U.S. Department of Commerce
Docket No. 100402174-0175-01
Information Privacy and Innovation in the Internet Economy

Comments of Google Inc.

Google thanks the Department of Commerce – including the Secretary, the National Telecommunications and Information Administration, the International Trade Administration, and the National Institute of Standards and Technology – for its welcome focus on privacy and online innovation.

It is difficult to overstate the social and economic benefits of the Internet for the United States and for the world. More than any technology in history, it has empowered entrepreneurs to bring their ideas directly to market – without tolls, without gatekeepers, without limitations. And by bringing the world's knowledge to the fingertips of each connected individual, the Internet has begun to unleash the true power of information to help consumers, create jobs, ensure government transparency, and achieve other societal benefits.

The Department of Commerce has a broad mandate to advance economic growth, jobs, and opportunities for the American people, as well as cross-functional responsibilities in trade, technology, entrepreneurship, economic development, environmental stewardship, and statistical research and analysis. The Department also has a strong history of thoughtful Internet policymaking. In the 1990s, the Department played a leadership role in the federal government's e-commerce activities, which encouraged and spurred responsible private sector leadership on issues ranging from privacy, private international law, and Internet governance. The Department's role and track record make it ideally suited to play a central role in developing the policies that will continue to organize, govern, and nurture the Internet.

The Department's Notice of Inquiry is timely and important. Existing regulatory frameworks for privacy, both domestic and international, are incomplete and sometimes in tension with one another to the detriment of both Internet users and online providers.

Google therefore urges the Department to work to develop comprehensive, baseline privacy rules that both help establish user trust and support the global data flows necessary for building new content and services in the data-centric Web. Such a framework also offers a consistent platform for providers to develop innovative, flexible tools that empower users to make privacy choices and self-regulatory structures that can keep pace with changing technology. The Department has a unique opportunity to shape this unified, comprehensive privacy framework in the U.S. and to encourage consistent, pro-innovation rules internationally.

Google has been a leader in developing user-friendly tools to inform and empower our users, including promoting data portability, creating educational privacy videos, developing an Ads Preferences Manager that allows users to see and control what interests are associated with their browser, and providing a centralized dashboard designed to help users view their information and control their individual privacy settings. To protect our users' communications, we encrypt all Gmail traffic by default, and we remain the only major search provider to allow users to encrypt search queries. These types of privacy tools educate and empower consumers, provide enhanced transparency, improve security, and offer meaningful choice and control. We have attached to this submission our recent privacy comments filed with the Federal Trade Commission, which expand on these tools and Google's approach to privacy.

In the comments below, we apply some of what we have learned about privacy to address the strengths and weaknesses of existing domestic and international privacy regulations and their impact on users and innovation. We then suggest ideas for how to conceive a comprehensive, baseline privacy framework and about how the Department can play a central role both here and abroad in developing this framework.

Domestic Privacy Regulation

Although the U.S. privacy system needs a comprehensive vision, the system has protected online users and encouraged innovation

Although Google believes that the U.S. would benefit from a unified, principles-based legal framework specific to privacy, we nevertheless believe that there are real and effective protections established under U.S. privacy laws and regulations. Moreover, Internet innovation has flourished in the United States in part *because* of the flexible nature of U.S. privacy laws and an enforcement framework that places substance over form. Accordingly, we believe that before policy makers discuss what could be improved in the domestic arena they must start with the very real successes of the current system.

Between sectoral laws, Federal Trade Commission policy and enforcement, state consumer protection laws, and self-regulation, the U.S. has assembled a system that protects user privacy and supports innovation. In fact, the success of this system is perhaps the best evidence that user privacy and data innovation are not mutually exclusive.

Increasingly, privacy is not merely a laws-based construct, but rather one that is driven by technological innovation and evolving consumer expectations. As Professors Kenneth Bamberger and Deirdre Mulligan recently explained in the *Stanford Law Review*, while the U.S. may suffer from a incomplete set of "privacy on the books" (the privacy laws that establish minimum standards for the protection of information) it has developed a flexible and powerful tradition of "privacy on the ground" – the practices and policies devised and implemented to meet evolving consumer expectations, as well as comply with existing privacy laws.

