Santa Clara University

Comments to the California Department of Justice's (DOJ) Draft Regulations for the California Consumer Protection Act (CCPA)

December 6, 2019

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

By email: PrivacyRegulations@doj.ca.gov

I am a tenured law professor at Santa Clara University School of Law, where I teach Internet Law. I submit these comments on the "proposed text of regulations" (the "regulations") published by the California Department of Justice (DOJ) on October 11, 2019. These comments represent only my views and not the views of my employer or any third party.

The "Average" Consumer

Echoing California Civil Code 1798.185(a)(5), the regulations use the term "average consumer" five times (999.305(a)(2), 999.306(a)(2), 999.307(a)(2), 999.308(a)(2), and 999.315(b)). However, the term "average consumer" isn't defined.

The "average consumer" standard does not represent the prevailing national approach in consumer protection law. The FTC expressly considered the appropriate standard for measuring consumer confusion in its 1983 Policy Statement on Deception. In that statement, the FTC adopted the standard of "a consumer acting reasonably in the circumstances." This standard has served consumers and the FTC well for over three decades. Among other advantages, it avoids the indeterminacy of defining what constitutes an "average" consumer when a business caters to multiple heterogeneous consumer segments. The DOJ should define the term "average consumer" to track the FTC's reasonable consumer standard.

999.301(s) defines a "typical consumer," but its definition does not acknowledge either the "average" or "reasonable" consumer standard. The "typical consumer" definition should be harmonized with the "average consumer" definition and, like "average consumer," should reflect the FTC's "reasonable consumer" standard.

Exceptions to Requests to Know

999.313(c)(4) provides a list of items that pose too great a privacy/security risk if disclosed in response to a bogus request to know. The DOJ should consider expanding the list of undisclosable items that pose a heightened security risk.

Verifiable Consumer Requests and Rules vs. Standards

The legal requirements for verifiable consumer requests play a critical role in the CCPA. Businesses are legally required to honor verifiable consumer requests, but illegitimate requests can lead to major security violations that severely harm targeted victims. The regulations create legal liability for businesses in both directions: they face liability for dishonoring valid requests and liability for honoring some invalid requests. Because every consumer request creates potential legal exposure, businesses frequently will feel compelled to route consumer requests through customized legal review at substantial expense.

The DOJ can ameliorate the need for these expensive individualized determinations by providing concrete and specific bright-line rules of exactly what constitutes a verifiable consumer request, instead of requiring businesses to conduct fact-intensive, potentially irresolute, and expensive evaluations of legal "standards," such as requiring "reasonable" behavior or balancing multi-factor tests.

The regulations for verifiable consumer requests represent a mix of rules and standards. The portions that are "rules" are helpful. For example, 999.325(b) and (c) provide bright-line rules for when businesses must disclose categories and specific pieces of personal information (indeed, these bright-line rules ought to apply to all consumer requests). Business' ability to rely on password authentication is another helpful rule.

Elsewhere, the regulations adopt legal standards that will create substantial dilemmas for businesses trying to do the right thing. Most conspicuously, 999.323(b)(3) requires businesses to navigate a multi-factor test when evaluating consumer requests. The commentary in the Initial Statement of Reasons reinforces the imperative to get it right; the commentary says that "businesses have the responsibility to establish a reasonable method for verifying the identity of the person making the request."

999.323(b)(3)'s multi-factor test creates many scenarios where well-meaning businesses won't be sure what is the right decision. Further, those circumstances lend themselves to second-guessing by the DOJ. These dynamics will cause businesses to over-spend on these decisions. Thus, as a general proposition, with respect to what constitutes a "verifiable consumer request," the DOJ should rely less on multi-factor tests and rely more on bright line rules.

Alternatively, the DOJ can provide more bright-line safe harbors, such as those in 999.325(b) and (c). As just one example, the DOJ could add a safe harbor for businesses that rely on an opinion of counsel about the reasonableness of their actions. However, opinions of counsel are expensive. Other safe harbors that businesses could implement at lower cost would benefit everyone.

