Google appreciates the opportunity to respond to the United Nations Human Rights Council's (UNHRC) invitation to provide input on the right to privacy in the digital age, and, in particular, the "principles, standards and best practices with regard to the promotion and protection of the right to privacy".

It is axiomatic that international legal frameworks are lagging behind the pace of technological innovation. Internet companies, the largest of whom are based in the United States, are now providing services to billions of users across the world. Prior to the advent of the Internet, individual users often stored personal data on devices with limited storage capacity. Now, Internet companies provide cheap and often limitless storage of data on servers that are located throughout the world.

In many cases, there may not be a close relationship between the nationality of the user and the location of her data. Modern Internet networks increasingly transmit and store data intelligently, often moving and replicating data seamlessly between data centers and across borders in order to protect the integrity of the data and maximize efficiency and security for users. The emerging trend away from data localization, as well as law enforcement access rules based on data location, is encouraging in light of the way that modern distributed networks function.

The growth of modern distributed networks necessitates new legal frameworks that can rise to the challenge of facilitating cross-border law enforcement requests in a way that enhances privacy and the concomitant values of due process and human rights. As we noted in a white paper released in June 2017, inaction ultimately redounds to the detriment of both privacy rights and legitimate law enforcement interests.

We are at an inflection point. Government access laws are due for a fundamental realignment and update in light of the proliferation of technology, the very real security threats to people, and the expectations of privacy that Internet users have in their communications. There is reason to be optimistic, however, that we can address and reconcile these various equities in light of recent developments, but it will require vigilance from interested stakeholders in the coming months and years.

The CLOUD Act

In its call for input, the UNHRC sought relevant information about "[r]ecent developments in national or regional legislation", among other issues. In March 2018, the Clarifying Lawful Overseas Use of Data ("CLOUD") Act was enacted into law in the United States. Prior to enactment of the CLOUD Act, U.S. law prohibited U.S. service providers from disclosing communications content directly to foreign governments, including those with a strong tradition of respect for privacy, due process, and human rights.

The CLOUD Act authorizes U.S. service providers to disclose communications content directly to certain, "qualifying foreign government[s]", provided that such governments meet baseline privacy, due process, and human rights criteria set forth in the bill. Under the CLOUD Act, qualifying foreign governments can enter into executive agreements with the U.S.. These agreements establish the parameters for foreign law enforcement requests to U.S. service providers, consistent with the criteria set forth in the CLOUD Act.

While many countries are going to rely on Mutual Legal Assistance Treaties (MLATs) and comparable diplomatic mechanisms for the foreseeable future, the CLOUD Act creates a complementary legal mechanism for qualifying foreign governments to obtain communications content directly from U.S. service providers. Making this avenue available to other countries will have the salutary effect of incentivizing such countries to raise their privacy and due process standards so that they can avail themselves of the new process created by the CLOUD Act.

Google supports the CLOUD Act, and we are committed to ensuring that it is implemented in a manner that genuinely improves privacy and due process in the digital age. We appreciate that the CLOUD Act represents a seismic change to the legal regime for cross-border law enforcement requests. That only underscores the importance of promoting the adoption of standards that can improve privacy and due process rights and consequently promote the right type of international harmonization.

Improving Privacy and Due Process Standards

There is no international consensus about what concrete measures governments must take to respect and codify the values of privacy, due process, and human rights. With the growth of cross-border law enforcement requests and proposed frameworks for such requests, however, there are increasingly bedrock principles around which governments, companies, and civil society groups are coalescing. The CLOUD Act creates a new sense of urgency to build consensus around these values, which can provide a model framework for countries that understand that the capacity to

make cross-border law enforcement requests in the future will hinge upon improving domestic privacy and due process standards.

In 2013, the first version of the Necessary and Proportionate Principles were unveiled at the UNHRC in Geneva. The Necessary and Proportionate Principles, finalized in 2014, constitute a framework that other governments can emulate in fashioning government access statutes that comport with international human rights law. The thirteen guideposts that comprise the Necessary and Proportionate Principles, as the prefatory text notes, provide a "framework to evaluate whether current or proposed surveillance laws and practices are consistent with human rights."

In light of the CLOUD Act, the Necessary and Proportionate Principles can serve as a useful lodestar for countries that understand the bargain struck by the CLOUD Act; countries must commit to baseline principles of privacy, due process, and human rights in their domestic legal frameworks in order to make cross-border law enforcement requests directly to U.S. providers. Notably, the CLOUD Act is consonant with the Necessary and Proportionate Principles in important respects:

- **Legality**: Government requests for user data must be authorized by law and must include robust procedural and substantive protections for privacy and civil liberties.

- **Basis for Legal Request**: There must be a reasonable justification for government requests for user data that must be based on articulable and credible facts.

- **Prior Independent Review:** Government requests for user data must be subject to review or oversight by an independent authority prior to or in proceedings regarding enforcement of the order.

- **Specificity and Particularity**: Government requests for user data must identify a specific person, account, address, personal device, or other specific identifier as the object of the order.

- **Legitimate Aim and Proportionality:** Government requests for user data must relate to the prevention, detection, investigation, or prosecution of serious crime.

While the Necessary and Proportionate Principles and the CLOUD Act have different areas and degrees of emphasis, both frameworks can inform the development of legal regimes for government access standards that establish the baseline for strong privacy and due process protections. To be clear, these frameworks should not operate to the exclusion of others that can amplify, enhance, and codify these values. For example, the Center for Democracy and Technology unveiled human rights

criteria for cross-border law enforcement demands in advance of the European Commission's introduction of its E-Evidence Regulation on April 17. Like the CLOUD Act, the E-Evidence Regulation endeavors to fashion rules for cross-border law enforcement requests that both address modern law enforcement challenges and reinforce privacy values that are enshrined in the European Charter of Fundamental Rights.

Forging consensus around the aforementioned values is critical in light of developing legal frameworks for cross-border law enforcement requests. Such frameworks advance legitimate law enforcement equities in light of the trajectory of technological innovation and the growth of the commercial Internet. But they also present a unique opportunity to improve international privacy, due process, and human rights standards, and we look forward to working with like-minded stakeholders to codify these values.