PrivacyCheq

December 5, 2019

The Honorable Xavier Becerra
Attorney General
ATTN: Privacy Regulations Coordinator
300 South Spring Street, First Floor
Los Angeles, CA 90013

Comments on Proposed Regulations

Dear Mr. Becerra:

I am writing on behalf of PrivacyCheq, a Pennsylvania corporation. We specialize in the design and implementation of transparency and consent management software solutions embracing consumer privacy.

In our work, we focus squarely on optimizing the consumer's overall privacy experience as they interact with businesses to share personal information.

As such, we wish to commend you on the "consumer friendliness" of the proposed regulations, noting our agreement with the following concepts in particular:

- The regulations clearly set forth that there is a difference between a privacy policy[1] and a privacy notice[2]. A clear distinction is drawn between the purpose of the privacy policy[3] and the purpose of the Notice at Collection[4] relating to their respective use during data collection. The regs make it

[1] §999.301(m) "Privacy policy" means the policy referred to in Civil Code section 1798.130(a)(5), and means the statement that a business shall make available to consumers describing the business's practices, both online and

[2] §999.301(i) "Notice at collection" means the notice given by a business to a consumer at or before the time a business collects personal information from the consumer as required by Civil Code section 1798.100(b) and specified in these regulations.

[3] § 999.308(a)(1) The purpose of the privacy policy is to provide the consumer with a comprehensive description of a business's online and offline practices regarding the collection, use, disclosure, and sale of personal information and of the rights of consumers regarding their personal information. The privacy policy shall not contain specific pieces of personal information about individual consumers and need not be personalized for each consumer.

[4] §999.305(a)(1) The purpose of the notice at collection is to inform consumers at or before the time of collection of a consumer's personal information of the categories of personal information to be collected from them and the purposes for which the categories of personal information will be used.

clear that the privacy policy document is static and all-inclusive, while the notice is designed to support and promote "just-in-time" individual interactivity.

- In defining and specifying three new types of notices[5] designed to better inform the consumer, the regulator has obviated the "click the I AGREE box or go away" model for transparency at consumer touchpoints. This is a huge benefit to California consumers.

- The regulations clearly state the requirement for Notice at Collection of Personal Information[6] prior to collecting PI. As well, they set forth the need for notices to be in plain, straightforward language, avoiding technical and legal jargon, in a readable format (including on smaller screens), accessible to consumers with disabilities, and useful with venue signage. This is another major bonus for California consumers.

- Using Privacy by Design[7] principles, drafters of the regulations have leveraged important relevant research[8]. The resulting "performance-based" notice design raises the bar for privacy regulation well beyond California's borders as the privacy world looks for thought leadership in how to effectively communicate privacy information to consumers.

But the October 10th regulations stop short of prescribing or even suggesting what format the new notices might take in actual operation.

PrivacyCheq believes that over time, the presentation of just-in-time privacy notice information will evolve to a loose standard. We believe that CCPA has a golden opportunity at this time to provide general guidance around what an

[5] §999.305. Notice at Collection of Personal Information, §999.306. Notice of Right to Opt-Out of Sale of Personal Information, and §999.307. Notice of Financial Incentive

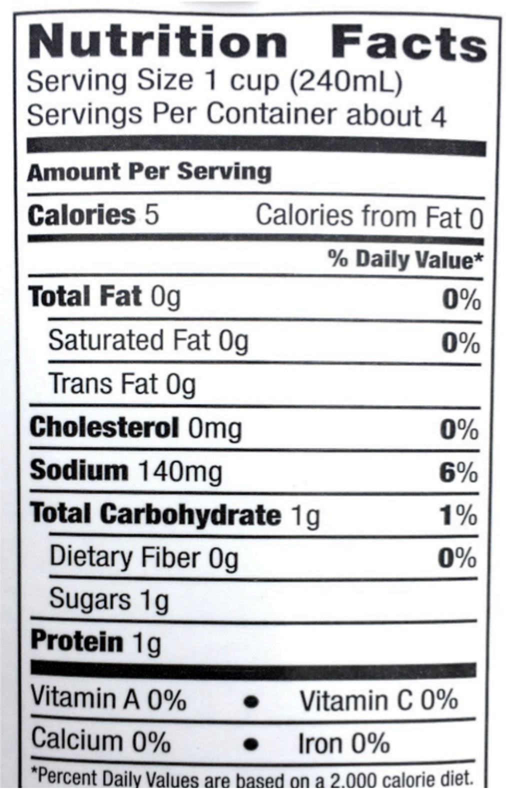
[6] §999.305(a)(5) If a business does not give the notice at collection to the consumer at or before the collection of their personal information, the business shall not collect personal information from the consumer.

