Google

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW,
Room 4725

Re: NTIA Request for Public Comments on Developing the Administration's Approach to Consumer Privacy, Docket No. 180821780-8780-01

Google appreciates the opportunity to provide comments in response to the National Telecommunications and Information Administration (NTIA) Request for Comments on Developing the Administration's Approach to Consumer Privacy[1]. We commend NTIA and the Department of Commerce, including the Secretary, International Trade Administration, and the National Institute of Standards and Technology, for its leadership on data privacy and continued innovation, and its open and consultative process on developing its policy and technical frameworks. The NTIA's efforts are both timely and important, and we welcome the opportunity to comment on the Administration's proposal, and to contribute to this renewed discussion on how best to improve the U.S. privacy regulatory framework.

We support the approach as set out by NTIA. The application of a comprehensive, balanced, risk- and outcomes-based framework will improve privacy and security protections for individuals and communities and establish user trust while promoting continued societal and economic benefits made possible by the free flow and innovative uses of data.

Across every single economic sector, government function, and organizational mission, data and technology are critical keys to success. With advances in artificial intelligence and machine learning, data-based research and services will continue to drive economic development and social progress in the years to come, from agriculture and medicine to charitable and government services, and beyond. Businesses of all types and sizes collect and use data to drive efficiency, reduce costs, connect to markets, and improve the consumer experience.

At Google, we combine cutting-edge technology with data to build and improve the quality of products and services. These products help enhance people's productivity, grow the economy,[2] improve accessibility[3] and make the web safer and more secure.[4]

[1] https://www.ntia.doc.gov/files/ntia/publications/fr-rfc-consumer-privacy-09262018.pdf
[2] Last year, Google's tools helped provide $283 billion of economic activity in the U.S. for more than 1.5 million businesses, website publishers, and nonprofits nationwide (https://economicimpact.google.com/).
[3] For example, we have used data analysis and machine learning to enable closed captioning on over 1 billion YouTube videos in 10 languages making them accessible to the over 300 million deaf or hard of hearing people around the world (https://youtube.googleblog.com/2017/02/one-billion-captioned-videos.html).
[4] Google Safe Browsing (https://safebrowsing.google.com) helps protect over three billion devices every day, and it is free and publicly available for developers and other companies to use.

With partners, we are working to tackle big challenges[5] and enable medical[6] and scientific breakthroughs.[7]

For 20 years, our flagship products have been free, with advertising as our main source of revenue. We make the choice to build products for everyone, regardless of their economic circumstances, what connectivity they have, or what devices they use. By showing relevant, useful ads, we can deliver products like Search or Maps for free. Moreover, much of what we all enjoy online everyday — from free apps to independent media to services offered by small businesses — is supported by advertising.

All these benefits rely on the responsible collection and use of data, and must come with, and not at the expense of, privacy and security.

Toward A Comprehensive Baseline Privacy Framework

Google firmly believes that federal legislation is the best path to realize NTIA's stated goals, and reaffirms our long-standing support for smart and strong comprehensive baseline privacy legislation that enshrines high standards of privacy for everyone.[8] Though there are meaningful and effective privacy protections in existing domestic law, regulations, and jurisprudence, we can improve upon the current framework with a comprehensive baseline privacy law that extend rights and protections by codifying long-standing privacy principles and unifying the U.S. approach. If well-crafted, the new baseline could make privacy more workable for all Americans and provide the certainty and flexibility businesses of all types and sizes depend upon to continue investing and innovating.

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 baseline 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-innovation rules globally.

---

[5] http://refreshfoodandtech.com

[6] Working with physicians and other healthcare experts, we've developed systems that can detect diabetic eye disease (https://ai.googleblog.com/2016/11/deep-learning-for-detection-of-diabetic.html) and breast cancer tumors (https://ai.googleblog.com/2018/02/assessing-cardiovascular-risk-factors.html), help predict medical outcomes (https://ai.googleblog.com/2018/05/deep-learning-for-electronic-health.html), and even shed light on connections between cardiovascular disease and images of the eye (https://ai.googleblog.com/2018/02/assessing-cardiovascular-risk-factors.html).

[7] We've shown machine learning can help predict molecular properties, which could aid everything from pharmaceuticals to photovoltaics to basic science (https://ai.googleblog.com/2017/04/predicting-properties-of-molecules-with.html). Another example is that Google's AI technology helped discover the first 8-planet system outside our own solar system (https://www.blog.google/technology/ai/hunting-planets-machine-learning/).

[8] 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 baseline privacy legislation.

In furtherance of those goals, we recently released a Framework for Responsible Data Protection,[9] based on the Fair Information Practices Principles (FIPPs), OECD Privacy Principles, Asia-Pacific Economic Cooperation (APEC) Privacy Framework, aspects of the European General Data Protection Regulation (GDPR), and our 20 years of experience offering services that depend on information, privacy protections, and user trust. It is aligned with many of the NTIA's stated outcomes and goals and provide the foundation of our comments.

