

*Before the*  
**Department of Commerce**  
**National Telecommunications and Information Administration**  
Washington, D.C.

*In the Matter of*

Information Privacy and Innovation in the  
Internet Economy

Docket No. 101214614-0614-01

**COMMENTS OF**  
**COMPUTER AND COMMUNICATIONS INDUSTRY ASSOCIATION**

In response to the Department of Commerce's release of a green paper entitled *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, the Computer and Communications Industry Association (CCIA) submits the following comments.<sup>1</sup>

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.<sup>2</sup>

The Department of Commerce raised many more important and interesting questions than could be answered in the space of this comment. These comments will therefore focus on three issues of particular importance to our members: 1) establishing clear and reasonable regulations limiting government surveillance; 2) the importance of

---

<sup>1</sup> National Telecommunications and Information Association, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (2010) ("IPTF Privacy Green Paper"); "Information Privacy and Innovation in the Internet Economy; Notice and Request for Public Comments," 75 Fed. Reg. 244 (Dec. 2010), pp. 80042-80044.

<sup>2</sup> A complete list of CCIA's members is available online at <http://www.ccianet.org/members>.

encouraging Fair Information Practices Principles (FIPPs) as a minimum basis for protection of consumers' data, and; 3) instituting a collaborative process for developing flexible but enforceable codes of conduct for particular industries to supplement the baseline FIPPs with voluntary rules tailored to particular privacy challenges.

## **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 in the data they share with each other socially and with the personal 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, and consumers, and implicate the First, Fourth, and Fourteenth Amendments with respect to government action.

CCIA commends the Department of Commerce for the work it has done on the green paper and for its determination to address questions of consumer privacy, data collection, and innovation in the Internet marketplace. 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 collaborate. The ingenuity that has driven that explosion has flourished in the environment of light touch regulation that has been the hallmark of Internet policy for the past two decades. Continuing that legacy is essential to ensuring the continued growth of the Internet and the promise of the digital age.

That same diversity of opportunity on the Internet and through technology has led consumers to move more and more of their private lives into the digital realm, even without an intention to share that information with friends.<sup>3</sup> This shift has ramifications for privacy that are now starting to be explored, including by the Department of Commerce in this paper. 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 internet 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 (ECPA) is a vital step toward increasing consumer trust and providing certainty to businesses**

---

<sup>3</sup> 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).

While the provisions of ECPA<sup>4</sup>, 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 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 revisions 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.<sup>5</sup> 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,<sup>6</sup> 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 the 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.

---

<sup>4</sup> The Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510, *et seq.* (“ECPA”).

<sup>5</sup> *See, e.g., Ex parte Jackson*, 96 U.S. 727 (1878).

<sup>6</sup> 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).

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 search the contents of his or her e-mail account.<sup>7</sup> 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 rejected extension of Fourth Amendment protection to e-mails. 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."<sup>8</sup> 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."<sup>9</sup>

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

---

<sup>7</sup> *In re Application of U.S. for Search Warrant*, 665 F.Supp.2d 1210 (D. Or. 2009).

<sup>8</sup> *Rehberg v. Paulk*, 611 F.3d 828 (11th Cir. 2010).

<sup>9</sup> *Id.*

protected under the Fourth Amendment.<sup>10</sup> 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.<sup>11</sup> As a consequence, the court also held that the sections of ECPA that authorized access to the stored emails without a warrant were unconstitutional.<sup>12</sup>

While the court in *Warshak* did not see the need to draw further analogies to make its decision, it is worth pointing out that 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.<sup>13</sup> 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 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 from these technologies that they receive in a handwritten letter.

---

<sup>10</sup> *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).

<sup>11</sup> *Warshak*, 2010 U.S. App. LEXIS at 25415.

<sup>12</sup> *Id.*

<sup>13</sup> *Katz*, 389 U.S. at 361.

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 Amendment should be extended to those communications in order to preserve consumer confidence. The Department of Commerce Court should encourage, to the extent possible, decisions 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 helps to 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.<sup>14</sup> 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.<sup>15</sup> Such a revision merely extends to the Internet realm the traditional privacy protections provided to documents physically held in the home. The second revision would require law enforcement to obtain a search warrant before tracking people’s location via cell phones or other devices.<sup>16</sup> The third revision would require law enforcement to submit proof that the information sought is relevant to a criminal

---

<sup>14</sup> “Specific Background on ECPA Reform Principles,” Digital Due Process Coalition, available online at <http://www.digitaldueprocess.org/index.cfm?objectid=C00D74C0-3C03-11DF-84C7000C296BA163>.

