U.S. Department of Commerce
Information Privacy and Innovation in the Internet Economy
Docket No. 101214614–0614–01

Via electronic filing: privacynoi2010@ntia.doc.gov
January 28, 2011

Comments of Google Inc.

Google thanks the Department of Commerce for the opportunity to comment on its report "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework." Google supports the concept of a Dynamic Policy Framework as set out in the Department's report. Our comments address the following key issues to be addressed as it moves forward with the implementation of the framework:

- **Effective protection of consumer privacy must encourage continued innovation and competition in the online marketplace generally and the development of privacy solutions and tools in particular.** Consumers and the American economy have reaped breathtaking benefit from the innovative use of data -- from search, to email, to social networking, to mobile. We have also witnessed welcome innovation in the protection of consumer privacy. Just this week, major browser companies launched tools designed to improve users' control over data use in online advertising -- including Google's Keep My Opt-Outs extension, which enables users to permanently opt out of interest-based advertising. Promoting the continuation of this innovation must be the primary goal of policymakers. As privacy scholar Ryan Calo recently wrote, "Privacy has nothing to fear from innovation."

- **A Dynamic Privacy Framework requires a comprehensive set of fundamental privacy principles and seeks to eliminate substantive inconsistencies in application between technologies, regulations, and international regimes.** While fundamental principles underlie most U.S. and international data protection law, in practice these various regimes and sectoral rules sometimes lead to inconsistency, rigidity, and privacy by form and not substance. These problems, for example, are slowing the growth of online "cloud" services, without corresponding benefit to consumers. We encourage the Department to develop a comprehensive framework to encourage consistent protection of privacy and increased trust in data-based services.

- **The Department of Commerce, in consultation with other departments and agencies, must lead.** The Department has the expertise, position, and ability to develop this baseline policy framework, educate consumers and industry, and provide guidance and a forum for the development of technological standards and industry codes. The Department must also represent the U.S. internationally to ensure that cross-border data transfer rules protect consumers without unnecessarily impeding the free flow of information, creating barriers to international trade, or

hurting the competitiveness of U.S. businesses.

In this submission, Google first offers a few general comments related to fundamental principles that should inform further policy development in this area. We then comment specifically on some of the recommendations and questions raised in the Department's report.

I. Key Characteristics of a Dynamic Privacy Framework

A. The primary goal of a Dynamic Privacy Framework should be to protect consumers while encouraging continued online innovation.

The U.S. government has historically been careful not to impose rules on Internet activity that would stifle pro-consumer innovation, and for good reason. Innovation has transformed the Internet from a limited tool for government and academic research into a platform for global commerce, social networking, political engagement, and individual creativity. Overly complex or rigid regulatory regimes, including those based on technological mandates, thwart the ability of companies to develop new services and tools, and in turn make U.S. Internet companies less competitive globally and make the Internet a less robust medium.

Moreover, it is important to recognize that an anti-innovation framework would counterproductively choke off the development of new tools and services to protect personal privacy. The fast-paced introduction of new Internet services drives equally rapid shifts in consumer expectations and preferences. An effective privacy regime must allow for realtime reactions to address changes in consumer privacy preferences resulting from the introduction and adoption of new tools and services. Particularly in the Internet environment, technological solutions are often more efficient and effective than regulatory ones. CAN SPAM, for example, created important tools in the fight against unsolicited and unwanted commercial e-mail, but technology solutions -- not regulation -- are largely responsible for the dramatic decline in the amount of SPAM that reaches consumer e-mail inboxes. Similarly, just this last year, protection of Internet communications has advanced significantly by the development and deployment of technologies such as SSL encryption tools, including by Google across its services.

As the Department's Green Paper reiterates, a combination of government-established baseline principles and sector-specific self-regulatory implementation will best protect personal information in the commercial context and deliver meaningful transparency, control, and security for Internet users. The benefits of such an approach are already visible in the multiple tools being developed by the private sector, informed by government guidance and enforcement, to address consumer concerns about online behavioral advertising.

Accordingly, Google welcomes the Department's basic policy recommendation that the government should work with all stakeholders to establish baseline Fair Information Practice Principles (FIPPs), and then provide guidance and incentives for industry to respond to consumer demands as technology and user expectations evolve. This approach is in keeping with the OECD National Implementation guidelines that call on countries to adopt appropriate domestic legislation and encourage and support self-regulation -- backed up by government enforcement where appropriate.

