November 9, 2018

David J. Redl, Assistant Secretary for Communications and Information
National Telecommunications and Information Administration
U.S. Department of Commerce
privacyrfc2018@ntia.doc.gov

Dear Mr. Redl,

The Council of Better Business Bureaus (CBBB) welcomes the opportunity to comment on the proposals of the Department of Commerce (Department) on Developing the Administration's Approach to Consumer Privacy, as put forward in the National Telecommunications and Information Administration's (NTIA) request for comment (Docket No. 180821780–8780–01).[i]

I. Introduction: BBB, Independent Self-Regulation, and Data Privacy

For more than 100 years, the Better Business Bureau has been helping people find businesses, brands, and charities they can trust. In 2017, people checked BBB profiles on businesses over 154 million times, and sought out over 403,000 BBB charity reviews—all available for free at bbb.org. Each day, BBB also processes thousands of consumer complaints about business practices, serving as a trusted intermediary between businesses and consumers.

In keeping with the BBB mission, CBBB has a long history of operating successful national and international programs focused on dispute resolution, advertising review, and independent third-party self-regulation. Notably, three of our longstanding programs are focused on data privacy practices: the Children's Advertising Review Unit (CARU), the Online Interest-Based Advertising Accountability Program (Accountability Program), and our Privacy Shield program (BBB EUPS), which operates as an official Independent Recourse Mechanism (IRM) under the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks.

CBBB is not an industry association. It is an independent, nonpartisan, nonprofit organization with a mission of fostering trust between consumers and businesses. As such, CBBB does not represent the views of any company or group of companies.

For this reason, we do not write to the Department as advocates for or against particular policy proposals. Instead, we write because of our expertise in consumer privacy and self-regulation.

Specifically, CBBB's expertise falls within the following domains:

1. Building and operating independent self-regulatory privacy programs that align incentives to encourage widespread, voluntary adoption of privacy best practices.
2. Independently substantiating and enforcing businesses' statements about certain data privacy practices, including public reporting on the outcomes of remedial actions.
3. Processing, responding to, and acting on consumer privacy complaints.
4. Serving as a mediation and arbitration mechanism to resolve privacy disputes between consumers and companies.

CBBB has decades of experience with these issues, both as an institution and as a collective of experts with a history of bringing independent self-regulatory programs from theory to practice. Our view is that any statutory or regulatory model that seeks to influence the internal operations of businesses should acknowledge the value of self-regulation. Self-regulation may be just one tool in a robust regulatory toolkit, but when deployed properly it can provide the flexibility and utility of a Swiss Army knife.

Businesses understand that aligning their practices in a way that fosters trust among their customers can redound to their benefit. At the company level, self-regulation manifests as changes in structure, policies, and operations. But self-regulation is most effective when it does not rely *entirely* on companies policing themselves. Self-regulation is at its best when an independent third party is able to demonstrate that businesses are accountable for the promises they make. Whether through pre-review and verification, audits and investigation, or the provision of a platform for consumers to resolve their grievances, some type of independent accountability is vital to any successful self-regulatory approach. (See section III for more details on the necessary characteristics of *effective* self-regulation.)

One of self-regulation's benefits is that it can function absent a regulatory regime. But the core features of effective self-regulation are also vital to and can complement any government-driven approach. Any successful data privacy regime should have external means of accountability to substantiate claims, pre-screen operations against best practices, and/or respond to complaints. It should include clear and transparent means for consumers to be heard and feel vindicated when promises and expectations are not met. It should include support for recognizable trust marks to aid consumers in understanding companies' privacy practices.

In this comment, CBBB provides an overview of the role of self-regulation as it has existed in the history of data privacy practices in the U.S. As part of this, we outline lessons learned through our decades of experience, with the hope that this will provide insight for this Administration into the structures of self-regulation—and perhaps regulation—that most benefit consumers and competition.

We hope that the Department will consider self-regulation, broadly conceived, as a central part of any strategy this Administration may adopt for regulating data privacy in the U.S. Even without the creation of formal independent programs, we hope that the Department will take seriously the fundamental need to establish clear lines of communication between consumers and businesses and other possibilities for working to instill trust in business privacy operations.

II. Outline of CBBB's Comments

A. **Independent self-regulation can be a useful tool in shaping and enforcing business practices related to data privacy.** When thoughtfully developed, it achieves this by:

1. Providing consumers with a direct industry response that is more collaborative, pragmatic, and scalable than traditional litigation or regulatory enforcement.

