Testimony of Will DeVries
Senior Privacy Counsel, Google
March 12, 2019

United States Senate Committee on the Judiciary
Hearing on "GDPR & CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation"

Chairman Graham, Ranking Member Feinstein, and distinguished members of the Committee: thank you for inviting me to appear before you this morning. I welcome the opportunity to discuss Google's work on data privacy and express our support for Congress' efforts to legislate on this issue.

My name is Will DeVries, and I am a Senior Privacy Counsel for Google. I have worked at the intersection of privacy, technology, and the law for 15 years, including teaching Privacy Law at the George Washington University Law School. In my current role, I advise on global data protection compliance and product development, focusing on US and EU data protection regulation and the harmonization of global data protection rules. My team's work is aligned closely with Google's Privacy and Data Protection Office, which is responsible for data protection compliance, the application of Google's privacy principles to product development, and working to ensure we meet our users' expectations of privacy.

Google's approach to privacy and data protection stems directly from our founding mission: to organize the world's information and make it universally accessible and useful. A key part of fulfilling that mission is building products for everyone, regardless of their economic circumstances, what connectivity they have, or what devices they use. For 20 years, our flagship products have been free, with advertising as our main source of revenue. Moreover, much of what we all enjoy online everyday — from free apps to our trusted sources of news to services offered by small businesses and organizations — is supported by advertising.

We need to maintain our users' trust, and we do this by operating with respect for users' interests and by clearly explaining how Google makes money, how our products use personal information, and how to find and use our powerful controls to manage privacy. We also invest in research and development of cutting-edge privacy and security engineering techniques, and share what we learn to benefit the broader ecosystem.

We have not always gotten it right, but we aim to continually learn and improve our privacy program and the transparency, control, and security that we build into our products. With tools like Download Your Data and Chrome Incognito mode, we have been at the forefront of how to apply privacy controls and protections into service offerings and data governance. We have practical experience building systems that apply our privacy principles, which helps us meet legal compliance obligations in the US and around the world. We hope our experience can help this Committee as it considers the future of privacy law in the United States.

With that perspective in mind, I will briefly explain why we believe comprehensive privacy legislation is needed and describe the essential elements of such a law.

The Need For Federal Legislation

There is, rightly, increasing focus on the impact of data collection and use on individuals. A healthy data ecosystem requires that people trust that all entities who use personal information will be held accountable for protecting it.

Now more than ever, there is momentum for and consensus around creating a federal privacy law. We welcome this, and reaffirm our long-standing support for smart and strong comprehensive privacy legislation.[1] Though there are meaningful and effective privacy protections in existing sectoral and consumer protection laws, we can improve upon the current framework by codifying universal privacy principles and individual rights.

Moreover, digital trade has become an engine of economic growth for large and small businesses around the world, and the flow of data now contributes more to GDP growth than the flow of goods. A federal comprehensive privacy law would help promote and sustain US global leadership around the free and open Internet, including promoting cross-border data flows and compatible, pro-privacy, and pro-innovation rules in other countries. The US is a leader in technology and data-based services, and should remain a leader in data protection as well.

Key Components Of A Comprehensive Privacy Law

To give detail to our call for a comprehensive privacy law, we recently published a framework for data protection legislation[2] and provided additional detail in comments to the National Telecommunications and Information Administration.[3] My testimony today will focus on this suggested framework, which is based in part on Google's practical experience developing products and services that make use of personal data, as well as from our experience with US and international data protection compliance.

At its core, comprehensive federal legislation should be risk- and outcomes-based, consistent, adaptable, and 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 all

[1] In comments to the Department of Commerce [Docket No. 101214614-0614-01 and Docket No. 1004] in 2010, Google called for the passage of comprehensive privacy legislation.
[2] https://www.blog.google/outreach-initiatives/public-policy/proposing-framework-data-protection-legislation/ and https://services.google.com/fh/files/blogs/google_framework_responsible_data_protection_regulation.pdf
[3] NTIA Request for Public Comments on Developing the Administration's Approach to Consumer Privacy, Docket No. 180821780-8780-01. Available at: https://www.ntia.doc.gov/files/ntia/publications/google_comments_for_ntia_rfc_on_privacy.pdf

data that can be used to identify an individual. I provide more detail about these principles below.