Yet in developing this framework, the government and all stakeholders must understand that consumer-facing companies like Google have powerful market incentives to protect user privacy, and must respond to user demands in order to remain competitive. Google receives and uses data foremost to provide our users with better and more useful services. Conversely, we understand that we will lose those same users' trust if we collect or use personal information in a manner that is non-transparent or contrary to their preferences.

After all, our competition is always just one click away. Google's business therefore depends in large part on its ability to innovate in a manner that delivers value to end users, responds quickly and flexibly to shifting consumer demands, and respects consumer concerns and expectations regarding the collection and use of personal information.

A Dynamic Privacy Framework should set a baseline, industry-wide level of privacy protection, but always preserve the ability of a user-facing service to respond and compete through innovation. Indeed, current market examples demonstrate that industry has already been responding to consumer concerns about data privacy designing products and services based on the principles of transparency, choice, and control. As we described in our earlier submissions to the Department and to the Federal Trade Commission, in just the last couple years, Google has developed:

- A privacy Dashboard that gives users with a one-stop, easy-to-use control tool to manage the use and storage of personal information associated with their Google accounts.
- An Ads Preferences Manager tool that empowers users to review and edit the interest categories associated with their browsers or opt-out of interest-based ads completely and permanently.
- Industry-leading privacy and security technology, including encryption of email by default and the option to encrypt search queries.

And we have continued to innovate. Just this week, Google launched the Keep My Opt-Out extension, which enables users to permanently opt out of ad tracking or serving targeted ads from all companies participating in industry self-regulation opt-out programs. What's more, Google has released the code on an open-source basis, so that other developers can examine, assess, enhance, or even extend the code's capabilities. We'll also be developing versions that work on other major browsers.

Moreover, vibrant competition in the marketplace has produced a wide array of privacy-protection options. For example, while we are proud of the privacy features of our search service, some engine providers openly compete on the basis of privacy considerations. There is also a large and growing group of privacy tools, including browser plug-ins, that are available to enable users to delete cookies, block online tracking and opt out of online ad networks to varying degrees. Indeed, the *Wall Street Journal* recently reported that venture funding has spotted the market demand for privacy protection technology and is flowing to privacy-related start-ups. Finally, the development of voluntary industry codes and standards, including by the Network Advertising Initiative and the Digital Advertising Alliance, demonstrate that companies are taking concrete steps to address these issue on a industry-wide basis.

Government has a critical role to play in developing a baseline policy framework, educating consumers, providing guidance and a forum for the development of voluntary industry codes, and holding companies accountable for actions that harm consumers. As we discuss below, there are also opportunities for government to drive immediate, consensus improvements to current privacy laws. Government must, however, ensure that its efforts to deliver strong consumer privacy protection are designed to encourage the innovation and competition that have characterized the online marketplace generally and the development of online privacy tools in particular.

B. Inconsistent or conflicting regulations -- both here and internationally -- undermine the benefits of a national Dynamic Privacy Framework by creating unnecessary barriers to innovation and trade.

Inconsistent, overlapping privacy laws and regulations undermine consumer privacy by creating consumer

confusion, imposing inefficient compliance costs on companies striving to compete in the global marketplace, and erecting barriers to efficient service provision and cross-border trade. This has been true since the emergence of the commercial Internet, but becomes far more significant as increasing amounts of data are collected and stored in cloud-based applications. A Dynamic Privacy Framework can and must be used to promote mutual recognition of industry and country specific implementation of fundamental privacy values and to eliminate formalistic inconsistencies, including as between technologies, sectoral laws, state regulations, and international regimes, that impede the free flow of data on the global Internet and irrationally constrain competition and innovation.

First, the framework must be set out in a manner that applies neutrally and comprehensively, without regard to specific technologies, industries, or business models. It is vitally important that we do not create a rigid baseline regulatory regime that atrophies as technology and business evolves, thereby ceasing, over time, to provide adequate privacy protection. Such a regime also stifles the evolution of new socially or economically valuable services and results in a loss of potential consumer benefit, economic growth, and job creation. Instead, the situation calls for a set of comprehensive, flexible baseline principles that can be implemented in manner that is neutral to choice of technology and business model.

Second, in the U.S. there is a need to address inconsistencies created by overlapping state regulations, which impose significant costs on businesses without delivering commensurate benefits to consumers. In particular, Google appreciates the Department's recognition of the need for a uniform breach notification regime in the U.S., which is specifically discussed later in this submission.

