



August 23, 2022

**Introduction**

The ISL Consumer Scorecard compares the text of the proposed California Consumer Privacy Act Regulations, released on July 8, 2022, against ISL regulation safety criteria listed below. Note that this scoring does not reflect the overall CPRA regulations.






**Legend**






ISL SAFETY SCORE	SCORE KEY
	Regulation aligns with/supports the ISL safety regulation principle.
	Regulation partially supports the ISL safety regulation principle.
	Regulation does not support the ISL safety criteria.
N/A	Not within current topics for rulemaking

**Terminology Mapping**




ISL Terminology	CCPA/CPRA	GDPR
<i>Data Subject</i>	"Consumer"	"Data Subject"
<i>Data Controller</i>	"Business"	"Data Controller"
<i>Data Processor</i>	"Service Providers" and "Contractors"  *both added by CPRA	"Data Processor"
<i>Data Co-Controller</i>	Not Included	"Joint Controller"
<i>Personal Information</i>	"Personal Information"	"Personal Data"
<i>Data Broker</i>	"Third Party"	"Third Party"
<i>B (business) includes Data Controller, Data Processor, Data Co-Controller, Data Broker</i>	"Business", "Service Provider", "Contractor, and "Third Party"	"Data Controller", "Data Processor", "Joint Controller", and "Third Party"

## ISL CONSUMER SAFETY SCORECARD v1.0

#	ISL SAFETY CRITERIA	ISL SAFETY SCORE	CCPA REFERENCES & RATIONALE	RECOMMENDATIONS TO THE AGENCY
<b>SAFE BY DEFAULT</b>				
1	Regulation requires that all software be private by default.	N/A	N/A	
<b>SAFE NOTICE PRINCIPLES</b>				
2	Regulation requires all B-s to provide data subjects with complete & accurate notice.		§7010-7012	Consumers deserve to know the identity of the third parties that have their personal information. This knowledge would enable consumers to act on their behalf or empower trusted third parties to act on their behalf for their best interest. Without having this knowledge consumers are forced to rely on limited government resources.
a	All B-s must provide complete & accurate notices.		§7010-7011 B-s that control the collection of personal information must provide notice at collection including comprehensive description of online & offline practices.	
b	Including identification of all third-party entities that receive personal information.		§7012 Notice does not require B-s to disclose a list of all third parties. Instead, B-s are given the option to either identify third parties or provide information about the third parties' data practices within its notice.	Regulation should require B-s to list all third parties. We understand that there are situations where third parties aren't known to the B such as with the use of AdTech, which is discouraged in our ISL Safety Criteria #13 below.
3	Regulation ensures that notices are monitored & enforced.		§7300-7304 See also ISL Safety Criteria #17	
<b>SAFE PERMISSION/CONSENT</b>				
4	Since online "Notice & Consent" is inherently unsafe for people, regulation must ensure that "Notice & Consent" not be the sole legal basis for data processing.		§7002; §7004 B-s shall design and implement methods for submitting CCPA requests and obtaining consumer consent that incorporate the principles listed in §7004. (Methods that do not comply may be considered a Dark Pattern). Symmetry in choice is a principle that is required for consent. Any agreement obtained with the use of dark patterns shall not constitute consumer consent.	Note that during the preliminary rulemaking activities many of us urged the Agency to rephrase the term "dark pattern." We continue to advocate for the use of "harmful pattern" instead.

