Written Testimony of Richard Salgado
Director, Law Enforcement and Information Security, Google, Inc.
Senate Judiciary Subcommittee on Privacy, Technology and the Law
Hearing on "The Surveillance Transparency Act of 2013"
November 13, 2013

Chairman Franken, Ranking Member Flake, and members of the Subcommittee, thank you for the opportunity to appear before you this morning to discuss the Surveillance Transparency Act of 2013.

As the Director for Law Enforcement and Information Security at Google, I oversee the company's response to government requests for user information under various authorities. I am also responsible for working with teams across Google to protect the security of our networks and user data. I have served as a Senior Counsel in the Computer Crime and Intellectual Property Section in the Department of Justice, and have taught and lectured on these issues at Georgetown University Law Center, George Mason University Law School, and Stanford Law School.

In September, Google joined a diverse array of companies, trade associations, and civil society organizations to express strong support for the Surveillance Transparency Act of 2013. The signatories to this letter include AOL, Apple, Facebook, LinkedIn, Microsoft, Twitter, and Yahoo! — all of whom, like Google, believe that service providers should be permitted to disclose basic statistics about Foreign Intelligence Surveillance Act demands that they may receive.

We commend Chairman Franken for introducing, with Senator Heller, the Surveillance Transparency Act of 2013 and for the leadership he has shown on this important issue. Transparency can and should play a critical role in the broader debate around substantive reforms that would address concerns raised by the government's use of existing surveillance authorities.

In my testimony today, I will make four principal points:

- **First**, recent disclosures concerning the extent of government surveillance undermine confidence in Internet services reliant on user trust, create significant risks for economic security and growth, and threaten to jeopardize the current global Internet governance

structure. These disclosures, however, provide a unique opportunity to revisit existing surveillance laws.

- **Second,** Google has long been committed to increasing transparency around government demands for user data. Lumping domestic and national security requests together in ranges in our Transparency Report, as the DOJ has proposed, would be a significant step backward for our users and the general public, who would receive less information than we disclose in our current Transparency Report.

- **Third**, companies' right to publish aggregate statistics about the nature and scope of government surveillance programs promotes a more open dialogue about reform without jeopardizing national security. Transparency is an essential component to inform the debate over broader reforms to our surveillance laws, and efforts to prevent companies from publishing statistics about national security demands hinder the debate.

- **Fourth,** transparency is only one step among many needed. It can and should be a critical part of broader reforms with the goal of ensuring that government surveillance programs are rule-bound, narrowly tailored, transparent, and subject to oversight.

Transparency Can Help Restore Trust with Users and Governments and Inform the Broader Debate Around Comprehensive Reform

The revelations about the U.S. government's and other governments' surveillance practices over the past few months have sparked a serious debate about the need to revisit the laws governing surveillance of private communications by the intelligence community. Google recognizes the very real threats that the U.S. and other countries face today, and of course governments have a duty to protect their citizens. The current lack of transparency about the nature of government surveillance in democratic countries, however, undermines the freedoms most citizens cherish. It also has a negative impact on our economic growth and security and on the ultimate promise of the Internet as a platform for openness and free expression.

In the wake of press reports about the so-called "PRISM" program, governments around the world have been considering ways to limit the impact of the U.S. government's and other governments' surveillance on their citizens. One way that some governments are seeking to achieve this goal is by limiting the flow of information over the Internet between their country and the U.S. However, the free flow of data globally is critical to ever-expanding amounts of economic activity throughout the world, and limitations on that flow could have severe unintended consequences, such as a reduction in data security, increased costs, decreased competitiveness, and harms to consumers. And the impact on U.S. companies, and the broader U.S. economy, could be significant. Two

reports, for example, estimate that the effect on U.S. companies may be in the tens of billions or even hundreds of billions of dollars.

One concrete example that Google, other companies in numerous industries, and civil society are grappling with is the movement towards so-called "data localization," which has gained considerable traction since the revelation of the PRISM program. As we speak, the Brazilian Congress, for example, is considering legislation that would require data relating to the Brazilian operations of both domestic and international companies — as well as Brazilian citizens — to be stored in Brazil. Companies like Google that do not comply with such a requirement could be barred from doing business in one of the world's most significant markets or be obligated to pay hundreds of millions of dollars in fines.

