Before the
Federal Trade Commission
Washington, D.C.

In re Exploring Privacy: A Roundtable Series	Project No. P095416 (Comment)

COMMENTS OF
COMPUTER AND COMMUNICATIONS INDUSTRY ASSOCIATION

In response to the Federal Trade Commission (FTC or "the Commission") announcement of a roundtable series that will explore online privacy issues, the Computer and Communications Industry Association (CCIA) submits the following comments.

CCIA is a non-profit trade association dedicated to open markets, open systems, and open networks. CCIA members participate in many sectors of the computer, information technology, and telecommunications industries and range in size from small entrepreneurial firms to some of the largest in the industry. CCIA members employ nearly one million people and generate annual revenues exceeding $200 billion. [1]

These comments focus on and analyze three topics: commercial privacy practices and online targeted advertising, government surveillance, and U.S. privacy policy. To address the first topic, these comments analyze the concerns and benefits associated with information collection for online targeted advertising (also known as behavioral advertising or interest based advertising). To address the second topic, these comments urge the Commission not to ignore the risk of government abuse if information is not properly protected. To address the third topic,

[1] A complete list of CCIA's members is available online at <http://www.ccianet.org/members>.

these comments analyze existing policies geared towards consumer online privacy, including both legal and self-regulatory regimes, and make recommendations.

I. Introduction

The Internet has changed the way consumers connect, contribute to society, communicate, and learn. As more information is shared online, data and communications privacy issues will continue to present unique philosophical and practical challenges for businesses, consumers, and the government.

CCIA commends the Commission for hosting a series of roundtable discussions to explore privacy issues related to information collection practices, online targeted advertising, e-commerce, and consumer value. We believe it is vital for regulators and policymakers to take the opportunity to understand emerging technologies and their impact on consumers.

The United States is faced with a unique opportunity to lead the world toward expanding human rights through access to knowledge and global opportunities. To have credibility, we must adopt and promote policies that protect Internet users' rights of free speech and privacy from abuses by overreaching government surveillance practices.

Unfortunately, current efforts are focused on deputizing Internet companies for potential abuses related to technologies that are still in development. CCIA encourages these efforts to look beyond speculative commercial abuses and safeguard against very real government intrusions.

II. Commercial Privacy Practices and Online Targeted Advertising

Consumers enjoy a wide array of online services, such as e-mail, social networking, and online banking, and some transactions may require them to share information about themselves. CCIA's members recognize the importance of consumer confidence and trust and have provided them with innovative privacy and security resources that emphasize transparency and meaningful choice.

As new services, such as online targeted advertising, explode onto the marketplace, they present unique challenges and great opportunities for both businesses and consumers. CCIA's member companies, guided by the efforts of the Commission and industry self-regulatory principles, have responded to challenges with even greater education and tools that expand user control. Our members remain at the forefront of efforts to design clear and concise policies that put consumers first.

Given the current competitive online ecosystem, it is vital for companies to maintain pro-consumer practices in order to retain customers, credibility and brand recognition. We are encouraged by reports that show companies are already locked in competition over their security solutions. There is evidence of this in a 2009 report by the Center for Democracy & Technology that explored competition amongst the privacy settings and consumer controls offered by companies behind the five leading Web browsers and browser features. [2]

A. Concerns

In order to better understand privacy challenges, it is important to explore what constitutes commercial harm and abuse of consumer privacy in a constantly evolving

[2] Center for Democracy & Technology. (2009). *Browser Privacy Features: A Work In Progress, Version 2.0.* Retrieved from <http://www.cdt.org/privacy/20090804_browser_rpt_update.pdf>.

information-based society. Privacy policy should not be founded on hypothetical situations or injuries that are purely speculative in nature. Nor should policy focus on subjective assessments of the merits of particular product features. Rather, privacy policy should encourage companies to safeguard consumer trust and discourage companies from violating that trust.

There are also valid privacy concerns related to computer intrusion and unauthorized access to information. These issues are top priorities for high-tech companies that continually work on building innovative security solutions into their products. This is an opportunity for industry and the federal government to work together to share information and coordinate responses to combat attacks, fraud and scams. In this context, penalties will be needed and federal enforcement efforts will continue to play a role in deterring bad actors and ensuring that consumers are confident in their online experience.

CCIA continues to raise concerns with end user tracking conducted at the network level by IAPs through techniques such as Deep Packet Inspection (DPI). IAPs are in a position to collect massive amounts of data on their customer activities, both commercial and non-commercial, as they travel over the IAP's infrastructure – from e-mails to chats to financial information. Whereas an Internet service that violates consumer trust may find consumers fleeing to a competitor that is only a click away, the lack of major competition among broadband providers poses problems for consumers and businesses alike. Many consumers cannot escape their IAP if the IAP breaches its privacy policy or otherwise violates consumers' trust. Due to the essential nature of this relationship between the consumer and IAP, increased scrutiny and obligations are necessary. It is appropriate, therefore, to require network operators to obtain explicit, informed, opt-in consent from consumers before using DPI technology for tracking and information collection.

