Testimony of Alastair Mactaggart

Chair, Californians for Consumer Privacy

United States Senate Committee on the Judiciary

Hearing on:

Tuesday, March 12th, 2019

<u>Written Testimony</u>

Chairman Graham, Ranking Member Feinstein, and distinguished members of the Committee: Thank you for the opportunity to testify about the background, intent and competitive impact of the California Consumer Privacy Act ("CCPA").

My testimony is in two sections. As background, I have included portions of my written testimony to the Senate Commerce Committee on October 10th, 2018, which deals with the history and goals of CCPA.

I have also included a new sections dealing with my motivation for beginning this journey, and more importantly, issues of **<u>Competition,</u>** which I believe are central to this Committee's interests. In it I discuss how different privacy approaches, including CCPA's, impact competition and the overall business landscape in the United States.

CCPA Principles:

Transparency

My initial conviction was 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 you know what companies have collected about you, you can decide whether their data collection and sharing practices present a problem. My approach was guided by Justice Brandeis' famous quote, in that making clear what is now completely opaque, seemed worthwhile: any unsavory practices would not survive the cleansing light of day.

Control

It seemed to me that knowledge would inevitably lead to a desire on the part of consumers, to be able to control the information they uncovered. 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 I 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.

The right to control who could obtain your personal information, seemed fundamental to any law designed to increase consumer privacy.

Accountability

The third piece in this approach, is designed to address data security. Of all the areas I 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, I venture to guess, all Americans—are tired of giant corporations being careless with their sensitive personal information.

CCPA Background:

In settling on this approach, I met with dozens of legal and technical experts around the country, with businesses and privacy advocates. Essentially I spent the 18 months starting January 2016 doing research, which allowed me to settle upon the three pillars outlined above of Transparency, Control and Accountability.

Once I had settled on this architecture, I began drafting the actual bill in the summer of 2017, and submitted a version 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, I met with the LAO to review this response, and was so impressed by their suggestions that in mid-October 2017 I refiled a second version of the initiative, because we felt that would allow us to improve certain aspects of the law.

That second version, the culmination of approximately 2 years of discussion and negotiation, received its Title & Summary from the Attorney General's office in mid-December, 2017.

From Initiative to Legislation

Once I received the Title & Summary, I began the necessary steps to enable us to put the measure on the 2018 ballot. From January to May of this year, I obtained the signatures of 629,000 Californians in support of the measure. This was greatly in excess of the legal 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 qualified for the ballot. I had been in contact with members of the California Legislature, notably Senator Robert Hertzberg, Assemblymember Ed Chau, and and Senator Bill Dodd, and in June of 2018 reached a compromise with those members on language that I felt would achieve substantially all of our initiative's goals.

On June 28, 2018, Assembly Bill 375 was voted out of both houses **unanimously**, and signed into law by Governor Brown. (I should note that without the support of Senator Jackson, Chair of the Senate Judiciary Committee, Assembly Speaker Anthony Rendon, and Senate Pro Tem Toni Atkins, 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.)

As proponent, it was my belief that the certainty of a law was preferable to the uncertainty of an election, so I agreed to withdraw the ballot measure. More importantly, CCPA obtained many important consumer rights that were not in the initiative; 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. Overall, I was very pleased with where the law ended up.

GDPR vs CCPA: some major differences

Some have compared CCPA to the recently passed European General Data Protection Regulation. While there are conceptual similarities, the CCPA is significantly different.

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 I was concerned that given the massive pull and market share of 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. [As it turns out, subsequent to GDPR's introduction, this concern has been validated[1]].

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

Current Status

At this point, the law is scheduled to go into effect on July 1, 2020. A "clean-up" bill, SB 1121, passed the legislature in August 2018 (also unanimously, as did its predecessor AB 375), 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 2018.

There will certainly be a battle in the coming years, either in the California Legislature or in Congress, as companies seek to return to a world free of any limitations on what they can do with consumers' personal information.

However, 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.

Motivation Behind CCPA:

I get asked all the time why I got involved in this matter.

I am not a technologist; I don't have some vendetta I'm trying to pursue. I didn't spend twenty years as a privacy advocate.

[1] (Kostov, May 31 2018) *Google Emerges as Early Winner From Europe's New Data Privacy Law.* Wall Street Journal.

And yet, to paraphrase Samuel Johnson, one doesn't have to be a carpenter to say a table's badly made. As a citizen of the country, the more I looked into this problem, the more obvious it was that it needed fixing; and the more I realized that given the current state of political affairs, and the power and influence of giant corporations, it was unlikely to get fixed via a normal legislative process.

