Responses of Will DeVries, Senior Privacy Counsel, Google LLC
Hearing on "GDPR and CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation"
Senate Judiciary Committee
April 3, 2019

Written Answers to Questions Submitted by Chairman Graham to Will DeVries

1. **What was your estimated initial cost (both time and expense) to become GDPR compliant?**

   We estimate it cost us hundreds of years worth of person-hours and a great deal higher than millions of dollars to develop and enact our GDPR reforms.

2. **What are your estimated recurring annual GDPR compliance costs (both time and expense)?**

   Even though Google did not start from scratch — far from it — both initial and annual GDPR compliance continues to be an enormous investment of time and resources for us. Because our work is built into our infrastructure, an estimated cost is difficult to quantify, but certainly it involves the time of hundreds of employees and many millions of dollars as referenced above.

3. **What is your estimated initial costs (both time and expense) to become CCPA compliant?**

   We are unable to provide an accurate estimate at this time, in part because the regulations required by the law have not yet been promulgated. Nevertheless, we anticipate that, because of the differences between CCPA and GDPR, we will have to invest considerable time and resources to meet the specific obligations of the CCPA.

4. **What are your estimated recurring annual CCPA compliance costs (both time and expense)?**

   As CCPA has not yet gone into effect, we cannot quantify recurring compliance costs at this time.

5. **Are you differentiating your products based on consumers or businesses in the EU and California?**

Our commitment to providing users with transparency and control over their privacy extends across Google's products and is built into the services we offer around the world. Google users around the world have access to this same set of privacy tools that European and US residents enjoy today, including Google Account and Download Your Data (our data portability tool). For example, last year as part of our GDPR compliance efforts we updated our global privacy policy to make it easier for all users to understand what information we collect and why we collect it and also improved both the controls and the information in the privacy tools we offer to users around the world.

That said, the GDPR is a European law and some aspects of it are specific to the EU. For example, the so-called "right to be forgotten" may come into friction with the American tradition of free speech codified in the First Amendment, and in light of that we have limited our search index de-listing approach to Europe.

6. **Part of the hearing focused on the contrast between contextual advertising versus behavioral. How much would Google be impacted financially if behavioral advertising were made illegal? What would be the non-financial impact?**

Contextual signals (rather than personalization or behavioral advertising) drive the majority of Google's advertising revenue. In general, however, personalized advertising helps sustain a flourishing and diverse ecosystem of quality, independent content. Google itself often has strong contextual signals that can help it identify useful and relevant ads for individuals; someone searching for "best washing machines," for example, is a strong candidate for a washing machine advertisement. Many smaller publishers, in contrast, lack such signals, and depend on revenue from personalized ads to support their businesses.

We take seriously our role in supporting an independent web, and we are committed to sustaining a healthy advertising ecosystem that supports individuals' choices. That is why we have built robust controls over personalized advertising, including controls that allow individuals to disable it entirely. While we are proud of what we have built, as with our overall approach to privacy, we are constantly striving to do better. We regularly engage in consumer research and meet with regulators to ensure our practices are in line with user expectations.

7. **Under GDPR, a "controller" determines how and why data is processed while a "processor" does the actual processing on the controllers behalf. Each designation has different requirements as to how it handles the personal data of consumers. Google has various subsidiaries in the ad tech and data collection marketplace.**

    a. **Are there different Google products for which Google is a processor and others that Google is a controller?**

b. If there are differentiations, can you please list each product's designation and the basis for that designation?

c. How does this designation impact Google's interactions with third parties that utilize Google products, including obtaining consumer consent?

We answer 7.a through 7.c together.

Google is committed to compliance with GDPR and other regulations and, as part of our efforts to provide more information about our compliance, we have a created public website dedicated to these issues, available at https://privacy.google.com/businesses/compliance/. Under the section titled "Our Commitment to GDPR," you can find information regarding our products and their designation as a processor or controller of data. In addition, there are helpful links about our terms and conditions for certain products, which include requirements regarding user consent.

8. What are the specific areas of the CCPA that could have a negative impact on competition and innovation? What areas of the CCPA need more clarity, improvement, or removal?

We support thoughtful privacy legislation that both protects individuals and encourages businesses to continue innovating.

With regard to the California Consumer Privacy Act (CCPA), we support the goals of the law, including increased transparency and user control, but share the concerns that many have expressed about how the law is drafted and its impacts on businesses and individuals. In particular, we hope that the law can be clarified to make it easier for individuals to understand and exercise their rights, and ensure that companies of all sizes and sectors can comply and continue to offer innovative products and services individuals rely on.

Generally, we believe the CCPA does not go far enough in codifying the rights and obligations included in consensus frameworks such as the Fair Information Practices Principles (FIPPs), OECD Privacy Principles, APEC Privacy Framework, and even Europe's General Data Protection Regulation (GDPR). Our principles for a responsible data framework are based on these frameworks and on our 20 years of experience offering services that depend on information, privacy protections, and user trust. The CCPA's provisions around individual control, non-discrimination, access and deletion requirements, and accountability are examples of where the CCPA can and should be improved.

