Written Testimony of Keith Enright

Chief Privacy Officer, Google

United States Senate Committee on Commerce, Science, and Transportation

Hearing on "Examining Safeguards for Consumer Data Privacy"

September 26, 2018

Chairman Thune, Ranking Member Nelson, and distinguished members of the Committee: thank you for the opportunity to appear before you this morning. I appreciate your leadership on the important issues of data privacy and security, and I welcome the opportunity to discuss Google's work in these areas.

My name is Keith Enright, and I am the Chief Privacy Officer for Google. I have worked at the intersection of technology, privacy, and the law for nearly 20 years, including as the functional privacy lead for two other companies prior to joining Google in 2011. In that time, I have been fortunate to engage with legislators, regulatory agencies, academics, and civil society to help inform and improve privacy protections for individuals around the world.

I lead Google's global privacy legal team and, together with product and engineering partners, direct our Office of Privacy and Data Protection, which is responsible for legal compliance, the application of our privacy principles, and generally meeting our users' expectations of privacy. This work is the effort of a large cross-functional team of engineers, researchers, and other experts whose principal mission is protecting the privacy of our users.

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. Doctors use data to save lives; farmers rely on data to increase yields; and charities analyze data to better serve our communities. I have had the privilege of working with government agencies to better leverage data to advance their mission and provide improved care and benefits to Americans efficiently and reliably. Businesses of all types and sizes, far beyond those represented at this hearing today, collect and use data. In my previous experience, I saw first-hand the transformative efforts by traditional brick and mortar retail businesses to improve efficiency, reduce costs, and delight consumers through the innovative use of data.

At Google, we combine cutting-edge technology with data to build products and services that improve people's lives and enhance their productivity, help grow the economy,[1] improve

[1] 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/).

accessibility[2] and make the web safer and more secure.[3] With partners, we are working to tackle big societal challenges and enable medical[4] and scientific breakthroughs.[5] These types of benefits all rely on the collection and use of data, and must come with, and not at the expense of, privacy and security.

Privacy That Works For Everyone

We acknowledge that we have made mistakes in the past, from which we have learned, and improved our robust privacy program.

The foundation of our business is the trust of people that use our services. To maintain user trust, we must clearly explain how our products use personal information, and to provide easy-to-find and use controls to manage privacy. We also invest in research and development of cutting-edge privacy and security engineering techniques, sharing what we learn to benefit the broader ecosystem.

Google's approach to privacy stems directly from our founding mission: to organize the world's information and make it universally accessible and useful. Providing most of our products for free is a key part of meeting that mission, and ads help us make that happen. With advertising, as with all our products, users trust us to keep their personal information confidential and under their control. We do not sell personal information. Period.

As the world becomes increasingly data-focused, there is, rightly, increased focus on the impacts on consumers and whether there should be better rules of the road for data privacy. We understand that Congress may be legislating on privacy and we support that effort. We look forward to constructively engaging with you as your work develops.

To that end, I want to briefly cover four key issues that we believe are critical elements to this discussion: transparency, control, data portability, and security. These components are also central to Google's recently released framework for responsible data protection regulation, which I will discuss as well.

Informing Users And Explaining Our Practices

First, transparency is a core value of our approach to serving users. Google strives to be upfront about the data we collect, why we collect it, and how we use it. We get that privacy policies are not users' first choice in reading material, but we work to make ours clear and

---

[2] 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).

[3] 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.

[4] 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 cardivascular disease and images of the eye (https://ai.googleblog.com/2018/02/assessing-cardiovascular-risk-factors.html).

[5] 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 (https://www.blog.google/technology/ai/hunting-planets-machine-learning/).

concise. Outside experts have praised ours as best in class.[6] Just this year we updated our Privacy Policy to be easier to understand, with informative videos that explain our practices and settings. In addition to making our privacy controls easy to find in user accounts and through Google Search, we have also made them immediately accessible from the Privacy Policy so that users can make decisions about their account settings as they learn about our practices.

We also look for ways to add transparency into our products directly, so that users can understand the privacy implications of their choices in context. For example, if you add a Google Drive file to a shared folder, we'll check to make sure you intend to share that file with everyone who has access to that folder. With Why This Ad,[7] you are able to click or tap 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. Another example is if someone wants to install a new app on their Android mobile phone, they can see the types of personal information that apps can access right on the screen before deciding whether to install it. If they change their mind or want to learn more, they can learn about the different permissions, and disable specific ones. Finally, our Transparency Report[8] 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.

Google Account Controls

Second, with regard to user control, our privacy tools are built for everyone. Different people have different preferences about how they want their information to be used, and preferences can vary over time, so we build products and controls that do not presume all users are the same. For instance, a Search user can choose not to sign in when they search, and a Chrome user can choose to use Chrome's Incognito mode. For users who have a Google account, we put their privacy and security settings in a single place -- Google Account [9] -- so users don't have to visit several different apps or pages to see their data and set their preferences for how Google should store and use their information.

Google was one of the first companies to offer users this type of centralized dashboard[10] in 2009, and we continue to develop and improve these and other tools to make them more robust and intuitive. These efforts are working: in 2017, nearly 2 billion people visited their Google Account controls.[11]

I particularly want to call attention to our Security Checkup[12] and Privacy Checkup[13] tools, which respectively, 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. These

---

[6] 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/).
[7] https://support.google.com/ads/answer/1634057?hl=en
[8] https://transparencyreport.google.com/?hl=en
[9] https://myaccount.google.com/intro?hl=en-US
[10] Dashboards are a recognized best practice (https://www.ivir.nl/publicaties/download/PrivacyBridgesUserControls2017.pdf).
[11] 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.
[12] https://myaccount.google.com/security-checkup
[13] https://myaccount.google.com/privacycheckup?otzr=1

checkups help users make decisions about what information they are sharing, who they are sharing it with, and what to expect when they share it. It is not enough to just have these tools available: we actively encourage users to do privacy and security reviews by reminding them to use these tools through service-wide promotions and individual prompts.

