Questions for the Record from Senator Lindsey O. Graham
To Mr. Alastair Mactaggart
U.S. Senate Committee on the Judiciary
GDPR & CCPA: Opt-ins, Consumer Control, and
the Impact on Competition and Innovation"
Submitted on March 15, 2019

1. Please explain how the non-discrimination provisions of the CCPA would impact businesses that provide "free" services to consumers and derive revenue from other means, including advertising. Will companies now have to offer paid alternative products? How will this impact customer loyalty and discount programs?

Answer: Section 1798.125 of the California Consumer Privacy Act allows consumers to know that they will not be discriminated against merely because they do not wish to be pervasively tracked across all websites, all the time, and have their browsing history collected and monetized.

Please note that 'advertising' is not subject to this non-discrimination provision, i.e. a consumer cannot opt out of the use of their personal information by a covered business for advertising and marketing purposes. Please refer to Sec 1798.140(d)(5), which enumerates "advertising or marketing" as one of the allowed "Business Purposes" which, under the definition of 'sell' and 'third party,' do not qualify as a sale when information is disclosed pursuant to one of them. In fact, CCPA does not restrict a business's ability to use consumers' personal information for advertising and marketing purposes, it only restricts what subsequent recipients of that information can do with it. Put simply, a first party, say a newspaper, can use personal information it collects about its readers, to show them ads; however, the ad network that serves that ad, cannot then go out and sell that information on the open market.

1798.125 ensures that consumers are allowed to opt-out of the sale of their information; but equally, it ensures that in a scenario where a business exists entirely by collecting personal information and monetizing it, that the business can charge a fee "if that [fee] is directly related to the value provided to the business by the consumer's data." [Please note that there is a typo in this sentence which will be corrected by AB 1355, assuming it passes into law in the coming month. The existing language reads "…provided to the consumer by the consumer's data." The revised language will read "…provided to the ***business*** *by the consumer's data."]*

Further constraints on this allowable charge are that it cannot be "unjust, unreasonable, coercive or usurious."

I think this outcome strikes the right balance: businesses that rely on monetizing consumer data, will be able to continue to do so by charging a fee to consumers who opt-out of the sale of their data, as long as the opt-out charge to the consumer is "fair," a term I am using as shorthand for the above constraints. Businesses will not be able to 'force' consumers to consent to the sale of their data, by setting the fee at some artificially inflated rate that would

coerce essentially all consumers into accepting the business's terms and continue to have their data sold.

One final point: many businesses exist by collecting and monetizing consumers' data, unbeknownst to the consumer. This provision will bring such practices into the light. If a business can convince its customers that it is delivering value even while selling its customers' information, it will be fine. If it cannot convince its customers to allow their data to be sold, my hypothesis is that the business exists today simply because of customer ignorance, by pretending to be one thing, but actually being something else (a collector of personal information which surreptitiously sells that information).

Compare it to food labelling: if a food manufacturer is worried about transparency, about disclosing what's on the can, then perhaps it should change its ingredients. Businesses will have to disclose what they do with their customers' data, and how much they're making off each customer by selling his or her data.

In conclusion, I think this provision strikes the correct balance between protecting consumers and allowing businesses to continue to operate.

Questions for the Record from Senator Chuck Grassley of Iowa

GDPR & CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation

Questions for the First Panel

1. Please briefly explain the importance of transparency and ensuring that consumers can make informed decisions about the information they share.

Answer: right now many businesses exist pretending to be one thing—delivering a consumer weather information, for example—but in reality are something totally different, and are in fact gathering data under the guise of providing a service, but in fact are doing so in order to sell it. What better way to track a person, than via a weather app, since most consumers give such apps access to their location, rather than laboriously type in a city name every time they check the weather? (This by the way is why the Los Angeles District Attorney is suing the Weather Channel's app for deceptive advertising).

Increasingly, Americans live their lives online, and cannot exist without turning over tremendous amounts of their personal information to giant corporations, from whether they were late to work, to how much they weigh, to how often they eat at a fast food restaurant, to who they spend time with.

Many consumers don't know what's being collected; and where it's going, whether it's being deleted or instead sold to the highest bidder.

Transparency is essential to allowing consumers to make informed choices about who they do business with—think of the food labeling laws, which help us all make better choices about what brands to buy.

2. Transparency is critical in ensuring that consumers can make informed decisions. That can become more complicated, however, as our lives are increasingly connected to the technologies around us, like autonomous vehicles. According to one report, by 2025 each person will have at least one data interaction every 18 seconds – or nearly 5,000 times per day.[1]

    a. How do we balance the need for transparency and informed consent with the reality of our increasingly data-connected daily lives?

    b. Should consumers have to consent to every data interaction throughout their day?

Answer: I would like to combine a) and b) into one answer, since I think the two questions are so connected. The reality is that, as they point out, more and more of our lives are measured and tracked by more and more companies, and even though the resultant profiles that a few giant companies obtain about us are incredibly detailed, opting-in to every data interaction, every day, will present roadblocks to consumers and businesses alike.

[1] David Reinsel et al., *The Digitization of the World—From Edge to Core*, IDC (Nov. 2018).

Transparency is essential to giving a consumer the necessary information to choose who to do business with. With respect to consent, however, while equally important, I think the opt-in model misses the mark. For me, consent is more about what happens to my data, and how it is used, and less about whether it's collected by a company in the first place.

My difficulty with the "opt-in" approach is based on its architecture, which I think can give a consumer a false sense of control.

Put simply, once a business has gotten a consumer to opt-in to the collection of their data, it is business as usual (for the business). In other words, opt-in is a temporary roadblock. If you want to use Google, or Uber, or Amazon, and the business says "we need you to opt-in in order for you to use our services"—well, the vast majority of consumers will simply click "accept."

Opt-in without a consequence is not meaningful, and it's very difficult to have a consequence because, in fact, in many cases the businesses do need to collect consumers' personal information—and importantly, consumers' sensitive information—to function properly.