[7] Cavoukian, Ann *Privacy By Design…*, Available at https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf

[8] Schaub, et al., *A Design Space for Effective Privacy Notices*, Symposium on Usable Privacy and Security (SOUPS) 2015, Available at https://www.usenix.org/system/files/conference/soups2015/soups15-paper-schaub.pdf

acceptable paradigm for "just in time" notice delivery might look like. It is in that spirit that we present the following analysis and suggestion:

- What form would a new paradigm for transparency take? What is a real-world example of how enterprises regularly inform citizens of copious and complex information in a way that is explicit, specific, intelligible, concise, and easily accessible? We believe that one example of such a paradigm is the ubiquitous Nutrition Facts-style label (Figure 1).



Nutrition Facts
Serving Size 1 cup (240mL)
Servings Per Container about 4

Amount Per Serving	
Calories 5	Calories from Fat 0
	% Daily Value*
Total Fat 0g	0%
Saturated Fat 0g	0%
Trans Fat 0g	
Cholesterol 0mg	0%
Sodium 140mg	6%
Total Carbohydrate 1g	1%
Dietary Fiber 0g	0%
Sugars 1g	
Protein 1g	
Vitamin A 0% •	Vitamin C 0%
Calcium 0% •	Iron 0%

*Percent Daily Values are based on a 2,000 calorie diet.

Figure 1

- The Nutrition Facts title name and font are familiar and iconic around the world. The label's gridded framework supports clear and plain language presenting a prospective buyer/user with a select, concise list of best questions about this specific product. Each issue or question prompts a clear and explicit answer. The user can digest every detail of the information (unlikely), focus in on a fact of particular interest (calories, sodium, carbs?) or choose to ignore the notice completely ("I trust this business, and know that the facts are here if I ever need them").

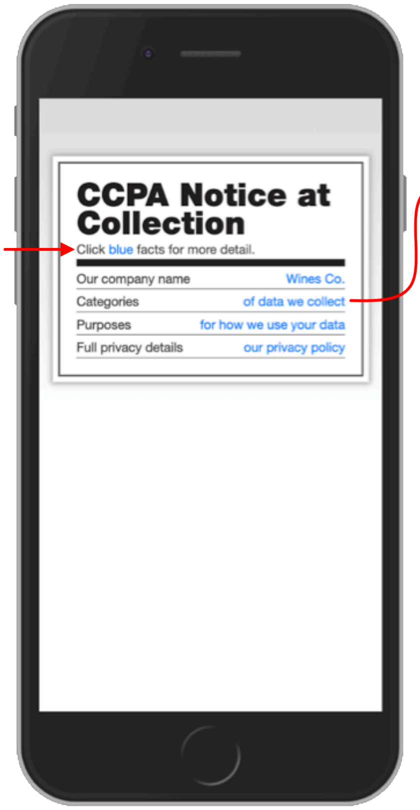
- This nutrition facts information format goes a long way towards organizing the transparency requirements of CCPA, but two major concepts are missing that would make this disclosure format ideal for operational privacy notices.

- First, privacy is much more complicated than food. Single digit or single-word right-hand "answers" to elements of the framework are often inadequate to describe privacy concepts. For privacy facts, each answer needs to have “drill down” capability to present multiple sublayers of information on request.

- Secondly, unlike the flat visual nutrition presentation, a privacy facts notice needs to be interactive. It needs to place digital control into the hands of the consumer to navigate, view, select, drill down on, expand on, respond to, and exit or ignore the presentation.

- Both of these issues can be overcome by purpose-built Privacy-by-designed application software, wherein “drill-down” simplicity and user interactivity become key features. For our purposes, PrivacyCheq has named the resulting tool a Privacy Facts Interactive Notice or PFIN.

- Fully enhanced with drill down and interactive functionality, here are three successive screenshots of how a PFIN might look on a mobile device as a California consumer first views the Notice at Collection (Figure 2), chooses to learn about categories (Figure 3), then chooses to investigate purposes (Figure 4).