Google Account is where users can:

- download a copy of their personal information;
- see or delete their Google activity, such as search queries or browsing, 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.

Privacy From The Ground Up

Protecting users is about more than just being transparent and offering control -- it requires building products that reflect our privacy commitments and principles at every stage of their development. Doing this properly requires a comprehensive data protection program that includes privacy design reviews, engineers dedicated to privacy to review code and data flows, and a system to manage and address any issues discovered before users are put at risk. Google has had such a program for over seven years, and we continue to expand and refine it.

Data Portability

Third, we believe data portability is a key way to drive innovation, facilitate competition, and best serve our users - that's why we have been working on it for over a decade.[14]

Google has always believed that people should use our products because they provide unique value and features. Download Your Data[15] is a practical tool that lets users backup or archive important information, organize information between multiple accounts, recover from account hijacking, and explore the data stored in their account.

Currently, users average around one million exports per month covering eight billion files. We enable export from more than 50 Google products, even offering the option to import data directly into our competitors' systems. If a user wants to try out a new product or service or even switch because they think it is better, they should be able to do so as easily as possible, not be locked into an existing service.

Portability is one way we ensure that users can trust Google with their data. This is why we led the development of the Data Transfer Project,[16] an open-source platform that enables you to move a copy of your data directly from one account to another without downloading and reuploading. For people who rely on phones and mobile networks for connectivity, this is a tremendous improvement. We're grateful for our industry partners' contributions to this project, and look forward to working with others.

---

[14] https://publicpolicy.googleblog.com/2009/09/introducing-dataliberationorg-liberate.html
[15] https://support.google.com/accounts/answer/3024190?hl=en
[16] See website (https://datatransferproject.dev/) and white paper (https://datatransferproject.dev/dtp-overview.pdf) for more information.

Security

Fourth, security considerations are paramount in all of these efforts. The security threat landscape that we see is increasingly complex and wide ranging. Securing the infrastructure that provides Google's services is critical in light of the growing and sophisticated nature of many threats directed at our services and users.

All Google products are built with strong security protections at their core to continuously and automatically detect threats and protect users. We devote significant resources to fortify Google's infrastructure and this includes continuous and proactive efforts to identify and block a wide range of security risks. The insights we've gained serving billions of people around the world help us stay ahead.

We have also worked to help our users improve their own cybersecurity posture. For example, we have offered two-step verification to our users since 2011,[17] and last year, we unveiled the Advanced Protection Program,[18] which provides the strongest account protection that Google offers.

Our focus on security is not limited to Google's users. We share technologies and collaborate with partners to help people stay safer whenever they are online. In 2007, we launched the first version of our Safe Browsing tool.[19] This tool helps protect users from phishing, malware, and other potential attacks by examining billions of URLs, software, and website content. We have made Safe Browsing free and publicly available to webmasters and developers so that they can protect their websites and applications from malicious actors.

Finally, it is important to note that small and midsize businesses are leveraging Google's cloud technology to protect the security and confidentiality of their business data. In the past, many such businesses managed their own online security infrastructure, putting them at a disadvantage. Now, these small and midsize businesses can avail themselves of the security expertise previously only available to the largest, most sophisticated enterprises, significantly reducing their information technology costs while vastly improving the security, confidentiality, integrity, and availability of business critical data.

Toward A Comprehensive Baseline Privacy Framework

Now, more than any time I've seen in my career in privacy, there is an interest in setting out baseline privacy requirements in law. We welcome this: a healthy data ecosystem requires people feel comfortable that all entities who use personal information will be held accountable for protecting it.[20]

The U.S. approach to privacy is admirable for its focus on protecting consumers while encouraging innovation and investment, but there is room for improvement. To demonstrate

[17] https://www.google.com/landing/2step/
[18] https://google.com/advancedprotection/
[19] https://safebrowsing.google.com/
[20] Comments filed in U.S. Department of Commerce, Docket No. 100402174-0175-01 and Docket No. 101214614–0614–01 : Information Privacy and Innovation in the Internet Economy (2010).

our commitment to the goal of comprehensive baseline privacy legislation, we recently put forward principles for a responsible data framework. The framework is 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 includes many of the principles I have talked about today: transparency, control, data portability, and security.

I am submitting a copy of Google's framework with my testimony. We hope it can contribute to this Committee's work.

Our framework is high-level, and of course, the manner in which general principles are implemented will matter a great deal. We urge the Committee to take into consideration the impacts on service functionality, the consumer benefits of free and low-cost products, the future of the open web and app ecosystem, the unique compliance needs of new entrants and small businesses, and competitive market dynamics.

Conclusion

Privacy and security work is never finished. Our work will continue, and we stand ready to do our part in building a better ecosystem for everyone. Sound practices and smart regulations can help, particularly when they are applied across the board to those making decisions regarding the collection and use of personal data. We share your goals of ensuring consumers are protected and businesses have an opportunity to innovate and grow.

Thank you again for the opportunity to tell you about our continued efforts in this space. We look forward to continuing to work with Congress on these important issues. I welcome any questions you might have.