Google works better if it understands that I mean a California law when I type in AB ##, vs some other state's. Uber needs to know my billing address, my credit card number, and my exact geolocation, in order to work. Evite may well know my religion, if I've invited everyone to my son's bar mitzvah.

Contrast that with 'opt-out of the sale of your personal information.' This seemed, and seems to me still, to be a better tool to give consumers. It says to a consumer, yes, you can use this or that service, but also you can tell them not to sell your information. It gives the consumer choice, which feels more American, but I would argue it also gives them more actual power to do something about their privacy, than even GDPR, which often simply results in a consumer's knowing that the business is collecting their data—which they knew anyway.

Finally, CCPA's approach is very powerful in that it allows for consumers to have an agent opt-out of the sale of their information, on their behalf. What this will mean in practice, is that browser manufacturers and other companies will create global settings allowing a consumer to "set it and forget it," i.e. to select a "do not sell my information" setting, which will then be communicated to all apps on the consumer's device, and all websites the consumer visits.

We think this is among the most impactful aspects of CCPA, in that it will be simple for consumers to use, and because of that, far reaching for their privacy.

Therefore I feel that CCPA arrives at the right point: it allows consumers the ability to find out what businesses are doing with respect to their data; and it gives them the right to opt out of the sale of that information. This choice-based model will allow for consumers to know more about which businesses they do business with.

3. If Congress enacts federal data privacy legislation, how do we ensure that companies are still incentivized to innovate in their privacy and data protections, rather than just 'check the box' of regulatory compliance?

Answer: I think it crucial, if federal legislation is enacted, that it not preempt state legislation.

The Electronic Communications Privacy Act of 1986, a federal law, allows any law enforcement agency to obtain any email that is older than 180 days, from any internet service provider, without a warrant. This was because in 1986 email was new, and everyone thought of it in an analogous manner to physical mail: i.e, if it was old, it was unimportant and unwanted.

Of course, this has not turned out to be accurate, but despite the obvious privacy implications of allowing citizens' communications to be freely available to law enforcement without a warrant, the law has still not been changed. In 2016 and 2017, a bill to amend this egregious government power has passed on a voice vote out of the House, but each time has stalled in the Senate.

The fact of the matter is, it is incredibly difficult to get any legislation passed through Congress, and even if a privacy law were passed in 2019 or 2020, the thought that such a law might sit like a blanket on the area of privacy legislation, with obvious errors, for the next thirty-three years, is concerning.

Privacy is just another name for an area where many companies are growing and experimenting in new and important ways, and regulations must keep up with this rapidly-changing area of business and law. We cannot rely on the federal government to be able to react appropriately to new developments, given its history of being unable to amend something even so seemingly obvious as a federal law allowing unlimited, warrantless access to citizens' communications.

In terms of innovation, I am a passionate believer in the power of the market to foster competition: as soon as consumers can get reasonable information about which companies are doing what with their data, I believe that privacy will become just another axis on which businesses compete with each other. As soon as one mobile phone company says they are not going to sell consumers' location, the pressure on others to follow suit will be immense.

Questions for the Second Panel

1. Please briefly explain the importance of transparency and ensuring that consumers can make informed decisions about the information they share.

2. Often times, comprehensive regulations end up just benefiting the large, entrenched entities that have teams of lawyers to ensure compliance. Should small businesses be treated differently in any federal data privacy framework? And if so, how?

3. If Congress enacts federal data privacy legislation, how do we ensure that companies are still incentivized to innovate in their privacy and data protections, rather than just 'check the box' of regulatory compliance?

4. How do we best craft a federal data privacy law that keeps pace with our ever-evolving tech and data landscape? And can we do that without giving unfettered discretion to the regulators?

Written Questions from Senator Dick Durbin
Hearing on "GDPR & CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation"
March 19, 2019

For questions with subparts, please respond to each subpart separately.

Questions for Alastair Mactaggart

1. **Do you believe that states are likely to be more aggressive and proactive in protecting online privacy than the federal government?**

Answer: I agree with this statement absolutely, if for no other reason than in a resource-constrained world, more regulatory resources brought to bear on the issue of privacy, will be more effective than less. It is well-documented that the FTC has approximately 40 privacy professionals to deal with the largest developed economy in the world with over 300 million consumers, whereas much smaller countries have staff an order of magnitude larger. There seems to me low possibility that the federal government could provide the same resources as the 50 states, especially when considering smaller cases that might interest only a certain geographic area (consider a data breach case at a company with regional operations).

Add to this, that states' efforts will likely be led by elected politicians eager to fight to protect their citizens' privacy. There are many areas where state and local regulatory efforts are more effective and proactive than the federal government. One just has to think of recent history with the opioid-abuse epidemic to realize that often the states can move more quickly and effectively than the federal government, which so often depends on a particular administration's approach. Having 50 states able to regulate privacy, will prevent developments that weaken regulations, as happened with during this administration with the CFPB.

2. **Do you think state law experimentation with data privacy legislation might discover new and more effective ways to protect our personal information?**

Answer: Yes, absolutely. Currently many of the effective developments in privacy law have come from the states, from the CCPA to the Illinois Biometric Information Privacy Act, to the recent efforts in Washington State which, while unsuccessful last year, look likely to be reintroduced next year.

3. **Would a federal data privacy law that broadly preempts state law run the risk of stifling important innovations for protecting the privacy of personal information?**

The Electronic Communications Privacy Act of 1986, a federal law, allows any law enforcement agency to obtain any email that is older than 180 days, from any internet service provider, without a warrant, simply because in 1986 email was new, and everyone thought of it in an analogous manner to physical mail: i.e, if it was old, it was unimportant and unwanted.

Of course, this has not turned out to be accurate, but despite the obvious privacy implications of allowing citizens' communications to be freely available to law enforcement without a warrant, the law has still not been changed. In 2016 and 2017, a bill to amend this egregious government power has passed on a voice vote out of the House, but each time has stalled in the Senate.