Third, the U.S. government must work to ensure that international cross-border data transfer rules protect consumers without unnecessarily impeding the free flow of information, creating barriers to e-commerce, Internet cloud services, and other forms of international trade, or undermining U.S. competitiveness. The U.S. government should pursue an affirmative negotiating agenda to promote international acceptance of this principle. In particular, U.S. business is critically dependent upon the government to ensure that foreign governments regulate in a technology-neutral manner, understand the substantive protections offered by the U.S. approach to privacy, provide mutual respect and recognition of those protections, and eliminate the procedural barriers that deliver little in the way of substantive privacy protection but make compliance expensive, dependent upon elaborate filing and approval systems, and subject to inconsistent and sometimes extremely burdensome formal standards and highly subjective interpretation from country to country.

Both the OECD and APEC privacy frameworks already recognize that formal harmonization is not a necessary prerequisite to ensuring substantively equivalent levels of protection to consumers where data is transferred across borders. Google believes that the Department is ideally suited to provide the leadership necessary to advance U.S. interests in the ongoing work at APEC and at the OECD, and in connection with the revision of the EU Privacy Directive now underway.

The development of processes to facilitate transborder data flows based on the APEC Privacy Principles provide a particularly important opportunity to demonstrate that a regime allowing for the free flow of data across borders on the basis of shared principles and mutual respect for various implementation mechanisms can deliver strong privacy protection. The processes and procedures for implementing the APEC Privacy Pathfinder projects to facilitate cross-border data flows are to be submitted for Ministerial endorsement at the U.S.-hosted Ministerial in Hawaii in 2011. Google actively participates in and supports this work, and urges the U.S. government to continue to press for APEC's adoption of flexible mechanisms that leverage existing national or self-regulatory efforts, supported by the authority of U.S. regulators to enforce Section 5 of the

Federal Trade Commission Act's prohibition of unfair and deceptive acts and practices in commerce.

C. The Department is in the best position to the lead the development of a Dynamic Policy Framework.

Google urges the Department of Commerce, in consultation with the FTC and other departments and agencies, to lead the U.S. government's efforts to develop domestic and international privacy policy effort. The Department has a unique, dual role -- as a leader in developing a sound domestic privacy regime the protects privacy and innovation, and as a strong advocate internationally for a seamless and sensible trans-border data flow regime.

The Department has a demonstrated track record of success in providing domestic leadership regarding regulation of online commerce. In the 1990s, the Department was tasked with a leadership role in the federal government's e-commerce activities, spurring and encouraging responsible private sector leadership on issues such as domestic and international privacy, private international law, and Internet governance. Moreover, the proposed Privacy Policy Office would be ideally suited to draw seamlessly from the international negotiating and substantive expertise across the Department, including in ITA, NTIA and NIST, as well as the entire Executive Administration, to develop and implement the enhanced domestic privacy framework envisioned in the report. As it demonstrated in the late 1990's in the context of privacy, the Department can effectively bring its expertise to the table, and convene commercial and civil society actors in problem-solving mode.

As the Department's report also recognizes, the FTC -- as the primary privacy enforcer for most industry sectors -- must play a key role in a FIPPs-based privacy framework. In particular, FTC enforcement ensures that private sector practices and standards adequately prevent harm to consumers from unfair and deceptive trade practices and that service providers live up to their promises. In contrast, state enforcement agencies and NGOs -- while important stakeholders -- should not have overlapping enforcement authority that leads to inconsistency or dilution of the FTC's role.

II. Specific Comments on the Architecture of the Dynamic Privacy Framework

A. Fair Information Practice Principles

Google strongly supports the development of a comprehensive privacy framework for commercial actors, based on FIPPs, that create a baseline for privacy regulation that is flexible, scalable, and proportional. As the Department and stakeholders begin to develop a set of FIPPs applicable to commercial data, Google urges policymakers to take account of a few key overarching issues.

First, even as the Department focuses on enhancing the current U.S. privacy regime through the iteration of a set of comprehensive and binding baseline FIPPs, it is important to recognize that the U.S. has long grounded privacy law, regulation, and self-regulatory mechanisms in widely accepted fair information practices. The FTC measures commercial behavior against privacy principles issued in a 1998 report. Legislation, such as Gramm-Leach-Bliley, HIPAA, the Fair Credit Report Act, among others, are all industry-specific articulations of basic fair information practice principles. Private sector privacy policies are similarly build around baseline principles of notice, choice, compatible use, access, and security, and are enforceable under Section 5 of the FTC Act. While the articulation of a fresh, formal FIPPs-based comprehensive framework is a necessary step to provide clarity, uniformity, and a platform of trust for consumers, it is not a radical departure in practice from the current U.S. privacy protection regime.

