Before the
Federal Trade Commission
Washington, D.C.

In the Matter of

"Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"

COMMENTS OF
COMPUTER AND COMMUNICATIONS INDUSTRY ASSOCIATION

In response to the Federal Trade Commission (FTC) release of a preliminary staff report entitled *Protecting Consumer Privacy in an Era of Rapid Change*, the Computer and Communications Industry Association (CCIA) submits the following comments.[1]

CCIA is an international 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 $220 billion.[2]

While the FTC raised many important questions in its preliminary staff report, these comments will focus on four topics in particular: 1) establishing clear and reasonable regulations limiting government surveillance; 2) the importance of technology neutrality in the promulgation of privacy rules; 3) preserving innovation while protecting privacy, and; 4) the FTC's Do Not Track proposals.

---

[1] FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESS AND POLICYMAKERS (2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf [hereinafter FTC Report].
[2] A complete list of CCIA's members is available online at http://www.ccianet.org/members.

I. Introduction

The Internet has drastically changed the way that consumers learn, contribute to society, and shop. In particular, it has changed how they interact, both with each other and with the data that they produce. As a result of these interactions, more and more consumers are moving their sensitive and personal information and communications online. As this happens, 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 the work it has done on the preliminary staff report and for its ongoing determination to address questions of consumer privacy, data collection, and innovation in the Internet marketplace. The FTC has been a leader in this area for many years. We believe it is vital for regulators to take the opportunity to understand emerging technologies and their impacts on consumers.

The explosion in Internet services over the past decade has provided consumers with unprecedented ways to create, communicate, and work. The ingenuity that has driven that explosion has flourished in the environment of light touch regulation implemented by both Congress and the Commission. Continuing that legacy will ensure the future growth of the Internet and the promise of the digital age.

That diversity of opportunity on the Internet and broad access to technology has led consumers to moving more and more of their private lives into a digital realm without an intention to share that information with others.[3] This shift has ramifications for privacy that are now starting to be explored, both by the industry and by the FTC in this staff

[3] *See, e.g.*, Google Documents, http://docs.google.com (giving people the ability to compose, store, and edit office documents online but maintaining their privacy and secrecy from others).

report. Privacy loss and the threat of privacy loss can cause damage to consumers' wellbeing and to their confidence in the potential of the Internet. At the same time, harsh government regulation runs the risk of quashing the growth of online businesses. U.S. privacy policy should be carefully crafted to balance the need for innovation with threats to consumer confidence.

II. Government surveillance of Internet communications must be restricted in ways that comport with the reasonable expectations of consumers to avoid uncertainty and allow both individuals and businesses to understand privacy rights and how to comply with and invoke the protection of U.S. privacy laws.

Technologies are not immune from governmental overreaching and any review of U.S. privacy policy must take into account governmental intrusions. As a general proposition, CCIA believes in the robust application of basic Fourth Amendment protections against undue search and seizure of electronic communications. CCIA is also wary of any expansion of government mandates in the Communications Assistance for Law Enforcement Act that would apply beyond underlying telecommunications networks.

A. Modernizing the Electronic Communications Privacy Act is a vital step toward increasing consumer trust and providing certainty to businesses

While the provisions of ECPA[4], written in 1986, may have made sense in a world just beginning to experience the possibilities of the digital revolution, today's world, 25 years later, presents a vastly different landscape in the way that people interact with their data and the Internet at large. Many of the preconceptions underlying the operation of

[4] The Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510, *et seq*.

ECPA are no longer relevant, causing confusion for consumers and creating problems for business. To bring government access to data into line with the public's general expectations of privacy in online data, basic Fourth Amendment protections against unreasonable searches or seizures should apply to data stored online, just as it does under current caselaw to data stored on a personal computer. CCIA also supports the ECPA updates advanced by the Digital Due Process Coalition ("DDP"), of which CCIA is a member.

i. Courts are still divided over granting Fourth Amendment protections in the Internet realm, and much is still left to do.