For some time I thought "Someone should do something about this;" and then, to quote the old cliché, I realized I was someone.

I began to think about the idea of a ballot measure: I suspected most Californians were fed up with the notion that they had no privacy; that while they had submitted to the "take it or leave it" approach to privacy that has reigned for so long in this country, they probably didn't like it any more than I did. I began to believe that if I could get a simple question on the ballot, it might be impossible to spend enough money to defeat it.

Now, almost a year after we gathered our signatures, I am so pleased I took the risk, and took a stand.

We live in a world where giant companies, the most valuable companies the world has ever known, are tracking our every action. We live in a world of commercial surveillance.

As in so many previous situations, whether with the giant trusts of a century and more ago, or the invention of the telephone and related wiretapping concerns, or cigarettes and the dawn of the anti-smoking movement in the 1960s, 80 years after the invention of the (mass) cigarette rolling machines, or automobiles and the focus on safety that began in the 1950s, this latest technology too, has outpaced society's ability to fully comprehend it yet, or its impact on us all. We are still trying to understand what constant commercial surveillance means for us and for our society; and that's why I believe this is such a necessary step forward for our state and our country.

No one law can address the intersection of privacy and technology, any more than one law can address consumer protection, highway safety, or food inspection; but CCPA represents a giant step forward, and will help redress the imbalance between consumers and giant businesses that currently exists. I think California took an important step in the right direction, that it will continue to build on this law to ensure that consumers' privacy is protected and respected. I hope Congress will do nothing to undermine that step, as my belief is these new protections have profoundly positive implications for our democratic society going forward.

COMPETITION:

ARE PRIVACY LAWS GOOD OR BAD FOR BUSINESS? WHAT EFFECT WILL CCPA HAVE ON U.S. BUSINESSES, VS. GDPR IN EUROPE?

Competition: State of the Industry

Much has been written on whether privacy laws are good or bad for business, whether they will increase or reduce competitiveness, raise or lower the cost of goods to consumers, or ultimately even threaten the provision of free products (especially content) on the internet.

Many of the largest players would have you believe that the cure is so bad it will kill the patient.

I examine this topic below, but first, let's reflect on some key facts:

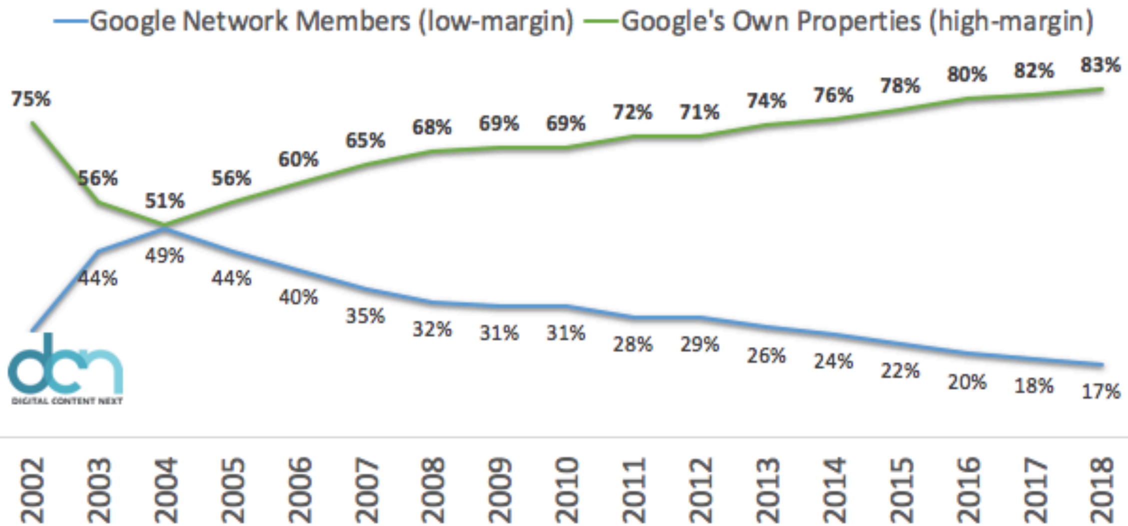
1) In 2017, Google & Facebook took in 63% of US digital ad revenue, which was projected to grow to ~69% in 2019.
2) In 2017 over 90% of the growth in global digital advertising went to Google & Facebook.

Google and Facebook (and other large internet companies, though none as much as these two) are collecting unimaginably vast troves of data about consumers, including nearly every email received, every search ever made, every site visited. They have the infrastructure in place to track essentially all consumers across all their devices.

This is a case of the rich getting richer, faster, which is having deleterious effects on the rest of the digital (and in many cases, brick and mortar) economy.