Individual-Centric Privacy Outcomes

At its core, comprehensive baseline federal legislation should be consistent, adaptable, and proportional. Legislation should focus on transparency; control; responsible and reasonable data collection and use; security; access, correction, portability, and deletion; and accountability.

Transparency

All organizations that collect and use personal data 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 user trust.

Privacy policies provide a comprehensive source of this information for individuals, regulators, and experts to more systematically review the organization's data collection and processing practices, and hold them accountable for the representations they make. Given the array of issues and services these policies need to address, they can be long and difficult to parse, turning off many individuals from reading them. A key challenge for organizations is how to provide individuals necessary information without extraneous details or difficult text that can be overwhelming.

At Google, we regularly refine our approach based on continuous research and feedback from our users to ensure we strike this balance effectively. Though our privacy policy has long been recognized as best in class,[10] we recently updated it to incorporate some of the insights we have gained and make it more understandable and accessible to users, regardless of how much time they spend to review it, while being a full and complete statement of our data practices. We simplified our language and incorporated clear headings, easier navigation, overlays and examples,

[9] https://services.google.com/fh/files/blogs/google_framework_responsible_data_protection_regulation.pdf
[10] 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/).

explanatory videos, and inline settings so users can make decisions about their account settings as they learn about our practices.

Regulators should encourage 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. For example, if you add a Google Drive file to a shared folder, we will check to make sure you intend to share that file with everyone who has access to that folder. With Why This Ad,[11] you are able to click or tap on an icon in or around each ad to find out why you are seeing that particular ad and understand more about how Google's ad system makes these decisions.

In addition to our efforts on transparency mentioned above, recently we improved transparency and user control in our flagship product, Search, with a tool that shows users exactly how their data is being used to improve their search results, along with direct access to controls.[12]

Finally, our Transparency Report[13] provides information to the public on how government actions can affect the free flow of information online. We are always working to expand the information we provide to users.

Control

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

Organizations must 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 a service and is not particularly risky. Similarly, requiring individuals to control every aspect of data processing can create a complex experience that diverts attention from the most important controls without corresponding benefits.

We support the GDPR's notion of "legitimate interests" as a meaningful way to permit standard or typical data uses that are consistent with individuals' interests while reserving express consent to those situations where individuals need to pause and consider their choice. The specifics of consent (e.g., what options should exist and how they are presented) should not be enshrined in statutory language but articulated

[11] https://support.google.com/ads/answer/1634057?hl=en
[12] https://www.blog.google/technology/safety-security/making-it-easier-control-your-data-directly-google-products/
[13] https://transparencyreport.google.com/?hl=en

in regulatory guidance and codes of conduct that can be updated as norms and technology changes. This will be particularly important as emerging technologies become more widespread, such as screenless devices and ambient computing systems.

Dashboards are a recognized best practice to make individual controls easy to find and practical to use, and we think should be broadly implemented.[14] Google was one of the first companies to offer users a centralized dashboard in 2009. Users who have a Google account can find their privacy and security settings in a single place - Google Account[15] - and need not visit several different apps or pages to access their data and set their preferences for how Google should use their information. Google Account is where users are able to download a copy of their personal information; access or delete their Google activity (such as search queries or browsing history) by date, product, or topic; disable personalized ads or see the information Google uses to personalize their ads; and locate a lost or stolen phone.

One part of the Google Account is the Google Security Checkup[16] and Privacy Checkup[17] tools, which help users identify and control the apps that have access to their Google account data, and guide users to review and change their security and privacy settings. We regularly and actively prompt users to do privacy and security reviews by reminding them to use these tools through individual prompts and service-wide promotions.

We continue to develop and improve these and other tools to make them more robust and intuitive, and these efforts are working: in 2017, nearly 2 billion people visited their Google Account controls.[18]

Responsible and Reasonable Data Collection and Use

Comprehensive baseline privacy legislation should require organizations to operate with respect for individuals' interests when they process personal information. Organizations must also take responsibility for using data in a way that provides value to individuals and society and minimizes the risk of harm based on the use of personal information, such as data that can be linked to a specific person or personal device. A key part of the responsible collection and use of data is reasonable data minimization obligations. We believe a regulatory framework should place reasonable limitations on the manner and means of collecting, using, and disclosing personal information. Reasonable data minimization obligations should be scoped as to not

[14] Dashboards are a recognized best practice (https://www.ivir.nl/publicaties/download/PrivacyBridgesUserControls2017.pdf).
[15] https://myaccount.google.com/intro?hl=en-US
[16] https://myaccount.google.com/security-checkup
[17] https://myaccount.google.com/privacycheckup?otzr=1
[18] See: https://www.blog.google/technology/safety-security/improving-our-privacy-controls-new-google-dashboard/, https://www.blog.google/technology/safety-security/celebrating-my-accounts-first-birthday/, and https://googleblog.blogspot.com/2015/06/privacy-security-tools-improvements.html for more information.

