Testimony of Scott Cleland, President, Precursor LLC
"The Blind Eye to Privacy Law Arbitrage by Google -- Broadly Threatens Respect for Privacy"
Before the House Energy & Commerce Subcommittee on Internet Hearing, July 17, 2008

I am Scott Cleland, President of Precursor LLC, an industry research and consulting firm. I am also Chairman of NetCompetition.org, a pro-competition e-forum funded by telecom, cable and wireless broadband companies. My testimony today reflects my own personal views and not the views of any of my clients.

The current patchwork of U.S. privacy laws, the lack of a holistic approach to Internet privacy, and selective oversight of privacy problems – have combined to create perverse incentives for some companies to: arbitrage privacy laws and push the privacy envelope. As a result, invasion/abuse of privacy is among the most serious problems users face on the Internet. **The lack of a holistic, comprehensive and balanced approach to privacy law and oversight is a serious threat to American's privacy**.

Broadband companies, (telecom, wireless and cable) have long been subject to strict privacy laws (sections 222, 551 & the ECPA), which created serious consequences for the misuse of personally identifiable information without a user's permission. Consequently, broadband companies have developed extensive policies, procedures and practices to respect users' privacy and protect personally identifiable information. This Subcommittee's oversight of experimentation by some, with "deep packet inspection" for advertising purposes, is entirely appropriate. Existing laws appear to cover these practices so oversight by Congress is expected.

I am concerned however, that selective oversight of only broadband privacy matters fosters a blind eye to arbitrage of privacy laws by application companies like Google, Yahoo and others. This creates perverse incentives for companies not covered by U.S. privacy laws to push the envelope on privacy to gain competitive advantage. **Americans' privacy should not be an unrestricted commodity to sell to the highest bidder or to gain competitive advantage**.

Specifically, I am troubled with the selective broadband focus of this hearing, because privacy is a cross-cutting, big picture issue that knows no boundaries between the access, application and content "layers' of the Internet. To add balance and to focus on the most serious threat to Americans' privacy, I humbly suggest the Subcommittee hold another hearing entitled: "*Why Google Knows Everything About You: Unauthorized Web Surveillance and Privacy Law Arbitrage*."

By turning a blind eye to what Google, the worst privacy offender on the Internet, is doing to systematically invade and abuse Americans' expectation of privacy, Congress is perversely encouraging copycat behavior by "deep packet inspection" advertising entrepreneurs who see that there is a huge privacy double standard to arbitrage. Companies like NebuAd are essentially just following the privacy-arbitrage leader – Google.

To illustrate my point of the extreme privacy law arbitrage that is occurring in the U.S. marketplace today, I explain in detail in my written testimony how Google is the single worst arbitrageur of privacy laws and the single biggest threat to Americans' privacy today.

Case Study: How Google Systematically Threatens Americans' Privacy:

1. Google's radical "publicacy" mission is antithetical to privacy.
2. Privacy is not a priority in Google's culture.
3. Google gives privacy "lip service."
4. Google threatens the privacy of more people than most any other entity.
5. Google collects/stores the most potential "blackmail-able" information.
6. Google's track record does not inspire trust.

As others have said, information is power. Power corrupts. Absolute power corrupts absolutely. Google's market power over private information is corrupting Google, just like former FBI Director J. Edgar Hoover was corrupted by his power and mastery of personally-sensitive information. Google's unprecedented arbitrage of privacy law combined with its exceptional lack of accountability is fast-creating this era's privacy-invading, unaccountable equivalent: "J. Edgar Google." Remember the timeless insight, those who don't learn from history -- are doomed to repeat it.

Written Testimony of
Scott Cleland
President, Precursor LLC

"The Blind Eye to Privacy Law Arbitrage by Google -- Broadly Threatens Respect for Privacy"

Before the
House Energy & Commerce Subcommittee
On Telecommunications and the Internet

Hearing on:
"What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies"

July 17, 2008

I. Introduction

Mr. Chairman and Members of the Subcommittee thank you for the honor of testifying on the important subject of Internet privacy. I am Scott Cleland, President of Precursor LLC, an industry research and consulting firm, specializing in anticipating the future of the converging techcom industry. I am also Chairman of NetCompetition.org, a pro-competition e-forum funded by telecom, cable and wireless broadband companies. My testimony today reflects my own personal views and not the views of any of my clients.