Posit an automaker going to Google with a $50M ad campaign. Google (and Facebook) have trackers on essentially all sites that all US consumers visit. So it's not only a simple technical matter, but business logic ***demands*** that these large 'platforms' surveil consumers to learn their interests, then wait (to the extent possible) to advertise to the consumer until s/he is on one of their owned and operated sites (whether Instagram or YouTube), thereby keeping all the advertising dollar in-house.

Please see this graphic below highlighting this trend.



Let's revisit this theme from a different angle, or rather, make the point differently.

First, the 'platforms' are by far the dominant destinations on the internet: Google, Youtube and Facebook are first, second and third ranked sites on the internet. These sites can attract and engage users more than any other site, which allows them to create in-depth profiles about ausers based on their intentional search activity and social network interactions.

Second, these sites are also among the most prominent *third* parties, which gives them incredible reach and visibility into trends and developments across the web and mobile. Facebook and Google have tracking mechanisms installed on the majority of the world's websites. This gives these companies a huge advantage with regards to the collection of valuable behavioral data across all forms of sites/services (i.e. they have more vantage points than any other enterprise).

One might ask why websites allow these two behemoths to have the third party tracking, and the answer is simple, and part of the puzzle: if you are advertising online, you more or less have to use both of these companies. They are where the eyeballs are, but more importantly, they *are* the ad networks (Google owns DoubleClick, and Facebook's Mobile Ad Network dominates in mobile). And if you're advertising, both Facebook and Google's ad services work better if you install their third party tracking mechanism (i.e. a Facebook pixel for Facebook, or Google Analytics for Google).

Sometimes this is overt, and sometimes implied. So for example, Facebook required reciprocity from its partners (i.e. if you were an app developer and wanted access to the Facebook API, Facebook demanded until recently that the app's users be able to easily share their social content with Facebook). Google implies that if a business shares its user information with Google in a way that Google can then combine it with all its *other* information, the business will benefit in multiple ways. Essentially they imply that Google Analytics, and Google search, will not work as well if the business doesn't share all its data with Google.

GDPR

GDPR was supposed to address many of these concerns. And in many areas, it has proved to be a landmark law. And even with respect to the problem I'm about to discuss, the EU data protection authorities are focused on addressing it.

However at the moment, Google is using the dominance of its platform in Europe to demand that traditional first parties, who are required to obtain user consent before collecting user personal information, also obtain consent **on behalf of Google** so that Google can be considered a first party, **thereby completely sidestepping the key provision in GDPR that restricts them from collecting information as a third party**. To use a specific example, Google requires that any publisher that relies on Google, such as The London Times – force the users of the London Times to consent to third party tracking by Google when they consent to using The London Times.

The effect of this is that with respect to third party tracking, nothing has changed as a result of GDPR for the giant platforms.

And again, the current architecture of watching consumers across the web, learning about them at a granular level never before contemplated, assembling vast dossiers on them, and then using that information to advertise to them once they are on a platform-owned site, is unchanged.

GDPR's 'NOTICE AND CONSENT' FRAMEWORK

In addition, we think GDPR's 'Notice & Consent' framework is clunky and problematic. Consumers report 'click fatigue' from all the pop-ups, which lose relevance (plus no-one reads the privacy policies, now, any more than they used to).

We think consumers are confused about the "take it or leave it" nature of GDPR. An Uber or Lyft customer really *does* need to turn over geolocation and credit card information; if they decline to let their personal information be collected and processed, how will the rideshare services work? And so do they really have any meaningful 'control' over the collection of their information, especially assuming that most consumers want to use these sites at the heart of the digital revolution?

Finally, we think Notice and Consent could potentially have a chilling effect on innovation. GDPR covers all entities—any business of any size. So we fear that consumers will give the right to process their information to companies they know—the giant consumer brands—but may not to the smaller companies that are starting out, which will make the data moat around the huge platforms even wider and deeper.

<u>CCPA's Impact on Current Landscape</u>

I believe CCPA will dramatically level the playing field when it comes to preventing the large platforms from learning about more or less every consumer's every interaction with every website.

Under CCPA, any information Google or Facebook (or any ad network) learns about an opted-out consumer on a first-party site, *must* stay silo'd with respect to that consumer and that first party.

Put another way, if Google is watching an opted-out consumer on the New York Times, anything it learns about that consumer, can only be used in that context, i.e. when the consumer is on the New York Times.

What will this change achieve? We think it will vastly increase the bargaining power of the first parties—among them, America's newspapers.