<sup>15</sup> *Id.*

<sup>16</sup> *Id.*

investigation before electronic surveillance begins.<sup>17</sup> 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 needed, before it may obtain bulk information about broad categories of unknown telephone or internet users.<sup>18</sup>

Additionally, 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. DDP's proposed ECPA revisions help solidify standards of when telecommunications companies can and cannot hand over users' geolocational data to law enforcement authorities.

Revisions of ECPA would help tech companies better craft policies that strike a balance between operational needs and user privacy and security. As it stands now, law enforcement agencies are strongly encouraging tech companies to keep large databases of retained consumer information, and are seeking legislation to make it mandatory. These requirements not only place onerous burdens on the tech companies themselves, but also result in weakened consumer trust in both companies and Internet technology itself.

---

<sup>17</sup> *Id.*

<sup>18</sup> *Id.*

Although companies are trying to draft such balanced data retention policies right now, the current state of ECPA results in companies being stuck between consumer privacy advocates demanding less retention and law enforcement favoring increased retention, with ECPA providing little to no clarity on how to proceed.

**B. Government attempts to expand CALEA should be treated warily and implemented, when absolutely necessary, in the narrowest way possible, to protect privacy and cybersecurity and maintain our great pace of 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.<sup>19</sup> The FBI has suggested revising the Communications Assistance for Law Enforcement Act<sup>20</sup> 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, 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,

---

<sup>19</sup> 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.

<sup>20</sup> The Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1001, *et seq.* ("CALEA").

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 faces 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 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. A focus on comprehensive Fair Information Practice Principles (FIPPs) is a much-needed departure from the previous simplistic focus on notice and choice alone, but enshrining them in legislation would be premature and difficult, and the government should focus on using other means to encourage adoption.**

For a long time, the focus in consumer privacy policy was on a regime often called “notice and choice.” This approach emphasized informing the user of the terms on which his data would be collected, used, and shared, and giving the user the ability to choose whether he wanted to use the service under those terms. Those terms usually took the form of long-winded and legalistic privacy policies that served more to confuse than enlighten the average user, when they were read at all. In addition, choice is only a useful mechanism if the consumer truly has a choice. In the case of duopoly Internet Access Providers, for example, the end user has no choice if both providers have the same or similar terms of service. Recognizing these problems in the overly simplistic notice and choice approach, bodies as diverse as the U.S. Department of Health, Education, and Welfare,<sup>21</sup> the Organization for Economic Cooperation and Development,<sup>22</sup> the U.S.

---

<sup>21</sup> U.S. Department of Health, Education and Welfare, Records, Computers, and the Rights of Citizens (1973), *available at* <http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm>.

Federal Trade Commission,<sup>23</sup> and the U.S. Department of Homeland Security<sup>24</sup> (DHS) have over the years developed sets of principles that provide a holistic and balanced approach to designing systems that will collect and use information from users.

These principles incorporate the ideas of notice and choice, but expand upon them and add further structure to the balance between the user and the collector of data. For example, the DHS FIPPs include a principle on security that discusses the appropriate ways for a collector to protect the data it holds from unauthorized access or use. These FIPPs have become an important tool for privacy professionals designing data systems for use in diverse situations. Encouraging their use across a broad swath of industry would be a strong step toward more robust privacy protections while still maintaining flexibility of implementation for each individual data collector to adapt in ways that best fit their business model.

Despite their usefulness in developing privacy practices, the Department of Commerce should refrain from encouraging the enactment of FIPPs practices into federal law for a number of reasons. As can be seen from the evolution of the commonly accepted FIPPs, from the original HEW principles developed in 1973, to the OECD, FTC, and finally to the DHS versions widely used today, the concept of what constitutes best practices is constantly changing. To enshrine today's understanding of the state-of-

---

<sup>22</sup> Organisation for Economic Co-operation and Development, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), *available at* [http://www.oecd.org/document/18/0,2340,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html).

<sup>23</sup> FTC Staff, Fair Information Practice Principles (1998), *available at* <http://www.ftc.gov/reports/privacy3/fairinfo.shtm>. *See also* FTC Staff, FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising (2009), *available at* <http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf>.

<sup>24</sup> Hugo Teufel III, Chief Privacy Officer, DHS, Privacy Policy Guidance Memorandum (Dec. 29, 2008), *available at* [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_policyguide\\_2008-01.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf).

the-art into a difficult-to-change law would prevent the innovation in privacy practices that has brought the existing FIPPs into their modern form.