First, privacy law should apply individual control over data processing wherever it can be reasonably offered, not just in certain categories. The GDPR's flexible and nuanced approach to control is a better model than the CCPA, which includes user control that is ambiguous and limited to "sale" of personal information. The GDPR, in contrast, generally requires some user control over all data processing unless the processing is necessary to provide a service to the user or other specific circumstances apply.

Second, we also urge Congress to carefully think through the issue of under what conditions businesses and organizations may make services contingent on a user's acceptance of some processing of their personal information, sometimes known as non-discrimination. Individuals should not be penalized for exercising their privacy rights, but some choices offered to individuals may affect the ability of a business to earn revenue, and even the financial viability of products and services that are of tremendous benefit to users and to society. Publishers provide an illustrative example. Many newspapers currently offer individuals a choice between free access to quality content supported by personalized advertising and a subscription model that is free of personalized ads. Different approaches can offer individuals a real choice and multiple revenue models to support businesses.

Regulators are currently grappling with this issue across Europe with respect to the GDPR, thinking about how best to reconcile the current funding model of the internet with choices individuals make around those services. The CCPA also tries to grapple with this issue, but does so in a manner that is difficult to interpret or apply. The balance between user control and business operations is critical for Congress to keep in mind as it considers this principle.

Additionally, in drafting access requirements, Congress should be careful to avoid creating privacy or security risks. The CCPA helpfully includes access and deletion requirements, but frequently without sufficient clarity or nuance. For example, it does not establish a clear framework under which competing rights and interests can be evaluated once a user has made an access request, or to enable businesses to ensure that a user requesting information has the right to receive that information. Requests for information associated with frequently-shared identifiers like IP addresses raise a number of substantial privacy concerns. In Google's experience, access to a secured account from which information is being requested has proven the most reliable indicator of a requesting user's identity and their entitlement to receive information associated with the relevant identifier. Absent such a showing, these kinds of requests can be exploited by fraudsters and other malicious actors.

Lastly, in considering accountability, it is important to keep in mind the distinction between consumer services and enterprise services, and the need to clarify obligations based on an organization's ability to meet those obligations. Much of the processing of personal information is done by one company on behalf of another,

Responses of Will DeVries, Senior Privacy Counsel, Google LLC
Hearing on "GDPR and CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation"
Senate Judiciary Committee
April 3, 2019

Written Answers to Questions Submitted by Senator Grassley to Will DeVries

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

Transparency is a core principle at Google, embedded in every product we make. We believe it should be a core principle in federal baseline privacy law.

All businesses and organizations that collect and use personal information should be required to provide notice about the types of personal information they collect, why they collect it, and how they use and/or disclose it, particularly when used to make decisions about the individual. Making this information available is critical to building and maintaining people's trust.

In our experience, privacy policies are important sources of information for individuals and can help hold businesses and organizations accountable. But privacy policies are not in themselves sufficient transparency. Regulators should encourage businesses and organizations to go beyond the privacy policy and actively inform individuals about data use in the context of the services themselves, helping to make the information relevant and actionable for individuals. This recommendation is built on Google's experience with providing transparency about data collection and use, which comes in two key ways: our privacy policy and in-product notices.

While we work to improve the user-friendliness of our privacy policy, based on research and user feedback, we look for ways to add transparency directly in products. For example, Why This Ad[1] enables you to click on an icon in each ad to find out why you are seeing that particular ad and understand more about how Google's system makes these decisions. If you add a Google Drive file to a shared folder, we will include a notice to make sure you intend to share that file with everyone who has access to that folder.

Recently we improved transparency and user control in our flagship product, Search, with a tool that shows our users exactly how their data is being used to improve their

[1] https://support.google.com/ads/answer/1634057?hl=en

search results, along with direct access to controls.[2] We are exploring expansion of this to other products.

Although our privacy policy has been recognized as best in class,[3] we recently updated it[4] to make it easier to understand, with informative videos that explain our practices and settings. We also made our privacy controls immediately accessible from the privacy policy so users can make decisions about their settings as they learn about our practices.

Google was one of the first companies to offer a centralized dashboard[5] in 2009, and today nearly 2 billion people visit Google Account each year. Google Account is home to the Google Security Checkup[6] and Privacy Checkup[7] tools, which help our users identify and control the apps that have access to their Google account data and guide our users to review and manage their security and privacy settings. We regularly and actively prompt our users to do privacy and security reviews by reminding them to use these tools through individual prompts and service-wide promotions. Each year more than 100 million people take a Privacy Checkup and 700 million people take a Security Checkup.

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.[8]**

   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?**

   We answer questions 2.a and 2.b together.

   Google believes in ensuring our users understand how their data is used, and are in control.

[2] https://www.blog.google/technology/safety-security/making-it-easier-control-your-data-directly-google-products/
[3] Time Magazine and the Center for Plain Language ranked Google number one among technology companies for best privacy policy (http://time.com/3986016/google-facebook-twitter-privacy-policies/).
[4] https://policies.google.com/privacy?hl=en-US
[5] Dashboards are a recognized best practice (https://www.ivir.nl/publicaties/download/PrivacyBridgesUserControls2017.pdf)
[6] https://myaccount.google.com/security-checkup
[7] https://myaccount.google.com/privacycheckup?otzr=1
[8] David Reinsel et al., *The Digitization of the World—From Edge to Core*, IDC (Nov. 2018).