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 regulatory guidelines. 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.

Another component of responsible and reasonable data collection and use is data quality. Comprehensive baseline privacy legislation should ensure organizations make reasonable efforts to keep personal information accurate, complete, and up-to-date to the extent relevant for the purposes for which it is maintained. Data access and correction tools, as mentioned below, can assist organizations in meeting this obligation.

Security
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, organizations should be required to expeditiously notify individuals of security breaches that create a significant 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 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. We encourage the NTIA to incorporate a national security breach notification standard as a component of the Administration's Approach to Consumer Privacy.

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.

Google strongly supports the notion that users 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. We believe this is critical to include in any privacy framework, but note data portability is not, and should not be, absolute. Portability efforts should be limited to content an individual user creates, imports, or has control over and should not include data companies generate that may be commercially sensitive or proprietary.

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 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 users to transfer data directly from one provider to another, without downloading and re-uploading it, is a significant advancement in making portability practical for users all over the world. However, service-to-service portability remains nascent, thus it should not be a requirement or included in control or other privacy obligations.

We are working with partner companies on the Data Transfer Project,[19] an open-source initiative to expand this capability and make it even easier for users 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.

We urge the Department of Commerce and Congress to explore ways to develop data portability to work for businesses of all types and sizes. One way to further this goal is for industry organizations and government entities like the Federal Trade Commission to explore best practices and methodologies that can be adopted by smaller players — perhaps via open-source projects or other low-cost options.

Accountability

A privacy regulatory framework should be principles-based and prioritize outcomes over means. We agree that when put in practice, goals and outcomes are often conflated, leading to one-size-fits all rules. To achieve both legal certainty and flexibility, Congress should set clear baseline requirements and enable organizations to decide how to meet those requirements.

[19] https://datatransferproject.dev

Google

Accountability can and should come in many forms. 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 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.

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 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. Sometimes 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.

Goals for Federal Action

We agree that high-level goals for federal action are important and should be considered separately from privacy outcomes. In the following section, we provide further information on what we suggest NTIA consider as it further develops its approach and how these goals might be achieved.

Create a Unified Approach that Accords with International Norms.
Privacy law should hew to established principles of territoriality, regulating organizations to the extent they are active within the jurisdiction. Extra-territorial application unnecessarily hampers the growth of new businesses and creates conflicts of law between jurisdictions. In particular, small businesses shouldn't have to worry about running afoul of regulators in different jurisdictions merely because a few people from another state or country navigate to their website or use their service.

Design Regulations to Improve the Ecosystem and Accommodate Changes in Technology and Norms.
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 can provide clarity, while ongoing reviews (e.g., regulatory guidance, codes of

conduct, administrative hearings) can provide more flexible and detailed guidance that can be updated without wholesale restructuring of the legal framework. Governments can support these goals by rewarding research, best practices, and open-source frameworks. Creating incentives for organizations to advance the state of the art in privacy protection promotes responsible data collection and use.

Comprehensive Application
User-centric privacy outcomes will also come from neutral, comprehensive, and consistent application of privacy rights and obligations. Data is increasingly important through all sectors of the modern economy, and generally individuals neither want nor expect different baseline privacy rules based on the provider collecting and using their personal information, the type of service they use, or where they live. At the same time, organizations are increasingly competing across sectors, and a regulatory regime should apply in a manner neutral to industry, technology, and business model.

NTIA and Congress should both take care to avoid unnecessary distinctions between industries or business models. We strongly believe that aside from the context of particular relationships that have existing rules, like with one's employer or attorney, legislation should apply to all economic sectors and all types of organizations that process personal information. While certain sectors (e.g., healthcare) may have additional rules, regulation should set a baseline for all organizations.

The application of the law should also take into account the resource constraints of different organizations, encouraging, rather than stymieing, new entrants and diverse and innovative approaches to compliance. One way to further this goal is for industry organizations, government entities, and civil society organizations to share best practices, methodologies, lessons learned, and techniques that can be adopted, particularly by smaller players. All organizations can and should innovate as much on protecting privacy and security and enabling individual control as they do on products and services.

Focus on Risk of Harm
A privacy law should encourage the design of products and services to avoid harm to individuals and communities. Enforcement and remedies should be proportional to the potential harms involved in the violation. Innovative uses of data shouldn't be presumptively unlawful just because they are unprecedented, but organizations must account for and mitigate potential harms. This includes taking particular care with sensitive information that can pose a significant risk. To enable organizations to develop effective mitigations, regulators should be clear about what constitutes a harm.

