Summary Testimony of Scott Cleland, President, Precursor LLC
"Why A Consumer-Driven, Technology/Competition-Neutral, Privacy Framework Is Superior to a Default 'Finders Keepers Losers Weepers' Privacy Framework"
Before the Joint House Energy & Commerce Hearing on Behavioral Advertising, June 18, 2009

Precursor LLC is an industry research and consulting firm specializing in the future of the converging techcom industry. For the last three years, I have also been Chairman of NetCompetition.org, a pro-competition e-forum funded by broadband companies. In addition, beginning in 2009, I have done consulting for Microsoft. **My testimony today reflects my own personal views and not the views of any of my clients.**

The Privacy Problem:

- *First*, **technology has turned privacy reality upside down**. Before the Internet most people enjoyed substantial privacy because it was inefficient, difficult and expensive to collect and disseminate private information. However, Internet technology has flipped that reality on its head by making it hyper-efficient, easy and near free incrementally to collect and disseminate private information. As a result, **we now have a technologically/competitively-skewed, *"finders keepers losers weepers"* privacy framework by default.**
- *Second*, the essence of the behavioral advertising or Internet privacy problem is captured well by the Consumer Reports 9-25-08 poll which spotlighted that **the average American consumer believes they are in much more control of their private information online than in fact they are**.
- *Third*, all of the technology megatrends (social media, cloud computing, Internet mobility, and the Internet of Things) are all converging to increase the risks to consumers who wish to safeguard their privacy online.
- *Fourth*, there is a growing collection of "publicacy" interests among the technology elite that view privacy online very differently than most Americans view privacy offline. Increasingly, Congress will be forced to weigh these increasingly competing and conflicting online/offline privacy interests and trade-offs.
- *Fifth*, **increasingly the "underground currency" of the Internet is private data**. Private information is valuable, because in the absence of a system where consumers can assert ownership of and control over their privacy, privacy can be taken from them for free and profited from with little to no obligation to, or compensation due, to the affected consumer. The increasing commercialization of privacy by publicacy businesses increasingly creates new risks for consumers in return for little to no protection or reward.
- *Finally*, **the current technology-driven, "Swiss cheese" privacy framework may be the worst of all possible worlds**. In the absence of a consumer-driven, technology/competition neutral, privacy framework, consumers have neither a meaningful role in protecting their privacy nor the freedom to exploit some of the value of their private information -- if that is their choice. Simply, the current haphazard privacy framework affords an individual no meaningful-informed choice to either protect or benefit themselves in the marketplace arena of their private information. The technology used should be irrelevant to privacy policy.

A Privacy Solution: A Consumer-Driven, Technology/Competition-Neutral Privacy Framework:
Since it is consumers' private information that is being taken and exploited without much meaningful consent by the consumer, and since it is consumers which are most at risk from having their most private information stolen or used inappropriately, wouldn't it be more logical for a privacy framework to be more oriented around a consumer' perspective rather than a technology perspective? Clearly businesses should be free to fairly represent and engage consumers in a fair market transaction over the disposition of their private information -- a fair market transaction where consumers are able to effectively understand and negotiate the risk/reward value of sharing their private information. Since a consumer is the only one who knows what information about their personal situation, interests, views and intentions, they are comfortable in sharing for what purposes, wouldn't it be logical to have a privacy framework that empowered consumers with real input and influence over either protecting or exploiting their own interests, whatever they may be?

Conclusion: *If* Congress decides to legislate on Internet privacy, a consumer-driven, technology/competition-neutral privacy framework would be superior to a technology-driven privacy framework, because it would:

- Emphasize protecting people not technologies;
- Empower consumers with the control/freedom to choose to either protect or exploit their own privacy;
- Prevent competitive arbitrage of asymmetric technology-driven privacy policies with a level playing field;
- Stay current with ever-evolving technological innovation; and
- Accommodate both privacy and publicacy interests by empowering real consumer privacy choice.