Adherence to privacy laws in a rapidly changing environment is necessary but by itself will not address consumer expectations. Certain approaches, however, provide a better framework to facilitate adaptation in light of evolving consumer expectations. The Gramm-Leach-Bliley Act (GLBA), for example, requires financial institutions to protect the "security and confidentiality of

customer records and information" while eschewing specific technological mandates that would effectively wed financial institutions to specific technology solutions. Under the GLBA Safeguards Rule, financial institutions have the flexibility to implement privacy and security protocols that address new and emerging threats to the security and confidentiality of customer records and information. A more prescriptive approach – *e.g.*, mandating the use of specific technologies or administrative protocols – would likely constrain the ability of financial institutions to design and implement solutions that are attuned to the unique privacy challenges presented by specific products and services.

The FTC, too, has used its authority to stop unfair and deceptive trade practices to develop flexible, standards-based privacy rules that reflect consumer expectations. Under its existing statutory authority, the FTC has penalized bad actors, enforced privacy promises, and sent important signals about evolving standards for proper notice, choice, consent, and data security. The FTC communicates its expectations clearly, effectively, and prospectively to protect consumer privacy without unnecessarily disrupting legitimate business practices and innovation.

In its enforcement role, the FTC has sought to articulate consumer expectations in the privacy and data security arena – asserting itself in cases where specific practices failed in its view to satisfy evolving consumer expectations concerning privacy and data security. As Professors Bamberger and Mulligan noted, "a key to the effectiveness of FTC enforcement authority is the agency's ability to respond to harmful outcomes by enforcing evolving standards of privacy protection as the market, technology, and consumer expectations change – the very opposite of the rule-based compliance approach frequently embodied in regulation."

The FTC's guidance in privacy and data security enforcement compels both the subjects of such enforcement actions and others in the industry to embrace forward-looking and creative solutions to new and emerging privacy and data security issues. Simultaneously, the Commission seeks to educate consumers about emerging privacy issues. Finally, the Commission and staff use roundtables and town hall meetings to engage in a discussion with industry and advocates, and to offer flexible guidance based on information about evolving user needs and provider practices discussed in those settings. Public dialogue with industry and advocates helps to develop consensus about emerging issues and to create incentives for industry to identify appropriate solutions. Its self-regulatory guidance for the online advertising industry, for instance, has helped spur broad industry support for improved advertising notice and opt-out functionality.

To provide greater context, it is instructive to compare Internet innovation in the U.S. and the European Union. For instance, many of the Internet advertising companies in the U.S. were established at a time when European regulatory models already presented a barrier to entry in terms of the need for implementing varying and complex data protection legislation. In fact, the European Commission itself admitted, in 2003, that the European data protection regime had failed to anticipate new technological developments. Noting the huge changes in "the means of collecting personal information," the European Commission wondered "whether legislation can fully cope with some of these challenges." This is precisely the advantage of the flexible U.S. approach.

Despite successes, further consistency and comprehensiveness in U.S. privacy regulation will help strengthen user privacy and promote continued innovation

Although we believe that privacy regulation and enforcement mechanisms in the United States have both encouraged Internet innovation and evolved to meet consumer expectations, there are improvements to the U.S. system that the Department can help promote. Inconsistency and gaps in the rules create unnecessary costs and burdens to innovation and undermine user trust.

Generally, Internet users neither expect nor want different baseline privacy rules based either on the type of provider processing their information, the type of device or service that is being used, or the local jurisdiction in which they or the provider reside. In many respects, our current legal framework often creates precisely these distinctions – upsetting users' reasonable privacy expectations and complicating the competitive marketplace with inequitable rules. For instance, privacy can be implicated by offline practices just as much as in online environments. Proposed privacy legislation at both the state and federal level, however, often ignores the former while regulating the latter. A comprehensive approach to privacy must focus on both offline and online privacy and must seek to avoid wherever possible artificial distinctions.