Two other places where the DOJ imposes standards that should be converted to bright-line rules or subject to bright-line safe harbors:

- 999.313(c)(3) says that businesses should not honor a consumer request when disclosure creates a "substantial, articulable, and unreasonable" security risk. All three adjectives are standards, not rules, and they require substantial (and expensive) expertise and judgment to implement properly.
- 999.325(b) and (c) require businesses to verify a consumer's identity with a "reasonable" and "reasonably high" degree of certainty. 999.325(d) then requires businesses to determine the applicable level of scrutiny "in good faith." While many businesses will act in good faith, the indeterminacy of the "good faith" standard and fear of DOJ second-guessing will cause businesses to spend time and money preparing unnecessary documentation validating the good faith of their decision.

Note: 999.325(a) makes a cross-reference to a subsection (g) that does not exist.

999.325(b) requires some consumer requests to be made under "penalty of perjury." In theory, this encourages submitters to submit only valid requests. However, will the DOJ devote any resources to prosecuting any perjured declarations? If not, the perjury declaration requirement will not adequately deter bogus requests. We've seen a similar dynamic with 17 U.S.C. § 512(c)(3), which specified the elements of proper copyright takedown notices. Per 17 U.S.C. § 512(c)(3)(A)(vi), the takedown notice sender must declare under penalty of perjury that he or she is the copyright owner or its authorized representative. However, in the two decades since the law's enactment, I am not aware of any perjury prosecutions for misdeclarations. Perhaps not surprisingly, bogus copyright takedown notices are rampant. *E.g.*, Jennifer Urban et al, *Notice and Takedown in Everyday Practice*, Mar. 22, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755628. If the DOJ expects the "penalty of perjury" declaration to discourage bogus consumer requests, it will need to commit resources to enforcement.

Rejecting Deletion Requests

999.313(d)(1) says that an unverifiable request to delete shall be treated as a request to opt-out of data sales. However, like other unverifiable consumer requests, the only proper outcome should be to disregard it. Otherwise, unrelated third parties—including malicious actors—can disrupt a consumer's relationship with a business.

999.315(h) does not adequately mitigate this problem. A business can dishonor any request that it "has a good-faith, reasonable, and documented belief" is fraudulent. Unfortunately, there is a significant gap between *dubious unverified* requests and *obviously fraudulent* requests, even though dubious unverified requests may be pernicious. Due to 999.315(h)'s high legal standards and 999.313(d)(1)'s low legal standards, businesses will feel pressured to treat requests in that gap as opt-out requests even when pernicious to the victim.

The regulations could fix this by lowering the 999.315(h) standard or raising the 999.313(d)(1) standard. The better approach would be to scrap the concept entirely. The DOJ has assumed, without any supporting empirical evidence, that deletion requests are perfectly correlated with consumers' desire to opt-out of data sales. Unless and until the DOJ validates this assumption, the DOJ should not codify it.

Applying Deletion Requests to Archival Information

999.313(d)(3) says that businesses must process deletion requests on archival material upon its access or use. How will this work in practice? If a business wants to consult archival material for any reason, including for reasons that will never involve the data of consumers who have made deletion requests, the business must first process all prior deletion requests before doing anything else. This could add substantial and problematic time delays and expense to any attempts to access archival materials. Instead, the regulations should require businesses to process past deletion requests on archival materials only when the business' engagement with the archival materials relates to such consumers or when the business is converting archival materials into active usage.

"User-Enabled Privacy Controls"

999.315(a) and (c) require businesses to honor opt-out signals communicated by "user-enabled privacy controls," an undefined term. Unfortunately, this proposal misunderstands the technology in two key ways.

First, though most consumers use one of only a few browser software programs, there are dozens or hundreds of other browser software programs in use, and new versions are constantly issued. Further, each software program independently decides how to indicate user preferences. Businesses cannot easily keep abreast of the complete universe of browsers and their idiosyncratic indications of consumer intent. Plus, honoring any new or changed browser signal takes time and money; it can't be implemented instantly.

Second, the browser software programs may ambiguously indicate consumer intent. The programs may give consumers a range of options, not just a binary yes/no to data sales. Or the program's way of characterizing its options to consumers may not clearly specify that it governs data sales, or the option may cover multiple unrelated topics.