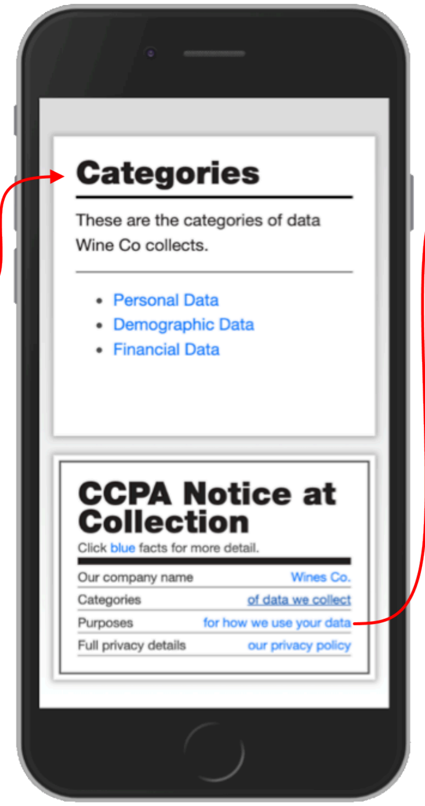


CCPA Notice at Collection

Click blue facts for more detail.

Our company name	Wines Co.
Categories	of data we collect
Purposes	for how we use your data
Full privacy details	our privacy policy

Figure 2



Categories

These are the categories of data Wine Co collects.

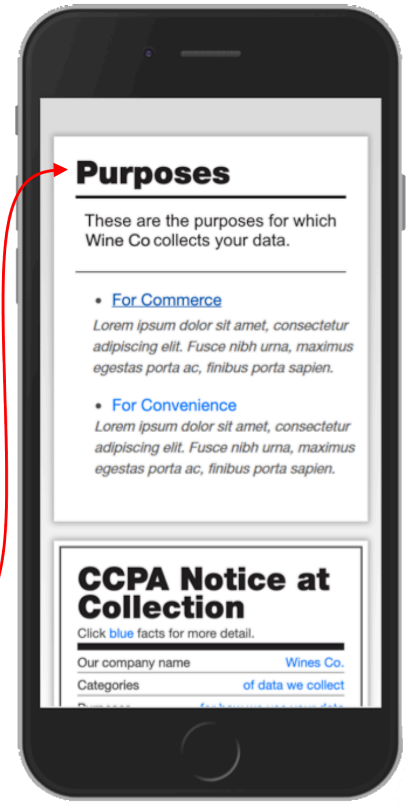
- Personal Data
- Demographic Data
- Financial Data

CCPA Notice at Collection

Click blue facts for more detail.

Our company name	Wines Co.
Categories	of data we collect
Purposes	for how we use your data
Full privacy details	our privacy policy

Figure 3



Purposes

These are the purposes for which Wine Co collects your data.

- For Commerce
  Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce nibh urna, maximus egestas porta ac, finibus porta sapien.
- For Convenience
  Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce nibh urna, maximus egestas porta ac, finibus porta sapien.

CCPA Notice at Collection

Click blue facts for more detail.

Our company name	Wines Co.
Categories	of data we collect

Figure 4

- A major benefit emerges from marrying nutrition label simplicity with modern digital technology. The resulting consumer-paced dialogue now becomes operational across the full spectrum of consumer-facing touchpoints (websites, tablets, smartphones, mobile apps, IoT devices, venue signage, QR codes, etc.).

- This concept places privacy control into the hands of the consumer to navigate, view, select, drill down on, expand on, respond to, and exit or ignore the presentation.

- Like nutrition facts labeling, the simplicity and familiarity of PFIN notices operate to build trust between business and consumers. Implementation of this new notice paradigm could go a long way towards simplifying and standardizing businesses' compliance with CCPA … a major benefit to California consumers.

In summary, PrivacyCheq is enthusiastic about operationalizing CCPA under the proposed regulations to deliver on Californians' right to privacy by giving consumers positive and effective control over their personal information.

Additionally, we have proposed an open paradigm for notice delivery that we believe could be useful as CCPA regulations face operationalization in the real world. Thank you for the opportunity to comment. We stand ready to help however we can.

Sincerely,

Dale R. Smith, CIPT
Futurist
drs@privacycheq.com

via email to: PrivacyRegulations@doj.ca.gov