Furthermore, the FIPPs work best when they are used as a guideline and as a statement of intent. They contain aspects of principles or recommended behaviors that are inapplicable in some instances. Similarly, they may also not have principles that readily address the challenges of unforeseen business cases. The strength of the FIPPs are their flexibility in application. By creating a legislative solution that enforces the FIPPs as they are, the law would create waste in situations where not all the principles were necessary and be inadequate in cases that the FIPPs do not anticipate.

- A. **The principle of transparency is a fundamental aspect of privacy protection, and the Department of Commerce should encourage a focus on going beyond the previous concept of pure notice, and consider liability concerns raised by simpler-to-understand notice schemes.**

The FIPPs element of transparency is one of the more important of the principles. It is concerned with the many ways in which a data collector can and should inform the user of what information is being collected and how it will be used, along with a number of other pieces of important information. This principle calls for more than the strictly legal language usually contained within privacy policies that users generally agree to. Transparency may require alternate models of informing the user. For example, the concept of “layered notice” maintains the legalese of the privacy policy but adds simpler and more descriptive notices on top of the privacy policy, in an attempt to give the user an easier to understand description of what may happen if he agrees. The flexibility of the transparency principle allows individual companies to experiment with the most effective way of communicating with their customers.

Privacy policies themselves should not generally be done away with, however. They still provide an element of transparency for those consumers who want to know the intimate workings of a company's privacy operations, and provide exhaustive details for more legally minded observers in civil society, among other uses. In addition, they are an important accountability resource for enforcement elements of the government. The FTC, in a number of cases, has successfully used companies' privacy policies to bring Section 5 actions when those policies are violated.<sup>25</sup>

This accountability aspect of privacy policies raises a final transparency related issue that the Department of Commerce should address. Companies that are trying today to implement modern FIPPs are experimenting with alternate means of educating consumers about their collection and use of data. These alternate means often supplement the privacy policies and are easier to understand. There is some concern, however, that the simpler privacy explanations may be legally binding, but without the context that would be provided by the full legal language in the privacy policy. There is no settled legal answer to this question yet, and CCIA encourages the Department of Commerce to consider means of encouraging this sort of simplified transparency while balancing the concerns of expanded and unclear legal liability.

B. **The principles of purpose specification and use limitation can stifle innovation, as “serendipitous reuse” of gathered information can serve the consumer without leading to improper disclosure of data.**

The Department of Commerce should be careful with two particular principles often articulated in FIPPs: purpose specification and use limitation. Purpose specification

---

<sup>25</sup> See, e.g., *In the Matter of Twitter, Inc., a corporation*, Complaint, FTC File No. 092 3093 (2010) available at <http://www.ftc.gov/os/caselist/0923093/100624twittercmt.pdf> (Section 5 action against Twitter for violating their privacy policy when an outside party gained administrative access to the server and read profiles set to private and messages sent between users, both of which should have been private).

states that a data collector should inform the user of why data is being collected, and to what purpose it will be put. Use limitation recommends that the data collector constrain its usage of the data to those purposes it listed in the purpose specification. The two working together restricts a data collector to only engaging in uses of data that it informed the user of ahead of time.

This is generally a desirable result. Users should have some reassurance that a data collector will do what it says it will with the data it collects. When implemented overly strictly, however, the principles discourage innovation and what Tim Berners-Lee (the inventor of the World Wide Web) refers to as the “serendipitous reuse” of data.<sup>26</sup> Companies that collect data for one purpose, and later discover a different purpose that both benefits the consumer and results in no further disclosure of the data than has already occurred should not be prohibited from expanding their business model and developing novel products or services.

CCIA would recommend that the Department of Commerce carefully consider the effect that strict enforcement of the use limitation and purpose specification principles would have. It may be better to seek a middle way that recognizes the value in these principles but still gives a data collector some latitude to develop novel and beneficial uses for the data. As an example, unanticipated uses of the data may be acceptable if they do not involve transfer of the data beyond the original collector. Other reasonable balances with such “serendipitous reuse” can be imagined and experimented with, but the importance of innovation should not be overlooked.

**IV. The Department of Commerce should work to gather interested parties and encourage the development of industry-specific, flexible,**

---

<sup>26</sup> See Jonathan Bennett, *Berners-Lee: Semantic Web's success lies in cooperation*, CNet News, Sep. 19, 2006, [http://news.cnet.com/2100-1030\\_3-6117334.html](http://news.cnet.com/2100-1030_3-6117334.html).