Historically, the Fourth Amendment protected postal mail from governmental inspection during delivery.[5] This privacy right in one's mail extended to mail carried by the U.S. Postal Service as well as private carriers such as United Parcel Service and Federal Express. While some minimal exceptions applied,[6] people generally held privacy rights in mail sent by or delivered to them. As e-mail and other electronic messaging systems (such as Facebook's internal messaging system) become more dominant forms of communicating, U.S. courts have generally been hostile to the idea of extending these postal mail Fourth Amendment protections to electronic communications.

A recent decision by the U.S. District Court for the District of Oregon highlights the potential troublesome outcome for Fourth Amendment protection in the context of ECPA. In *In re Application of U.S. for Search Warrant*, the District Court concluded that law enforcement officials did not have to inform an e-mail account holder of a warrant to

[5] *See, e.g., Ex parte Jackson*, 96 U.S. 727 (1878).
[6] No privacy right extended to USPS mail sent as "fourth class," which reserved for the USPS the right to inspect the mail. Further, the protection applied only to the *content* of the mailing, not to anything on the outside of the envelope or package (i.e. addresses and names).

search the contents of his or her e-mail account.[7] Instead, the court found sufficient notice served only to the Internet Access Provider (IAP) and not the account holder. The court premised its decision on the theory that a person must access the Internet through an IAP and, in doing so, the user's information passes through, or may even be stored on, servers owned by the IAP. By means of this process, the Court concluded that the information was no longer private information contained in the home and, thus, not protected by ECPA or the Fourth Amendment.

Similarly, the Eleventh Circuit recently also rejected extension of Fourth Amendment protection to e-mails based on a third-party access rationale. In *Rehberg v. Paulk*, the Eleventh Circuit held that, "a person . . . loses a reasonable expectation of privacy in emails, at least after the email is sent to and received by a third party."[8] The court found the government's subpoenaing of defendant's e-mails from an IAP not to violate the defendant's Fourth Amendment rights as the e-mails were subpoenaed directly from the IAP and not, "an illegal [search of defendant's] home computer for e-mails."[9]

In contrast, the Sixth Circuit in December took the opposite view. In *U.S.* v. *Warshak*, the court of appeals held that e-mails stored with an IAP on behalf of a customer naturally carry a "reasonable expectation of privacy" and therefore must be protected under the Fourth Amendment.[10] The court recognized that e-mail is an obvious modern analogy to paper mail, and distinguished it from mere business records provided to a third party, such as bank records.[11] As a consequence, the court also held that the

---

[7] *In re Application of U.S. for Search Warrant*, 665 F.Supp.2d 1210 (D. Or. 2009).
[8] *Rehberg v. Paulk*, 611 F.3d 828 (11th Cir. 2010).
[9] *Id.*
[10] *U.S. v. Warshak*, ___ F.3d ___, 2010 U.S. App. LEXIS 25415 (6th Cir. 2010); *Katz v. U.S.*, 389 U.S. 347, 361 (1967).
[11] *Warshak, 2010 U.S. App. LEXIS at 25415.*

sections of ECPA that authorized access to the stored emails without a warrant were unconstitutional.[12]

While the court in *Warshak* did not see the need to draw further analogies to make its decision, it is worth pointing out that consumer expectations surrounding e-mails today can easily be compared to those surrounding telephone conversations, which the government requires a warrant to intercept under the Fourth Amendment.[13] Indeed, an e-mail sent today is the functional equivalent of a paper letter delivered using the same underlying telecommunications networks as the telephone system has always used. It is difficult to understand why a new communications technology that is an amalgamation of two older technologies that both enjoy Fourth Amendment protections should go without that same protection.

This uncertainty in extending Fourth Amendment protections to electronic communications, in a world where e-mail serves as a dominant form of communication, will continue to shake consumer confidence in adoption of broadband as an efficient tool for daily communications. Protection from government intrusion must evolve as technology evolves. In order for the pervasiveness of e-mail to continue and for innovative means of communicating to evolve, it is vital that consumers can expect to receive the same protections while using these technologies that they receive for a paper letter.