The Electronic Privacy Communications Act starkly illustrates the problems created by privacy laws that are oriented toward technologies rather than baseline standards. Enacted in 1986, ECPA made assumptions about a static technology marketplace that bears little resemblance to the way in which individuals communicate, interact, and engage on the Internet in 2010. The advent of "cloud computing" – where users store their data with online providers and access them via the Internet – is leading to a vast migration of data from personal computers, filing cabinets, and offices to remote third-party servers. ECPA, however, affords lesser protections to e-mail communications based on where messages are stored, whether messages have been opened, and how long messages have existed. Such distinctions belie consumer expectations concerning the privacy of e-mail communications. The Digital Due Process Coalition, of which Google is a leading member, has proposed ways to update ECPA to ensure that its privacy protections are consistent with privacy expectations.

In addition, state laws occasionally impose rigid technology mandates that embody a "checklist" mentality to privacy and data security that stymies innovation and does not serve online users. In Nevada, for example, a business entity that either transfers "personal information" outside of its secure system or moves storage devices containing personal information beyond its physical or logical boundaries must use encryption to protect this information. Even if less expensive and more effective technologies become available, Nevada statutorily prohibits businesses from deploying such technologies to protect personal information. If, however, a business accepts payment cards from Nevada residents, the business must comply with the current version of the Payment Card Industry Data Security Standard, which does not necessarily mandate encryption. In a borderless environment such as the Internet, it is often impossible to ascertain the state residency of a specific user, much less deploy a specific technology solution based on nuances in state laws. Although well-intentioned, these laws often provide few appreciable benefits to consumers while imposing substantial burdens on and creating significant legal risks for Internet companies.

As we outline below, the Department can play a vital role in bringing greater consistency and comprehensiveness to domestic privacy regulation by formulating a usable, pro-innovation, pro-consumer framework for privacy together with the ongoing efforts at the FTC and in Congress.

International Privacy Regulation

Inconsistencies in the international patchwork of data protection rules have economic costs and impact free expression without corresponding benefit to user privacy

Economic cost

It is difficult to quantify the economic impact of inconsistent privacy regulations, but there can be little doubt that the growth of online, data-intensive services will suffer. Information, when collected and used responsibly and transparently, can offer tremendous value to users. Google, for instance, has used non-personally-identifiable data collected from users of our search service to add new features – such as spelling correction and suggested results – and to develop entirely new services, such as Flu Trends. Google engineers discovered that certain search terms are good indicators of flu activity, and developed Google Flu Trends using aggregated Google search data to estimate flu activity. This allows health officials, the media, and the public to learn about local flu outbreaks sooner than using traditional public health methods. Researchers have used Google Trends data and other sources like Twitter to develop economic trend data ahead of official numbers. The value of innovative services like this would be lessened or lost completely by rigid or inconsistent data protection rules.

Researchers have drawn similar conclusions. Canadian and U.S. academics recently found that E.U. data protection laws reduced effectiveness of online advertising, as measured by purchase intent, by over 65% compared to other countries. While there may be important user benefits to more restrictive data use policies not addressed by this study, policy makers should take a close look to determine if user privacy can be protected at lower cost to business and innovation.

The difficulties and costs of international compliance are most obvious for global cloud-based providers. Cloud computing providers, including Google, allocate storage and processing resources in the network as efficiently as possible through an essentially global infrastructure of data centers. The most prominent international data protection laws were, in contrast, developed in an era of bulk data transfers, stable databases, and location-specific processing. The Department should work with its international colleagues toward a unified and flexible set of multilateral agreements and national standards that preserve user privacy and trust and encourage the growth of the cloud.

Impact on global free expression

Google acts every day to promote and expand free expression online and increase global access to information. As new technology empowers individuals with more robust free expression tools and greater access to information, we believe that governments, companies, and individuals must work together to protect the right to online free expression.

Strong privacy protections must be crafted with attention to the critical role privacy plays in free expression. The ability to access information anonymously or pseudonymously online has enabled people around the world to view and create controversial content without fear of censorship or retribution by repressive regimes or disapproving neighbors. While we cabin this right

in important ways – including individual liability for defamation or harmful speech – it is invaluable to the ability to exercise freedom of expression.

As the Web evolves, free expression can be affected by rigid application of access rights and mandated opt-in policies for information collection. For more than a decade, scholars such as Fred Cate have discussed the potential tension between the U.S. First Amendment protection of free information flow and some international models of data protection. Moreover, while appropriate in certain circumstances, broad opt-in requirements can create perverse incentives for companies to collect more identifying information than necessary and to obtain "consent" in inappropriate or confusing ways. If all online behavior were traced to an authenticated identity to preserve proof of consent or allow rights of access, the free expression afforded by anonymous web surfing would be jeopardized.