The fact of the matter is, it is incredibly difficult to get any legislation passed through Congress, and even if a privacy law were passed in 2019 or 2020, the thought that such a law might sit like a blanket on the area of privacy legislation, with obvious errors, for the next thirty-three years, is concerning.

Privacy is just another name for an area where many companies are growing and experimenting in new and important ways, and regulations must keep up with this rapidly-changing area of business and law. We cannot rely on the federal government to be able to react appropriately to new developments, given its history of being unable to amend something even so seemingly obvious as a federal law allowing unlimited, warrantless access to citizens' communications.

4. In 2008, my home state of Illinois passed the Biometric Information Privacy Act. This law regulates the commercial use of facial, voice, finger, and iris scans to make sure that companies do not scan and use biometric data without getting users' consent. It has been described by *The New York Times* as "one of the nation's toughest regulations for how companies like Facebook and Google can use facial recognition technologies to identify you online."

   This law creates a right of action allowing individuals to sue technology companies for collecting their biometric information without informed consent. Tech companies like Facebook have tried to weaken this law and have challenged it in court, but a few weeks ago the Illinois Supreme Court upheld the law unanimously.

   Some stakeholders argue that a new federal data privacy law should preempt state laws, presumably including the Illinois Biometric Information Privacy Act. Do you believe that laws like this should be preempted by a federal data privacy law?

Answer: absolutely not. I believe that states should have the right to pursue legislative remedies to problems affecting their own citizenry, reflecting the concerns and priorities of their own citizens.

More to the point, as you correctly point out, many important examples of federal privacy legislation already allow states to chart their own course: Both HIPAA and GLBA, respectively federal health and financial services privacy laws, are "floors, not ceilings." I.E., they put in place minimum national standards, but allow states to pass laws that are more privacy-protective, and in the case of California, it has done just that.

The technology industry has expressed very loudly, this past year, that technology is 'different,' and that a federal law must preempt state laws, so that all the wonderful aspects of the internet can be preserved. My response to that is, last time I checked, both banks and hospitals continued to operate in California, and the idea that state laws might differ

between states, is not to my mind either unusual or out of the ordinary in our federal republic.

As a businessperson, I can point to many laws, from minimum wage, to opening hours, to building codes, to employment licensing, that are state-based, and commerce has not suffered as a result. I find the tech argument disingenuous: it's not like every state would pass a new privacy law every few months, and in fact many will follow the lead of the bigger states. Companies will be able to comply with various state laws, just as retailers manages to collect not just state sales taxes, but all the way down to county and city sales taxes.

The example of data breach is a good one: the federal government was unable to act, so now we have 50 different state laws on the books—and again, last I checked, Amazon was delivering goods in all 50 states, and Google was available to answer questions to all Americans, no matter which state they were searching from.

I do not believe there is a justification for preemption, given that I do not believe that having different privacy laws is a restraint of trade in any sense. I think certainly, it would be more convenient for businesses to have one law, but equally, 'convenience for business' should not, in my view, outweigh important consumer privacy rights for the country's citizens.

Now, as an American, I understand the benefits of a federal system, and would of course support a great federal privacy law. But my thought is that that federal law should be a floor not a ceiling; and that it should allow for state, large county, and large-city enforcement (for the sake of argument, any city or county in the country that has a population greater than the lowest-population state).

Finally it must include the CCPA's fundamentally important rights: of access to your information, of control over it (not allowing it to be sold); of simplicity (allowing one button on any page that collects your information, to be the opt-out—or allowing a third party to do your opting out for you, so that you achieve Do Not Track through legislation); of deletion; and of protecting your information by keeping it secure.

Questions for the Record for Alastair Mactaggart
From Senator Mazie K. Hirono

1. During the hearing, I mentioned that there is significant evidence that a consumer's privacy settings are "sticky," with consumer's rarely altering their default privacy settings.

   Do you agree that the vast majority of consumers rarely change their default privacy settings?

Answer: I totally agree with this statement. In my experience, most consumers think of privacy as almost an abstraction, i.e. they would like to improve their privacy, but they know from experience that it is so difficult and perplexing to do anything about it, that they have learned it's not worth trying.

*It's not that they don't want to: it's that they know that even if they do spend the time to find the one page that might address the issue, they won't be able to do anything meaningful—or worse, they won't understand what the company actually does (I am someone who probably knows more about this subject than the average consumer, and even *I* often cannot understand, after reviewing a privacy policy, whether a company is or is not selling my information).*

Just think of the different mobile phone companies' approaches with respect to sharing privacy location with apps: in the iPhone ecosystem, a consumer has three options: Always, Never, or While Using the App.

In Android, it is either "Always" or "Never." Since you inevitably need to use maps (perhaps for your job), you will inevitably default to putting the setting on "Always," which means Google knows where you are once every minute or so.

The point is, consumers know not to bother with fiddling with their default privacy settings, since the system is rigged against them.

2. In view of the "sticky" nature of privacy settings, my inclination is to have a system in which, by default, a consumer is considered to have opted out of data collection and a company can only collect that consumer's data if the consumer expressly opts in to data collection. I understand from the hearing that you do not support such an "opt-in" privacy regime.

   Please explain why you do not think an "opt-in" privacy regime is the right approach and how you propose to ensure that each consumer is aware that his or her data is being collected and that the consumer consents to that collection.

Answer: My difficulty with the "opt-in" approach is based on its architecture, which I think can give a consumer a false sense of control.

Put simply, once a business has gotten a consumer to opt-in to the collection of their data, it is business as usual (for the business). In other words, opt-in is a temporary roadblock. If you

want to use Google, or Uber, or Amazon, and the business says "we need you to opt-in in order for you to use our services"—well, the vast majority of consumers will simply click "accept."

Opt-in without a consequence is not meaningful, and it's very difficult to have a consequence because, in fact, in many cases the businesses do need to collect consumers' personal information—and importantly, consumers' sensitive information—to function properly.