Since the Fourth Amendment should extend to anywhere "a reasonable expectation of privacy" exists, and it is likely that reasonable consumers today expect privacy in their electronic communications, the protections prescribed by the Fourth

[12] *Id.*
[13] *Katz*, 389 U.S. at 361.

Amendment should be extended to those communications in order to preserve consumer confidence. While the FTC is clearly not in a position to dictate the future interpretation of the Fourth Amendment, it should encourage, to the extent possible, decisions in the courts that better develop U.S. privacy policy in this way. This approach should, however, be accompanied by revisions to ECPA as well.

ii. DDP's proposed ECPA revision help clarify privacy standards for both individuals and businesses and effectively accommodate technological advancements, including the tracking and collection of geolocation data.

DDP advocates four specific ECPA revisions that seek better protection for data shared or stored online.[14] These revisions will also allow for better protection from governmental bulk data requests. CCIA agrees with DDP's assessment that such revisions are necessary to better ensure clarity for both individuals and business in what ECPA standards to apply to information and data online.

The first recommended ECPA revision would require law enforcement to obtain a search warrant based on probable cause before obtaining private communications or documents stored remotely.[15] Such a revision merely extends the traditional privacy protections provided to documents physically held in the home to the Internet realm. The second revision would require law enforcement to obtain a search warrant before tracking people's location via technological measures such as cell phones, GPS receivers, or other devices with such capabilities.[16] The third revision would require law enforcement to submit proof that the information sought is relevant to a criminal investigation before

[14] "Specific Background on ECPA Reform Principles," Digital Due Process Coalition, available online at http://www.digitaldueprocess.org/index.cfm?objectid=C00D74C0-3C03-11DF-84C7000C296BA163.
[15] *Id.*
[16] *Id.*

electronic surveillance of a particular person begins.[17] The fourth revision would require law enforcement to submit proof the information sought is not only relevant to a criminal investigation, but is in fact essential, before it may obtain bulk information about broad groups of unknown and likely unrelated telephone or Internet users.[18]

In particular, DDP's proposed ECPA revisions would help companies and individuals better understand the privacy concerns of an increasingly important technological development: the tracking and collection of geolocation data. Mobile phone service providers are being bombarded with law enforcement requests for both real-time tracking of mobile devices and collected geolocational data of mobile devices in connection with searches and surveillance. Meanwhile, privacy advocates argue that disclosure of such information violates the subscriber's privacy. Geolocational data may also be collected by social networking websites, based on the user's location, often through a global positioning system ("GPS") on the user's mobile device or triangulating the device's signal via cell towers. ECPA today gives no clear guidance on the process necessary to obtain this information, and different districts – and even different judges within a given district – have varying interpretations and requirements.[19] DDP's proposed ECPA revisions help solidify standards of when telecommunications companies can and cannot hand over users' geolocational data to law enforcement authorities.

Finally, revisions of ECPA would help tech companies better draft policies that strike a balance between law enforcement needs and user privacy and security. As it

---

[17] *Id.*
[18] *Id.*
[19] *Electronic Communications Privacy Act Reform and the Revolution in Location Based Technologies and Services Before the Subcomm. On Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. (2010) (statement of the Hon. Stephen Wm. Smith, United States Mag. J.) (giving an overview of the approach to judicial process requirements for cell site location data) *available at* http://judiciary.house.gov/hearings/pdf/Smith100624.pdf.

stands now, law enforcement seeks access from tech companies to any databases of retained consumer information they may keep under unclear aspects of ECPA. These large numbers of requests not only place onerous burdens on the tech companies themselves, but also result in weakened consumer trust in both companies and Internet technology itself. Although companies are trying to walk this fine line now with balanced data acccess policies, the outdated aspects of ECPA results in companies being stuck between privacy advocates demanding less access and law enforcement favoring increased access, with ECPA providing little to no clarity on how to proceed.