Written Testimony of
Scott Cleland
President, Precursor LLC

"A *Consumer-Driven, Technology/Competition-Neutral Privacy Framework Is Superior to a Default 'Finders Keepers Losers Weepers' Privacy Framework*"

Before the
House Energy & Commerce Subcommittees On:
Communications, Technology, and the Internet
&
Commerce, Trade, and Consumer Protection

Joint Hearing on:
"*The Potential Privacy Implications of Behavioral Advertising*"

June 18, 2009

I. Introduction

Mr. Chairmen and Members of the Subcommittees thank you for the honor of testifying on the important subject of: "*The Potential Privacy Implications of Behavioral Advertising*." I am Scott Cleland, President of Precursor LLC, an industry research and consulting firm, specializing in the future of the converging techcom industry. For the last three years, I have also been Chairman of NetCompetition.org, a pro-competition e-forum funded by telecom, cable and wireless broadband companies. In addition, beginning in 2009, I have done consulting for Microsoft. **My testimony today reflects my own personal views and not the views of my clients.**

My purpose today is to help the Subcommittees see the business of behavioral advertising through the lens of consumer/user privacy. At core, behavioral advertising is the commercialization of privacy or "publicacy." "Publicacy" is simply the antonym or opposite of privacy. Increasingly, private information is becoming a de facto underground currency of the Internet.

A wide range of Internet and behavioral advertising trends are coalescing to force Congress to grapple with some fundamental public policy questions with regard to privacy:

1. Is respect for privacy still important and relevant in America in the Internet Age?
2. Is an individual's privacy or freedom from intrusion, more or less important than others' freedom to uncover private information and make it public without permission?
3. Do American's have the right to own and control their own private information, in order to either protect or benefit their selves?
4. To what extent should accountability exist for violating expressed right to privacy?
5. What overall privacy framework is the most appropriate, effective and adaptable in the Internet Age?

The outline of my testimony is as follows:

I. Introduction
II. Trend Convergence
III. The Privacy Problem
IV. A Privacy Solution
V. Conclusion

II. Trend Convergence

Privacy norms and expectations developed over decades in the physical world are rapidly being over taken by events in the virtual or Internet world. Increasingly a convergence of many Internet and behavioral advertising trends is undermining consumer expectations of respect for privacy.

Consumer Expectations Trends: The first and maybe most relevant trend to the Subcommittees is that most consumers are largely unaware that they are not in control of their private information online. For example, a Consumer Reports 9-25-08 consumer poll found:

- "*61% are confident that what they do online is private and not shared without their permission;*
- *57% incorrectly believe that companies must identify themselves and indicate why they are collecting data and whether they intend to share it with other organizations;*
- *48% incorrectly believe their consent is required for companies to use the personal information they collect from online activities...*"
    - http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html

Technology Trends: Second, is the well-known trend of Internet convergence which has an outsized impact on privacy because Internet convergence enables for the first time the widespread and micro-detailed collection, storage, aggregation, access, analysis, sharing, distribution, and commercialization of any digitizable form of private information (e.g. data, text,

image, video, voice, click-streams, etc.). Simply, the Internet has enabled the potential for unprecedented invasion of privacy.

- Moreover, all the biggest Internet technology megatrends will only exacerbate privacy concerns over time because:
    - *The Web 2.0 Social Media megatrend* often views respect for privacy as "friction" and an impediment to "open" sharing and community-building on the Internet;
    - *The Cloud Computing megatrend* of outsourcing data processing and storage elsewhere to the "cloud" and not on an individual's desktop or laptop, often views respect for privacy as a cost and an inefficiency;
    - *The Internet Mobility megatrend* of accessing the Internet anywhere wirelessly and not just through a tethered stationary connection, increasingly impacts respect for privacy because it can enable others to know users' exact locations and to track where they go or have gone; and
    - *The Internet of Things megatrend* of assigning web addresses to sensor-chips on objects or physical things impacts privacy in that it could make public private property as never before.