The impact of the revelations goes beyond the economic losses cited. They come at a time when many governments and other stakeholders are increasingly critical of the role the U.S. has played in safeguarding the free and open Internet through its support of the multi-stakeholder governance model, a model where the Internet is not governed only by states, but through institutions comprised of civil society, business, government and users. Today, calls for the Internet to be regulated by the U.N.-chartered International Telecommunications Union or other United Nations institutions and put solely under government control are louder than ever. At last month's Internet Governance Forum, a gathering of key Internet stakeholders in Bali, calls for limiting the role of the U.S. were significant and accompanied by proposals now under consideration.

These trends, both within individual countries and in broader international forums, pose a significant threat to the free and open Internet that we benefit from today. If data localization and other efforts are successful, then what we will face is the effective Balkanization of the Internet and the creation of a "splinternet" broken up into smaller national and regional pieces with barriers around each of the splintered Internets to replace the global Internet we know today.

Committing to more transparency by enacting the Surveillance Transparency Act would allow the U.S. to take a first step towards rebuilding trust. It would do so by clarifying for all stakeholders the number and nature of national security-related orders that companies like Google may receive, if any. If Google, for example, could publish those numbers as Google and other service providers have proposed — and as Chairman Franken's bill would allow — our users and the broader public would have a better understanding of our posture in response to any national security demands that we may receive, as well as the volume, scope, and type of such demands that we may receive.

Publishing the number of demands by legal authority and the number of users or accounts impacted would go a long way to putting the relationship between U.S.-based companies and the U.S. government into a more accurate perspective. And as I note later on in my testimony, we

believe that transparency is a critical part of the broader set of reforms that are needed in order to address the issue of government surveillance of the world's communications networks.

Google Has Long Been Committed to the Principle of Transparency as Part of Broader Efforts to Reform Surveillance Laws

Our interest in providing more transparency around government requests for user data long preceded the recent revelations about the government's use of its surveillance authorities. In 2010 we issued our first Transparency Report regarding requests for user data going back to 2009. The goal was to provide useful information to our users and the general public about such requests that we receive from governmental entities throughout the world. We were the first company to publish such data, and we applaud other companies that have released transparency reports.

We release our Transparency Report on a biannual basis, and we strive to surface new and useful information and data with each iteration. For example, for the second half of 2012, we broke down legal requests in the U.S. by type *(i.e.*, subpoena, search warrant, and other requests) for the first time, shedding more light on the nature of the information sought by governmental entities in the U.S. And, earlier this year, after long negotiations with the DOJ, we began providing more information about the volume and scope — albeit in broad ranges — of National Security Letters that we receive.

Transparency helps our users understand our practices, and it allows us to correct inaccurate characterizations of our posture in response to national security demands that we may receive. For instance, contrary to some initial media accounts, Google has not given the U.S. government or any other government access to Google's servers. Google refuses to participate in any program that requires it to provide the U.S. government or any other government with access to its systems or to install their equipment on Google's networks.

Transparency Reports Promote Reform Without Jeopardizing Security

Earlier this year, Google approached the DOJ about including aggregated statistics reflecting requests Google may receive under FISA as part of its normal transparency reporting cycle. Unfortunately, the DOJ refused, and has taken the position that providers cannot even acknowledge receipt of FISA orders, let alone publish aggregate statistics around national security demands that they may receive.

There are important First Amendment principles at stake. The DOJ's position that service providers can't publish data concerning national security demands is a prior restraint on speech.

Prior restraints, as the Supreme Court has held, carry a heavy presumption against constitutional validity under the First Amendment. Moreover, any blanket prohibition on the ability of providers to speak about national security demands that they may receive is a content-based restriction on speech. Like prior restraints, content-based restrictions are heavily disfavored. The government has to show that the prohibition on speech is narrowly tailored to support a compelling governmental interest; that is, that there are no less restrictive alternatives that would be at least as effective in achieving the government's objectives.

Accordingly, Google filed a Motion for Declaratory Judgment before the Foreign Intelligence Surveillance Court in June asserting a First Amendment right to publish statistics regarding Google's receipt of various national security demands, if any. We subsequently amended our Motion, seeking permission to publish the total number of compulsory requests we may receive under various national security authorities and the total number of users or accounts that may be impacted by each category of request.

In its heavily redacted Response and accompanying Declaration to our Motion for Declaratory Judgement before the FISC, the DOJ reiterated that it would only allow companies to combine domestic law enforcement and national security demands together. Lumping domestic law enforcement and national security demands together, however, would be a significant step backward for Google's users and the broader public.