B. Government attempts to revise CALEA should be treated warily and implemented, when absolutely necessary, in the narrowest way possible, to protect privacy and cybersecurity and encourage innovation.

Recently, federal law enforcement has begun to suggest that modern communications trends have created an environment in which the government cannot obtain the evidence they need because the infrastructure does not exist to capture and turn over that information.[20] The FBI has suggested revising the Communications Assistance for Law Enforcement Act[21] to include mandates that would make access to this information easier for the government to obtain. While CCIA is mindful of the challenges that law enforcement faces in the modern age, we are wary of the implications and unintended side effects of implementing a wide array of backdoor access features in an uncountable number of new and yet-to-be-invented communications software, services,

[20] *See* Charlie Savage, "Officials Push to Bolster Law on Wiretapping," N.Y. Times, October 19, 2010, at A1; Charlie Savage, "Wider Web Wiretap Law is Sought," N.Y. Times, November 17, 2010, at B5.
[21] The Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1001, *et seq*. ("CALEA").

and devices. The effects on privacy, cybersecurity, and innovation must be carefully weighed before sweeping changes like those the government seeks are implemented.

To begin with, the government should be able to demonstrate, at least to key members of Congress, that the restrictions placed on law enforcement by current communications technology are actually leading to concrete difficulties in investigating and prosecuting crimes. Such information would allow Congress, the non-profit sector, and the business sector to determine whether the problems raised require a solution beyond current law and, if so, what the contours of that solution should be. If not, innovative solutions within current law might be developed. Without this information, all of these parties will be operating in the dark in an important area of public policy, risking the creation of bad law. The government understands the importance of this disclosure because they presented their specific needs to industry (then, only the phone companies) when they began the conversation that led to the current CALEA law.

If the law enforcement community can show that mandates of the type they seek are indeed necessary, any resulting law should be targeted and narrow in scope. Difficulties that law enforcement currently face should not be used as an excuse for surveillance power grabs that may lead to vastly more access than was anticipated. A narrow mandate would suffice to solve any existing problem and has the best chance of avoiding negative impacts on innovation and privacy.

There are also many substantive reasons to view the sort of mandate called for by law enforcement with suspicion. CCIA would highlight two particular problems important to our members. First is that the mere act of designing communications technologies to facilitate surveillance compromises their security. This kind of design

inevitably produces vulnerabilities that can be exploited by others, including hackers, identity thieves, and malicious insiders within a given company. This fact undermines the goals of cybersecurity, which are vitally important to our economy and national safety.

Secondly, communication over the Internet is the fundamental technological driver beneath many of the innovative and entrepreneurial business ideas that are making money and employing people in America today. These technologies are allowing people around the world to interact and share with each other in new and exciting ways and those users become customers of U.S. businesses. Extending CALEA mandates to cover these applications could stifle innovation, impact small businesses disproportionately, delay cutting-edge communications technologies from getting to market, and advantage foreign competitors over U.S. companies. They also put established companies in the unenviable position of betraying their own customers' interests. That sort of regulation is precisely what the rebounding market in Internet services in this country does not need.

III. Protecting and encouraging innovation should be a primary focus of the FTC as it addresses privacy, and those concerns should caution against calling for legislation at this time.

Avoiding consumer harm and encouraging consumer trust should be the ongoing mission of the FTC, however it must be careful to do so in in balance with other important goals such as realizing the many market benefits of data collection and furthering innovation in the online space. Online targeted advertising, for example, brings competition and innovation to the Internet. CCIA believes that before the FTC moves forward in this area, it is important to emphasize some of the positive effects of data collection.