Encourage Regulatory Compatibility and Cross-Border Data Flows.
Mechanisms allowing for cross-border data flows are critical to the modern economy.

Organizations benefit from consistent compliance programs based on widely shared principles of data protection. Countries should adopt an integrated framework of privacy regulations, avoiding overlapping or inconsistent rules whenever possible. Regulators should avoid conflicting and unpredictable requirements, which lead to inefficiency and balkanization of services and create confusion in consumer expectations. In particular, geographic restrictions on data storage undermine security, service reliability, and business efficiency. Privacy regulation should support cross-border data transfer mechanisms, industry standards, and other cross-organization cooperation mechanisms that ensure protections follow the data, not national boundaries.

Some countries have taken steps to limit cross-border data flows through forced data localization requirements. Such requirements fail to recognize the way that modern distributed networks function and could have the unintended consequence of weakening privacy and security protections.[20] A comprehensive federal data protection law that explicitly eschews data localization would serve as a bulwark against data localization requirements and lend credence to the idea that countries can protect privacy on a cross-border basis without compromising key digital trade principles. A federal law could also build on recent steps taken by the US, Mexico, and Canada in the United States-Mexico-Canada Agreement (USMCA) to require protection of the personal information of users of digital trade and to promote compatibility between different privacy frameworks. As NTIA recognized in its request for comments, it is important to promote a regulatory landscape that is consistent with international frameworks for protecting privacy, including the APEC Cross-Border Privacy Rules System.

Incentivize Research and Development

Google is grateful to have a close relationship with the privacy and security research community, and maintains a permanent privacy and security research team that is dedicated full time to researching privacy and security issues. This research serves both to inform the teams building products about important privacy and security issues, as well as to engage and contribute to the vibrant research community, and is frequently published and presented in external journals and conferences. These teams also engage directly with users through user experience studies, to ensure that our products and policies are built with users in mind and based on their feedback.

Though organizations like Google invest significantly in research and development, Google believes the federal government has a critical role in enabling advancement of privacy and security enhancing technologies, techniques, and approaches.

We encourage the federal government to continue providing funding for the research and development of products, services, and techniques that improve privacy and

[20] https://www.blog.google/products/google-cloud/freedom-data-movement-cloud-era/

security protection. Basic research remains cost intensive, and educational institutions and research organizations need sustained funding to make the critical long-term investments that lead to new and improved ways to protect privacy and security. However, in its support, the government should not only focus only on the products and services that consumers see as an end-result, but also on expanding the types of tools and training available to practitioners. For example, techniques for internal data management and expanded availability of ethics training in schools can promote better outcomes for consumers.

The federal government should also consider establishing local centers of excellence for privacy and security research and applications, perform privacy and security research at government labs and agencies, create frameworks and mechanisms to facilitate public-private sector collaboration, and explore incentives for researchers who receive public funding to explore priority research areas. Google has long supported open-source research, and we encourage open access to publicly funded research.

Lastly, the U.S. government should leverage its convening power to disseminate best practices and effective tools and approaches to ensure that every organization that processes personal data, including the government itself, can keep abreast of and implement the state of the art. Publications, public events, technical workshops, digital literacy programs, and advisory committees, are potential ways the government could achieve this goal.

Defining Key Terms

Finally, the definitions that establish the foundation of any legal privacy framework are essential to scope appropriately. We encourage personal information to be defined flexibly to ensure appropriate incentives and handling. The scope of legislation should be broad enough to cover all information used to identify a specific user or personal device over time and data connected to those identifiers, while encouraging the use of less-identifying and less risky data where suitable. The law should clarify whether and how each provision should apply, including whether it applies to aggregated information, de-identified information, pseudonymous information or identified information.

In crafting privacy regulation, the federal approach should be closely bound to an articulation of risk of harm. For example, Google's Framework for Responsible Data Protection Regulation suggests that "sensitivity" of personal information should be tied in law to risk of harm to individuals and communities, rather than a specific list of

data types that might quickly become out of date. We think this is the right approach, but does require thought to avoid unnecessarily shifting regulatory standards.

Conclusion

As the NTIA considers the Administration's approach to privacy, and Congress potential comprehensive baseline privacy legislation, we recommend consideration of the importance of responsible data practices for consumers, the impact of a regulatory framework on service functionality, the consumer benefits of free and low-cost products, the future of the open web and app ecosystem, and the unique compliance needs of small businesses.

Thank you again for this opportunity to provide comments. Google appreciates the opportunity to share its perspective and experience. We are happy to answer questions or provide further information with respect to privacy and the Administration's work to develop a regulatory framework.

Respectfully submitted,

Google