We also believe that a privacy law should set a baseline of protections without placing the burden on individuals. Our proposed regulatory framework[9] recommends a requirement for businesses and organizations to operate with respect for individuals' interests when they process personal information. Businesses and organizations must also take responsibility for using data in a way that provides value to individuals and society and minimizes risks to users based on the use of personal information. This means considering individuals' interests, assessing the impact of data use on those interests, and implementing safeguards to protect individuals.

These responsibilities are discussed in the European General Data Protection Regulation (GDPR). The GDPR requires businesses and organizations to incorporate transparency and fairness into their practices, and permits processing that balances the "legitimate interests" of the organization processing the data against the impact of that processing on the rights and interests of the individual. Where processing of personal data satisfies this balancing test and respects privacy principles, it can be processed without specific consent under the GDPR. We believe that US law should similarly encourage businesses and organizations to balance these same interests. Consent might be more appropriate for data uses that involve a high risk to users and might not be well understood based on context.

Though controls are vital, there is a growing consensus amongst regulators, researchers, and companies that asking users to opt-in for all uses of information is impractical and leads to fatigue that diverts attention from the most important choices. For example, some data processing is necessary to make products work, and to ensure they are secure and reliable. Users expect their personal information to be used in this way, and asking them to separately consent presents the odd decision of "agree" or "don't use the service." This could have the perverse effect of teaching users to simply click "agree" to everything without paying attention.

Our privacy framework recommends federal privacy law require businesses and organizations to provide appropriate mechanisms for individual control, including the opportunity to object to data processing where feasible in the context for the service.

We urge Congress to consider different levels of control, rather than a one-size-fits-all approach. The GDPR's approach, with multiple valid bases for processing personal data, is a useful starting point.

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?**

[9] https://services.google.com/fh/files/blogs/google_framework_responsible_data_protection_regulation.pdf

We agree that companies should continue to innovate in their privacy and data protection processes, policies, and techniques. Just as we continuously work to improve our products, we also strive to create new and innovative ways for individuals to be in control of their privacy choices. Services that did not exist two years ago are ubiquitous today, and technologies — like machine learning and AI — that we can use to understand and protect user data also are evolving.

We believe that Congress should support investments in research that result in techniques and protocols to enable productive uses of personal data while protecting personal information of individuals.

To make sure that companies are incentivized to innovate with regard to data protection, federal baseline privacy legislation should be risk- and outcomes-based, consistent, and adaptable, and should work for all types and sizes of businesses and organizations. Legislation should focus on responsible and reasonable data collection and use; transparency; control; security; access, correction, portability, and deletion; adaptability; and accountability. It should apply to all businesses and organizations that process personal information, and to all data that can be used to identify an individual. We lay out more specifics on our recommendations for legislation in our proposed regulatory framework,[10] which we published in September 2018, and in comments we filed with the Department of Commerce in March 2019.[11]

[10]https://services.google.com/fh/files/blogs/google_framework_responsible_data_protection_regulation.pdf
[11] https://www.ntia.doc.gov/files/ntia/publications/google_comments_for_ntia_rfc_on_privacy.pdf

where the service provider or “processor” lacks legal authority to make independent decisions about how to use the data or operate outside the bounds of the client’s direction. In the GDPR, this distinction is described as “processors” versus “controllers,” allowing for the efficient use of vetted, qualified vendors with minimal additional compliance costs, which is particularly important for smaller entities. Controllers remain responsible for meeting their obligations under the law, including transparency, control, and access, but processors must still meet basic programmatic and security responsibilities. In contrast, though the CCPA echoes and even borrows some language from the GDPR’s distinction between “controllers” and “processors,” it suffers from remaining ambiguities concerning the precise requirements for entities to qualify as “service providers,” as well as the scope of those entities’ responsibilities.

Responses of Will DeVries, Senior Privacy Counsel, Google LLC
Hearing on "GDPR and CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation"
Senate Judiciary Committee
April 3, 2019

Written Answers to Questions Submitted by Senator Durbin to Will DeVries

1. **In your testimony you say that "[p]rivacy law should also ensure individuals, where practical, have the ability to access, correct, delete and download and export personal information."**

   Do you support giving individual Americans an enforceable right to request that commercial websites and online services delete personal information that was collected from or about the individuals when they were children under age 13? I note that it should be both possible and practical for commercial websites and online services to identify personal information in their possession that was collected online from kids when they were under age 13, because under COPPA there had to be parental consent to collect the information.

   Along with access and correction, deletion is a foundational principle that supports user control and trust. Google offers our users around the world a range of tools to delete their information, including, for example, the ability to delete their entire account, or activity from particular services. These tools are extended to the Family Link[1] accounts that Google offers for parents to manage their children's privacy online.