II. The Problem of Privacy Law Arbitrage and Selective Privacy Oversight:

The current patchwork of U.S. privacy laws, the lack of a holistic approach to Internet privacy, and selective oversight of privacy problems – have combined to create perverse incentives for some companies to:

- Arbitrage privacy laws,
- Try and "fall between the cracks" of privacy oversight, and
- Push the privacy envelope.

As a result, invasion/abuse of privacy is among the most serious problems users face on the Internet. The lack of a holistic, comprehensive and balanced approach to privacy law and oversight is a serious threat to American's privacy.

Broadband companies, (telecom, wireless and cable) have long been subject to strict privacy laws (sections 222, 551 & the ECPA), which created serious consequences for the misuse of personally identifiable information without a user's permission. Consequently, broadband companies have developed extensive policies, procedures and practices to respect users' privacy and protect personally identifiable information. Like medical providers operate under HIPPA privacy protections and financial services providers operate under FCRA/FDCPA privacy protections, broadband providers operate under sections 222, 551 and the ECPA, privacy protections. As a result, the broadband, medical and financial industries have **made respect for privacy an integral part of their business models and cultures**.

This Subcommittee's oversight of experimentation by some, with "deep packet inspection" for advertising purposes, is entirely appropriate. Existing laws appear to cover these practices so oversight by Congress and regulators is appropriate and expected.

I am concerned however, that selective oversight of only broadband privacy matters fosters a blind eye to arbitrage of privacy laws by application companies like Google, Yahoo and others. This creates perverse incentives for companies not covered by U.S. privacy laws to push the envelope on privacy to gain competitive advantage. **Americans' privacy should not be an unrestricted commodity to sell to the highest bidder or to gain competitive advantage**.

- Specifically, I am troubled with the selective broadband focus of this hearing, because privacy is a cross-cutting, big picture issue that knows no boundaries between the access, application and content "layers' of the Internet.
    - If the Subcommittee holds a hearing entitled: "*What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies*" – to add balance and to focus on the most serious threat to Americans' privacy, I humbly suggest the Subcommittee hold another hearing entitled: "*Why Google Knows Everything About You: Unauthorized Web Surveillance and Privacy Law Arbitrage*."
- By turning a blind eye to what Google, the worst privacy offender on the Internet, is doing to systematically invade and abuse Americans' expectation of privacy, Congress is perversely encouraging copycat behavior by "deep packet inspection" advertising entrepreneurs who see that there is a huge privacy double standard to arbitrage.
    - If you are a broadband provider strict privacy laws apply, if you are an "application" provider like Google, it's the Wild West – there's no privacy protection.
    - Like water seeking its own level, market forces can be expected to arbitrage the huge gaps in privacy protection among companies.
    - Companies like NebuAd are essentially just following in the footsteps of the privacy-arbitrage leader – Google.

To illustrate my point of the extreme privacy law arbitrage that is occurring in the U.S. marketplace today, let me explain in detail how Google is the single worst arbitrageur of privacy laws and the single biggest threat to Americans' privacy today.

III. Case Study: How Google Systematically Threatens Americans' Privacy:

To begin, I am not alone in believing Google's privacy practices are a particularly serious consumer protection problem.

- **Privacy watchdog, Privacy International, ranked Google worst in its world survey on privacy in 2007 and described Google as "hostile to privacy**."
- EPIC, CDD, and USPIRG filed suit with the FTC last year challenging Google's privacy practices as deceptive trade practices.
- Recently, a broad coalition of privacy advocates pressured Google to finally comply with California privacy law and put a link to their privacy policy on their home page.

1. Google's mission is antithetical to privacy.

- Google's megalomaniacal "*mission is to organize the world's information and make it accessible and useful*."
    - **Google's mission is so uniquely antithetical to privacy – it actually warrants the creation of a new term: "publicacy."**
    - Google's unique and radical "publicacy" mission believes "the world's information," is, and should be public not private. (Note the mission statement puts no qualifier on "information" other than "the world's.")
- The fact that most of the world's most valuable information is *copyrighted or owned by others* hasn't stopped Google from making other's property universally available – without permission or compensation. As a result, several different content industries are suing Google for theft. Google supports radical copyright reform to remake the Internet

into a less-propertied, "information commons" where most all content is free to the user and supported by Internet advertising -- the business that Google dominates.