2. Promoting a trustworthy marketplace, developing recognizable trust marks, and encouraging publicly accountable adoption of privacy best practices, leading to swift industry adoption of privacy-protective practices.

3. Dynamically evolving to keep pace with market and technology changes by providing direct means for industry feedback, while focusing on boots-on-the-ground operational realities.

4. Reducing burden on government resources by establishing independent consumer redress mechanisms.

B. **Effective self-regulatory models meet certain criteria.** They must be:

1. Adequately funded and sufficiently independent;

2. Based on clear, meaningful and fair principles;

3. Backed by effective accountability and enforcement mechanisms; and

4. Transparent in procedures and outcomes.

C. As NTIA considers best steps to foster privacy outcomes in line with its high-level goals, **self-regulatory programs like CBBB's existing privacy-related programs provide informative case studies.**

1. The Children's Advertising Review Unit (CARU) shows that self-regulation can both inform and help to enforce formal regulatory activity through the recognition of robust safe harbor programs, which independently verify that practices meet standards of transparency, control, and data minimization, even in the high-stakes area of children's privacy.

2. The Online Interest-Based Advertising Accountability Program, as the independent accountability mechanism for the Digital Advertising Alliance's privacy rules, shows that self-regulation can rapidly shift to anticipate and mitigate harms, in this case through the adoption of formal transparency and control standards with a robust accountability mechanism.

3. BBB EU Privacy Shield, a co-regulatory program for international data transfers, shows that transparency and consumer access/correction rights can be secured by providing businesses with guidance through the self-certification process and a fully-fledged dispute resolution mechanism, reducing the burden on government regulators.

III. Independent Self-Regulation Can Foster Privacy Outcomes in Line with the "High-Level Goals"

This section is responsive to the Department's question C. Specifically, we focus on the next steps and measures this Administration should take to achieve an end-state in line with the high-level goals. We also consider closely sub-question 3: "What aspects of the Department's proposed approach to consumer privacy, if any, are best achieved via other means?" We are glad for the opportunity to describe independent self-regulation as a possible means—either in tandem with or apart from changes to U.S. law—for achieving the Department's "High-Level Goals for Federal Action."

There are many potential paths to achieve these high-level goals. No matter which path is ultimately chosen, self-regulation can be a useful complement. The proven benefits of self-regulation for consumers and businesses alike, taken together, significantly advance the stated interests of the Department.

Benefits of Self-Regulation

As part of its efforts to foster pro-competitive business behavior that protects consumers, the United States—through the expert guidance of the Federal Trade Commission—has long recognized the benefits of self-regulation. Appropriately structured self-regulatory initiatives provide benefits to consumers, the competitive marketplace, and the government. These benefits have recently been summarized in a comprehensive review by former FTC Commissioner Maureen Ohlhausen.[ii]

For consumers, the benefits of self-regulation include the obvious—a direct industry response to quickly stop practices like misleading advertising or the unauthorized collection of personal data—and the less obvious, the promotion of a more trustworthy overall marketplace. Properly structured, self-regulation can provide independent verification and/or enforcement of business promises. Trusted intermediaries, such as the BBB, can also provide consumers with a secure platform for addressing their concerns, whether as the impetus for self-regulatory enforcement or through formal dispute resolution programs.

As noted by Commissioner Ohlhausen, the benefits of appropriately structured self-regulatory programs for the industry include the opportunity to apply "boots on the ground" experience in fashioning a response that is consistent with industry practices and thus responsive but less disruptive than regulation. In addition, self-regulatory regimes are inherently more flexible than government regulatory actions and can dynamically evolve as industry practices change. Thus, self-regulation can more readily adapt to future industry changes by covering new practices without acting as a drag or delay on innovation.

Effective self-regulation can also improve an industry's reputation in the marketplace. This reputational gain is a principal motivation for many ground-breaking industry efforts. Improvements in the industry's reputation also benefit consumers when they are based on a more truthful marketplace. The FTC has a long history of recognizing these efforts, once proven successful, just as it appropriately identifies problems in the marketplace.

Finally, effective self-regulation programs are valuable to the government as the programs can supplement government enforcement resources or, in appropriate instances, substitute for them entirely. Even in instances where the government ultimately judges that some level of regulation is needed in the marketplace, the experience of self-regulatory bodies in implementing self-regulatory standards can inform the government on workable approaches, and self-regulation can adapt to assure higher levels of compliance once implemented. The advertising industry's experience with self-regulation of children's privacy before the passage of COPPA, for example, helped inform the FTC's original rulemaking. Once the final rule was adopted, CARU quickly moved to begin self-regulatory enforcement of COPPA.