Because the "user-enabled privacy controls" concept involves too much speculation about how browser software programs work, it's premature for the DOJ to adopt it. If the DOJ nevertheless retains the concept, it should (1) precisely define "user-enabled privacy controls," (2) implement a formal certification process run by the DOJ (or DOJ-approved third party certification bodies) to validate which precise versions of browser software programs contain a "user-enabled privacy control" that unambiguously indicates its users' opt-out desires, (3) specify the technological details of each certified program so that businesses can accurately recognize and interpret the program's signals, and (4) provide a phase-in window for businesses to implement any newly certified programs.

Transparency Reports

999.317(g) creates a new obligation for bigger businesses to disclose various statistics about consumer requests. Disclosures like these are sometimes called "transparency reports."

In general, I support transparency efforts. Transparency can encourage businesses to improve their behavior (because "what gets measured gets done") and provide helpful data to researchers and government enforcers to identify problems with the existing laws and advocate for reform.

Unfortunately, I do not see how the regulation's transparency report obligations will advance those goals. The regulations aren't likely to improve business behavior (businesses are already obligated to comply with the law), nor is it clear who plans to mine the disclosed data and how the required disclosures will be helpful to them. Meanwhile, the transparency report obligations impose substantial additional expenses on businesses. The fact that larger businesses might have better financial capacity to bear the costs doesn't obviate the need for cost/benefit justification.

The DOJ should eliminate the transparency report requirement from this version of the regulations and possibly reconsider it in future drafts when it's clearer who plans to use the transparency reports and exactly what information those users need. If the DOJ nevertheless retains the requirement, it should include a phase-in requirement for businesses that newly cross the 4 million consumer threshold.

"Aggregate Household Information"

The DOJ should define the phrase "aggregate household information" as used in 999.318(a).

Non-Discrimination Provisions

Example 2 (999.336(c)(2)) did not make sense. How can a business keep providing price discounts to a consumer who deletes their identifying information?

Also, while the options in 999.337(b) are helpful, the validation requirements remain onerous overall. Many businesses, especially smaller businesses, lack precise data to take advantage of any of the options.

A GDPR Safe Harbor

In its Notice of Proposed Rulemaking Action, the DOJ indicates:

> A less stringent regulatory alternative would, among other things, allow limited exemption for GDPR-compliant firms. Limitations would be specific to areas where GDPR and CCPA conform in both standards and enforcement, subject to auditing as needed. This approach could achieve significant economies of scale in both private compliance and public regulatory costs. The Attorney General rejects this regulatory alternative because of key differences between the GDPR and CCPA, especially in terms

of how personal information is defined and the consumer's right to opt-out of the sale of personal information (which is not required in the GDPR).

The GDPR offers many protections for California consumers that the CCPA does not. Thus, it's likely that if consumers actually understood both laws, many California consumers would regard the GDPR as equal or superior to the CCPA at protecting their interests. Meanwhile, everyone—including consumers—would benefit from the "significant economies of scale" and associated cost reductions that would come from a GDPR-compliance safe harbor to the CCPA.

What's Missing

The following two suggestions, related to the definition of "business" in California Civil Code 1798.140(c)(1), would help reduce unnecessary compliance costs.

First, the regulations should specify that the DOJ will only enforce the CCPA against businesses that generate $25M revenue *in California*. As currently drafted, the law requires full compliance from out-of-state businesses that have $25M in global revenue and "do business in California" (a notoriously ambiguous phrase) but derive minimal or no revenue from California residents.

Second, the regulations should provide a phase-in period for businesses that cross the CCPA's quantitative thresholds, such as a business approaching $25M in annual revenue. Right now, the law functionally requires that business to implement the law before reaching the threshold so that it will be in compliance if revenues actually cross the threshold. However, this means the CCPA affects companies expressly outside its scope. To avoid this outcome, the regulations should specify that CCPA compliance is only required 6 or 12 months after the business crosses the applicable threshold. The same issue arises with the 50,000 consumer threshold in (c)(1)(B) and the 50% threshold in (c)(1)(C).

Thank you for considering my comments.

Professor Eric Goldman
Co-Director, High Tech Law Institute
Supervisor, Privacy Law Certificate
Santa Clara University School of Law
500 El Camino Real
Santa Clara, CA 95053
408-554-4369
egoldman@gmail.com
http://www.ericgoldman.org
http://twitter.com/ericgoldman