   We support a federal baseline privacy law that codifies individuals' right to request deletion of their personal information, taking into consideration legitimate business reasons for retaining data, such as the need to protect systems and data (e.g., security, guarding against malware).

2. **You say in your testimony that GDPR "reflects the European regulatory tradition that in some ways would be inapplicable in the U.S., such as the so-called 'Right to be Forgotten'…"**

   Please explain why you testified that a right to be forgotten is "inapplicable" in the United States.

   In May 2014, in a landmark ruling, the European Court of Justice recognized the "Right to be Forgotten," (RTBF) more accurately known as the "right to delist" or "right to

[1] https://families.google.com/familylink/

erasure," allowing European citizens to ask search engines to delist information about themselves from search results.

The GDPR codified this in its Article 17 and made clear this does not apply only to search engines but to all data controllers, who have the obligation to erase an individual's personal data without undue delay if one of several grounds for erasure are met.

We support the ability for users to delete the personal information they have provided to businesses and organizations. Google offers tools for our users globally, via Google Account and Download Your Data.

Separate from deletion of personal information, the RTBF in Europe provides Europeans with the right to erasure from the search results, which is a fundamentally different action than that of personal data erasure from the records of an operator or backend of an online service. Since 2014, we have worked hard to implement the RTBF ruling thoughtfully and comprehensively in Europe. To date, we have examined some 3 million URLs. In accordance with the CJEU's 2014 ruling, any decision to delist is made on a case-by-case basis, following a balancing exercise that must take into account the individual's privacy right, but also others' free expression rights, right to access information, and the public's interest in the information. We published a white paper about our experience.[2]

This balancing is, of course, very delicate. It doesn't only vary from one request to another, but from one country to another: different governments, courts, and regulators strike the balance between these rights differently depending on their country's history, legal traditions, and culture. As a result, most countries outside the EU do not recognize a right to be forgotten with respect to online search; even within the EU, Member States don't apply RTBF in the same way.

In particular, there are significant differences between different countries' approaches to free speech. The US is one of the countries with the strongest protections of free speech, codified in the First Amendment, and it is very likely that a law requiring search engine services to de-list public websites in their search results would come into friction with this tradition.

[2] https://drive.google.com/file/d/1H4MKNwf5MgeztG7OnJRnl3ym3gIT3HUK/view

Responses of Will DeVries, Senior Privacy Counsel, Google LLC
Hearing on "GDPR and CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation"
Senate Judiciary Committee
April 3, 2019

Written Answers to Questions Submitted by Senator Klobuchar to Will DeVries

1. **I have concerns about consumers' ability to protect their privacy online as users are generally forced to either accept all of a platform's privacy practices or forego using the platform at all. My bill, the Social Media Privacy and Consumer Rights Act, would give consumers the ability to tailor their privacy preferences—instead of the take-it-or-leave-it approach that we see now.**

   a. **To what extent do you believe that users should have control over their privacy online?**

   We believe strongly that users should have control over their privacy and online data. That is why we support passage of a smart and strong federal baseline privacy law that, among other things, would require all businesses and organizations that collect and process user data to provide appropriate mechanisms for an individual to control how their data is collected and used, including the opportunity to object to data processing where feasible in the context of the service.

   In addition to individual control, we also believe that a key part of a privacy law should be a requirement for businesses and organizations to respect individuals' interests when they process personal information. Businesses and organizations also must take responsibility for using data in a way that provides value to individuals and society and minimizes risks to users based on the use of personal information. This means considering individuals' interests, assessing the impact of data use on those interests, and implementing safeguards to protect individuals. We believe this approach puts strong protections in place without placing the burden on individuals.

   b. **What can companies that operate digital platforms, like Google, do to give users meaningful control over the privacy of their personal information – including preventing the collection of information regarding their online activity or their offline activity, such as where they are at any given time? What steps has Google taken toward that end?**

   People want to be in control of the information they share and have choices about the services they use. When people use Google services, they are trusting us with their personal information. That is why we build transparency and individual control into the

products we make. We want our users to understand what data is collected and how that data may be used, and we provide and improve tools that enable their control.

We offer a number of choices and settings that keep users in control of their privacy. One example is Google Account, which we launched as My Account 2015, building on the centralized dashboard we have offered since 2009. This tool provides users with quick access to easy-to-use tools to help manage their privacy and security. Nearly 2 billion people visit Google Account each year. Most people who visit their Google Account page make changes or adjustments to their privacy settings — demonstrating not only that users are aware of the controls available through Google Account but also that they use this tool to make informed choices about their privacy.

In addition, the Privacy Checkup[1] tool makes it easy for Google users to quickly review and make privacy decisions. We make it easy to manage the types of data Google collects, to review what personal information users share with friends or make public, and to adjust the types of ads users would like Google to show them, including turning off personalized advertising entirely. We promote Privacy Checkup on a recurring basis so we can help our users keep their privacy choices up to date as their use of Google services changes over time. We also created Security Checkup,[2] which is designed to help users make informed decisions about security and privacy, including by identifying the apps that have access to their data and letting them revoke access to those apps.