Publicacy Attitude Trends: Third may be the trend that Congress is probably least aware of, the emergence of "publicacy" attitudes in the technology community. Before the Internet, there was no need for an antonym for privacy or a new word that captured being opposed to or in conflict with privacy. That's because in the past there simply weren't significant forces working against respect for privacy as there are today. I coined the term "publicacy" in my previous Internet privacy testimony before this Subcommittee to spotlight and help Congress understand that the only way to fully understand the evolving issue of Internet privacy is to understand the new emerging Internet trends and attitudes that are increasingly in tension with well-established privacy norms and expectations in the physical world.

- The origin of "publicacy" attitudes that digital private information should not be viewed as personal property that requires permission to use may be rooted in part in the Free Software Foundation's definition of Free Software: "*Free software is a matter of the users' freedom to run, copy, distribute, study, change and improve the software. … Being free to do these things means… that you do not have to ask or pay for permission*."

- Some in the Information Commons movement appear to have expanded the Free Software notion that "*you do not have to ask or pay for permission*" from software code to include most content created online. To the extent that interactions occur in the so called "public" domain of the Internet, the Information Commons movement tends to see that information as public even if others may consider it private information.
- Some in the Web 2.0 Social Media movement, appear to have further expanded on the notion that "*you do not have to ask or pay for permission*" from most content created online to community building and sharing online. Asserting one's privacy in this context is looked upon by some in the social media movement to be the opposite of sharing, and not being open and transparent.
- On top of these emerging attitudes, many in the behavioral advertising business community have viewed respect for privacy as a friction, an inefficiency or an impediment to business models based on perfecting the efficient targeting or relevance of online advertising.

Commercialization of Privacy Trends: Finally, is another trend that Congress may not be as aware of as they may want to be – that is -- why is there such a driving force to commercialize privacy online? What makes private information so valuable?

- Private means economically rare or having scarcity value. Value increases with the amount of scarcity.
- Private can mean a secret weakness/vulnerability that someone does not want to be revealed and would pay to keep private.
- Private information now can be efficiently and effectively collected, skimmed, mined, analyzed and disseminated via automation at exceptionally low incremental cost or transactional friction on the Internet.
- Private information can be arbitraged for competitive advantage.
- What can make intrinsically valuable private information even more valuable?
    - No one else has it or can get it.
    - No one knows one has it so they can use it secretly to not arouse suspicion, alarm, or distrust.

- Not having to share any of the value creation from the private information with the owner of the private information.

The commercialization of privacy is becoming increasingly sophisticated. In essence, the long-held sales and marketing axiom of know thy customer/target is morphing online from an art to a science to ultimately math.

Overall, the convergence of these trends: consumer expectations, technology, publicacy attitudes and commercialization of privacy – all suggest increasing pressure on Congress and the legislative process to sort out these increasingly conflicting interests.

III. The Privacy Problem

First, technology has turned privacy reality upside down. Before the Internet most people enjoyed substantial privacy because it was inefficient, difficult and expensive to collect and disseminate private information. However, Internet technology has flipped that old reality on its head making it hyper-efficient, easy and near free incrementally to collect and disseminate private information. **As a result we have moved from a stable respect for privacy framework to an unstable, technologically/competitively-skewed, *"finders keepers losers weepers"* privacy framework.**

Second, the essence of the behavioral advertising or Internet privacy problem is captured well by the Consumer Reports 9-25-08 poll which spotlighted that the average American consumer believes they are in much more control of their private information online than in fact they are. The obvious implication for Congress is that American consumers' guard is way down and that they either need to be better informed about their increasing lack of privacy online or afforded more choice to better protect or benefit from their private information online.

Third, all of the technology megatrends (social media, cloud computing, Internet mobility, and the Internet of Things) are converging to vastly increase the risks to consumers who wish to safeguard and protect their privacy online.

Fourth, there is a growing collection of publicacy interests among the technology elite that view privacy online very differently than most Americans view privacy offline. Increasingly, Congress will be forced to weigh these increasingly competing and conflicting online/offline privacy interests and trade-offs.