Google works better if it understands that I mean a California law when I type in AB ##, vs some other state's. Uber needs to know my billing address, my credit card number, and my exact geolocation, in order to work. Evite may well know my religion, if I've invited everyone to my son's bar mitzvah.

Contrast that with 'opt-out of the sale of your personal information.' This seemed, and seems to me still, to be a better tool to give consumers. It says to a consumer, yes, you can use this or that service, but also you can tell them not to sell your information. It gives the consumer choice, which feels more American, but I would argue it also gives them more actual power to do something about their privacy, than even GDPR, which often simply results in a consumer's knowing that the business is collecting their data—which they knew anyway.

Finally, CCPA's approach is very powerful in that it allows for consumers to have an agent opt-out of the sale of their information, on their behalf. What this will mean in practice, is that browser manufacturers and other companies will create global settings allowing a consumer to "set it and forget it," i.e. to select a "do not sell my information" setting, which will then be communicated to all apps on the consumer's device, and all websites the consumer visits.

We think this is among the most impactful aspects of CCPA, in that it will be simple for consumers to use, and because of that, far reaching for their privacy.

Therefore I feel that CCPA arrives at the right point: it allows consumers the ability to find out what businesses are doing with respect to their data; and it gives them the right to opt out of the sale of that information. This choice-based model will allow for consumers to know more about which businesses they do business with.

I understand that during negotiations of the California Consumer Privacy Act, or CCPA, you demanded that a private right of action be included in the law. The private right of action ultimately included in the bill, which permits consumer lawsuits only in the case of a traditional data breach, is far narrower than what you included in your initial referendum.

a. Why, in your view, was it important for the CCPA to include a private right of action?

Answer: I like where the private right of action ("PRA") landed in CCPA because it is aimed at a very defined and concrete harm: the practice of businesses collecting your intimate, personal information, and then not bothering to keep it safe.

Data breach is an area well-suited to a PRA, as it is easily defined, and as there are existing laws on the books (now, in all 50 states) that require companies that have had a data breach, to

inform regulators and consumers. CCPA simply says, did the business take reasonable steps to keep consumers' information secure and safe? Was it encrypted? Was it redacted? If the business took any of those actions, (which are all minimum standard acceptable operating practice if the business is collecting consumers' personal information), then the PRA is not applicable.

Again, the PRA is an example of the law's balanced approach: I didn't want to create a threshold that was focused solely on whether or not a data breach happened, in case for example the North Korean government decided to hack into a well-meaning company's data. That might have been unfair to a company that was doing its best to comply with CCPA.

If, however, the business was not taking reasonable steps to protect consumer personal information, then I thought it was appropriate to allow for a PRA, as those cases seemed to be of the more egregious type, and I thought the prospect of a PRA in these instances, would spur companies to encrypt or redact any personal information they had collected.

There are currently proposals in California to expand the CCPA's private right of action to include all violations of the law. Do you agree that an expanded private right of action would better protect the privacy of Californians?

Answer: I was totally satisfied with the compromise I struck with the California Legislature when CCPA passed, and I am still satisfied. I think the existing PRA addresses an area of privacy that many consumers care about very deeply, i.e. the scourge of identity theft, and I think the Attorney General enforcement is adequate for the balance of the Act.

I think the fines in the law with respect to enforcement by the California Attorney General, are potentially extremely high, and will provide the AG's office with sufficient leverage to effectively regulate the rest of the practices covered by the CCPA.

The fines for intentionally ignoring CCPA's provisions are potentially extraordinarily large, and could dwarf the celebrated "4% of turnover" figure in the European GDPR that has generated so much press.

Writing as a businessperson, I believe the prospect of the might of the largest state in the union, pursuing a business, is enough to focus the attention of all businesses on complying with the law.

Industry groups have called for federal privacy legislation that preempts state law.

Do you think that federal preemption is appropriate? If you do, what minimum requirements do you think federal legislation should include before preempting state law?

Answer: I do not believe that federal preemption is appropriate for privacy. I believe that states should have the right to pursue legislative remedies to problems affecting their own citizenry, reflecting the concerns and priorities of their own citizens.

More to the point, as you correctly point out, many important examples of federal privacy legislation already allow states to chart their own course: Both HIPAA and GLBA, respectively federal health and financial services privacy laws, are "floors, not ceilings."

I.E., they put in place minimum national standards, but allow states to pass laws that are more privacy-protective, and in the case of California, it has done just that.

The technology industry has expressed very loudly, this past year, that technology is 'different,' and that a federal law must preempt state laws, so that all the wonderful aspects of the internet can be preserved. My response to that is, last time I checked, both banks and hospitals continued to operate in California, and the idea that state laws might differ between states, is not to my mind either unusual or out of the ordinary in our federal republic.

As a businessperson, I can point to many laws, from minimum wage, to opening hours, to building codes, to employment licensing, that are state-based, and commerce has not suffered as a result. I find the tech argument disingenuous: it's not like every state would pass a new privacy law every few months, and in fact many will follow the lead of the bigger states. Companies will be able to comply with various state laws, just as retailers manages to collect not just state sales taxes, but all the way down to county and city sales taxes.

The example of data breach is a good one: the federal government was unable to act, so now we have 50 different state laws on the books—and again, last I checked, Amazon was delivering goods in all 50 states, and Google was available to answer questions to all Americans, no matter which state they were searching from.

I do not believe there is a justification for preemption, given that I do not believe that having different privacy laws is a restraint of trade in any sense. I think certainly, it would be more convenient for businesses to have one law, but equally, 'convenience for business' should not, in my view, outweigh important consumer privacy rights for the country's citizens.

Now, as an American, I understand the benefits of a federal system, and would of course support a great federal privacy law. But my thought is that that federal law should be a floor not a ceiling; and that it should allow for state, large county, and large-city enforcement (for the sake of argument, any city or county in the country that has a population greater than the lowest-population state).