- Data collection directly enables some of the most innovative and useful features of Internet services. To take one example, Amazon's personalized recommendations would be impossible if they did not keep collect data on each user's purchases and movement around the website, and compare them with that of all the rest of their customers.
- Targeted advertising is responsible for underwriting a rich variety of online content and services. This support allows providers to offer valuable services to consumers for little or no cost and increases the richness of content online.
- Relevant ads are preferable to those that are not relevant. Given that advertising supported services are the dominant mode of revenue for Internet content and service providers, and that consumers have shown relatively little inclination to pay out of pocket for those providers' services, consumers are better served by seeing advertisements that are tailored to their interests and which have a better chance of leading them to products or services they may genuinely enjoy.
- Targeted advertising encourages competition by lowering the barriers to entry and underwriting the ongoing costs of innovative services. Consumers therefore have robust choices about which services and products they use. This competition encourages companies to innovate, not just in the services and products they offer, but also in their privacy practices in order to attract and retain customers.

- Finally, the new online services and products supported by ad revenue, such as blog platforms and social networking sites, are able to offer free or low-cost services. The inexpensive access to the means of publication has leveled the playing field for creative output and led to the explosion in free expression that has made the Internet the true inheritor of the promise of the First Amendment.

These benefits at their heart derive from the innovation of companies and users exploring the possibilities of the Internet and were born in the culture of light touch regulation that has characterized the government's approach to online space since its early days. The industry, in concert with users, civil society, and government, is still in the process of discovering the best means of providing new and exciting services while ensuring the best protections for privacy. CCIA's member companies have been at the forefront of this dialog, inventing ways to be more transparent, give users the maximum amount of control, and securing the data with which they are entrusted. CCIA believes that civil sector solutions to privacy problems exist and that government should not cut off the industry while it searches in good faith for those answers.

The government's role in the current market should be encouraging industry, providing a space to convene, and carrying the threat of enforcement. The FTC has shown itself to be an integral part of all three of these roles, through the behavioral advertising self-regulation process, and its ongoing Section 5 enforcement proceedings.

IV. The scope of any potential regulations in the consumer privacy arena must be carefully drawn: it should be neutral across the range of technologies and actors, and should exclude some commonly accepted practices.

While CCIA believes that federal privacy legislation is premature, as discussed above, any regulation promulgated by the government should apply neutrally across the wide spectrum of parties that gather and use consumers' data in the country today. That spectrum includes companies that gather data for use in online targeted advertising, but there are many other occasions in which data is collected, and for many different reasons. The FTC explains in the scope section of its report that its recommendations apply to all companies that collect data, both online and off.[22] This language is heartening, but CCIA is worried that other sections of the FTC's preliminary staff report may give the impression that the FTC is unduly focused on the impacts of specific collection in specific circumstances: the online collection by websites and advertisers for use in targeted advertising. CCIA encourages the FTC to continue to keep a broad view of the scope of regulation and to avoid regulations tailored only to a subset of companies. CCIA also recommends that the FTC instead take into account distinctions between collectors of data based upon the level of intrusion into the consumer's data and the consumer's access to competing services.

The universe of companies that gather data on consumers is not limited to online services. Supermarkets and other retailers, for example, offer customers discounts on items in exchange for the ability to track every purchase the consumer makes and to use that data for their own purposes. These retailers get the consent of the consumer using disclosures that are generally no clearer than those used online.[23] Data brokers, who have an enormous impact on consumer privacy and have little to no transparency in their business processes, similarly collect some of the data they use offline.

---

[22] FTC REPORT, *supra* note 1, at 42.
[23] *See, e.g.*, Daniel Terdiman, *Gaming the Safeway Club Card*, WIRED, July, 11, 2003, *at* http://www.wired.com/techbiz/media/news/2003/07/59589.