Second, we must acknowledge that all data derived from individuals, whether personally-identifiable data or not, deserves some manner of protection. But rather than apply identical protections to both categories of data, it is important that any set of comprehensive FIPPs allows for tailored applications that are properly calibrated to fit the different types and uses of the wide range of data that are collected. In particular, FIPPs must be flexible enough to take account of the spectrum of identifiability, linkability, and sensitivity of various data in various contexts. For example, access and correction rights are very relevant where data such as date of birth, income or physical characteristics are being used to make eligibility determinations. But access and correction rights are far less relevant where the consequences of reliance on incorrect or incomplete information are minimal, and make no sense where a service provider cannot be sure that the user seeking access is the data subject, such as unauthenticated search query logs. (For a detailed discussion of different data and data use contexts, see Hordern, Victoria, Finding Space For a Third Category of Data, BNA International World Data Protection Report, February 2010).

Third, FIPPs must be appropriately tailored and relevant for their intended use -- in this case, to guide the treatment of personal information by commercial entities. The Department's report refers to the DHS FIPPs as an example of a set of privacy principles, but it is important to recognize that the DHS FIPPs were designed to guide *government* fair information practices. Thus, for example, DHS's statement of purpose specification and data minimization are necessary to address constitutional mandates and legal requirements, including the Privacy Act, that are not directly applicable in the commercial environment. Some of the specific formulations in the DHS FIPPs make sense in that context; the need to ensure data quality and integrity (and the possible consequences of misidentification or mistake) is much more urgent where the data in question is used to combat terrorism and protect national security, as compared, for instance, to serving online advertising.

The OECD Guidelines and APEC Principles, by contrast, were developed with the commercial sector in mind, and incorporate important statements regarding the need to achieve the multiple objectives of protecting personal information, allowing for innovation, and respecting cultural and other diversity considerations. They therefore offer a better starting place for the development of a domestic commercial data privacy regime. For example, the APEC "preventing harm" principle recognizes that the focus of a commercial privacy framework is to prevent wrongful collection and misuse of information, not to otherwise limit legitimate and economically or socially valuable uses of data. Accordingly, the APEC principles related to transparency, collection, and use also reflect the nature and range of consumer interests and commercial uses.

* * *

In addition, we offer a number comments on the principles that the Department has highlighted for particular focus in its report.

1. Transparency

The transparency principle that the Department discusses in its report reflects the fundamental notice and choice rubric that characterizes all privacy frameworks. The question in designing a FIPPs regime is how to provide guidance so that these basic principles can be made effective in a particular context.

The discussion about "enhanced notice" underway in many fora is, in our view, really a discussion about ensuring *effective* notice. Similarly, some FIPPs regimes also incorporate a distinct "individual participation"

prong that can be primarily addressed in the context of affording meaningful choice and providing appropriate levels of access and the ability to correct information.

In Google's experience, effective notice is the key to any well-functioning privacy regime because it allows users to understand, and hopefully become comfortable with, the kind of information being collected and how it is used. Effective notice can actually alleviate consumer harms related to concern or anxiety about an organization's data practices. Recent data about how consumers use Google's Ads Preferences Manager tool, for instance, indicates that for every unique user who opts out, more than seven remain opted in. These data, similar to that in other consumer research, indicate that users curious about their privacy options are more likely to stay opted in once they understand how their data is being used.

For notice to be effective, however, it needs to be clear, conspicuous, and most importantly, relevant to the use of the product or service. At Google, we have worked hard to ensure that our privacy notices reflect our actual practices and communicate the information in easy to understand formats -- including through a simplified written privacy policy, videos and FAQs -- and to organize it all under a single Privacy Center. In addition, we work to offer notice right where it is relevant -- such as by an icon in an advertisement, or right at the point of installing a new service or application.

A transparency principle must leave room for companies to experiment with creative solutions to make privacy notices effective, particularly as services and technology continues to evolve. Consumers are ill-served by a regulatory regime that values rote compliance over innovation, or pressures companies to "overlawyer" their privacy policies and notices or lock in litigation-tested messaging and delivery mechanisms rather than experimenting with new content or new ways to inform and empower consumers.