When CCPA goes into effect, if Google or Facebook wants to access a high-value audience—say, at the New York Times—they will not be able to observe and essentially take all the important information generated by NYT's users on the NYT website, and use it elsewhere, if that consumer has said Don't Sell My Information. Say Facebook thinks a consumer may be in the market soon to book a trip to Europe, which it learns from watching her read the NYT travel section. Today it can take that information and use it on its own site, or when she's on Instagram, to advertise an air ticket or hotel.

That will change with CCPA: in this scenario, Facebook could only use that data to advertise to that consumer on the NYT, which is a huge sea change in how the flow of valuable personal information will work.

<u>CCPA: Do Not Sell My information ~ Do Not Track</u>

One question which has been raised, is just how CCPA will allow consumers to opt out of the sale of their information?

CCPA achieves this critical step in user-friendly fashion, building heavily on the "Do Not Track" regime.

Thus: every site doing business in California will be required to have a "Do Not Sell My Information" button. All sites will also be required to accept what are called "third party opt-

outs", which will allow consumers to delegate a third party to opt them out of all the sites they visit. This is a *critical* element of CCPA, one of its most central.

Thus we envisage that browser companies (we've talked to some who agree they will do this) or mobile phone makers will simply create controls, like a browser button that users can enable, which will indicate to every single site a consumer visits not to sell that consumer's information. The consumer experience will be "set it and forget it," i.e. the consumer will only need to do this once, and essentially permanently opt out of having their information sold. It essentially mimics what was referred to as the 'user preference expression' in the 'Do Not Track' proposal.

This means that unlike in Europe, where users may currently have a false sense of security, thinking that only the first party they are dealing with, can collect and process their information, CCPA will grant users a much more concrete right, albeit less ostensibly dramatic at first blush.

CCPA doesn't prevent businesses collecting information on consumers—unlike in Europe—which has led some to charge that it does not respect user privacy. But we think CCPA will give more, and more meaningful, control over personal information to users, than GDPR, precisely because under CCPA users will be able to set their browser once, and then all covered entities will be prevented from selling or disclosing their information. All winners and losers of real time bids will ***not*** be able to reuse that information, except back with the same first party.

Branding: Dissimilar Brands are Separate Businesses

One of the other big benefits of CCPA is that it treats large companies with multiple brands, as separate businesses. Unless the companies are commonly branded, then data held by one cannot be obtained or shared with the other. This has very pro-competitive consequences for smaller companies seeking to catch up to the duopoly.

Part of the power of the duopoly is the sheer volume of personal information they have, which allows them to better target consumers. There is practically no way to catch up with them now, especially since all information can be combined across all aspects of their various businesses.

Conclusion

I think CCPA will enhance US competitiveness.

It will give consumers meaningful control over what happens to their data, as opposed to the impression of control.

CCPA will begin to redress the imbalance that currently exists between consumers, publishers/content generators, and the platforms. Right now, the giant platforms benefit from the work that is done to create content and assemble audiences, by learning about consumers,

then waiting until that consumer is on one of their owned and operated sites (i.e. YouTube for Google, Instagram for Facebook) and advertising to them at a much higher margin.

CCPA is balanced: it treats all covered entities the same way, avoiding the GDPR requirement for consumer consent before data is processed, which could lead to consumers only giving their assent to brand name companies. Furthermore, it permits advertising, but given its architecture and impact, we feel that it will emphasize more traditional "contextual" advertising (read an article about New Zealand, see an ad for Air New Zealand), over "behavioral" advertising (track that you're a single mother at the end of the month running low on funds, send you coupons for cheap fast-food restaurants).

We think there is plenty of evidence that the allure of behavioral advertising is overblown, and would remind readers that contextual advertising is the technology that built Google and Facebook. The world will still turn on its axis if advertising is a little less creepy and invasive, and the behemoths will still make money on a scale and at a margin never seen before in business history.

Personnel

While I used the first person above, I would be remiss not to thank the team I was lucky enough to assemble, who really made CCPA a reality.

First, Richard Arney, my brilliant friend and the Californians for Consumer Privacy vice-chair: a volunteer, but one who provided assistance and inspiration throughout.

Ashkan Soltani, an expert in privacy and technology, and former chief technologist at the FTC, consulted for me while we were drafting the law, and provided invaluable strategic and technical direction.

James Harrison Esq. of Remcho, Johansen & Purcell is the actual author of the law, and having worked with many attorneys in my career, I can safely say that he is at the top of his field: diligent, careful and insightful.

In Sacramento, my campaign consultant Robin Swanson and press secretary Inez Kaminski were also vital team members, essential allies when up against (as it turned out) opponents with a combined market capitalization in excess of $6 trillion.