Even among those companies that collect consumer data online, search engines, social networks, and other websites are not the sole source of privacy related concern. In particular, Internet Access Providers (IAPs) have given us plenty of reason to worry about the unfettered access they have to consumers' online information. Internet Access Providers can, though a technique known as deep packet inspection (DPI) – which intercepts and stores the contents of every piece of data that is sent or received by the user – monitor the online behavior of a consumer at the network level across every website and service on the Internet, including the content of e-mail messages.[24] Moreover, whereas an online service or website that violates consumer trust may find consumers fleeing to a competitor that is only a click away, the lack of significant competition among broadband providers poses problems for consumers and businesses alike.[25] Many customers have no alternative to their IAP if the IAP breaches its privacy policy or otherwise violates consumers' trust. Other consumers may simply find that any competitors they do have access to have identical policies and that switching costs – such as early termination fees – are too high. These factors argue in favor of greater levels of disclosure of network activity monitoring practices to the consumer in these cases and heightened requirements for consumer choice.[26]

There are many threats to consumer privacy in today's data driven world. The above examples are just a few of them. The FTC should be commended for laying out

---

[24] *See* Nate Anderson, *Deep Packet Inspection Meets 'Net Neutrality, CALEA*, Ars Technica, July 25, 2007, *at* http://arstechnica.com/hardware/news/2007/07/Deep-packet-inspection-meets-net-neutrality.ars (providing an in depth description of deep packet inspection technologies and uses).

[25] *See* FEDERAL COMMUNICATIONS COMMISSION, INTERNET ACCESS SERVICES: STATUS AS OF DECEMBER 31, 2009 64 (2010) *at* http://www.fcc.gov/Daily_Releases/Daily_Business/2010/db1208/DOC-303405A1.pdf (map of number of providers of at least 3 mbps Internet access, by census tract, showing much of the country served by fewer than 3 providers and in many cases none).

[26] FEDERAL COMMUNICATION COMMISSION, PRESERVING THE FREE AND OPEN INTERNET, GN DOCKET NO. 09-191, para. 56 (requiring disclosure of network management practices affecting consumer service).

such a broad scope for its proposals and CCIA encourages solutions that address all collectors of data, both offline and on, equally, and that instead distinguish based on users' access to competitive services and on the invasiveness of the monitoring.

That scope is also important in what it excludes from potential regulation. The CCIA commends the FTC for proposing a privacy framework that includes the concept of "commonly accepted practices". Certain important business functions that are data-driven, such as security access controls and cybercrime and fraud prevention, should be available to companies as a matter of course and without having to wait for the consent of users. It is important, however, not to set in stone what practices fall into this category, as commonly accepted business practices shift quickly in the online marketplace and a preset group of business functions could serve to stifle that innovation.

V. A "Do Not Track" system may do much to protect consumers and give them effective choice, but its contours and definition are far too unclear to give concrete feedback.

In the staff report, the FTC suggests a system they refer to as "Do Not Track" which would give consumers the ability to opt-out of online behavioral advertising through some mechanism, potentially using a configuration within the user's browser.[27] While on the surface, this recommendation would seem to give users enhanced opportunity to exercise their choices about how their data is collected and used online, CCIA is concerned that the idea, as expressed by the FTC in its report, is too vague to be the basis for substantive comments.

[27] *See* Editorial, *Netizens Gain Some Privacy*, N.Y. Times, Jan. 29, 2011 *at* http://www.nytimes.com/2011/01/30/opinion/30sun3.html (summarizing some of the available options to implement do not track in web browsers).

Before addressing the concept of a "Do Not Track" system, CCIA would reiterate that while online targeted advertising is one way in which personal data is collected and used, it is not unique in that aspect. There are many other commercial practices that may impact consumer privacy, some of which, such as deep packet inspection by IAPs, present a much more comprehensive invasion of privacy and would not necessarily be addressed by a Do Not Track regime. CCIA would urge the FTC and others to seek broader solutions that are tailored to the many different ways in which people's privacy are put at risk.