The Department has also asked a specific question about the role that privacy impact assessments (PIAs) in particular could play in advancing the objective of transparency. In Google's experience, PIAs should be, and in most cases are, an important aspect of any responsible company's internal practices. This has long been Google's practice, and, as Google explained in a recent blog post, it has implemented changes that will make its internal privacy assessments more rigorous and more effective. Specifically, (1) every engineering project leader will be required to maintain a Privacy Design Document to record how user data is collected and managed, and (2) these documents will be reviewed regularly by managers and an independent internal audit team. But the very characteristics that make privacy impact assessments valuable for internal purposes make them ill-suited to contribute to the transparency objective. PIAs are complex, detailed technical documents that present the same problem (to an ever greater degree) as privacy policies that are rarely read by consumers. (In fact, it is a challenge to get users to take the time to read privacy policies even when they are kept short and clear, as Google has sought to do.) Thus, while we strongly agree with the importance of improving the effectiveness of transparency mechanisms, our experience suggests that publication of PIAs is not likely to advance that goal.

2. Purpose specifications and use limitations

Google applauds the Department's recognition that a privacy regime should protect users without stifling innovative uses of data. Creative, even serendipitous re-use of collected data has enabled enormous advances in online products and services that enable creativity, education, the creation of businesses, and deeper social and political engagement. In Google's experience alone, purpose-compatible re-use of existing data has delivered enormous value to Google users and led to product improvements such as Gmail's priority inbox, automated spell checking, auto-complete, spam, fraud and virus protection tools, and the development of

new services such as FluTrends and Translate. Mechanistic or overly prescriptive purpose specifications, data minimization and collection limitations, or use limitations would frustrate such economically and socially valuable innovation without protecting consumers from harm.

The issue in designing these principles it how to achieve both innovation and consumer protection. A key factor in achieving this objective is role of provider-consumer relationships in reducing the potential for consumer harm. When a user has a direct relationship with a provider, and can easily jump ship if the provider violates the user's trust or fails to offer a valuable service, the fact of the relationship can give the user assurance that her data will be used responsibly. In this instance, rigid data minimization or use restriction principles can actually frustrate the user's interest in innovative, cutting-edge services. In contrast, a data minimization or use restriction principle based on a "directly relevant and necessary" standard may be appropriate where the data processor is a government or does not have any relationship or interaction with the data subjects.

It is also important for a data minimization principle to account for situations where services are collecting and storing data *on behalf of users*, such as email or online documents. In these cases minimization becomes a matter of user choice and should not be subject to arbitrary regulatory restrictions.

3. Auditing/accountability

Google agrees with the Department's observation that auditing and accountability play a critical role in any privacy regime. In particular, these mechanisms contribute to the development of the user trust that is necessary to engage with a given service. Accordingly, many industry bodies include such auditing and reporting functions. The Network Advertising Initiative members, for example, are now audited for compliance with the Self-Regulatory Code of Conduct. In addition, while an individual company's privacy policies may not be read by every user, they are an important internal tool for achieving organizational accountability to the FTC, state attorneys general, and other regulators.

Indeed, the FTC has its own inquiry authority, even absent evidence of a violation, and its investigatory authority also serves what is effectively an audit function. As its track record demonstrates, the FTC utilizes its existing authority to ensure that companies are abiding by their fair information practice obligations and representations.

B. Enforceable voluntary industry codes

Effective FIPPs can create a powerful baseline framework for privacy and continued innovation, but in order to be generally applicable, they cannot provide the specific guidance needed for detailed implementation and enforcement in individual industry contexts. However, Google supports the Department's recommendation that the Dynamic Privacy Framework should generally accommodate and defer to enforceable codes of conduct and standards that are developed by individual industries and can be adjusted in cooperative settings to reflect changing practices, technologies and shifting consumer expectations. While self-regulation is no panacea, the benefits of such a regime are evident in the context of, say, social networking or mobile advertising -- where technology and services are evolving so rapidly that a solution imposed by legislation or regulation would be outdated as soon as it was agreed, and difficult and costly to revise.

The Department poses specific questions that relate to how government might encourage the development of these codes. Google considers that there are three key mechanisms that government can employ to facilitate and incentivize the development of effective industry codes.

First, the Department (including through a newly created Privacy Policy Office) -- alone or in conjunction with relevant enforcement agencies such as the FTC -- can convene working groups and synthesize recommendations to provide clear guidance on industry-specific measures needed to protect consumer privacy in a particular context or industry, and to update those recommendations as technology evolves. For this approach to be effective, however, the regulators must participate as an open-minded convener without preconceived assumptions as to the best outcome; otherwise, the process is merely government-driven regulation by another name.