[1] https://myaccount.google.com/intro/privacycheckup
[2] https://myaccount.google.com/security-checkup

Responses of Will DeVries, Senior Privacy Counsel, Google LLC
Hearing on "GDPR and CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation"
Senate Judiciary Committee
April 3, 2019

Written Answers to Questions Submitted by Senator Hirono to Will DeVries

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?

   Yes. Our experience is that users expect us to select defaults that are reasonable and that protect their interests. In addition, we regularly and actively prompt our users to do privacy and security reviews and use the powerful controls we offer, by reminding them to use these tools through individual prompts and service-wide promotions. Additionally, users can sign up for periodic reminders to review and adjust their settings.

   The Google Security Checkup[1] and Privacy Checkup[2] tools help our users identify and control the apps that have access to their Google Account data and guide our users to review and manage their security and privacy settings. Each year more than 100 million people take a Privacy Checkup and 700 million people take a Security Checkup.

   Google Account is also home to My Activity, where users can access all the personal information we collect about the user across our services. Each month over 90 million people visit My Activity to review their activity and over 50% delete some of it from their account.

   We are committed to continuing to develop and improve these and other tools to make them more robust and intuitive, and we encourage users to manage the information stored in their Google Account and review and adjust their privacy and security settings.

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**

[1] https://myaccount.google.com/security-checkup
[2] https://myaccount.google.com/intro/privacycheckup

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.

Google believes in ensuring that our users understand both how their data is used and that they are in control.

There is a growing consensus among regulators, researchers, and companies that asking individuals to opt-in for all uses of information is impractical and leads to fatigue that diverts attention from the most important choices. For example, some data processing is necessary to make products work and to ensure they are secure and reliable. Users expect their personal information to be used in this way, and asking them to separately consent presents the odd decision of "agree" or "don't use the service." This could have the perverse effect of teaching users to simply click "agree" to everything without paying attention.

Our proposed regulatory framework[3] recommends, as a starting point, that businesses and organizations be required to respect individuals' interests when they process personal information, to use data in a way that provides value to individuals and society, and to minimize risks to users based on the use of personal information. We believe this sets a baseline for data protection without placing the burden on individuals.

These responsibilities mirror those in the European General Data Protection Regulation (GDPR). The GDPR requires businesses and organizations to incorporate transparency and fairness into their practices and permits processing that balances the "legitimate interests" of the organization processing the data against the impact of that processing on the rights and interests of the individual. Where processing of personal data satisfies this balancing test and respects privacy principles, it may rely on legitimate interest as the legal basis for the processing, which would be an alternative to consent. We believe that US law should similarly encourage businesses and organizations to balance these same interests.

Our privacy framework also recommends that federal privacy law require businesses and organizations to provide appropriate mechanisms for individual control, including the opportunity to object to data processing where feasible in the context for the service.

[3]https://services.google.com/fh/files/blogs/google_framework_responsible_data_protection_regulation.pdf

We urge Congress to consider different levels of control rather than a one-size-fits-all approach. The GDPR's approach, with multiple valid bases for processing personal data, is a useful starting point.

3. **California Governor Gavin Newsom recently suggested that consumers should be paid a so-called "data dividend" by companies that collect and use their personal information.**

   Does Google support the idea of a "data dividend"? Why or why not?

   Google believes that privacy is most effectively protected as part of a rights framework rather than through an economic or market framework. A model focused on monetary compensation to individuals for the use of their data fails to take into account the enormous value that free online services provide to users of all types and backgrounds, regardless of their socioeconomic status or subscriber activity. It could also effectively create a financial incentive for users to give access to their data, which would tie privacy protection to each person's economic situation, rather than the inalienable right to privacy.

   We have not seen details on Governor Newsom's proposal so are not in a position to provide specific comments. However, we are generally concerned that 'data dividend' or similar proposals could exacerbate privacy concerns by incentivizing more data collection or bolstering companies whose business relies on the buying and selling of personal data.

   We believe a better approach is a risk- and outcomes-based comprehensive federal privacy law that will improve data protection, individual control, and accountability, and provide value for individuals and society.

4. **In response to a question from Sen. Graham, you said that behavioral advertising is a benefit to the users that ask for it.**

   a. **Do Google users opt in to behavioral advertising or is it turned on by default?**

      When a user creates a new Google Account, we specifically ask the user to review and confirm whether they would like to see personalized ads or not. Regardless of what the user chooses at the time, they have the option to turn off personalized ads at any time, as we describe below.

   b. **What percentage of Google users change the default setting with respect to behavioral advertising?**

Contextual signals (rather than personalization or behavioral advertising) drive the significant part of Google's advertising revenue. In general, however, personalized advertising helps sustain a flourishing and diverse ecosystem of quality, independent content.

Our ads personalization setting is directly within our account creation process, so users make a choice about personalized advertising when they set up a Google Account and can change that choice at any time by visiting their account settings. For existing users, we routinely prompt them with our Privacy Checkup tool, which asks them to confirm their ad settings along with several other important privacy choices. Users can see their profile and change their settings at any time via the Why This Ad[4] or AdChoices[5] notices that are in the corner of almost every ad we show. Between February 26 and March 27, our data show that 43% of signed-in users who visited their Ad Settings made a change to one or more settings.

