Testimony of Alastair Mactaggart

Chair, Californians for Consumer Privacy

United States Senate Committee on Commerce, Science, and Transportation Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security

Hearing on:

Wednesday, October 10th, 2018

Written Testimony

Chairman Thune, Ranking Member Nelson, and distinguished members of the Committee: Thank you for the opportunity to testify about the background, rationale and intent of the California Consumer Privacy Act ("CCPA") of 2018, passed on June 28, 2018.

CCPA Principles:

Transparency

Our 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. Our 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 us 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 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.

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

Accountability

The final component of our approach, was the piece designed 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.

CCPA Background:

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

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

That second version received its Title & Summary from the Attorney General's office in mid-December, 2017.

From Initiative to Legislation

Once we received the Title & Summary, we began the necessary steps to enable us to put the measure on the 2018 ballot. From January to May of this year, we obtained the signatures of 629,000 Californians in support of our 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. We had been in contact with members of the California Legislature, notably Senator Robert Hertzberg and Assemblymember Ed Chau, 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. (I should note that without the herculean efforts of Mr. Chau and Mr. Hertzberg, 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.) Additionally, Common Sense Media supported and co-sponsored the bill.

Differences between the Initiative and the Law

The 'deal' that allowed the initiative to become law revolved around three main components:

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.[1]
        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).
        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

[1] 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 2019. The 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."

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.

As proponent, it was my belief that the above compromise was the right one to make. The June passage of CCPA obtained many more consumer rights; 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.

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 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. [As it turns out, subsequent to GDPR's introduction, this concern has been validated[2]].

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

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

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, 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.

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:

We live in a world where giant companies, the largest companies the world has ever known, are tracking us continually. We live in a world of commercial surveillance. During our research I became aware of the scale and scope of this surveillance, and include below some recent examples that have appeared in the press:

Google has a patent on using in-home[3] devices to track whether alcohol is being consumed; whether (and presumably, what kind of) smoking is taking place; whether teeth are being brushed, and for how long, and whether the water is being left running during the teeth-brushing. The patent extends to determining whether 'mischief' is occurring in the home, to determining the emotional state of the home's occupants (based on voice and facial expression), and to tracking whether foul language is being used.

Advertisers can erect "geofences"[4] around any physical location or building[5], which are essentially just lines with latitudinal and longitudinal coordinates, and can tag smartphones[6] crossing such a fence, in order to send advertisements to that device. As a result, through no overt action of a consumer, the companies know who is in rehab, who goes to AA, who just got an abortion[7], what your religion is, and whether you have a drug problem. If you're in rehab, or in jail, or go to an HIV clinic regularly, that information can be sold, and resold, simply because you have a mobile phone. This is the new reality—if the company can track your phone, they can track you.

---

[3] Fadell, M., A., & al, e. (2016). United States Patent Application 20160261932. *US Patent Office.*

[4] (White, November 1, 2017) *What is geofencing? Putting location to work.* CIO.

[5] (Copley, Last visited 10-2-18) *Geofencing--How it works [http://copleyadvertising.com/#how_works].* Copley Advertising Blog.

[6] (White, November 1, 2017) What is geofencing? Putting location to work. *CIO*.

[7] (Healey, 2017) Massachusetts Attorney General Press Release (2017). *AG Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities.*

Wearable activity monitors (think Fitbit) collect your most intimate data, and none of it is covered by HIPAA until it reaches a doctor[8], hospital, or other covered entity—as a result much of it is available for sharing or sale with third parties[9].

Employers can obtain information about their workforce from benefits managers[10], who use sophisticated tools to figure out which employees might be trying to get pregnant, or be pre-diabetic; and in a small company with say only 20 women working, it is likely that if 10% of the workforce is trying to get pregnant, the manager knows who those two women are. Then, if the economy slows, and the manager needs to lay someone off...it might be easier to decide on the person who might be pregnant next year.

5 low-resolution images of your face are enough[11] [12] for an algorithm to determine your sexual orientation (91% confidence for men, 83% for women). And remember, there are 10 countries in the world where to be gay is a crime punishable by death[13].

300 likes on Facebook are enough for an algorithm[14] to predict your answers to a well-established personality profile, better than even your spouse, and much better than your co-workers. If we're all looking for someone to truly understand us, what does it say when that person is...the algorithm?

Amazon has a patent to use photos taken in the home[15] to determine whether consumers are wearing certain images on their clothing (think a musician) and then using that to offer the consumer similar items for purchase.