Effective Self-Regulatory Models

Of course, not all industry self-regulation initiatives are effective. Commissioner Ohlhausen's review points to several indicia of effective self-regulation. Effective self-regulation must be:

- Adequately funded and maintain sufficient independence from the industry. Both structure and funding must allow for objective oversight of industry practices to ensure that self-regulatory principles are followed by the industry.
- Based on principles that are clear, meaningful, and fair. As the Commissioner noted, vague or indefinite principles do not provide actual protection to consumers.
- Backed by effective oversight and enforcement mechanisms. According to Commissioner Ohlhausen, "[w]ithout an effective enforcement mechanism, a self-regulatory framework is in danger of becoming toothless."

We would add to this excellent summary that to meet these three criteria the program must be transparent in its procedures and outcomes. Unless consumers and the government can see the work of self-regulation and judge its effectiveness or ineffectiveness, a lack of confidence in the program can result in underutilization.

All CBBB-administered self-regulatory programs have been designed to meet these standards of effectiveness.

IV. The Advantages of Self-Regulation: Clarity, Flexibility, Scalability

This section responds to the Department's question B related to two of the high-level goals laid out in the RFC: *legal clarity while maintaining the flexibility to innovate* and *scalability*.

The self-regulatory efforts of CBBB's privacy-related programs demonstrate methods of working towards these goals, enhancing protections offered to consumers in ways that preserve the benefits of a competitive market. Each was made possible by a combination of support from the industry for a truthful and functional consumer marketplace and government leadership, most notably from the Federal Trade Commission and the Department of Commerce. This leadership has encouraged the development of self-regulatory structures that supplement—or in some cases substitute for—government regulatory activities.

Legal clarity while maintaining the flexibility to innovate.

- The Department should consider the role that self-regulation can play in providing effective, pro-competitive, and privacy protective approaches based on the accumulated expertise of industry members.
- Having access to guidance from self-regulatory bodies can make complex rules easier to apply in practice.
- Self-regulatory bodies can react before problematic business practices become widespread, proactively consulting with companies to make sure they are addressing consumer privacy throughout the business cycle.
- In the case of self-regulatory codes, they can evolve with changing technology, practices, and norms, reacting more quickly than the legislative or rulemaking process both in terms of capturing a new issue or pruning outdated, counterproductive requirements

Scalability

- Self-regulation takes pressure off of limited government resources, helping to establish baseline standards in order to allow regulators to pursue egregious actors, while allowing fewer businesses to slip through the cracks. In this way, industry itself can step up to spread the burden in a way that is pro-competitive and consumer friendly.
- Self-regulation can be adaptive and responsive to the needs of differently-situated businesses. Because self-regulation happens in conjunction with businesses, rather than apart from them, it invites a flexible, results-oriented process that acknowledges the wide diversity of companies' practices and capabilities. This enables proportional adoption of best practices across the business ecosystem that is responsive to business realities.

V. Case Studies of CBBB's Self-Regulatory Privacy Programs

We believe that self-regulation is a net positive and can assist in reaching the Department's goals based on our decades-long track record of setting and enforcing standards that make the marketplace fairer, more efficient, and more trustworthy.

There are many possible forms of effective self-regulatory programs, from independently funded enforcement agents like the Online Interest-Based Accountability Program to co-regulatory independent recourse mechanisms like the BBB EU Privacy Shield. Any possible model presents its own set of challenges and opportunities. When programs are carefully designed to align the interests of business participants, consumers, and regulators, they can lead to significant net positive gains for consumers and swift advancements in business adoption of best practices.

Below, we provide more details about the operations of CBBB's existing privacy-related programs, along with specific examples that highlight how they have each worked to address

some of the "Privacy Outcomes" laid out in the Department's RFC: Transparency, Control, Reasonable Minimization, Security, Access and Correction, Risk Management, and Accountability.

CARU and Self-Regulation of Digital Media

The Children's Online Privacy Protection Act (COPPA) expressly incorporated self-regulation in its statutory scheme through its safe harbor provision. The Children's Advertising Review Unit (CARU) provides guidance through The Self-Regulatory Program for Children's Advertising,[iii] which includes CARU's guidelines on privacy and COPPA compliance. CARU has published more than 200 COPPA enforcement decisions.[iv]

CARU protects children from deceptive or inappropriate advertising and online privacy practices by evaluating child-directed advertising in all media, and online privacy practices as they affect children. CARU both monitors advertising directed to children under 13 and works with organizations to ensure their advertising and data collection practices comply with The Self-Regulatory Program for Children's Advertising, which includes CARU's guidelines. The guidelines take into account the uniquely impressionable and vulnerable child audience.