We think this sets a good balance between the interests of individuals and publishers that depend on personalized ads for their revenue, but we are always looking at ways to improve.

[4] https://support.google.com/ads/answer/1634057?hl=en
[5] https://youradchoices.com/

Responses of Will DeVries, Senior Privacy Counsel, Google LLC
Hearing on "GDPR and CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation"
Senate Judiciary Committee
April 3, 2019

Written Answers to Questions Submitted by Senator Booker to Will DeVries

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?**

   We believe that a comprehensive privacy law should be primarily enforced by the Federal Trade Commission (FTC), with the appropriate staff and resources to support it. In addition to the FTC's years of experience with privacy enforcement, it is the right regulatory agency to provide expert guidance and facilitate and disseminate best practices.

   Over the past couple of decades, they have developed a strong track record in the context of privacy and data protection, with significant enforcement activity and consent decrees requiring companies to implement privacy and

security programs under FTC oversight and with periodic independent assessments. They have proven to be a rigorous regulator in this space, driving both large and small companies to improve their privacy practices, and would be best situated to continue to hold companies and organizations accountable under federal privacy legislation.

b. 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?

We oppose discrimination in all its forms, including through use of proxy information. Google has enacted strong protections against this kind of behavior. Google doesn't allow targeting based on sensitive characteristics like race, sexual orientation, or health. Our personalized advertising policies defining "sensitive information," for example, are the strongest in the industry. We recognize that seemingly benign categories can be proxies for sensitive criteria or otherwise create problematic outcomes. We do not engage in such behavior and actively work to prohibit advertisers from such targeting where possible.

c. 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?

We support passage of a smart and strong federal baseline privacy law that applies to all businesses and organizations that collect and process data. We understand that the FTC and the Government Accountability Office have both examined this issue and provided legislative recommendations. We defer to their judgement on the best approach.

2. 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]

[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.

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."**

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

We answer questions 2.a and 2.b together.

We read Kashmir Hill's series with interest and applaud her thoughtful work.

In examining companies' data footprint, it is important to distinguish between consumer-facing services such as Google Calendar, Chrome, or Gmail, and services such as Google Cloud Platform or Google Analytics that provide platforms and services for business and organizations. Known as "business-to-business services" or "data processors", this latter category of services operate differently. The data that is collected as part of the provisioning of such services is controlled by the business customer, not by Google.

We recognize that Google offers a range of consumer services used by millions or billions of users, and are part of their daily lives. But competition is fierce. Switching services online is easy, as users can easily switch to a competing service online, of which there are many, or use multiple services. Our Download Your Data tool helps to ensure that switching services is smooth for those users that choose to.

The current market for web search and web browsers provide illustrative examples. DuckDuckGo's testimony at the hearing highlighted how rival search engines can grow and be profitable. Alex Chisholm, head of the UK Competition and Markets authority, recently noted: "The barriers to switching for individuals is very low in online markets. If I am unhappy with my search engine, I can stop using it at a click of a button." Data from the Play store also bears this out: browsers such as Opera Mini and Firefox have been downloaded by Android phone users more than 100 million times, and the UC Browser more than 500 million times.

That said, we agree that a consent-for-everything framework is not a good regulatory model because it leads to take-it-or-leave-it choices that aren't helpful. We speak more to this in response to question 5.

Google has invested considerable resources into protecting user privacy. From developing cutting-edge engineering techniques to a robust compliance program,

Google is making the investments necessary to ensure we protect the privacy and security of our users' data. Just as we continuously work to improve our products, we also strive to create new and innovative ways for individuals to be in control of their privacy choices. We also note there are also multiple ways to use Google, and many services can be accessed without an account.

3. **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?**

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

   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?**

   We answer questions 3.a, 3.b, and 3.c together.

   We agree that transparency should go beyond the privacy policy. Regulators and privacy regimes should encourage businesses and organizations to actively

---

[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.

inform individuals about data use in the context of the services themselves, making information about data collection and use and user controls more relevant and actionable for individuals.

As discussed in our testimony, Google looks for ways to incorporate our privacy settings and transparency directly into our products. For example, Why This Ad,[5] which Google introduced in 2011, provides you with a drop-down notice explaining exactly what criteria any ad you see is based on. (e.g. "This ad was based on your current search terms.") It also links to your ad settings and our tools for reporting bad ads.

We also recently created a feature called "Your Data in Search"[6] that makes it easier to review, delete, and understand your recent Search activity. without ever leaving Search. By clicking the menu on their browser, users can get quick access to the most relevant privacy controls in your Google Account, and learn more about how Search works with your data. We specifically highlight answers to some of the most common questions people have about how Search works. For example, you can choose to learn "How Search uses information about your current location."