International privacy rules have unfortunately been applied in ways that implicate free expression rights. As we have recently seen in several different cases, liability for third party intermediaries under data protection law in some countries remains unclear. An Italian court recently held three Google executives criminally liable for a user's uploading of an illegal video – a result at odds with widely accepted theories of intermediary liability in the U.S. and elsewhere. As the Center for Democracy and Technology noted in a recent report:

> Protecting intermediaries from liability is critical for preserving the Internet as a space for free expression and access to information, thereby supporting innovation and economic development goals. User-generated content sites in particular have become vital forums for all manner of expression, from economic and political participation to forging new communities and interacting with family and friends. If liability concerns force private intermediaries to close down these forums, then the expressive and economic potential of [information and telecommunication] technologies will be diminished. Governments everywhere should adopt policies that protect intermediaries as critical actors in promoting innovation, creativity and human development.

Different interpretations of third party liability create uncertainty, provider risk, and threats to free expression that chill innovation and growth of Internet services.

International harmonization

Compliance with differing standards imposes costs without obvious user benefits. International data protection law is far from harmonized, and attempts to improve consistency have been disappointing. The European Commission directive on data protection has been implemented variously in the member states, and interpretation of national law by data protection authorities have created even greater variations. Global companies that operate in Europe are subject to different compliance regimes in each of the Commission's 27 member states. Many such countries require elaborate filings and prior approvals for data transfers – even when using a mechanism that has been pre-approved by the European Commission. As noted in one recent paper, "The International Law Commission (ILC) has stated that 'the international binding and non binding instruments, as well as the national legislation adopted by States, and judicial decisions reveal a number of core principles' of data protection; however, it is doubtful whether such principles have won broad recognition among States."

The Department of Commerce's experience with negotiating and maintaining the U.S./EU Safe Harbor Framework and its leading role at Asia Pacific Economic Cooperation makes it the appropriate United States Government agency to lead the U.S. in discussions toward greater global privacy harmonization. Moreover, the Department can encourage global recognition of the real strengths of the current U.S. system of "on the ground" enforcement and flexible standards.

We encourage the Department to play a leading and active role in establishing a global privacy framework that encourages innovation and allows for the global flow of data. There is widespread recognition that industry and users need a widely accepted and practical international standard of privacy protection if online commerce is to flourish. The APEC Privacy Framework is a good step toward helping member countries develop privacy laws and regulations that achieve effective privacy protection and continuity for cross-border information flows. We encourage similar efforts to create a set of global privacy principles.

Similarly, the Organization for Economic Cooperation and Development is this year marking the 30th anniversary of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The review of these Guidelines, which have served as the foundation for virtually all privacy laws around the world, offers another important opportunity for the Department of Commerce to lead a thoughtful effort to continue protecting privacy through the harmonization of standards and the enhancement of mutual recognition among member countries.

Towards a Comprehensive, Baseline Privacy Framework

The Department should develop and encourage the adoption of a comprehensive framework for unifying legal standards and creating a platform for responsible innovation

The solution to the challenges posed by existing incomplete and inconsistent privacy standards is a unified, comprehensive, and flexible privacy framework that can encourage harmonization of law and multilateral agreements on data transfers and enforcement. Developing such a framework will be a long process and we look forward to working closely with the Department on this issue. To begin, however, we can articulate several foundational characteristics of such a framework.

It must be comprehensive

To protect users and offer consistency to providers, the privacy framework must cover all collection and use of data, all providers, and all manner of privacy harms. While not a complete list, the framework should include the following:

- **Even-handed application.** A pro-innovation privacy framework must apply even-handedly to all personal data regardless of source or means of collection. Thus, offline data collection and processing should, where reasonable, involve similar data protection obligations.

- **Recognition of benefits and costs.** As with any regulatory policy, it is appropriate to examine the benefits and costs of regulatory initiatives in this area, including explicit

attention to actual harm and compliance costs.

- **Security.** We pride ourselves at Google for industry-leading security features, including use of encryption for our search and Gmail services. The privacy framework should promote reasonable security principles – developed under evolving standards formulated by responsible industry actors and experts and reflective of current best practices. This will offer users a consistent, dependable and enforceable level of protection while offering clear, flexible guidelines for providers.

