Santa Clara University

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

February 25, 2020

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

By email: PrivacyRevisions@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 "Modifications" to the CCPA proposed regulations (the "revisions") published by the California Department of Justice (DOJ) on February 10, 2020. These comments supplement my prior comments on the proposed regulations that I submitted on December 6, 2019, available at https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=3093&context=historical. These comments represent only my views and not the views of my employer or any third party.

* * *

Notice at Collection

Several sections refer to notice being given to consumers "at or before the point" businesses collect their information. I do not understand the phrase "before the point." I'm not clear how a business could give notice only "before the point" of collection and still satisfy all of the regulations. The DOJ should clarify the phrase.

IP Addresses as Personal Information

The overbreadth of the CCPA's "personal information" definition—which inherently includes IP addresses—causes the CCPA to unintentionally apply to too many small businesses. Thus, I was pleased to see 999.302 propose to exclude IP addresses from the definition of "personal information," at least in some circumstances. That is an excellent policy goal, and I commend the DOJ for pursuing it.

However, the revisions' language doesn't achieve its apparent goal. The qualifier "could…reasonably link the IP address with a particular consumer or household" swallows up the exception. IP addresses almost always *could* be reasonably linked to an individual consumer

in the future—even if the service currently lacks the technology to do so and never plans to attempt the linkage.

To eliminate these inconsequential scenarios, the DOJ should delete the words "and could not reasonably link the IP address with a particular consumer or household." With that change, IP addresses automatically would become "personal information" only when a business links them to particular consumers or households. That way, possession of IP addresses in the abstract would remain outside the CCPA, and that would helpfully correct the CCPA's overreach.

Oral Disclosures

999.305(a)(3)d contemplates oral disclosures will be made via phone calls and face-to-face conversations. How will such disclosures work? Can the disclosures be highly abstract, such as "we collect your information, check our website for details"? Or will they need to be so detailed that disclosers will need to follow a written script?

The Opt-Out Button

The opt-out button in 999.306(f) has at least three problems:

- The iconography sends mixed messages to consumers who want to opt-out. Consumers won't know if they should want to toggle (the circle), cancel (the X), or not act at all because they are OK with the default state.
- The red color warns consumers to stay away.
- Despite the iconography looking like a functional button, a consumer who clicks on the button doesn't actually complete the action. The button just links consumers to a page with more information (999.306(f)(3)). Consumers may not realize that they need to take additional steps to effectuate an opt-out.

User-Enabled Global Privacy Controls

The revisions made some improvements on the topic of user-enabled global privacy controls, but the provisions still are not administrable by businesses. Businesses need specific and unambiguous guidance about which versions of which software programs constitute a "user-enabled global privacy control"—due to the extraordinary diversity of browser software (and setting options) as well as plug-ins, plus the fact that these programs change from version to version.

I continue to believe the DOJ should revisit this issue in future regulations rather than impose any obligations now, when the technology does not currently exist and businesses are scrambling to comply with other aspects of the law and regulations. If the DOJ insists on pushing the issue now, the DOJ should run a certification process to validate the specific program versions that qualify with the regulations' standards; coupled with an adequate phase-in period to let businesses update their systems. Anything else, such as the ill-defined standards in the revisions, does not put businesses on fair notice of what they must do to comply, and it imposes

unreasonable obligations on businesses to monitor and instantly respond to a vast ecosystem of software programs.

CCPA Compliance Transparency Reports

I reiterate my prior comments about the utility and cost of these transparency reports. The raised threshold to 10M+ consumers helps reduce the pernicious effects of these requirements. However, the DOJ still has not adequately justified imposing the requirement on any businesses at all.

Minor Typos

- 999.313(c)(5): "doings" should be "doing."
- 999.318(a): "deleted" should be "delete."

What's Missing from the Revisions

A few points from my prior comments that I reiterate:

- The provisions for verifying consumer requests remain too much like standards and don't have enough bright-line safe harbors.
- The DOJ should commit resources towards prosecuting "perjured" consumer requests per 999.325(c).
- The CCPA should provide a safe harbor for GDPR-compliant businesses.
- The $25M threshold in the definition of "business" should be limited to revenues generated in California.
- The regulations should provide a phase-in period for all businesses that newly cross a numerical threshold in the statute or regulations, rather than forcing unregulated businesses to be 100% compliant in case they possibly cross the threshold.

Delay in Enforcement

CCPA compliance has been mandatory for 2 months, and the DOJ can start enforcement in 4 months. Despite that, the draft regulations remain a moving target for businesses. The February modifications introduced hundreds of new changes to the draft regulations, many of which have substantial financial implications (such as revisions to the definitions of "personal information" and "households" and the transparency reporting thresholds).

At this point, the DOJ will not be able to give businesses more than a few weeks' notice of the final regulations' text before the DOJ can commence enforcement, and well-meaning businesses cannot anticipate what the final regulations will say or how the goalposts might move again. This uncertainty imposes avoidable expenses and confusion, none of which can be mitigated by well-meaning businesses doing their best to comply with the unfinished law.

Thus, the DOJ should provide an adequate advance notice period for businesses to comply with the final regulations, instead of requiring 100% compliance on July 1, 2020. Not extending the

deadline would be grossly unfair to businesses that can't comply with regulations that are still evolving.

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