CCIA also believes that it is important to point out that a comprehensive and broadly adopted "Do Not Track" system already exists in the area of online targeted advertising today, and was created by industry through a self-regulatory process that the FTC heartily endorsed. Most of the companies that operate advertising networks allow individuals to opt-out of tracking by their networks. CCIA members Google,[28] Microsoft,[29] and Yahoo[30] provide mechanisms for consumers to opt-out of targeted ads. Furthermore, the Network Advertising Initiative (NAI) operates an industry-wide opt out in the form of cookies placed on consumers' computers and a browser plugin that preserves the opt-out request, even if cookies are deleted from a computer.[31] The NAI opt-out cookies are respected by nearly all of the companies engaged in targeted advertising.[32]

---

[28] Google Privacy Center, http://www.google.com/privacy/ads/.
[29] Microsoft Display of Advertising, http://privacy.microsoft.com/en-us/fullnotice.mspx#display
[30] Yahoo! Privacy, http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/
[31] Network Advertising Initiative, http://www.networkadvertising.org/participating/ (listing the participating ad networks).
[32] *Id.*

A "Do Not Track" mandate may also run the risk of limiting innovation in the area of privacy protection. As an example, Google's online targeted advertising system allows consumers to opt-out, if they wish, but also gives users the ability to add, edit, or remove categories from those that Google's algorithms thinks they might be interested in.[33] Google has found that consumers, once they understand how the system works, become more comfortable and are therefore more likely to modify Google's stored preferences than they are to opt-out entirely.[34] Yahoo!'s advertising system contains a similar system.[35] This sort of innovation in privacy protection should be encouraged, and any "Do Not Track" system should be carefully tailored to leave room for new developments that give consumers more control over how data about them is used.

With all of that said, it may still be the case that an official government-sanctioned "Do Not Track" system would be of benefit to consumers while protecting innovation. It is hard to provide commentary on such a proposal, however, without further details on what might be mandated or prohibited and how the program would be implemented. In fact, this dearth of information has led to a multitude of differing interpretations in the public mind about the potential details of a framework and multiple implementations by browser providers, each envisioning a different approach.[36]

The FTC's proposal may be as simple as a government mandate to provide a means of opting-out, which will be met already by many online companies, and which is meant to force the hand of those small number of companies that track online behavior

[33] Google Ad Preferences Manager, http://www.google.com/ads/preferences/.
[34] GOOGLE, INC., COMMENTS TO THE DEPARTMENT OF COMMERCE IN RESPONSE TO INFORMATION PRIVACY AND INNOVATION IN THE INTERNET ECONOMY 7 (2011), http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/FINALCommentsonDepartmentofCommercePrivacyGreenPaper%20(3).pdf.
[35] Yahoo! Ad Interest Manager, http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/.
[36] *See* Harlan Yu, *Some Technical Clarifications About Do Not Track*, FREEDOM TO TINKER, Jan. 11, 2011, http://www.freedom-to-tinker.com/blog/harlanyu/some-technical-clarifications-about-do-not-track.

but do not recognize an opt-out. If that were the case, CCIA would have no strong opposition to the proposal. If, however, the FTC is suggesting mandates that will modify the existing technological and economical structures of the web, CCIA would advise caution against that approach. Similarly, a broader requirement that would involve new technical obligations on every U.S. website would be an overreaching step by government. Among other problems, these suggestions would constitute a specific technological mandate by government on the operation of the Internet, an area where government has historically not tread, and for good reason.

VI. Conclusion

Maintaining consumer confidence and trust in the online marketplace is essential to the continued openness and growth of the Internet. Protecting users' privacy in both personal and commercial communications is an integral part of that trust, but that protection must be balanced against the rapid innovation by companies both large and small that has been the driving force behind the growth of the Internet. CCIA looks forward to working with the FTC to achieve that balance.

Respectfully submitted,

/s/ Ed Black
Ed Black, President & CEO
Ross Schulman, Public Policy & Regulatory Counsel
Computer & Communications Industry Association
900 Seventeenth Street NW, Suite 1100
Washington, D.C. 20006
(202) 783-0070