Fifth, increasingly the "underground currency" of the Internet is private data. Private information is valuable to many Internet businesses, because in the absence of a system where consumers can assert ownership of and control over their privacy, privacy can be taken from them for free and profited from with little to no obligation to, or compensation due, to the affected user/consumer. In effect, the increasing practice of commercializing privacy by publicacy businesses increasingly creates new risks for consumers in return for little to no protection or reward.

Finally, the current technology-driven, "Swiss cheese" privacy framework may be the worst of all possible worlds. In the absence of a consumer-driven, technology/competition neutral, privacy framework, consumers have neither a meaningful role in protecting their privacy nor the freedom to exploit some of the value of their private information -- if that is their choice. Simply, the current haphazard privacy framework affords an individual no meaningful-informed choice to either protect or benefit themselves in the marketplace arena of their private information.

The current technology-driven privacy framework ironically puts privacy and consumers last; the technology used should be irrelevant to privacy protection. Even more ironic, it also can be decades out-of-date with technology advances. Technology-driven privacy is all about what's best for the technology model -- consumers are an afterthought. The ultimate irony here may be that the Internet publicacy interests that say they believe in empowering end users with choice often are opposed to empowering end-users/consumers when it comes to privacy choice.

IV. Solution: Consumer-Driven, Technology/Competition-Neutral Privacy Framework

Since it is consumers' private information that is being taken and exploited without much meaningful consent by the consumer, and since it is consumers which are most at risk from having their most private information stolen or used inappropriately, wouldn't it be logical for a consumer privacy framework to be more oriented around a consumer's ongoing perspective rather than the technology snapshot perspective of a particular point in time?

- Clearly businesses should be free to fairly represent and engage consumers in a fair market transaction over the disposition of their private information -- a fair market transaction where consumers are able to effectively understand and negotiate the risk/reward value of sharing their private information.
- Since a consumer is the only one who knows what information about their personal situation, interests, views and intentions, they are comfortable in sharing for what purposes, wouldn't it be logical to have a privacy framework that empowered consumers with real input and influence over either protecting or exploiting their own interests, whatever they may be?

Isn't it logical for consumer privacy to be a matter of a consumer's meaningful individual choice?

V. Conclusion:

The essence of the Internet privacy problem is that technology has turned privacy reality upside down. Before the Internet most people enjoyed substantial privacy because it was inefficient, difficult and expensive to collect and disseminate private information. However, Internet technology has flipped that old reality on its head by making it hyper-efficient, easy and near free incrementally to collect and disseminate private information. As a result we have moved from a stable respect for privacy framework to an unstable, technology-driven, "*finders keepers losers weepers*" privacy framework – by default.

Consequently, Congress faces some big and important decisions.

- Should technology or people decide if there is respect for privacy?
- Is respect for privacy still important in the Internet Age?
- If so, should Americans be able to largely own and control their private information?
- Is an individual's right to privacy online of greater or of less importance than Internet openness and transparency?
- Is a consumer-driven or technology-driven privacy framework better for Americans?

If Congress decides to legislate on Internet privacy, a consumer-driven, technology/competition-neutral privacy framework would be superior to a technology-driven privacy framework, because it would:

- Emphasize protecting people not technologies;
- Empower consumers with the control and the freedom to choose to either protect or exploit their own privacy;
- Prevent competitive arbitrage of asymmetric technology-driven privacy policies which harms consumers with a competitively neutral, level playing field;
- Stay current with ever-evolving technological innovation; and
- Accommodate both privacy and publicacy interests by empowering consumers to individually decide how they want to protect or exploit their private information (from strong broad privacy protections, to tailored protections, to free use of their private information.)

Thank you again Mr. Chairmen for the opportunity to share my personal views and analysis on "*The Potential Privacy Implications of Behavioral Advertising*."

Bio:

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 a pro-competition e-forum 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.