- The fact that much of the world's information is also *private*, or enables privacy because it is not easily accessible publicly by anyone, hasn't stopped Google from trying to make this *private* information *publicly* accessible. The business reason for this is that Google knows that the most valuable information is private (scarce) information that was not available before. Google also knows that its competitive advantage is its world-leading "database of user intentions," i.e. search histories on several hundred million Google users worldwide. Google also understands that it can earn a premium because it knows more private information on users' intentions, preferences and secrets than any other company in the world – by far. Simply, Google's business edge is that it collects, stores and uses more private information than any other entity in existence, which enables it to "target" "relevant" advertising better than anyone else.
- The fact that Google's web "crawlers" are the world's most pervasive and invasive, Google indiscriminately searches websites for whatever it can find, and automatically assumes if their crawlers can find it, it must be "public" information. This indiscriminate web crawling has resulted in Google exposing private information like social security numbers, as Google did in making hundreds of California university students' social security numbers public -- as reported by the Sacramento Bee (3-7-07.)

2. Privacy is not a priority in Google's culture.

- Google celebrates an "innovation without permission" culture. Google's obsession with innovation comes at a cost, because it comes with a cultural disdain for internal controls, management supervision, and internal vetting of issues for privacy concerns. Let me illustrate this cultural disdain for privacy with three high-profile examples of Google proceeding full-speed-ahead with "beta" releases -- without regard to privacy implications of their actions.
    - Google introduced gmail, which enables Google to automatically read the content of users' private gmail messages in order to send them "relevant" advertising –

without meaningful internal privacy review. This caused a widely reported public uproar over users' privacy being abused.

- Google introduced Google Earth, which exposed the roof tops of the White House, public buildings and military installations, without meaningful internal review of the privacy, safety, or national security implications. The uproar that ensued over this suggests Google learned little from the gmail incident about the importance of internal review to address external concerns like privacy.
- Google then introduced StreetView, which is video of people's homes, apartments and neighborhoods, without meaningful internal review of the privacy or safety concerns involved. The uproar over this invasion of privacy is so significant that Google is very secretive about where and when Google's "spycars" will be videoing a particular neighborhood in order to protect the safety of the Google drivers from irate residents.

- The inescapable conclusion from this pattern of behavior is that Google's culture exhibits a fundamental and sustained disdain for privacy.

3. Google gives privacy "lip service."

- Only this month did Google begrudgingly comply with longstanding California Privacy law to post a link to their privacy policy on their webpage. Google's founders did not want to "clutter" the signature simplicity of their homepage with the addition of another word. Google's leaders spoke loudly on their assessment of the value of privacy policies with their stubborn recalcitrance on this most basic of privacy compliance. The message internally is that privacy is not a priority to the founders. We also know that organizations listen and follow the cues from their leaders about which values to follow in conducting business.
- Google has not bothered to update its privacy policy since October 14th, 2005 despite a number of major external developments that objective observers would think would merit an update or a change in their privacy policy.
  - Since the last update, Google has entered several new businesses which operate under very different privacy laws:

- YouTube – viewing habits;
- Feedburner – reading habits;
- GrandCentral – voiceprints and wiretapping;
- DoubleClick – ad viewing
    - (Note: a few years ago the FTC sanctioned DoubleClick for its privacy practices.);
- Google Health (which arbitrages HIPPA); and
- FriendConnect (after state Attorney Generals acted on privacy/safety related issues of minors.)

o In the fall of 2007, Privacy International ranked Google worst in its world survey, and called the company "hostile to privacy."

o In 2007, privacy watchdog EPIC, sued Google via the FTC review of the Google-DoubleClick merger, for deceptive trade practices.

o In late 2007, the FTC staff proposed new behavioral advertising privacy principles that run counter to Google's current privacy practices.

- If Google really cared about privacy and it was an important priority, wouldn't Google have updated its privacy policy to adapt to any of the above mentioned developments? Not only does Google not a lead by example on privacy matters, it doesn't even follow others lead.