**and enforceable codes of conduct that provide guidance to industry members and protection to consumers.**

The experiences of the past decade have shown that the industries that collect user data are acutely aware of the trust that is placed in their hands and that their own ability to protect the data they collect is fundamentally important to gaining and retaining customers. That is why self-regulatory efforts have been pursued by players within the industry and coordinated with the federal government. They create an opportunity to have a set of rules that assures consumers that privacy will be protected. They can also be individually tailored to particular industries, addressing the detailed concerns of a given business model, and are flexible enough to permit innovation while being enforceable by regulators when the need arises. CCIA supports the Department of Commerce's proposal to convene industry players in order to create these codes of conduct and to give the FTC the resources it needs to act as an effective enforcement body for those agreements.

It is easy to see that these types of self-regulatory efforts work, because they have been ongoing for the past few years. The most famous of these efforts involves the online targeted advertising marketplace. Led by the Federal Trade Commission, the industry gathered, along with civil society and representatives of government, at a series of roundtable discussions, out of which arose an industry cooperative dedicated to developing self-regulatory principles that have been in effect for around 18 months.<sup>27</sup>

One particular element that grew out of the process was the universal opt-out

---

<sup>27</sup> FTC Staff, "Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles (Dec. 20, 2007), *available at* <http://www.ftc.gov/os/2007/12/P859900stmt.pdf>; FTC Town Hall, "Ehavioral Advertising: Tracking, Targeting, & Technology" (Nov. 1-2, 2007), *available at* <http://www.ftc.gov/bcp/workshops/ehavioral/index.shtml>; FTC Staff, FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising (2009), *available at* <http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf>. *See also* "Self-Regulatory Principles Overview," The Self-Regulatory Program for Online Behavioral Advertising, *available at* <http://www.aboutads.info/principles>.

implemented by the Interactive Advertising Bureau, which gives users the ability to remove themselves from targeted advertising by nearly every existing ad network with just one click.<sup>28</sup> This sort of industry collective effort is exactly the type of enforceable restriction that provides assurances to users, but which is adapted to the industry in question, and gives them the ability to evaluate privacy concepts that are inapplicable to them, and develop new ones that pertain better.

The progress of the self-regulatory effort surrounding online targeted advertising shows that criticism of the concept of industry codes of conduct is premature. In the years that the effort has been ongoing, it has developed into a robust conversation on protection of privacy, managed by a coalition of advertising groups. Because of its self-regulatory nature, the coalition is always engaged in reexamining and revising their progress, and making advancements, including the recent announcement of a program to use universal icons to highlight targeted ads from many different ad networks around the Internet and provide a convenient link to more information for consumers and an opportunity to opt-out.<sup>29</sup> Declaring today that self-regulatory efforts are incapable of providing a workable solution is to ignore the fact that they are in the process of doing so in at least one instance. The Department of Commerce should recognize the potential in this system and make effective use of it as suggested in the green paper.

## **V. Conclusion**

---

<sup>28</sup> See “Opt Out From Online Behavioral Advertising,” The Self-Regulatory Program for Online Behavioral Advertising, *available at* <http://www.aboutads.info/choices>.

<sup>29</sup> See “Advertising Option Icon Application,” The Self-Regulatory Program for Online Behavioral Advertising, *available at* <http://www.aboutads.info/participants/icon>. See also “Google Ad Preferences Manager”, Google, *available at* <http://www.google.com/ads/preferences/>; “Yahoo! Privacy: Ad Interest Manager,” Yahoo!, *available at* [http://info.yahoo.com/privacy/us/yahoo/opt\\_out/targeting/details.html](http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/details.html).

CCIA thanks the Department of Commerce for taking the time to think carefully about the many complex issues surrounding consumer privacy and business data security in today's marketplace, and for the opportunity to present comments in response to the green paper. Consumer and small business trust in online companies is as vital to the Internet's growth as is the freedom on the part of companies large and small to innovate. Our public policy must strive to balance these two interests to best serve the society at large. In questions of government access to data, this means that the rules for information stored online should not vary much from those for information sent by paper mail or from the expectations of users.

Where companies are the ones collecting the data, we encourage the Department to explore options such as FIPPs and self-regulatory codes of conduct. CCIA believes, however, that it is too early in the development of our understanding of how we protect privacy to enshrine current practices in legislation. Companies that are working in good faith to develop forward-looking solutions to privacy questions should be encouraged, not overruled by Congress implementing a one-size-fits-all remedy.

CCIA applauds the Department of Commerce's efforts in this area, and looks forward to helping with further analysis and policy development in any way needed.

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