Finally it must include the CCPA's fundamentally important rights: of access to your information, of control over it (not allowing it to be sold); of simplicity (allowing one button on any page that collects your information, to be the opt-out—or allowing a third party to do your opting out for you, so that you achieve Do Not Track through legislation); of deletion; and of protecting your information by keeping it secure.

Alastair Mactaggart
Chairman
Californians for Consumer Privacy
Questions for the Record
Submitted March 19, 2019

QUESTIONS FROM SENATOR BOOKER

1. Marginalized communities, and specifically communities of color, face a disproportionate degree of surveillance and privacy abuses. This has been the case since the Lantern Laws in eighteenth-century New York City (requiring African Americans to carry candle lanterns with them if they walked unaccompanied in the city after sunset) up through the stop-and-frisk initiatives of more recent years.

   There are echoes of this tradition today in the digital realm as marginalized communities suffer real harm from digital discrimination. For example, in recent years we have seen many instances of housing discrimination and digital redlining, employment discrimination through digital profiling and targeted advertising, exploitation of low tech literacy through misleading notice and choice practices, discriminatory government surveillance and policing practices, and voter suppression and misinformation targeting African Americans and other minorities.

   I am concerned that—rather than eliminating the bias from our society—data collection, machine learning, and data sharing may actually augment many of the kinds of abuses we fought so hard to eliminate in the Civil Rights Movement. We need privacy legislation that is centered around civil rights.

   a. In your view, is a private right of action critical to protecting the civil rights of individuals affected by data collection and disclosure practices?

Answer: I do not believe so. I was totally satisfied with the compromise I struck with the California Legislature when CCPA passed, and I am still satisfied. I think the existing PRA addresses an area of privacy that many consumers care about very deeply, i.e. the scourge of identity theft, and I think the Attorney General enforcement is adequate for the balance of the Act.

CCPA has many provisions which address the important civil rights ramifications referred to in the questions. Most importantly, by giving consumers the ability to uncover what information companies are collecting about them, to find out where that information is being sold, and by giving them the right to require that information's deletion, CCPA will provide consumers the ability to see and manage their information landscape clearly, for the first time. Is a website nominally aimed at informing consumers about their health, in fact selling their search information to health insurers? Are consumers being tracked and categorized by how often they visit a fast-food establishment? How about whether their race is being inferred from their music playlists—and whether that information is being sold?

I believe the fines in the law with respect to enforcement by the California Attorney General, will provide the AG's office with sufficient leverage to effectively regulate the rest of the practices covered by the CCPA.

The fines for intentionally ignoring CCPA's provisions are potentially extraordinarily large, and could dwarf the celebrated "4% of turnover" figure in the European GDPR that has generated so much press.

Writing as a businessperson, I believe the prospect of the might of the largest state in the union, pursuing a business, is enough to focus the attention of all businesses on complying with the law.

2.

a. How easy is it for seemingly non-sensitive information like a ZIP Code to become a proxy for protected class or other sensitive information? How can that information be used to discriminate?

Answer: this is a great question, and the answer is: very (easy). Please see the attached articles about very successful efforts to identify such sensitive information as sexual orientation from nothing more than five low-resolution images of a consumer's face; or the ability to forecast a consumer's responses to a well-known personality quiz, more accurately than the consumer's spouse, with access to a mere 300 of the consumer's likes from Facebook.

Playlists reveal race, sexual orientation, age; your car can infer you have a drug problem long before any other person in your life.

This is one of the best questions to ask, so thank you. Stay focused on this, because as companies know everything about you, the power they obtain over you grows immensely.

b. Significant amounts of data about us are gathered by companies most people have never heard of. Do we need a registry of data brokers, similar to what Vermont established last year?

Answer: in a word, yes. This is an extremely good idea, and a similar law has been proposed this year in California by one of the CCPA co-authors, Assemblymember Ed Chau, and I am hopeful it passes.

3. The tech journalist Kashmir Hill recently wrote a widely circulated article on her efforts to leave behind the "big five" tech companies—Facebook, Google, Apple, Microsoft, and Amazon. Using a VPN, she blocked all of the IP addresses associated with each company and then chronicled how her life changed. She experimented first by blocking individual companies, and then, at the end of the series, she blocked all five at once. Ms. Hill found that—to varying degrees—she could not get away. Repeatedly, her efforts to intentionally block one company created unpredictable ripple effects for engaging with other, seemingly unrelated, companies and services. Ms. Hill's article spoke to how pervasive these companies

are and how much data they capture about us when we're not even (knowingly) using their services.[1]

a. How would you respond to the following argument? "If people are uncomfortable with the data practices of certain tech companies, they simply shouldn't use their services."

Answer: I would respond like this (which is just one of the many similar scenarios I could construct):

1) *Try living in America without a job*
2) *Try getting a job without having a mobile phone.*
3) *Your mobile phone company shares your location history; how fast you drive; how often you eat at a fast food restaurant, etc.*
4) *Try holding down the job without a car (for the many who don't live in a city center with adequate commuting options). Your car knows everything about you, and either the car manufacturer, or the satellite radio company, or the emergency locator service, or the leasing company, will be tracking your location, and have the right to sell that information.*
5) *If you can only afford an Android phone, your privacy choices (with respect to apps) for Location Sharing are limited to "Always" or "Never." Since you inevitably need to use maps (perhaps for your job), you will inevitably default to putting the setting on "Always," which means Google knows where you are once every minute or so.*
6) *It goes on and on. Basically, if you want to live in 2019 and hold down a job and keep your kids in school, your information is collected and sold or shared.*
7) *CCPA aims to change this.*

b. What does providing consent mean in a world where it's extremely difficult to avoid certain companies?

Answer: I think consent, for me, refers to what can be done with my information.

The reality is that more and more of our lives are measured and tracked by more and more companies, and even though the resultant profiles that a few giant companies obtain about us are incredibly detailed, opting-in to every data interaction, every day, will present roadblocks to consumers and businesses alike.