4. Google threatens the privacy of more people than most any other entity.

- Google-DoubleClick track the search histories and ad-viewing habits of an estimated 90% of global Internet users, approaching a billion people worldwide.
- Google has the largest network of advertisers, ~1,000,000 compared to Yahoo's ~300,000 and Microsoft's ~75,000.
- Google has relationships with over 1 million websites, orders of magnitude more content relationships than its competitors.
- What this means is that **Google has both the means and the business model to learn more private information about more people than any other company in the world**.

5. Google collects/stores the most potential "blackmail-able" information.

- Consider the depth and breadth of intimate information Google collects:
  - *What you search for*;
    - (a Ponemon Institute survey of 1,000 Google users found that 89% thought that their searches were private and 77% thought Google searches could not reveal their personal identities – wrong on both accounts.)
  - *Where you go on the web*;
    - Google has pervasive unauthorized-web-surveillance capability (web tracking/stalking) through a combination of Google's search, Google's cookies, DoubleClick's ad-view recording capability, Google's extensive content affiliate network of hundreds of thousands of sites, and the wide variety of Google apps.
  - *What you watch* -- through YouTube;
    - (Remember Supreme Court nominee Robert Bork was politically attacked for the videos he rented.)
  - *What you read* -- through Google News, Feedburner and Blogger.
  - *What you say* -- in your emails through gmail's automated reader.
  - *What you produce* -- in Google Docs or spreadsheets.
    - (In return for the free Google Apps like Docs and spreadsheets, users grant Google some search rights in perpetuity to any content a user produces using Google's Apps.)
  - *What your family and friends look like* -- through Picassa images.
  - *Your medical conditions, medications, and medical history* -- through Google Health.
  - *Your purchase habits* -- through Google Checkout.
  - *Your call habits and voiceprint* -- through Google Talk.
  - *Your travel habits and interests* -- via Google Maps.
  - *Your interest in other people/places* -- via Google Earth & StreetView.
  - *Your personal information* -- through Orkut (social networking) Gmail, Google Checkout, etc.

- *Where you go/hang out* -- through Google wireless ventures and Android.
- *Where you'll be or where you were* -- through Google Calendar.

- The scale and scope of Google's unauthorized-web-surveillance is truly Orwellian "Big Brother." While Google is not the Government, all this private information that Google collects and stores is certainly available to the Government via subpoena.
- It is also important that this capability of Google's is very different from Microsoft reach because as a software provider, your private information mostly resides on your PC where you control it.
    - In stark contrast, all of the private information listed above that Google collects *resides on Google's servers.*

6. Google's track record does not inspire trust.

- Google does not fairly represent its business to users.
    - Google's rhetoric and public relations intimate that Google works for users – they don't. Google is not paid by users – Google is paid by advertisers and websites.
        - Like investment banks hurt investors during the bubble for not disclosing that their research had a financial conflict of interest, Google puts users at serious risk by not disclosing to them that Google has a financial conflict of interest in looking out for advertiser/website/Google interest before the users' interest.
        - How this conflict could hurt consumers today is that when websites are infected with dangerous malware like phishing for ID theft, Google has not been flagging certain search results as dangerous, when doing so would protect users from sites Google knows not be safe. They are being silent and not protecting users from potential harm because that would discourage traffic, clicks and revenue from Google's real clients: advertisers and websites.
- If the Ponemon survey of Google's users is even remotely accurate, most consumers do not understand that they have forfeited their privacy to Google in return for Google's

free applications. In other words, few people understand that Google thinks they have users' full permission/assent to sell their privacy to the highest bidder.

- Another trust undermining aspect of Google's business is the rampancy of fraud in Google's model.
    - Most people are not aware that click-search is one of the most fraud-prone industries in America. Click Forensics, which is the leading industry tracker of web fraud, estimates that 28% of all Internet clicks are fraudulent.
    - The dirty little secret here is that the gross-revenue business model for search, which was pioneered by Google, makes money off of fraudulent clicks. In other words, Google's gross revenue model does not have a financial incentive to be honest.
    - It is hard to imagine another legal industry in America that would tolerate a 28% gross fraud rate!
- Google also does not inspire trust because **Google's words don't match its deeds**. It is the master of the slippery, self-serving, double-standard:
    - Google's mission is to organize the world's information to make it accessible, when Google is among the most secretive, non-transparent, 'black box' public entities anywhere.
    - Google pushes "open" everything for everyone else, open access, open source, open social, open handset, open spectrum, but the auction process that is at the core of Google's business model is not open but an opaque 'black box' that users cannot see into.
    - Google supports net neutrality regulation for its broadband competitors, but maintains that Google, the world's most dominant access point for the Internet, should not be subject to net neutrality regulation.
    - Google aggressively protects its intellectual property of copyrights and patents, while strongly supporting "information commons" reforms that would decimate the intellectual property rights of their competitors.
    - Google runs its not-for-profit Google.org as a for-profit division of Google, when every other corporation in America abides by the clear separation of for-profit and not-for-profit entities to avoid even the appearance of tax evasion or impropriety.

