONS ON COMPANIES //

After the CCPA passed in 2018, it was widely criticized by privacy advocates for placing most of the burden on consumers to exercise their rights, without containing strong restrictions on the collection or uses of data. The California Ballot Initiative would go significantly further than CCPA by incorporating additional consumer rights and restrictions on the collection and use of "sensitive data." The WPA similarly places additional obligations on companies to act as responsible stewards of information, including mandated risk assessments for high-risk activities. Neither would go as far as the GDPR, which requires that companies have a "lawful basis" to collect data at all, where a "lawful basis" can include, for example, consent, fulfillment of a contract, or "legitimate interests" (for more, see FPF's report: Deciphering Legitimate Interests).

Both the California Ballot Initiative and the 2020 Washington Privacy Act incorporate elements of data minimization, purpose limitation, and avoidance of "secondary uses." Neither is as restrictive as the provisions in the GDPR's Article 5. However, the Ballot Initiative would require that a business's collection and use of data be "reasonably necessary and proportionate to achieve the purposes for which [it was] collected or processed . . . and not further processed in a manner that is incompatible with those purposes." (1798.100c). In comparison, the 2020 Washington Privacy Act would require that data collection be "limited to what is reasonably necessary" as well as "adequate, relevant, and limited" in relation to "the purposes for which such data are processed, as disclosed to the consumer," and prohibit further processing that is not "compatible with" those purposes (absent consent) (Section 8).

	EU GDPR	CCPA	CA Ballot Initiative	WPA 2019	WPA 2020
Lawful Bases for Collection	Y	N	N	N	N
Privacy Policies	Y	Y	Y	Y	Y
Risk Assessments for High-Risk Activities	Y	N	N	Y	Y
Data Minimization	Y (strongest)	N	Y	N	Y
Purpose Limitation	Y (strongest)	N	Y	N	Y
Duty to Avoid Secondary Use	Y (strongest)	N	Y	N	Y
Reasonable Security	Y	Y	Y	Y	Y
Non-Discrimination	Y (Indirectly)*	Y	Y	N	Y
** The GDPR does not include an explicit provision stating that a data subject must not be discriminated against on the basis of their choices to exercise rights. However, it is implicit from other principles of the GDPR that individuals must be protected from discrimination on these grounds. (Article 5, Article 13, Article 22, and elements of "freely given" consent and fair processing).*					

6. FACIAL RECOGNITION PROVISIONS //

The current version of the WPA contains special provisions for commercial uses of facial recognition technologies. Such provisions do not directly exist in the GDPR or other comprehensive privacy laws. However, other laws in the US and EU govern facial recognition technologies, whether as category of "sensitive data" (e.g. the Ballot Initiative would require consent for uses of biometric data), or as a form of sensitive data or automated profiling (under the GDPR).

Specifically, the GDPR regulates facial recognition technologies through several provisions. When facial recognition is used for identification purposes, "explicit consent" is required under Article 9, unless a narrow overriding justification applies, like a substantial public interest provided by law. In addition, GDPR imposes obligations for companies engaged in "solely automated decision-making and profiling" (Article 22), both of which can be part of real-world facial recognition use cases (see, e.g., EU guidance on collecting data through video).

Finally, compared to the facial recognition provisions in 2019, the 2020 WPA provisions are significantly stronger. In 2019, the bill that passed the Washington Senate allowed for implied consent for facial recognition: "The placement of conspicuous notice in physical premises . . . [shall] constitute a consumer's consent to the use of such facial recognition services . . . (Section 14). In contrast, the 2020 version does not permit this – instead, it would require businesses to obtain affirmative opt in consent from consumers prior to their enrollment in a facial recognition system (with narrow, limited exceptions). The 2020 WPA would also require covered entities to enable third-party auditing, and to address inaccuracies identified related to bias and discrimination.

	EU GDPR	CCPA	CA Ballot Initiative	WPA 2019	WPA 2020
Protections for Commercial Uses of Facial Recognition	Y (indirectly)	N	Indirectly	Y (limited)	Y (stronger)

7. PREEMPTION AND ENFORCEMENT //

The WPA aligns with other privacy laws in that it would preempt local regulations that would govern the same data processing activities. As a result, it would be likely to preempt local regulations for commercial uses of data that fall within the same jurisdictional scope of the law, but might not preempt local regulations of government or municipal entities.

The current WPA would be enforced by the Washington Attorney General. Similarly, the CCPA is enforced by the California Attorney General, whose office is currently engaged in regulatory rulemaking (see California's draft regulations). The CCPA does not allow for civil enforcement of most of the law's provisions, but contains a limited private right of action for data breaches. The GDPR allows individuals to exercise rights to "individual redress," in addition to each EU Member State having their own well-funded Data Protection Authority.

	EU GDPR	CCPA	CA Ballot Initiative	WPA 2019	WPA 2020
Preemption	Y	Y	Y	Y	Y
Enforcement by State AG or Government Body (DPA)	Y	Y	Y	Y	Y
Enforcement by Individuals	Y (mix of EU judicial rights & individual redress from regulators)	N (exception for security breaches)	N (exception for security breaches)	N	N *
** Unlike the 2019 version, the 2020 WPA has been amended to clarify that it would not override the existing rights of Washington residents to bring actions under Washington State's Consumer Protection Act (chapter 19.86 RCW) for conduct or behavior that would amount to an unfair or deceptive practice (Section 11). Similarly, residents of California (and many other states) have the ability to bring lawsuits to challenge privacy violations when they violate unfair and deceptive practices (UDAP) state laws.*					

CONCLUSION //

The Senate sponsor of the 2020 WPA, Senator Reuven Carlyle, recently noted: "I don't think that we're ever going to be done dealing with the regulatory framework of consumer data and the issue of privacy. We're living in a new era." We agree. The United States needs a comprehensive, baseline federal privacy law to set uniform standards and create clarity for companies and strong rights for individuals. In the absence of such a law, the Washington Privacy Act could serve as a useful regulatory model for other states and for Congress that improves upon the CCPA, provides rights to Washington residents, and helps companies build effective data protection programs.

Did we miss anything? Let us know at info@fpf.org as we continue tracking state and federal developments in privacy legislation.