CALIFORNIA
CONSUMER PRIVACY ACT

November 9, 2018

Alastair Mactaggart
Board Chair
Californians for Consumer Privacy
1020 16th Street, Suite 31
Sacramento, CA 95814

By Electronic Filing
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4725
Attn: Privacy RFC
Washington, DC 20230

Re: Developing the Administration's Approach to Consumer Privacy

Dear National Telecommunications and Information Administration:

As Chairman of Californians for Consumer Privacy and Chief Proponent of the California Consumer Privacy Act, I'm grateful for the opportunity to respond to your September 25, 2018 request for comments regarding the development of the U.S. Department of Commerce's National Telecommunications and Information Administration (NTIA) approach to consumer privacy.

In the interest of providing details NTIA may use in its two-pronged endeavor of identifying privacy outcomes and how those can be achieved through high-level goals[1], these comments reflect the background, rationale and intent of the California Consumer Privacy Act (CCPA) of 2018, passed on June 28, 2018.[2]

The California Consumer Privacy Act was drafted over the course of several years with a similar approach, using three guiding principles necessary in any consumer privacy framework: transparency, control and accountability. The CCPA began originally as a ballot initiative but was withdrawn after the successful passage of AB 375 (also called the California Consumer Privacy Act) by the California State Legislature.

A. CCPA PRINCIPLES

Transparency—The Right to Know
Our primary conviction is that for consumers to properly control their own data, they first need to understand what information is being collected about them. The right to find out what data a company has collected about you is the first step in understanding the scope of the issue—once

[1] Federal Register / Vol. 83, No. 187 / Wednesday, September 26, 2018 / Notices
[2] California State Assembly Bill 375 Privacy: personal information: businesses.

you know what companies have collected about you, you can decide whether their data collection and sharing practices present a problem. Our approach was guided by Justice Brandeis' famous quote about sunlight being the best disinfectant: any unsavory practices would not survive the cleansing light of day.

Control—The Right to Say No

Our second principle is to allow consumers to exercise reasonable control over the collection and sharing of information about them. This conviction led to the "Right to Say No," the right for a consumer to tell a corporation not to sell or share his or her personal information. It's one thing to do business with a company intentionally, but we heard from many advocates and consumers that the most objectionable part of this new, data-driven economy, was that their daily interactions ended up in the hands of hundreds of corporations they'd never heard of nor had any relationship with. The right to control who could obtain your personal information, seemed fundamental to any law designed to increase consumer privacy.

Accountability—The Right to Have Personal Information Kept Safe

The final component of our approach is to address data security. Of all the areas we surveyed around personal information, the one that most concerned Californians (and frankly enraged them), was the repeated instances of companies collecting their sensitive information, and not protecting it adequately from theft. Data breaches have become daily news events, and Californians—and, we venture to guess, all Americans—are tired of giant corporations being careless with their sensitive personal information.

B. CCPA BACKGROUND

To determine our approach, we met with dozens of legal and technical experts around the country, with businesses and privacy advocates, which allowed us to settle upon the three pillars outlined above of Transparency, Control and Accountability. We drafted the initiative and submitted it to the California Attorney General in September 2017.

The California initiative process includes an opportunity for any interested party to meet with the Legislative Analyst's Office to give feedback on a proposed initiative, and many groups from businesses to privacy advocates took advantage of this opportunity to give comments to the LAO.

Subsequently, we met with the LAO to review this feedback, and were so impressed by their suggestions that in mid-October 2017 we refiled a second version of the initiative, which we felt would allow us to improve certain aspects of the law. That second version received its Title & Summary from the Attorney General in mid-December, 2017.

C. FROM INITIATIVE TO LEGISLATION

Once in possession of the Title & Summary, we began the necessary steps to enable us to put the measure on the 2018 ballot. From January to May, 2018, we obtained the signatures of 629,000 Californians in support of our measure. This was greatly in excess of the legally-required minimum of 366,000 signatures, and the measure qualified for the November ballot.

California has a relatively new provision in the initiative statute, which allows a proponent to withdraw a measure which has already qualified for the ballot. We had been in contact with members of the California Legislature, notably Senator Robert Hertzberg and Assemblymember Ed Chau, and Senator Bill Dodd, and in June of 2018 reached a compromise with those two members on language that we felt would achieve substantially all of our initiative's goals. Assembly Bill 375 was subsequently voted out of both houses unanimously, and signed into law by Governor Brown, on June 28, 2018.

Without the herculean efforts of Mr. Chau and Mr. Hertzberg, and Senator Dodd's agreement to cooperate on a similar bill he was sponsoring; or the support of both Assembly Speaker Anthony Rendon's and Senate Pro Tem Toni Atkins' offices, the bill would never have become law, and much credit must go to that group of legislators for recognizing the importance of this issue, and the opportunity for California to become a leader in this field.

D. DIFFERENCES BETWEEN THE INITIATIVE AND THE LAW

The 'deal' that allowed the initiative to become law hinged on three main outcomes:

1) Increased consumer rights:
    a. Right to see your *actual* data. The initiative only gave consumers the right to see what *categories* of data had been collected about them, so this was a major, pro-consumer step forward.
    b. Right to delete the information *you have posted*. Not as comprehensive as the European "Right to Erasure," but still, more than the initiative had.
    c. Right to know the purposes for which a company is collecting your information. The initiative did not have this requirement.
    d. Increased age from 13 to 16, prior to which companies must obtain 'opt-in' permission from the consumer before selling their data.