B. The Benefits of Online Targeted Advertising

- *Low-cost Services* – Online advertising has greatly benefited consumers by underwriting the rich variety of online content choices and services available, enabling applications providers to offer their services at little or no cost to the consumer.
- *More Relevant Ads* – Online targeted advertising allows businesses to create a more convenient and personalized experience for consumers. Consumers are served relevant ads that are tailored to their online interests.
- *Low Barriers to Entry* – Small businesses and entrepreneurs now have the opportunity to connect with consumers that they may not have reached, using more traditional methods, creating robust competition and innovation online.
- *Expansion of Free Speech Applications* – Ad revenue has helped support new online applications, ventures and publications, such as blogs and social networking sites. Online publishers are better able to generate revenue from ads, allowing them to offer free or low-cost services and better serve their customers. Thus, online advertising has helped to level the playing field for small businesses and entrepreneurs, which leads to more opportunities for free expression.
- *Competition Supports Consumer Choice* – Because online advertising has both helped to preserve the low barriers to entry and underwritten the cost of services, consumers enjoy a competitive online environment that offers robust choices in products and services. Not only will this robust competitive environment encourage companies to innovate in the types of services and products they offer, but it will also drive them to compete over privacy practices in order to please customers.

III. User Privacy and Government Surveillance

CCIA recognizes that many government surveillance issues may exceed the scope of the Commission's jurisdiction, but a discussion of privacy issues impacting consumers cannot overlook undue government intrusion. Consumer privacy should be as secure from private sector intrusion as it is from public sector intrusion.

CCIA will continue to support and defend basic 4th Amendment protections against undue search and seizure and oppose efforts to further erode civil liberties. We urge the Commission and Congress to consider stronger safeguards that will protect consumer data from inappropriate government scrutiny.

As we have seen too often, and as evidenced throughout the debate on the Foreign Intelligence Surveillance Act (FISA), technology is not immune to overreaching government powers. Even the best privacy policies cannot effectively resist undue government intrusion in the name of national security. Given the current sector-specific approach to privacy, it is unclear what standards apply to the vast new array of online applications and remote computing services (or cloud computing).

The possibility of widespread and unchecked surveillance of consumers' digital information erodes the fundamental openness and freedom of our communications networks. Even a perceived loss of privacy in personal and confidential business communications may inflict widespread and lasting damage on user confidence, and thereby impair the dynamic and innovative growth of the Internet and high-tech sector.

One disturbing example comes from a recent Oregon case that raised major concerns about 4th Amendment protections for electronic communications. In considering whether the government must notify an account holder of a warrant to search the contents of their e-mail

account, the court concluded that merely serving notice to the Internet access provider (IAP), not the e-mail account holder, was sufficient. Because a person must access the Internet through an IAP, and have their information pass through or stored on servers owned by the IAP, the court reasoned that search target no longer constituted private information contained in the home. [3] However, consumers expect and deserve the same level of protection for their information whether it is filed in a desk drawer in the home or contained in a personal e-mail account. The time has come to update current law to reflect the innovative Internet ecosystem that consumers have grown accustomed to using.

CCIA actively participates in and supports efforts to revisit communications law and make common sense recommendations for modernizing existing frameworks, such as the Electronic Communications Privacy Act (ECPA), to include uniform safeguards for communications and information whether it is stored or in transit, online or offline, and regardless of age. These efforts seek to clarify 4th Amendment protections in light of fast-paced innovation and technological changes.

In addition, it is important that legal standards and practices safeguard consumer data across jurisdictions. Businesses are constantly inundated with requests for information from civil litigants and law enforcement officials across the globe, each with competing standards and procedures. This creates an overwhelming burden on businesses as they are forced to devote vast personnel resources to check for authenticity and legal authority and to satisfy the requirements of various jurisdictions. Often these requests are overly broad and require extra levels of scrutiny in order to respond appropriately.

[3] *See In re United States*, __ F. Supp. 2d __, 2009 WL 3416240 (D. Or. 2009).

IV. Current Privacy Landscape

A. FTC Needs to Evaluate the Current Legislative Framework

CCIA is hopeful that the Commission's proceedings will lead to a comprehensive and impartial review of consumer expectations and potential concerns associated with both government and commercial access to data, data collection practices, retention, use, and disclosure. The Commission should evaluate what baseline standards are needed to help consumers and businesses more easily understand their rights.

The U.S. approach to consumer privacy policy has historically been compartmentalized, based upon certain industry sectors and practices, creating an inconsistent framework that can be difficult for businesses and consumers to understand. The sector-specific approach has created non-intuitive variations in coverage where consumers often have more protection in one area and less in others.

Unfortunately, security lapses and exposed loopholes tend to evoke well-intentioned but overreaching policies that pose increased threats to privacy. For example, tech companies have crafted reasonable data retention policies that seek to balance operational needs, privacy and security, but are often pitted between privacy advocates who favor reduced retention periods and law enforcement which favors increased retention periods and the storage of vast amounts of data. Several legislative proposals have supported law enforcement efforts by calling on tech companies to maintain large databases of subscribers' information for extended periods of time, but these mandatory retention laws place onerous burdens on tech companies and weaken consumer trust.