Transparency is essential to giving a consumer the necessary information to choose who to do business with. With respect to consent, however, while equally important, I think the opt-in model misses the mark. For me, consent is more about what happens to my data, and how it is used, and less about whether it's collected by a company in the first place.

My difficulty with the "opt-in" approach is based on its architecture, which I think can give a consumer a false sense of control.

Put simply, once a business has gotten a consumer to opt-in to the collection of their data, it is business as usual (for the business). In other words, opt-in is a temporary roadblock. If you want to use Google, or Uber, or Amazon, and the business says "we need you to opt-in in order

for you to use our services"—well, the vast majority of consumers will simply click "accept."

Opt-in without a consequence is not meaningful, and it's very difficult to have a consequence because, in fact, in many cases the businesses do need to collect consumers' personal information—and importantly, consumers' sensitive information—to function properly.

Google works better if it understands that I mean a California law when I type in AB ##, vs some other state's. Uber needs to know my billing address, my credit card number, and my exact geolocation, in order to work. Evite may well know my religion, if I've invited everyone to my son's bar mitzvah.

Contrast that with 'opt-out of the sale of your personal information.' This seemed, and seems to me still, to be a better tool to give consumers. It says to a consumer, yes, you can use this or that service, but also you can tell them not to sell your information. It gives the consumer choice, which feels more American, but I would argue it also gives them more actual power to do something about their privacy, than even GDPR, which often simply results in a consumer's knowing that the business is collecting their data—which they knew anyway.

Finally, CCPA's approach is very powerful in that it allows for consumers to have an agent opt-out of the sale of their information, on their behalf. What this will mean in practice, is that browser manufacturers and other companies will create global settings allowing a consumer to "set it and forget it," i.e. to select a "do not sell my information" setting, which will then be communicated to all apps on the consumer's device, and all websites the consumer visits.

We think this is among the most impactful aspects of CCPA, in that it will be simple for consumers to use, and because of that, far reaching for their privacy.

Therefore I feel that CCPA arrives at the right point: it allows consumers the ability to find out what businesses are doing with respect to their data; and it gives them the right to opt out of the sale of that information. This choice-based model will allow for consumers to know more about which businesses they do business with.

4. It would take each of us an estimated 76 working days to read all the digital privacy policies we agree to in a single year.[2] Most people do not have that much time. They might prefer something simple, easy, and clear—something much like the Do-Not-Track option that has been featured in most web browsers for years.

   However, there is a consensus that Do-Not-Track has not worked, because despite the involvement and engagement of stakeholders across the industry, only a handful of sites actually respect the request. A 2018 study showed that a quarter of all adult Americans were using Do-Not-Track to protect their own privacy—and yet 77 percent of Americans were unaware that Google, Facebook, and Twitter don't respect Do-Not-Track requests.[3] Just last month, Apple removed the feature from its Safari browser because, ironically, Do-Not-Track was being used for browser fingerprinting, i.e., having the feature turned on was used to distinguish individual users and track them across the web.[4]

a. What purpose does a notice-and-consent regime serve if the most prominent consent mechanism is only regarded as a suggestion at best?

Answer: please see my response to 3 b) above. CCPA gives consumers actual, legal rights to have tremendous control over their own personal information.

b. How much faith should the failure of Do-Not-Track give us in the ability of the industry stakeholders to regulate themselves?

Answer: it is precisely the failure of Do Not Track which led to CCPA. If there had been an effective, easy way for me to opt out of having my data collected and sold, I would never have undertaken the journey which ended in CCPA.

I am a businessperson, through and through. Yet, sadly, not all businesses do the right thing on their own, all the time. So we need safety laws for buildings and elevators and factories; food cleanliness laws for processing plants; labeling laws for food manufacturers, lemon laws for car dealers.

It was clear to me that absent a legal mandate, the tech industry would never self-regulate with respect to using and monetizing consumers' personal information. It is too valuable.

c. In your view, should this approach be abandoned, or would federal legislation requiring companies to respect the Do-Not-Track signal breathe new life into the mechanism?

5. Given that California has enacted its own privacy legislation that will take effect next year, much of the discussion at the hearing centered on how a federal data privacy law will affect state-level efforts to regulate in the same space. However, most of our existing privacy

---

[1] Kashmir Hill, *I Cut the 'Big Five' Tech Giants from My Life. It Was Hell*, GIZMODO (Feb. 7, 2019), https://gizmodo.com/i-cut-the-big-five-tech-giants-from-my-life-it-was-hel-1831304194.

[2] Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, ATLANTIC (Mar. 1, 2012), https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851.

[3] *The "Do Not Track" Setting Doesn't Stop You from Being Tracked*, DUCKDUCKGO BLOG (Feb. 5, 2018), https://spreadprivacy.com/do-not-track.

[4] Ahiza Garcia, *What Apple Killing Its Do Not Track Feature Means for Online Privacy*, CNN (Feb. 13, 2019), https://www.cnn.com/2019/02/13/tech/apple-do-not-track-feature/index html.

statutes do not include provisions to overrule stricter protections under state law.[5] These preemption provisions are the exception rather than the rule, and became more prevalent starting in the 1990s in statutes like the Children's Online Privacy Protection Act of 1998, the CAN-SPAM Act of 2003, and the 1996 and 2003 updates to the Fair Credit Reporting Act.

a. In your view, should a federal data privacy law preempt state data privacy laws? Why?

Answer: absolutely not. I believe that states should have the right to pursue legislative remedies to problems affecting their own citizenry, reflecting the concerns and priorities of their own citizens.

More to the point, as you correctly point out, many important examples of federal privacy legislation already allow states to chart their own course: Both HIPAA and GLBA, respectively federal health and financial services privacy laws, are "floors, not ceilings." I.E., they put in place minimum national standards, but allow states to pass laws that are more privacy-protective, and in the case of California, it has done just that.