- **Clear process for compelled access.** As we have discussed above, the U.S. law governing government access to stored communications is outdated and out of step with what is reasonably expected by those who use cloud computing services. The problems in the law threaten the growth, adoption, and innovation of cloud technologies without a corresponding benefit. As part of the Digital Due Process coalition, we are working to address this issue. A privacy framework should also include clear rules for civil litigant and other compelled access.

It must be a baseline on which providers can innovate

Perhaps most importantly, a pro-innovation privacy framework offers providers the flexibility to both develop self-regulatory structures and individually innovate in privacy practices and tools. The advertising industry and online publisher efforts to develop self-regulatory rules for interest-based advertising (IBA, for short), for example, are a strong example of the need for and utility of industry-driven efforts.

Beyond cooperative industry efforts, baseline, principles-based rules give room for individual providers to innovate in the privacy space. Google, for its part, offers a number of industry-leading privacy tools:

- Prior to the industry IBA effort, for instance, Google launched its own IBA product with a number of groundbreaking privacy features in place. Google's interest-based ads contain notice in the actual advertisement indicating that it is a Google advertisement. The in-ad notice is linked to information about IBA, including our Ads Preferences Manager, which allows users to change the interest categories used to target ads or to opt-out of interest-based advertising altogether.

- Google also offers leading options for data portability. For Google, providing our users with control over their personal information must also mean giving them the ability to easily take data with them if they decide to leave. Starting with our Gmail service and now covering more than 25 Google products where users create and store personal information, our "Data Liberation Front" allows our users to "liberate" data if they choose to switch providers or to stop using one of our services.

- Google developed the Google Dashboard to provide users with a one-stop, easy-to-use control panel to manage the use and storage of personal information associated with their Google accounts. With the Dashboard, a user can see and edit the personally identifiable data stored with her individual Google account.

As noted above, more information on our innovative privacy tools is available in the attached comments, which we recently filed with the FTC.

Continued innovation in the privacy space is vital for users. Unfortunately, compliance-based rules can lock providers into a specific privacy model. A principles-based model encourages innovation and competition in privacy tools.

A baseline framework needs to encourage the development of innovative tools like these. We believe that stable, baseline principles set by regulation can permit flexible, adaptive structures to develop on top – much like the stable protocols and standards at the physical and network layers of the Internet allows flexible and innovative development at the content and application layers. With comprehensive, baseline privacy legislation establishing ground rules for all providers, self-regulatory standards and best practices of responsible industry actors will evolve over time. On top of that structure, individual providers will be free (and encouraged) to create innovative privacy tools and policies rather than stick with potentially outdated compliance structures.

How the Department can lead

The Department can lead in several important areas including the following:

- **Leverage its intra- and inter-agency competencies.** The Department is well-positioned to draw from relevant expertise at NTIA, ITA, and NIST. It can also take this expertise to help develop a privacy framework and inform the ongoing efforts at the FTC and in Congress.

- **Continue to work with international partners.** The Department should continue working with national data protection authorities as well as other foreign agencies and representatives to build international consensus around a privacy framework that recognizes the value of data and the need for consistency and, where consistency cannot be achieved, mutual respect and recognition.

- **Draw from experience and promote dialog.** The Department has a long history of seeking neutral economic and technological evidence. It should draw on this expertise to encourage innovation and competition in pro-privacy tools; to support and develop objective forums for gathering, analyzing, and reporting data on economic impact of privacy regulation; and to host discussions involving government, industry, and non-governmental organizations about emerging technology and associated privacy issues.

* * *

Google thanks the Department for this opportunity to comment, and urges its continued involvement in the privacy space. The Internet, cloud services, and data innovation will drive the U.S. and world economies for years to come. Just as the Department showed global leadership in early Internet regulatory policy, it should lead in the creation of sensible and strong baseline privacy principles. Google stands ready to assist the Department in these and any other efforts to help develop and implement a comprehensive, baseline framework for privacy.

Sincerely,

Pablo L. Chavez
Director of Public Policy
Google Inc.

Attachment: Comments of Google Inc. in FTC Privacy Roundtable Project