Second, regulators should should be willing to defer to effective self-regulatory organizations on enforcement matters where a company commits to abide by enforceable codes of conduct. In fact, these "safe harbors" need not be the product of legislation: the FTC and other enforcement agencies can create an equally effective "carrot" by providing clear guidance on how it will handle enforcement inquiries involving entities participating in enforceable codes and standards (unless, of course, the code enforcement entity fails to act, or refers a matter to the FTC's attention).

Third, if a "safe harbor" is the carrot, then the enforcement authority of the FTC is the stick. The FTC has already used its authority effectively, even in the absence of formalized FIPPs, to punish bad actors, enforce privacy promises, and send important signals about evolving standards for proper notice, choice, consent and data security. (For further discussion of the effective enforcement role played by the FTC , see Bamberger and Mulligan's recent study of "privacy on the ground.") The agency has the ability through its various procedures to communicate its expectations clearly, effectively, and prospectively. It also has the ability to ensure that companies abide by their commitments to self-regulatory codes of conduct (and that those mechanisms function as promised to protect consumer privacy), and protect consumer privacy even where they choose to remain outside a voluntary code. –

A private right of action, by contrast, is an enforcement tool that, while sometimes necessary, has the potential to seriously curtail innovation and slow economic growth. Such an enforcement tool should only be considered in contexts where there are significant, tangible harms to individual users that cannot be adequately addressed by existing regulatory enforcement.

C. Role for Legislation

1. Codifying the Fair Information Practice Principles

Google continues to support the passage of a comprehensive federal privacy law that would codify a baseline set of FIPPs to serve as the foundation upon which standards-setting, specific rules, and self-regulatory efforts could build. Comprehensive legislation that establishes a uniform framework for privacy protection in the United States is a key component of the broader effort to facilitate consumer trust and mutual recognition of national implementation in support of cross-border data flows. Given the importance of advancing the development of a Dynamic Privacy Framework, however, the Department need not and should not wait for legislation. Rather, the government should move forward to work with industry and civil society to jump-start the development of FIPPs, stakeholder convenings, and other progress envisioned in the Green Paper.

2. Standard Breach Notification

While the overall variation in state privacy laws create compliance problems for companies, one of areas in which preemptive federal legislation is needed is with respect to security breach notification requirements. As

the Department recognized in its report, there is wide agreement on this recommendation. Google supports the standard set out last year in H.R. 2221, which the House of Representatives passed in the 111th Congress. A bill along the lines of H.R. 2221 would ensure that consumers are notified when a security breach creates a reasonable risk of identity theft, fraud, or other unlawful conduct.

3. ECPA Reform

As Google previously commented in response to the Department's Notice of Inquiry in this matter, there is an immediate need for legislation to update the Electronic Privacy Communications Act. That law, enacted in 1986, makes assumptions abut a static technology marketplace that bears little resemblance to the way in which individuals communicate, interact, and engage on the Internet in 2011. For example, ECPA affords lesser protections to email communications based on where messages are stored, whether messages have been opened, and how long messages have existed. While those distinctions may have comported with assumptions at the time -- before the Internet was available for commercial use, and before advances in technology dramatically reduced the cost of electronic data storage -- they bear no relation to consumer expectations today concerning the privacy of e-mail communications. Moreover, the law undermines international trust in US-based cloud services and create confusion and cost for law enforcement and providers. As Google's Richard Salgado testified before Congress in 2010, "[b]y creating inconsistent privacy protection for users of cloud services and inefficient, confusing compliance hurdles for cloud providers, ECPA has perversely created an artificial and unnecessary disincentive to move to a more efficient, more productive business model."

There is also significant constitutional concerns about a law permitting government access to communications with less than a warrant. The Sixth Circuit Court of Appeals' recent decision in US v. Warshak, which held ECPA unconstitutional in this regard, provides even more impetus to revisit the outdated aspects of ECPA.

Thus, Google supports the proposals advanced by the Digital Due Process Coalition, of which it is a leading member, to update ECPA in a manner that ensures its privacy protections are consistent with privacy expectations and Constitutional requirements.

* * *

Thank you for this opportunity to comment. Google appreciates the opportunity to share its perspectives and experience with the Task Force with respect to privacy, as well as in other areas of inquiry.

Sincerely,

/s/ Pablo L. Chavez

Pablo L. Chavez
Director of Public Policy
Google Inc.