The technology industry has expressed very loudly, this past year, that technology is 'different,' and that a federal law must preempt state laws, so that all the wonderful aspects of the internet can be preserved. My response to that is, last time I checked, both banks and hospitals continued to operate in California, and the idea that state laws might differ between states, is not to my mind either unusual or out of the ordinary in our federal republic.

As a businessperson, I can point to many laws, from minimum wage, to opening hours, to building codes, to employment licensing, that are state-based, and commerce has not suffered as a result. I find the tech argument disingenuous: it's not like every state would pass a new privacy law every few months, and in fact many will follow the lead of the bigger states. Companies will be able to comply with various state laws, just as retailers manages to collect not just state sales taxes, but all the way down to county and city sales taxes.

The example of data breach is a good one: the federal government was unable to act, so now we have 50 different state laws on the books—and again, last I checked, Amazon was delivering goods in all 50 states, and Google was available to answer questions to all Americans, no matter which state they were searching from.

b. In your view, should a federal data privacy law implement the requirements of the California Consumer Privacy Act as a floor? If not, please explain the most significant change you would suggest.

Answer: yes. There are however some additional areas that I did not include in the original provision, that I wish I had, including:

1) *Biometric recognition (my strong belief is this should be opt-in, not opt-out. The technology is so intrusive, and so primed for discriminatory use, that we the people should have the right to consent, before it's used on us. Plus, the chance for misuse and discrimination is extraordinarily high).*

2) *The "Honest Ads" concept: we should be able to tell who has paid for an ad on the internet which is being shown to us based on our personal information.*
3) *Deep fakes: this technology is so disturbing, and so potentially destabilizing to a democracy, that limits must be put on its use. If voters can see politicians uttering terrible lies, but can't tell the difference between the truth and a fake, this is utterly terrifying for our country. (Or, choose any other hundred examples, including revenge pornography against women, etc).*

c. The specific wording of a proposed preemption provision will invite considerable debate in Congress and, ultimately, will still require courts to interpret and clarify the provision's scope. Should the Federal Trade Commission have notice-and-comment rulemaking authority to aid in the statute's interpretation and to clarify which types of state laws are preempted? Or, alternatively, is case-by-case adjudication of multiple state privacy laws preferable? Would rulemaking authority obviate the need for Congress to solve each and every preemption issue in drafting the text?

Answer: I believe that any federal legislation should give the FTC rulemaking authority, which would (or should, depending on the authority) go a long way to solving every preemption fight that might come up.

However, in repeating my plea for no preemption, consider that the Electronic Communications Privacy Act of 1986, a federal law, allows any law enforcement agency to obtain any email that is older than 180 days, from any internet service provider, without a warrant. This was because in 1986 email was new, and everyone thought of it in an analogous manner to physical mail: i.e, if it was old, it was unimportant and unwanted.

Of course, this has not turned out to be accurate, but despite the obvious privacy implications of allowing citizens' communications to be freely available to law enforcement without a warrant, the law has still not been changed. In 2016 and 2017, a bill to amend this egregious government power has passed on a voice vote out of the House, but each time has stalled in the Senate.

The fact of the matter is, it is incredibly difficult to get any legislation passed through Congress, and even if a privacy law were passed in 2019 or 2020, the thought that such a law might sit like a blanket on the area of privacy legislation, with obvious errors, for the next thirty-three years, is concerning.

Privacy is just another name for an area where many companies are growing and experimenting in new and important ways, and regulations must keep up with this rapidly-changing area of business and law. We cannot rely on the federal government to be able to react appropriately to new developments, given its history of being unable to amend something even so seemingly obvious as a federal law allowing unlimited, warrantless access to citizens' communications.

d. The preemption language in, for example, the amendments to the Fair Credit Reporting Act was included as part of a heavily negotiated process in which consumers received a

package of new rights in exchange for certain preemption provisions.[6] Rather than centering the federal privacy bill debate on the existence of a preemption provision, shouldn't our starting point be: "Preemption in exchange for what?" In other words, what basic consumer protections should industry stakeholders be willing to provide in exchange for preemption? Do the requirements of the California Consumer Privacy Act represent a good floor for negotiating preemption?

Answer: please see my response to 5 a). I do not believe there is a justification for preemption, given that I do not believe that having different privacy laws is a restraint of trade in any sense. I think certainly, it would be more convenient for businesses to have one law, but equally, 'convenience for business' should not, in my view, outweigh important consumer privacy rights for the country's citizens.

Now, as an American, I understand the benefits of a federal system, and would of course support a great federal privacy law. But my thought is that that federal law should be a floor not a ceiling; and that it should allow for state, large county, and large-city enforcement (for the sake of argument, any city or county in the country that has a population greater than the lowest-population state).

Finally it must include the CCPA's fundamentally important rights: of access to your information, of control over it (not allowing it to be sold); of simplicity (allowing one button on any page that collects your information, to be the opt-out—or allowing a third party to do your opting out for you, so that you achieve Do Not Track through legislation); of deletion; and of protecting your information by keeping it secure.

6. At the hearing, several witnesses indicated that opt-out requirements that permit users to tell companies not to process and sell their data are more protective of data privacy and more conducive to the user experience, since they do not impose the "take it or leave it" dynamic that opt-ins tend to create. In your view, are opt-outs preferable to opt-ins in terms of both data privacy and user experience? Why?

Answer: please see my reply to 3 b) above. I agree totally that opt-out is preferable to opt-in (i.e. the GDPR-esque opt-in before the business can collect your information), precisely because of the take-it-or-leave-it consequence to opt-in.

7. At the hearing, several witnesses also indicated that the Federal Trade Commission, and perhaps state attorneys general, should have primary enforcement authority for data privacy violations. In your view, what additional authority and/or resources would the FTC need to perform this function effectively?

Answer: as stated above in my response to 5)d), I believe any federal law should allow for state, large county, and large-city enforcement (for the sake of argument, any city or county in the country that has a population greater than the lowest-population state).