Although CARU was established in 1974, the guidelines have been regularly revised to reflect changes in the marketplace and especially changes in technology used to direct advertising to children. In updating its guidance to the industry, CARU is assisted by its 70-member CARU Supporters Council, which is comprised of the leading children's product companies, as well as its academic advisory group. CARU also works to educate parents on issues of children's advertising, marketing, and data collection practices.

As part of its commitment to protecting children, CARU in the 1990s, expanded its guidance to data collection and privacy issues. As an extension of its mission to help organizations deal sensitively with the child audience in a responsible manner, CARU applied for and was granted the first Safe Harbor designation under the Children's Online Privacy Protection Act (COPPA). In addition, pursuant to the guidelines, CARU monitors and takes action to bring companies voluntarily into compliance with COPPA. CARU is currently working with its supporters and academic advisors to assess the impact of streaming video and mobile technology on the important child protection goals of its guidelines.

Online Interest-Based Advertising Accountability Program

The Digital Advertising Alliance (DAA) was created by members of the online interest-based advertising ecosystem in response to calls from the FTC in December 2007 to create a stronger and more effective self-regulatory structure governing the collection and use of data for interest-based advertising.[v] The DAA created a new, highly innovative and effective notice-and-choice regime for interest-based advertising and multi-site data collection by requiring "enhanced notice" of data collection, again in response to the express suggestion of the FTC on the need for such a program. The CBBB-administered Accountability program, which enforces compliance with DAA standards, has brought more than 80 compliance actions with almost 100 percent voluntary compliance.

In response, CBBB worked with leaders of the digital advertising industry—including the Interactive Advertising Bureau (IAB), the ANA, and the 4A's—to create Principles for notice and choice for interest-based advertising data collection.[vi] Notably, and again in direct response to the FTC's request, this group created a groundbreaking AdChoices icon that provides enhanced, just-in-time notice of interest-based advertising data collection. In recognition of the need for a true industry-wide response, the Principles apply to all members of the digital advertising industry. Demonstrating the ability of self-regulation to dynamically evolve, the Principles have grown to cover multi-site data collection, mobile devices, and cross-device tracking.

As in other areas, Principles without enforcement do little to protect consumers. The founding partners of the DAA wisely recognized this and charged ASRC and the CBBB with development of an "accountability" program that could monitor digital advertising for compliance.

Employing a structure like existing, successful self-regulatory programs, but using advanced tools to monitor digital advertising, the Accountability Program was created to be a data privacy watchdog. The Accountability Program monitors websites and mobile apps to check whether companies are following the DAA Principles. Where it detects apparent non-compliance, it may initiate a formal inquiry. These inquiries are conducted in confidence with the company or companies in question, and where non-compliance is confirmed, the Accountability Program works with the companies to remedy it. The results are published online to provide guidance to the industry and to transparently document the Accountability Program's efforts.[vii] Where companies refuse to participate in this review process, the Accountability Program may refer the company to the appropriate government agency.

The Accountability Program also reviews consumer complaints regarding violations of the DAA Principles. The Accountability Program has processed over 23,000 consumer complaints in its seven years of operation, some of which have yielded viable enforcement cases. And whether a complaint raises a compliance concern under the DAA Principles or not, the Accountability Program responds individually to any consumer whose complaint includes return contact information.

Over the years, it has released the results of more than 80 cases and published five formal compliance guidance documents. Through this work, the Accountability Program has accomplished several noteworthy achievements:

- Enlisting publishers: The DAA Principles apply not only to advertising companies, but also to publishers. The Accountability Program has brought dozens of publishers into compliance, ensuring consumers are provided with real-time notice that data collection for IBA may be occurring even when no ads are being served.
- Tracking non-cookie IDs: As the web has grown beyond traditional HTTP cookies, the Accountability Program has grown, too, expanding its monitoring to include browser fingerprinting techniques and other non-cookie unique identifiers. These technologies can power IBA and fall squarely within the DAA Principles. The ability

to seamlessly adapt to this kind of change is a hallmark of self-regulation, particularly in the technology space.