With regard to Do-Not-Track (DNT), like most websites, Google does not respond to browser-based DNT headers because a common understanding of how to interpret DNT signals was never developed. The working group responsible for developing DNT abandoned its efforts in January 2019 without ever finalizing the standard. Their failure after almost a decade of negotiations showcases the difficulty of agreeing on a common technical solution that is workable, practical and acceptable to all stakeholders. It also demonstrates how significantly the internet ecosystem has changed since 2010. We encourage Congress to avoid a mandate of specific technical solutions that can quickly become out of date and set clear baseline requirements that enable flexibility in how best to meet those requirements.

In its place, effective account-based and industry standard options have emerged, and browser vendors are competing to build even more powerful controls for online tracking. Chrome has for years offered users the ability to control cookies and their online browsing experience. Users can also opt out of personalized ads via Ad Settings[7] and the AdChoices[8] industry program (via a notice served in almost every ad Google shows).

4. **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**

[5] https://support.google.com/ads/answer/1634057?hl=en

[6] https://www.blog.google/technology/safety-security/making-it-easier-control-your-data-directly-google-products/

[7] https://adssettings.google.com/anonymous?sig=ACi0TCjb2QP20ZnM-DEe40U-4-i103lkgm9bkXWH9pfy57_fkOJ5sLTingViprsWtgn0S9ZBgeMkqqyABRaRvTifLPKKd35MpbL7nAkLSXcZblYbl6W_VSA&hl=en

[8] https://support.google.com/accounts/answer/1634057

privacy law will affect state-level efforts to regulate in the same space. However, most of our existing privacy statutes do not include provisions to overrule stricter protections under state law.[9] 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?

Data flows cross borders, and services like Google's are often used across state lines. We encourage Congress to adopt a strong and comprehensive federal privacy law that codifies individual rights and baseline data protections, and also addresses overlapping and inconsistent rules. The federal government is in the best position to harmonize data privacy laws with other obligations.

As one example, some commentators are suggesting that the California Consumer Privacy Act (CCPA) requires businesses to retain all of a user's personal information for a specific period of time, whereas the European General Data Protection Regulation (GDPR) — rightly, in our view — emphasizes the concept of "data minimization," under which information should be retained only so long as needed for a legitimate purpose. An inconsistent patchwork of privacy laws can cause consumer confusion and higher compliance costs without improving privacy protections.

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.

We generally support the underlying goals of the CCPA, to establish legal protections for privacy and security of individuals, including increased transparency and control around personal information, which we have offered to our users for years.

We do not want to eliminate these protections, but there are issues in the CCPA that need to be addressed, and it should be aligned with other leading privacy regimes. We share the concerns many have expressed about how the law is drafted, and its impacts on individuals and businesses. In particular, we hope that the law can be clarified to

[9] 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.

make it easier for consumers to understand and exercise their rights, and ensure that companies of all sizes and sectors can comply and continue to offer innovative products and services consumers rely on.

Generally, we believe the CCPA does not go far enough in codifying the rights and obligations included in consensus frameworks such as the Fair Information Practices Principles (FIPPs), Organization for Economic Co-operation and Development (OECD) Privacy Principles, the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, and the European General Data Protection Regulation (GDPR). Our principles for a responsible data framework are based on these frameworks, and our 20 years of experience offering services that depend on information, privacy protections, and user trust. The CCPA's provisions around individual control, non-discrimination, access and deletion requirements, and accountability are examples of where the CCPA can and should be improved.

First, privacy law should apply individual control over data processing wherever it can be reasonably offered, not just certain categories. The GDPR's flexible and nuanced approach to control is a better model than the CCPA, which includes user control that is ambiguous and limited to "sale" of personal information. The GDPR, in contrast, generally requires some user control over all data processing unless the processing is necessary to provide a service to the user or other specific circumstances apply.

Second, we also urge Congress to carefully think through the issue of under what conditions businesses and organizations may make services contingent on a user's acceptance of some processing of their personal information, sometimes known as non-discrimination. Individuals should not be penalized for exercising their privacy rights, but some choices offered to individuals may affect the ability of a business to earn revenue, and even the financial viability of products and services that are of tremendous benefit to users and to society. Publishers provide an illustrative example. Many newspapers currently offer individuals a choice between free access to quality content supported by personalized advertising and a subscription model that is free of personalized ads. Different approaches can offer individuals a real choice and multiple revenue models to support businesses.

Regulators are currently grappling with this issue across Europe with respect to the GDPR, thinking about how best to reconcile the current funding model of the internet with choices individuals make around those services. The CCPA also tries to grapple with this issue, but does so in a manner that is difficult to interpret or apply. The balance between user control and business operations is critical for Congress to keep in mind as it considers this principle.

Third, in drafting access requirements, Congress should be careful to avoid creating privacy or security risks. The CCPA helpfully includes access and deletion

requirements, but frequently without sufficient clarity or nuance. For example, it does not establish a clear framework under which competing rights and interests can be evaluated once a user has made an access request, or to enable businesses to ensure that a user requesting information has the right to receive that information. Requests for information associated with frequently-shared identifiers like IP addresses raise a number of substantial privacy concerns. In Google's experience, access to a secured account from which information is being requested has proven the most reliable indicator of a requesting user's identity and their entitlement to receive information associated with the relevant identifier. Absent such a showing, these kinds of requests can be exploited by scammers, fraudsters, and other malicious actors.