In a resource-constrained world, more regulatory resources brought to bear on the issue of privacy, will be more effective than less. It is well-documented that the FTC has approximately 40 privacy professionals to deal with the largest developed economy in the world with over 300 million consumers, whereas much smaller countries have staff an order of magnitude larger. There seems

to me low possibility that the federal government could provide the same resources as the 50 states, especially when considering smaller cases that might interest only a certain geographic area (consider a data breach case at a company with regional operations).

Add to this, that states' efforts will likely be led by elected politicians eager to fight to protect their citizens' privacy. There are many areas where state and local regulatory efforts are more effective and proactive than the federal government. One just has to think of recent history with the opioid-abuse epidemic to realize that often the states can move more quickly and effectively than the federal government, which so often depends on a particular administration's approach. Having 50 states able to regulate privacy, will prevent developments that weaken regulations, as happened with during this administration with the CFPB.

If the FTC were to become the sole national regulator, it would be necessary to vastly increase the numbers of its privacy enforcement staff, and I believe that would be politically untenable—which is another reason why I don't support federal preemption. Just from watching Congress over the past few years, I believe it would be incredibly difficult to get the resources allocated to the FTC, that would be necessary to meaningfully enforce such a law. They would need literally hundreds of additional attorneys on staff, as well as comprehensive rule-writing authority, and it does not appear to me that such a scenario is a likely outcome.

---

[5] The following statutes do not preempt stricter protections under state law: the Electronic Communications Privacy Act, the Right to Financial Privacy Act, the Cable Communications Privacy Act, the Video Privacy Protection Act, the Employee Polygraph Protection Act, the Telephone Consumer Protection Act, the Drivers' License Privacy Protection Act, and the Telemarketing Consumer Protection and Fraud Prevention Act.

[6] The 1996 and 2003 amendments included, for example: new obligations on businesses to ensure the accuracy of reports, increased civil and criminal penalties, remedial rights for identity theft victims, and the right to free annual credit reports.

Post-Hearing Questions for the Record
Submitted to Mr. Alastair Mactaggart
from Senator Kamala Harris

"The General Data Protection Regulation (GDPR) & the California Consumer Privacy Act (CCPA): Opt-ins, Consumer Control, and the Impact on Competition and Innovation"
Senate Judiciary Committee
March 11, 2019

Private Right of Action in the Event of a Data Breach

You testified that the CCPA was organized around three central pillars: transparency, control, and accountability. In your view, the ability to hold companies accountable for failing to adequately protect consumer data is a critical part of advancing data security.

Although you testified that the CCPA secured important rights for consumers and that you are pleased with the law, you conceded that the bill as enacted contains a private right of action that is more limited than originally intended.

1. **Does Californians for Consumer Privacy support building upon the consumer protections in the CCPA by expanding the private right of action to cover other violations of the Act?**

Answer: I was totally satisfied with the compromise I struck with the California Legislature when CCPA passed, and I am still satisfied. I think the existing PRA addresses an area of privacy that many consumers care about very deeply, i.e. the scourge of identity theft, and I think the Attorney General enforcement is adequate for the balance of the Act.

I think the fines in the law with respect to enforcement by the California Attorney General, are potentially extremely high, and will provide the AG's office with sufficient leverage to effectively regulate the rest of the practices covered by the CCPA.

When I was asked to support recent efforts to reintroduce a private right of action into CCPA, covering the entire law, my response was that it would be unfair of me to support the reopening of one of the key compromises that allowed the law to pass in June of 2018, less than a year after its passage. I stated that if the tables were turned, and the tech lobby was now trying for example to remove the right of consumers to request their actual data, I would try to move heaven and earth to keep that right.

I suppose that fundamentally, I feel that I was part of a deal was in June 2018. In a few years, if it turns out that many businesses are willfully ignoring CCPA because they don't believe that the AG will be able to enforce the law, then it will be appropriate to revisit this issue, and the legislature will have ample reason to do so, and I will be a big proponent of that effort.

However, I believe the current fines in the law with respect to enforcement by the California Attorney General, will provide the AG's office with sufficient leverage to effectively regulate the rest of the practices covered by the CCPA

The fines for intentionally ignoring CCPA's provisions are potentially extraordinarily large, and could dwarf the celebrated "4% of turnover" figure in the European GDPR that has generated so much press.

Writing as a businessperson, I believe the prospect of the might of the largest state in the union, pursuing a business, is enough to focus the attention of all businesses on complying with the law.

2. **Do you believe that federal data protection legislation should include a private right of action for consumers whose private information is misused by a company or compromised in a data breach?**

Answer: absolutely, 100%. I believe it would be unconscionable for Congress to pass a law that didn't include this right, which is foundational to CCPA. If a federal law did not include such a private right, then by definition it would be weaker in an area that directly contributes to identity theft, which is one of the most hot-button issues with consumers (at least according to our polling).

Interestingly, the tech industry has not complained much about this aspect of the law, because it reflects a balanced approach, and because data breach is an area well-suited to a PRA, as it is easily defined, and as there are existing laws on the books (now, in all 50 states) that require companies that have had a data breach, to inform regulators and consumers.

CCPA simply says, did the business take reasonable steps to keep consumers' information secure and safe? Was it encrypted? Was it redacted? If the business took any of those actions, (which are all minimum standard acceptable operating practice if the business is collecting consumers' personal information), then the PRA is not applicable.

Again, the PRA is an example of the law's balanced approach: I didn't want to create a threshold that was focused solely on whether or not a data breach happened, in case for example the North Korean government decided to hack into a well-meaning company's data. That might have been unfair to a company that was doing its best to comply with CCPA.

If, however, the business was not taking reasonable steps to protect consumer personal information, then I thought it was appropriate to allow for a PRA, as those cases seemed to be of the more egregious type, and I thought the prospect of a PRA in these instances, would spur companies to encrypt or redact any personal information they had collected.