China is monitoring consumers' behavior—who they associate with, what they search for, whether they jaywalk[16]—to produce the famed 'Social Credit' score[17][18]. Combined with a comprehensive facial recognition system, this takes societal tracking and control to a new level—and yet, in what way does the Chinese government know less about its citizens, than the big search engines or social media companies know about Americans?

---

[8] (Mobile Health and Fitness Apps: What Are the Privacy Risks?, Dec 16, 2016)
[9] (Fitbit and Google Partnership May Raise Privacy Concerns, May 25, 2018)
[10] (Picchi, February 18, 2016)
[11] (Levin, 9-7-17) *New AI can guess whether you're gay or straight from a photograph*. The Guardian.
[12] (Kosinkski, 5-12-2017) *Deep neural networks are more accurate than humans at detecting sexual orientation from facial images.* PsyArXiv
[13] (Bearak, 6-16-2016) *Here are the 10 countries where homosexuality may be punished by death.* Washington Post.
[14] (Kosinksi, 1-27-2015) *Computer-based personality judgments are more accurate than those made by humans.* Proceedings of the National Academy of Sciences.
[15] (Maheshwari, March 31 2018) *Hey, Alexa, What Can You Hear? And What Will You Do With It?* New York Times.
[16] (Tracy, 4-24-2018) *China's social credit system keeps a critical eye on everyday behavior.* CBS News.
[17] (Rollet, June 5, 2018) *The odd reality of life under China's all-seeing credit score system.* Wired.
[18] (Larson, August 20 2018) *Who needs democracy when you have data?* MIT Technology Review.

Anyone can purchase a list of people taking certain medications[19] or police officers' home addresses[20]. Employers can easily advertise to only younger potential employees on Facebook[21], and do. Racists can specifically target certain ethnic groups in order to exclude them from renting an apartment[22], or to try to get them to join a hate group[23].

The majority of the world's websites have a Google[24][25], Facebook or Twitter tracker—so that your information is being sent back to those companies, and you are being tracked over the internet, wherever you go, using whatever device you're on.

And not just you: your children are being evaluated and tracked, often in direct contravention of laws like the Child Online Privacy Protection Act (COPPA), as was recently highlighted in a study showing almost 6,000 of the most popular children's Android[26] apps were potentially in violation of COPPA.

And not just online: in the physical world, Google recently was in the news, and is now facing multiple lawsuits, because it continued to track users up to 300 times *a day*[27], even when the user had turned off his or her "location history," and seen this message in response *"You can turn off Location History at any time. With Location History off, the places you go are no longer stored."* However, despite the obvious implications of this message, Google continued to track users—and seemed to make it intentionally very difficult for even tech-savvy users trying to stop from being tracked, to turn off this constant location surveillance.

Consumers do not also generally understand that in many cases these businesses and apps allow partners to install a small piece of software or code on the user's smartphone, which allows that third party to track the user and collect all the information pertaining to his or her use of that app; and furthermore not just information about that user's interactions with the original app, but what other apps the user might have installed, or have open.

Weather apps are prime examples of this[28], and many are in fact owned by data brokers, since consumers do not tend to turn off their location services for such apps, given it's more work to

---

[19] NextMark

[20] NextMark

[21] (Angwin, Dec 20, 2017) Dozens of Companies Are Using Facebook to Exclude Older Workers From Job Ads. *ProPublica*.

[22] (Angwin, Facebook (Still) Letting Housing Advertisers Exclude Users by Race, Nov 21, 2017)

[23] (Angwin, Facebook Enabled Advertisers to Reach 'Jew Haters', Sept 14, 2017)

[24] (Simonite, May 18, 2016) *Largest Study of Online Tracking Proves Google Really Is Watching Us All.* MIT Technology Review.

[25] (Narayanan, 2016) *The Long Tail of Online Tracking.* Princeton Web Census.

[26] (Reyes, April 25, 2018) Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale . *Berkeley Laboratory for Usable and Experimental Security*.

[27] (Tung, Aug 17, 2018) Google: To be clear, this is how we track you even with Location History turned off. *ZDNet*.

[28] (Mims, March 4, 2018) *Your Location Data Is Being Sold—Often Without Your Knowledge.* Wall Street Journal.

type in a zip code or a city, than to have the app simply display the weather forecast. But in so doing, they give the app real-time access to the consumer's exact location.

We call this whole suite of issues, the 'expectation gap,' i.e. 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 tens or hundreds of "third parties" the consumer has never heard of, suddenly get access to his or her interactions on their smartphone, and that his or her location is 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 yet, 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.