B. Industry Self Regulatory Efforts

The Commission's thoughtful review of behavioral advertising and the resulting principles for self-regulation were a welcome addition to the discussion of online privacy issues. It is clear that the Commission considered the full range of options and perspectives on this topic when issuing these guidelines and reflected consistent thinking throughout the online community. The Commission's focus on transparency and consumer control, reasonable security, affirmative express consent for changes in the use of information, and ban on the use of sensitive information shows a consumer-centric framework to guide industry in information collection practices. As a result, leading advertising industry associations went a step further and issued their own set of comprehensive principles for the use and collection of data for online targeted advertising. In addition to reinforcing key concepts highlighted in the FTC's principles, the industry principles also called for industry-wide participation in an educational campaign and accountability program. As a result, we have seen companies involved in consumer information tracking and targeted advertising widely adopt and expand upon the guidelines set forth. However, considering the industry principles were only released this past summer, it is too soon to judge the complete success of these efforts.

CCIA continues to support industry efforts to create self-regulatory principles and practices that are consumer-friendly and provide meaningful transparency and choice. CCIA's member companies have taken proactive steps to consult with consumer groups, privacy advocates and government experts when crafting policies and practices. We believe that companies on the front lines of user protection and customer service are in the best position to understand and anticipate consumer needs.

C. Federal Privacy Legislation

Given the patchwork, silo-like nature of current privacy law, calls for comprehensive federal privacy legislation that would create basic rules of the road and establish a uniform framework for online and offline privacy protection are not without basis. The Commission's proposed roundtables should assist the public and private sectors in identifying and exploring issues that require further study. Ultimately, these roundtables may assist in the formulation of federal privacy policy that takes a comprehensive and technology neutral approach, which would make it easier for businesses to comply across multiple jurisdictions.

Finally, privacy policy should not legislate business models. Technology continues to rapidly change and any attempt to regulate business practices could potentially stifle innovation. Instead government should encourage companies to innovate in how they provide notice and choice, and support new creative models. More specifically, the Commission should focus on working with industry to empower consumers to better understand policies and practices, as well as the costs and benefits. The Commission can also play a role in helping and encouraging industry to create policies that are transparent, easy to find, and easy to understand. After careful review and examination of these issues, the Commission will be better armed to help craft privacy solutions that put consumers first.

D. Emerging Technologies

Emerging services in the realm of cloud computing and mobile technology have experienced rapid growth in recent years. While cloud-based services are mainly the result of rapid technological innovation and increased high-speed broadband offerings, the recent financial crisis has accelerated their deployment as companies and consumers seek to trim the

large overhead costs associated with advanced IT services. Because many different areas of policy, including privacy policy, may affect the continued growth of these technologies not only must the infrastructure be designed in such a way as to resist computer intrusion, but policies and design must also discourage improper surveillance by foreign and domestic authorities. If privacy protections are eviscerated by political demands, it could have drastic effects on the accelerated move towards ubiquitous access. Companies with better guidance and the legal backing to confidently protect consumers from undue intrusions will feel compelled to invest in further innovations and deployment.

V. Recommendations

CCIA proposes that the Commission consider the following recommendations as it continues to explore consumer online privacy:

- *Consumer Report* – More research and information is needed to better understand consumer needs, expectations and concerns. Just as the FTC's 2003 *To Promote Innovation* report proved to be an invaluable resource in informing and shaping the patent reform debate, the FTC should consider preparing a similar report on privacy issues so that the policy process can benefit from an in depth look at the impact on consumers. Sound privacy policy must be based upon a clear understanding of what consumers expect, what consumers need, and what we need to protect consumers from.

- *Advisory Board* – The FTC should consider establishing an advisory board for a complete comprehensive review of the current privacy framework to understand what areas still present challenges for consumers. The advisory board should be composed of representatives of the various stakeholders with interests in consumer protection online, including the advertising

industry, website publishers that display contextual or targeted ads, bloggers, IAPs, companies deploying interest based advertising, the financial services sector, public interest and non-profit groups, consumer and privacy advocates, U.S. government officials, international government officials, the wireless industry, and remote computing services. The advisory board should review and outline the various areas of current coverage based on sector-specific pieces of privacy legislation. This information would be useful in recommending specific updates to existing privacy law and pinpointing any need for potential additional coverage. The advisory board would also further review industry self-regulatory regimes and best practices over a reasonable period of time. At the end of a certain period of time, the advisory board would submit a report and recommendations.

VI. Conclusion

A commitment to openness and growth in electronic commerce cannot be sustained if end users lack confidence in the privacy and security of their personal and business communications. Because this confidence can be undermined by both private and public action, the U.S. government can set an example as both a regulator and an actor in the privacy arena.

Respectfully submitted,

/s/ Ed Black
Ed Black, President & CEO
Danielle Yates, Director of External Affairs
Computer & Communications Industry Association
900 Seventeenth Street NW, 11th Floor
Washington, D.C. 20006
(202) 783-0070