			See also §7022; §7050-7051; §7052-7053	
5	Regulation requires that B-s receive uncoerced, informed permission from the data subject to use the data subject's personal information for any purpose that is inconsistent with the original purpose listed in the notice.		§7002; §7004 B-s must obtain the consumer's consent before collecting, using, retaining, and/or sharing PI for any purpose that is unrelated or incompatible with the purpose(s) for which the personal information collected or processed.	
6	Regulation requires that B-s provide data subjects with a definitive, recorded affirmation of permission(s).	N/A	N/A	
7	Regulation requires that the data subject's permissions be shared with all data processors and data co-controllers.		§7022 B-s must share consumer permissions and changes with all other service providers, contractors, and third parties.  <i>See also §7050-7051; §7052-7053</i>	
<b>SAFE IDENTIFICATION OF DATA SUBJECTS</b>				
8	Regulation minimizes identification of data subjects.	N/A	N/A	
9	Regulation minimizes the need for age validation by technology. If age verification must be done, it must be done in a way that is mandated to be both ephemeral and anonymous. <sup>1</sup>		§7070-§7072 No mention or reference of age verification.	
<b>SAFE DATA COLLECTION</b>				
10	Regulation limits the information that a B receives from the data subject or other, observes, or derives about the data subject to what is reasonably necessary and:		§7002	
a	proportionate to the service/product provided,		§7002 The collection and use of personal information is restricted to what is reasonably necessary and proportionate to achieve the purpose for which the personal information was collected or processed. To be reasonably necessary and proportionate,	

<sup>1</sup> Age must not be remembered, B-s must calculate age every time and forget it every session. Note that if safety principle #1 is in place, there is less of a need for age validation.




			<p>the B-s collection, use, retention, and/or sharing must be consistent with what an average consumer would expect when the personal information was collected.</p> <p><i>See also ISL Safety Criteria #5 and §7050-7051</i></p>	
b	<p>proportionate to the commitment and current state of the Me2B Relationship.<sup>2</sup> (see Fig. 1)</p>		<p>§7002 B-s collection, use, retention, and/or sharing of a consumer’s PI may also be for other disclosed purpose(s) if they are compatible with what is reasonably expected by the average consumer.</p>	<p>We suggest adding another example to illustrate that the deeper the Me2B relationship, the more data collection and processing is expected. For example, the first time a user visits a retail website they have a reasonable expectation of anonymity, but later in the Me2B relationship, they create an account at that site, and expect that their behaviors may be tracked, and their experience will be personalized. (i.e., they expect to be “recognized, remembered, and personally responded to”.)</p>
11	<p>Regulation regards any and all information that is or is likely to be correlated to a person as sensitive personal information, regardless of how it is collected.</p>	N/A	N/A	
12	<p>Regulation disallows B-s to maintain data about a data subject without a direct relationship<sup>3</sup> with that data subject.</p>		<p>§7050-7053 There is no requirement for a direct relationship, but the regulations do prohibit the use, disclosure, or retention of personal information obtained while providing services for any purpose, unless an exception applies.<sup>4</sup></p>	
a	<p>Unless the main data controller has strong and appropriate contractual management over all data processors and data co-controllers.</p>		<p>§7050-7053 Regulations require written contracts and establishes baseline requirements for Service Providers, Contractors, and Third Parties.</p>	
b	<p>Regulation includes an easy universal opt out for registered data brokers.</p>	N/A	N/A	

**SAFE DATA PROCESSING**

<sup>2</sup> Me2B Relationship refers to the relationship a user (Me) forms with a business (B) and with the products and services that the business provides. Just like human relationships, the Me2B Relationship changes over time, generally increasing in trust and intensity. The state of the Me2B Relationship is therefore crucial context for data sharing norms.

<sup>3</sup> Direct Relationship means the data subject has an account and has entered into some kind of service agreement with the company and can thus correct/view personal information. Data Brokers typically have no direct relationship with the data subjects.

<sup>4</sup> Exceptions listed in CCPA 1798.145(a)(1)-(a)(7).