Lastly, in considering accountability, it is important to keep in mind the distinction between consumer services and enterprise services, and the need to clarify obligations based on an organization's ability to meet those obligations. Much of the processing of personal information is done by one company on behalf of another, where the service provider or "processor" lacks legal authority to make independent decisions about how to use the data or operate outside the bounds of the client's direction. In the GDPR, this distinction is described as "processors" versus "controllers," allowing for the efficient use of vetted, qualified vendors with minimal additional compliance costs, which is particularly important for smaller entities. Controllers remain responsible for meeting certain obligations under the law, including transparency, control, and access, but processors must still meet basic programmatic and security responsibilities. In contrast, though the CCPA echoes and even borrows some language from the GDPR's distinction between "controllers" and "processors," it suffers from remaining ambiguities concerning the precise requirements for entities to qualify as "service providers," as well as the scope of those entities' responsibilities.

For example, the CCPA helpfully includes important access and deletion requirements, but without sufficient clarity, nuance, or balance. It could be interpreted to require businesses to provide access to personal information to individuals who cannot be properly be authenticated. If access requests aren't appropriately verified, this could lead to enormous privacy risks, through disclosure of sensitive information to scammers, fraudsters, and other malicious actors.

We have advocated for federal comprehensive, baseline privacy legislation for some time -- long predating the CCPA. A harmonized, consistent approach is good for individuals seeking to exercise their rights and businesses and organizations seeking to comply.

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?

A federal baseline privacy law would provide clarity, but Congress should thoughtfully evaluate when and where FTC rulemaking authority may be appropriate. Congress should also consider flexible mechanisms that can be updated without wholesale restructuring of the law and incentivize all businesses and organizations that collect and process data to innovate as much on protecting privacy and security and enabling individual control as they do on products and services.

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.[10] 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?

Google supports strong and balanced baseline privacy legislation to provide individuals with strong privacy rights and protections around their personal information and to foster and maintain the trust that enables innovation with accountability for companies that collect and use personal information.

Though we support preemption of relevant state privacy laws, we agree it should not be the only consideration when drawing up federal legislation. There are many provisions in a federal baseline privacy bill that should be carefully considered, including how best to codify individual rights and consumer protections. Our testimony,[11] framework for data protection legislation,[12] and comments to the Department of Commerce[13] describe our recommended approach.

With regard to the California Consumer Privacy Act (CCPA), as described above, we generally support the law's goals but do not recommend it as a model for federal baseline privacy legislation. We believe established privacy principles and

[10] 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.
[11] https://www.judiciary.senate.gov/download/devries-testimony
[12] https://services.google.com/fh/files/blogs/google_framework_responsible_data_protection_regulation.pdf
[13] https://www.ntia.doc.gov/files/ntia/publications/google_comments_for_ntia_rfc_on_privacy.pdf

frameworks, such as the FIPPs, OECD Privacy Principles, the APEC Privacy Framework, and the GDPR, would be a better starting point.

5. **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?**

   Google believes in ensuring our users understand how their data is used, and are in control. We also believe that a privacy law should set a baseline for data protection but not require individuals to actively monitor or control how their data is used.

   Our proposed regulatory framework recommends a requirement for businesses and organizations to operate with respect for individuals' interests when they process personal information. Businesses and organizations must also take responsibility for using data in a way that provides value to individuals and society and minimizes risks to users based on the use of personal information. This means considering individuals' interests, assessing the impact of data use on those interests, and implementing safeguards to protect individuals.

   These responsibilities are discussed in the GDPR. The GDPR requires businesses and organizations to incorporate transparency and fairness into their practices, and permits processing that balances the "legitimate interests" of the organization processing the data against the impact of that processing on the rights and interests of the individual. Where processing of personal data satisfies this balancing test and respects privacy principles, it may rely on legitimate interest as the legal basis for the processing, which would be an alternative to consent. We believe that US law should similarly encourage businesses and organizations to balance these same interests.

   Consent is particularly important for data uses that involve a high risk to users and might not be well understood based on context.

   While controls are vital, there is a growing consensus amongst regulators, researchers, and companies that asking users to opt-in for all uses of information is impractical and leads to fatigue that diverts attention from the most important choices. For example, some data processing is necessary to make products work, and to ensure they are secure and reliable. Users expect their personal information to be used in this way, and asking them to separately consent presents the odd decision of "agree" or "don't use the service." This could have the perverse effect of teaching users to simply click "agree" to everything without paying attention.

Our proposed privacy framework recommends federal privacy law require businesses and organizations to provide appropriate mechanisms for individual control, including the opportunity to object to data processing where feasible in the context for the service.

We urge Congress to consider different levels of control, rather than a one-size-fits-all approach. The GDPR's approach, with multiple valid bases for processing personal data, is a useful starting point.

6. 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?

In the context of privacy, our experience with the FTC is that they have been a rigorous and effective enforcement agency. We support a reasonable allocation of resources and authority for the FTC to continue its important work.

Congress should thoughtfully evaluate when and where additional FTC rulemaking authority and resources may be appropriate.