We also encourage Congress to look to established privacy principles and 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) to learn what is working, what can be improved, and how to support international interoperability for US-based companies that operate abroad. In particular, the GDPR is an important yardstick, and a product of years of deliberation and careful consideration. While it reflects the European regulatory tradition that in some ways would be inapplicable in the US, such as the so-called 'Right to be Forgotten', it is based on universal principles of individual control, transparency, and security, as well as strong recognition of individual rights and freedoms. The GDPR also includes mechanisms to seek consistency of interpretation and enforcement across EU member states.

Responsible and Reasonable Data Collection and Use

First and foremost, privacy legislation should require 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. The law should not require individuals to actively monitor how their data is used.

A key part of the responsible collection and use of data is reasonable limitations on the manner and means of collecting, using, and disclosing personal information. These obligations should be scoped as to not discourage data collection and use, so long as that collection and use is deliberate and thoughtful, in a manner compatible with individuals' interests and societal benefits, and circumscribed and in accordance with the organization's privacy program and regulations. At the same time, it should discourage collection and use of more identifying information if less identifying information (*e.g.*, pseudonymous or de-identified data) is sufficient.

The GDPR talks about the responsibility of businesses and organizations to consider individuals' interests and to protect against potential risks. It 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.

Transparency

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.

We know that privacy policies are not at the top of most people's reading lists, but we work to make ours user-friendly, and we regularly refine our approach based on research and feedback from our users. Though our privacy policy has been recognized as best in class,[4] we recently updated it[5] 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[6] in 2009 and today nearly 2 billion people visit Google Account each year. Google Account is home to the Google Security Checkup[7] and Privacy Checkup[8] 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.

Google also looks for ways to add transparency directly in products. For example, Why This

[4] 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/).
[5] https://policies.google.com/privacy?hl=en-US
[6] Dashboards are a recognized best practice (https://www.ivir.nl/publicaties/download/PrivacyBridgesUserControls2017.pdf).
[7] https://myaccount.google.com/security-checkup
[8] https://myaccount.google.com/privacycheckup?otzr=1

Ad[9] 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 search results, along with direct access to controls.[10] We are exploring expansion of this to other products.

Choice and Control

People have different preferences about how they want their information to be used, and preferences can vary over time. A privacy law should not presume all individuals are the same, but should ensure it is practical for individuals to control the use of personal information, no matter what entity is collecting or processing it.

Federal privacy law should require businesses and organizations to provide appropriate mechanisms for individual control, including the opportunity to object to data processing where feasible in the context of the service. This does not require a specific consent or toggle for every use of data; in many cases, the processing of personal information is necessary to simply operate the service the user requested. Similarly, requiring individuals to control every aspect of data processing can create a burdensome and complex experience that diverts attention from the most important controls without corresponding benefits.

This principle stems not just from existing privacy frameworks like the OECD principles, but from our experience offering our users with control over how their information is used within Google services. For individuals who have a Google account, we put their privacy and security settings in a single place — Google Account[11] — so our users have an easy way to see their data and set their preferences for how Google should store and use their information. Google Account is where our users can, for instance, pause or delete their Search or YouTube history or disable personalized ads. We continue to develop and improve these and other tools to make them more robust and intuitive, even absent requirements to do so, and will announce more improvements soon.

Individual control over data processing should apply wherever it can be reasonably offered, not just certain categories. We would suggest GDPR's flexible and nuanced approach to control is a better model than the California Consumer Privacy Act (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.

[9] https://support.google.com/ads/answer/1634057?hl=en
[10] https://www.blog.google/technology/safety-security/making-it-easier-control-your-data-directly-google-products/
[11] https://myaccount.google.com/intro?hl=en-US

We also urge Congress to think clearly 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. 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.

Security

Businesses and organizations must implement reasonable precautions to protect personal information from loss, misuse, unauthorized access, disclosure, modification, and destruction. Baseline precautions should apply to any collection of personal information, and additional measures should account for the sensitivity of the underlying information and be proportionate to the risk of harm.

As a corollary, businesses and organizations should be required to expeditiously notify individuals of security breaches that create a risk of harm. Google has long supported legislation that would establish a national security breach notification regime. All fifty states, the District of Columbia, Guam, Puerto Rico, and the US Virgin Islands have adopted security breach notification laws. While these laws share the common aim of protecting consumers in the aftermath of a security breach, they vary in specifying the manner in which consumers must be notified, the content of security breach notifications, and the regulatory entities that must be notified, among other things. A national security breach notification standard can simplify the notification process itself while ensuring that consumers are empowered to take measures that can reduce the likelihood of identity theft, fraud, or other types of harms.