13	Regulation disallows the use of data subject tracking for marketing or advertising purposes, including:		Not fully addressed in the regulation.	
a	Current RTB infrastructures.		§7052 Regulation only calls out cross contextual ads stating that cross contextual ads are not a Business Purpose for which a B & Service Provider can contract for.	The Agency's use of cross contextual behavioral ads is very narrow in scope, but it does limit the harms of current AdTech. Also, data brokers having to comply with the opt-out signal may change the behavior of AdTech for the better (especially if strictly enforced). We have concerns are about other profiling tactics, including emerging forms.
14	Regulation requires B-s that process large amounts of personal information for an ongoing period of time owe a duty of loyalty <sup>5</sup> to the data subject. Examples include social networks, email, and messaging services.		§7102 CCPA sets disclosure requirements for B-s collecting large amounts of personal information. Requirements apply only to B-s that know or reasonably should know that they sell the personal information of 10,000,000 or more consumers. The Agency's statement of reasons ties the 10,000,000 number to approximately 10% of CA's total population.	The Agency's assumption that "large" be based on large amounts of data held about a large amount of people is inadequate. It shouldn't only be about how many consumers' PI is collected. It's also about the depth of data collected in their records. Big data sets matter.  We believe the Agency has authority to promulgate a duty of loyalty. <sup>6</sup> To the extent the Agency does not have the authority they should get the authority to do so. The CCPA is weaker than ADPPA here given that the ADPPA provides a duty of loyalty.





**SAFE SCOPE OF REGULATION**

15	Regulation must reassess what is considered "reasonable public information" in light of the internet age where data can be weaponized through scraping and aggregation at massive scale.	N/A	N/A	
16	Regulation does not exclude the following B-s from the duties of data controllers, data processors, and data brokers:	N/A	N/A	
a	non-profits,	N/A	N/A	
b	government, law enforcement, etc.	N/A	N/A	

**SAFETY ENFORCEMENT**

<sup>5</sup> A duty of loyalty has well-established roots in the common law of fiduciaries and trusts. A hallmark of the obligation is to have no conflicts of interest between the client and third parties, and to always act in the client's best interest. Modern examples of entities with these same duties are doctors, lawyers, and certain financial advisors.

<sup>6</sup> It remains unclear whether the Agency has the power to promulgate regulations on duty of loyalty during this rulemaking period.

17	Regulation provides for a practical and scalable means for ongoing enforcement of software safety regulation.		<p>§7300-7304 Agency is authorized to audit B-s, Service Providers, Contractors to ensure compliance with CCPA.</p> <p>Agency may conduct audits if the collection or processing of personal information presents significant risk to consumers privacy or security or if there is a history of noncompliance with privacy law(s). Audits may also be conducted to investigate possible violations of the CCPA.</p>	Auditing is too large a job for a single entity. It will need a network of authorized, independent, auditing entities. Authorized auditing entities must be independent organizations that are not owned, operated, or compensated by data controllers, co-controllers, data processors, or data brokers.
a	Enforcement of Business Behavior		<p>§7100-7101 ^Changes had no regulatory effect (aka nonsubstantive changes).</p> <p>See also §7102, addressed in ISL safety criteria #14.</p>	
b	Enforcement of Software/Technology Behavior		<p>§7300-7304 Auditing measures the actual behavior of the technology.</p>	
c	Regulation must provide for authorized auditing and reporting entities to support the volume of audits required to ensure compliance.		Not addressed in the regulation.	<i>See response in #17 above. We're advocating for inclusivity, transparency, and accountability in authorized auditing entities: Transparency in qualifying criteria, selection, and ongoing performance of authorized auditors.</i>

## Additional Comments to The Agency

- **[§7011(e)(1)]**
  - (b) “Categories of sources” is a good start but would be much better to list the companies.
  - (e) “Categories of third parties” is inadequate; company names must be listed.
  - (g) “Actual knowledge” should be changed to “constructive knowledge” which enables efficient enforcement while minimizing age verification. The current knowledge requirement isn’t adequately robust and leaves children and minors vulnerable.
  - (i) “Categories of third parties” is inadequate; company names must be listed.
- **[§7051]** “B(6)(a)(6) Collect or sell a consumer’s personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer’s personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not permit a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California.”
  - Why isn’t CPPA applying the same logic as GDPR Article 3 “Territorial Scope” item 1 such that Californians would be protected regardless of whether the processing takes place in California <https://gdpr-info.eu/art-3-gdpr/>
    - In general, Californians will reasonably expect to be protected everywhere.
  - As written, these requirements could result in invasive location tracking of Californians.
  - This section is important and needs to be carefully revised.

Figure 1: Me2B Relationship & Lifecycle (referenced in ISL Safety Criteria #10b)