IV. Conclusion:

The lack of a holistic approach to Internet privacy combined with selective oversight of privacy problems encourages some companies to try and "fall between the cracks" of privacy law, to arbitrage privacy laws and to push the privacy envelope. This is unfortunate because invasion/abuse of privacy is among the most serious problems users face on the Internet. **In short, the lack of a holistic, comprehensive and balanced approach to privacy is a serious threat to American's privacy.**

Vigilant oversight of broadband companies subject to privacy law is appropriate. What is not appropriate is discrimination against broadband providers as the only companies that warrant privacy oversight. The greatest risk comes from application providers like Google and Yahoo, which are not subject to privacy law, and are arbitraging that legal gap, as a competitive advantage to the serious detriment of Americans' privacy. Given Google's exceptional and increasing market power over the business of the Internet, it appears as if **the Subcommittee risks turning a blind eye to the single biggest unaddressed threat to Americans' privacy**.

As others have said, information is power. Power corrupts. Absolute power corrupts absolutely. Google's market power over private information is corrupting Google, just like former FBI Director J. Edgar Hoover was corrupted by his power and mastery of personally-sensitive information. Google's unprecedented arbitrage of privacy law combined with its exceptional lack of accountability is fast-creating this era's privacy-invading, unaccountable equivalent: "J. Edgar Google." Remember the timeless insight, those who don't learn from history -- are doomed to repeat it.

Attachment I:

Precursor Blog posts on Google & Privacy:

J. Edgar Google: Information Is Power + No Accountability

- http://www.precursorblog.com/content/j-edgar-google-information-is-power-no-accountability

Can you trust Google to obey the rules? Is Google accountable to anyone?

- http://www.precursorblog.com/node/769

Why Google storing personal health records is a really bad joke -- the public should be worried...

- http://www.precursorblog.com/node/762

Google's Privacy Lip Service

- http://www.precursorblog.com/content/googles-privacy-lip-service

Google protecting its privacy to invade your privacy; Why Google is the King of Double Standards:

- http://www.precursorblog.com/content/google-protecting-its-privacy-invade-your-privacy-why-google-king-double-standards

J. Edgar Google compiling personal YouTube viewing dossiers

- http://www.precursorblog.com/content/j-edgar-google-compiling-personal-youtube-viewing-dossiers

Attachment II:

Scott Cleland

Founder & President, Precursor® LLC

Chairman, Netcompetition.org

Scott Cleland is one of nation's foremost techcom analysts and experts *at the nexus of*: capital markets, public policy and techcom industry change. He is widely-respected in industry, government, media and capital markets as a forward thinker, free market proponent, and leading authority on the future of communications. Precursor LLC is an industry research and consulting firm, specializing in the techcom sector, whose mission is to help companies anticipate change for competitive advantage. He previously founded The Precursor Group Inc., which *Institutional Investor* magazine ranked as the #1 "Best Independent" research firm in communications for two years in a row. He is also Chairman of Netcompetition.org, a wholly-owned subsidiary of Precursor LLC and an e-forum on Net Neutrality funded by broadband telecom, cable, and wireless companies.

Cleland has a high-profile track record of foreseeing big change before others. He coined the term "techcom" to define how information technology drives the communications future and to best name the new sector that converging communications technologies are creating. *Fortune* profiled Cleland as the first to call "WorldCom: Dead Model Walking" and to predict its bankruptcy. Then WorldCom CEO Bernie Ebbers tried to discredit Cleland's prescient and hard-hitting research on WorldCom by deriding him the "idiot Washington analyst." Cleland has testified before seven different Congressional subcommittees on a variety of forward-looking topics and was the first congressional expert witness asked to testify on what went wrong with Enron.