2) Altered prohibition on not charging different prices if a consumer selects a privacy option.
    a. The initiative had a total prohibition on any differential pricing – i.e. charging users for requesting that a company not share or sell their information.
    b. The bill provides some flexibility on this point. Companies can charge consumers more if a consumer chooses not to have their data shared or sold, but:
        i. Companies can only charge a differential that is '**directly related'** to the value of the consumer's data.[3]
        ii. Companies must inform consumers and get opt-in consent to such a 'financial incentive' program (i.e. if they 'pay' a consumer to allow his or her information to be sold).

[3] Note that when the bill emerged from the Legislative Counsel's office, a typo was made, which both industry and privacy groups have committed to fixing in 2019The existing language reads "A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data." In reality, it should read "...provided to the *business* by the consumer's data."

iii. **Any such financial incentives cannot be unjust, unreasonable, coercive or usurious.** We think this requirement is critical in order to ensure a fair market solution.

c. In conclusion, CCPA as written provides flexibility to companies, but with transparency that will allow consumers to make informed decisions about which companies to do business with.

3) Limited Private Right of Action
   a. The initiative had enforcement by both the Attorney General, and a broad private right of action covering essentially all violations.
   b. The law limits the private right of action to data breach violations, with penalties of from $100 - $750 per violation.
   c. The rest of the law is subject to Attorney General enforcement, at up to $2,500 per violation ($7,500 for intentional violations).

The June passage of CCPA obtained many more consumer rights than the ballot initiative originally sought; it clarified a section with respect to pricing differently based on privacy choices; and it lessened the Private Right of Action, but kept substantial and meaningful penalties in place to ensure compliance.

E. GDPR VS CCPA: SOME MAJOR DIFFERENCES

Item "F" of the RFC refers to the question of other countries' replications of NTIA's future outcomes and/or high-level goals and their potential interaction with the exchange of goods and services in those countries[4]. Clarifying major differences between the European General Data Protection Regulation (GDPR) and the CCPA might help inform NTIA's consideration of the aforementioned replications and interactions.

While there are conceptual similarities, the CCPA is significantly different from GDPR.

The most obvious difference is in who is a covered entity: in Europe, all entities of any size are subject to GDPR, whereas CCPA only covers **businesses with over $25M in revenue, and data brokers selling large amounts of personal information.**

The second big difference is in the European approach of requiring user consent before *any* processing can take place. Specifically, under GDPR, a corporation must obtain a consumer's approval before collecting and processing his or her data. The fact of notice and required consent prior to collection, is indeed a step towards greater respect for privacy, but we were concerned that given the massive pull and market share for some of the largest consumer-facing brands—think Google, or Facebook, or Amazon—the choice facing consumers to consent or not, was actually a false one, since most consumers would simply click "I agree" to the request for consent.

[4] Federal Register / Vol. 83, No. 187 / Wednesday, September 26, 2018 / Notices

Additionally, and very importantly, we are concerned that this provision may hurt new entrants to the marketplace, since consumers may be unlikely to agree to the collection and sale of their information by a new entrant—so how does the *next* Google or Facebook even get off the ground?

As an alternative, if a consumer could restrict the sale of their information by any company he or she was doing business with, that felt like giving the consumer a more useful tool.

F. CCPA ENFORCEMENT AND RULE-MAKING

CCPA enforcement is for the most part delegated to the California Attorney General ("AG"), with the exception of the limited private right of action. Additionally, the AG is given broad rights to issue regulations (Sec. 1798.185(a)(7)(B)) to further the purposes of CCPA.

We think any law in this complex area, needs to have effective enforcement; and in addition, needs to have the regulator in possession of rule-making authority, to enable the ability to respond quickly and effectively to changes in technology, while preserving the mission of protecting consumer privacy. While the AG seemed like the logical agency to do this in California, we assume that the FTC would be the agency so delegated for any federal law. In that case, we would simply urge that it be given a) adequate resources to enforce; b) the authority to issue regulations governing consumer privacy; and c) the ability to impose fines without entering into a consent decree first.

Finally, we would urge any federal legislation include the ability for state Attorneys General to enforce, along with city and county District Attorneys in larger cities and counties, for example with populations over half a million residents.

G. CURRENT STATUS

At this point, the CCPA is scheduled to go into effect on July 1, 2020. A "clean-up" bill, SB 1121, passed the legislature in August 2018, and despite efforts by the technology industry to substantially weaken key components of CCPA, our coalition was able to persuade the legislators to hold the line, and the law has remained substantially as intended when we agreed to a deal in June.

Californians for Consumer Privacy remains committed to ensuring that any bill passed in Sacramento or in Washington, contains at least the same protections for Californians, that they have so recently won.

H. CONCLUSION

As consumers using technology on a daily basis, most of us face an 'expectation gap,' i.e. the difference between what a user expects (that the app or company with which the consumer originally interacts, the "first party," will collect and process his/her data), and what actually happens (i.e. that hundreds or thousands of "third parties" the consumer has never heard of, suddenly get access to his or her searches, browsing history, or geolocation information, which is then sold and resold).

A major part of the rationale behind CCPA was to give consumers tools to deal with this 'expectation gap.'

CCPA is not anti-business. It was, on the contrary, written and proposed by businesspeople concerned that regulations were needed; that as in so many previous situations, whether of the giant trusts of a century and more ago, or of the telephone and related wiretapping concerns, or cigarettes and health, or autos and safety, this latest technology too, has outpaced society's ability to fully comprehend it, or its impact on all of us.

CCPA represents one step towards damming the flow of this river of information, from consumer towards giant, multinational corporation, and thence out to an entire ocean of companies the consumer has never heard of, and would never choose to do business with.

CCPA puts the focus on giving choice back to the consumer, a choice which is sorely needed.

Thank you for this opportunity to respond to your Request for Comment.

Alastair Mactaggart
Chair
Californians for Consumer Privacy