The DOJ's proposal would limit Google to reporting law enforcement and national security demands, if any, in a single range. Rather than promote transparency, this proposal would obscure important information about the volume and type of *all* government requests that Google may receive, not just national security demands. Google already discloses aggregate statistics about domestic law enforcement demands that we receive. As noted above, we have done so since 2010. Publishing future Transparency Reports where we could release this information only in ranges (rather than disclosing actual numbers) would provide less transparency.

In addition to masking information about domestic law enforcement demands that Google receives, there would be no discernible benefit for transparency around national security demands that we may receive. Reporting domestic law enforcement and national security demands together would only invite speculation about the import of the range reported and would yield no information whatsoever about any national security demands that we may receive. Indeed, Google would be prohibited from even acknowledging receipt of national security demands, if any, including NSLs, which we currently disclose in our Transparency Report.

Transparency and national security are not mutually exclusive. There has been no intimation from law enforcement that the data we've published so far has tipped off organized crime or caused

other individuals suspected of criminal activity to gravitate to other services. The Department of Justice has likewise given no signs that the publication of ranges of NSLs we receive has had such effects for terrorists. Indeed, the number of government requests that we receive in the U.S. as reflected in the Transparency Report has increased substantially since we first published our Transparency Report, suggesting that there is no correlation between transparency and hinderance of investigations. Google is not seeking to disclose the targets or substance of any national security demands that we may receive. Nor are we seeking to acknowledge national security demands contemporaneous with their receipt or to disclose sources and methods.

In light of these facts, publishing aggregated statistics around other foreign intelligence demands that we may receive would not damage national security investigations. We believe Google and other companies have a First Amendment right to publish basic, aggregate statistics about the volume, scope, and type of national security demands that we may receive. In a democratic society, the government simply cannot be the sole arbiter of who gets to speak and what they may say on issues of paramount national importance. The right to speak about such weighty matters of public interest is not and should not be the exclusive province of the intelligence community.

In Addition to Transparency, Congress Should Consider Broader Reforms to Surveillance Laws

Transparency is a critical step in informing the broader public about the extent to which covered entities are compelled to provide user data in response to national security demands. It is clear, however, that governments, both in the U.S. and abroad, must examine broader reforms to government surveillance programs that threaten to erode confidence in the privacy and security of data that is entrusted to covered entities.

We can start with fixing our domestic surveillance laws. Google strongly supports legislation that would update the Electronic Communications Privacy Act to require a warrant in all instances where governmental entities want to obtain the content of users' communications. This is the core goal of both S. 607, the Electronic Communications Privacy Act Amendments Act of 2013, bipartisan legislation sponsored in the Senate by Senators Leahy and Lee, and H.R. 1852, the Email Privacy Act, sponsored by Representative Yoder and cosponsored on a strongly bipartisan basis by over 140 members of the House. Each of the bills would update ECPA by creating a bright line, warrant-for-content standard. We urge Congress to pass ECPA reform as soon as possible, and to resist efforts to include carve-outs and exceptions that would whittle away at this bright line, warrant-for-content standard and contravene users' reasonable expectations of privacy.

Also, agreements like Mutual Legal Assistance Treaties guarantee that standards for due process are met and offer a consistent framework for expedient mutual assistance in investigations that

cross borders. Where countries other than the country in which a company is headquartered require user data and it is legally justified, MLAT can provide the right framework for law enforcement cooperation. More can and should be done to significantly improve efficiency and ease of use of the MLAT process.

With respect to broader reform of surveillance laws and practices, Google, AOL, Apple, Facebook, LinkedIn, Microsoft, and Yahoo! recently voiced support for broader FISA reforms that would include substantial enhancements to privacy protections and appropriate oversight and accountability mechanisms for FISA surveillance.

In the letter we stated:

> As companies whose services are used by hundreds of millions of people around the world, we welcome the debate about how to protect both national security and privacy interests and we applaud the sponsors of the USA Freedom Act for making an important contribution to this discussion… Transparency is a critical first step to an informed public debate, but it is clear that more needs to be done. Our companies believe that government surveillance practices should also be reformed to include substantial enhancements to privacy protections and appropriate oversight and accountability mechanisms for those programs.

We also strongly believe that governments throughout the world must revisit laws and practices governing surveillance of individuals and access to their information.

* * * * *

Google looks forward to working with this Subcommittee, the full Judiciary Committee, and Congress as a whole on the Surveillance Transparency Act of 2013 and other reform measures that ensure national security authorities are utilized in a way that is rule-bound, narrowly tailored, transparent, and subject to oversight.

Thank you for your time and consideration.