Access, Correction, Portability, and Deletion

Privacy law should also ensure individuals, where practical, have the ability to access, correct, delete, and download and export personal information. This not only empowers individuals, it also keeps the market innovative, competitive, and open to new entrants.

In drafting access requirements, Congress should be careful to avoid creating privacy or security risks. The detailed framework established by the GDPR could be helpful in this regard. For example, the GDPR enables organizations to both request more specific information about the nature and scope of a request, and to consider the rights and interests of other persons when responding to these requests. In reviewing access requests in Europe, Google considers and mitigates potential impacts on the privacy of other persons identified in the relevant information, as well as impacts on other public interests like law enforcement.

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, such as abusive partners.

Google strongly supports the notion that individuals should be able to export the personal information they have provided to an organization in a format that allows them to understand the information, store a local copy, download it and/or to import it into another provider's systems. Google has worked on portability for over a decade and was the first to offer a portability tool in 2011. We updated and broadened this tool, Download Your Data, last spring so that it now covers more products and data types. The tool allows our users to take personal information about them stored in more than 50 Google products, including search queries, Gmail messages and contacts, YouTube videos, and many others. The output is provided in formats designed to be importable into software on the user's own devices or other services.

The ability for individuals to transfer data directly from one provider to another, without downloading and re-uploading it, is a significant advancement in making portability practical for individuals all over the world, particularly with the continued migration to mobile devices. However, service-to-service portability remains nascent, thus it should not be a requirement in law, as of yet.

We are working with partner companies on the Data Transfer Project,[12] an open-source initiative to expand this capability and make it even easier for individuals to try a new service or otherwise control their data. The current partners (Google, Microsoft, Twitter, and Facebook) are working on building a user interface as well as bringing new and more diverse partners into the project. We will continue to encourage more partners to join our efforts and facilitate broader availability of service-to-service portability.

Scope and Adaptability

[12] https://datatransferproject.dev

The technology involved in data processing is not static, and neither are the social norms about what is considered private and how data should be protected. A baseline law provides clarity, but Congress should evaluate other flexible mechanisms that can be updated without wholesale restructuring of the law and incentivize all businesses and organizations to innovate as much on protecting privacy and security and enabling individual control as they do on products and services.

Congress should avoid making distinctions between industries, technology, or business models. Information is increasingly critical through all sectors of the modern economy and businesses and organizations are increasingly competing across sectors. Based on our experience, individuals generally neither want nor expect different protections based on the type of service they use.

Accountability

A privacy regulatory framework should be principles-based and prioritize outcomes over process. To achieve both legal certainty and flexibility, Congress should set clear baseline requirements and enable businesses and organizations to decide how to meet those requirements. The Federal Trade Commission, with the staff and resources to support it, is the right regulatory agency to provide expert guidance, facilitate and disseminate best practices, and enforce a comprehensive federal privacy law. 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.

Privacy and security are not and should not be check-the-box exercises. Accountability can and should come in many forms and application of the law should encourage new entrants and diverse approaches. For example, industry accountability programs and safe harbors can incentivize best practices, particularly in providing more flexible approaches to dealing with evolving technologies. Also, companies should be encouraged to create accountability through internal privacy programs that, among other things, build in privacy from the ground up for product development. At the same time, we believe the establishment of internal programs should be scalable: small businesses and organizations can achieve the same protections and accountability without building a privacy program with the same scope and scale that larger, more established companies like Google operate.

Over the last two years, we have engaged in a company-wide effort to prepare for the GDPR, further improving on the robust information and tools we provide to our users and on Google's industry-leading privacy program described earlier. Even though Google did not

start from scratch — far from it — GDPR compliance continues to be an enormous investment of time and resources for us and we hope that Congress keeps this investment that Google and many US-based businesses have made in mind as it considers legislation.

Also, 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.

Conclusion

Privacy is tied to user expectations, which are rapidly changing as technology evolves and individuals make decisions about how to use it to their benefit. As a result, privacy is not a one-time problem that can be solved, and our work in this space will never be finished. We are committed to doing our part to improve the ecosystem — ensuring individuals are protected and businesses and organizations have an opportunity to innovate and grow. We also want to constructively engage with Congress and other stakeholders as you consider privacy legislation.

Thank you again for the opportunity to share our perspective and experience. We look forward to continuing to work with Congress. I welcome any questions you might have.