- Transitioning to mobile: Another major tech transition was the move from desktop and laptop computers to mobile computing devices such as smartphones and tablets. The Accountability Program has been enforcing the DAA's Mobile Guidance since 2015 and has tackled cases involving both mobile app publishers and the advertising technology companies that help monetize those apps. To do this, the Accountability Program has expanded its technical forensics tools, from virtual testing environments and automated scanners to banks of test devices.
- Tackling location data: As part of the expansion into mobile, the Accountability Program has had to grapple with the difficulty of defining "precise" location data, a category of more sensitive consumer data that can geographically locate a particular person or device. Several of its cases have involved companies receiving this kind of data without first getting consumers' consent, and all of the companies involved have readily implemented the Accountability Program's recommendation either to first obtain consent or to reduce the precision of the data collected.

Remarkably, the program has received nearly complete voluntary compliance with only one regulatory referral since its creation, demonstrating strong industry support for the notice and choice principles it embodies.

In view of its success enforcing the DAA's Principles related to IBA, the Accountability Program will also serve as the enforcement agent for the DAA's Application of the Self-Regulatory Principles of Transparency & Accountability to Political Advertising, a set of best practices which aim to bring timely access to relevant information about certain paid political advertising. Enforcement is currently slated to begin in the spring of 2019.

BBB EU Privacy Shield

European Union law forbids transfers of personally identifiable information to the United States without a data transfer mechanism that guarantees an "adequate" level of privacy protection. The EU-U.S. Privacy Shield Framework is one such valid transfer mechanism. (A similar bilateral Framework also exists between Switzerland and the United States.) Companies participating in Privacy Shield self-certify publicly to the Department of Commerce that they will abide by the Privacy Shield Principles in their handling of EU data.

Privacy Shield requires self-certified U.S. companies to select an independent recourse mechanism (IRM), which assists with handling unresolved privacy complaints from EU individuals. Immediately following the formal adoption of the Frameworks, CBBB launched BBB EU Privacy Shield (BBB EUPS) as an IRM to support the new Framework. In its second year of operation, BBB EUPS provided services to around one thousand companies, including individualized guidance on the self-certification process and dispute resolution services.[viii]

The commitments that participating businesses make through Privacy Shield include enhanced consumer privacy protections (including the provision of a right of access and, in some cases,

correction of personal data) for EU individuals, greater transparency around data collection, use, and sharing, as well as the commitment to provide EU individuals with independent recourse for resolving privacy complaints. Participants must also verify on an annual basis that their public attestations regarding their Privacy Shield privacy practices are accurate, through self-assessment or outside compliance reviews.

Building on sixteen years of experience supporting the Safe Harbor Framework as BBB EU Safe Harbor, BBB EUPS continues to provide complaint handling and dispute resolution services as well as expert assistance to companies in the self-certification process and beyond, helping to ensure alignment between commitments and practices.

Privacy Shield supports multiple redress mechanisms to ensure accountability for the commitments that businesses make. First, EU and Swiss data subjects may contact the participating company. If this fails to result in a resolution, they may contact BBB EUPS, which sparks a formal conciliation—and sometimes arbitration—process between the consumer and participating business. In addition, consumers maintain the right to submit a complaint through a last-chance arbitration mechanism and/or the EU Data Protection Authorities and the Swiss Federal Information Commissioner.

VI. Conclusion

CBBB applauds NTIA's leadership in driving meaningful federal privacy policy, which is critically important at this time. CBBB stands ready to offer its expertise and guidance as the Department moves forward with this initiative.

---

[i] Department of Commerce, Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48,600 (Sept. 26, 2018), https://www.ntia.doc.gov/files/ntia/publications/fr-rfc-consumer-privacy-09262018.pdf.

[ii] Federal Trade Commission, Acting Chairman Maureen K. Ohlhausen, Opening Remarks for the 2017 DSA Fall Conference (Nov. 7, 2017), https://www.ftc.gov/system/files/documents/public_statements/1271503/2017-11-7_dsa_posting_version.pdf.

[iii] Council of Better Business Bureaus, Advertising Self-Regulatory Council, *The Self-Regulatory Program for Children's Advertising* (2014), http://www.asrcreviews.org/wp-content/uploads/2012/04/Self-Regulatory-Program-for-Childrens-Advertising-Revised-2014-.pdf.

[iv] Council of Better Business Bureaus, Advertising Self-Regulatory Council, *CARU Recommends Starmaker Interactive Modify Privacy Practices for Starmaker App* (July 9, 2018), http://www.asrcreviews.org/caru-recommends-starmaker-interactive-modify-privacy-practices-for-starmaker-app/.

[v] Fed. Trade Comm'n, *Statement of Federal Trade Commission Concerning Google/DoubleClick*; FTC File No. 071-0170 (Dec. 20, 2007), https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf.

[vi] Digital Advertising Alliance, *DAA Self-Regulatory Principles*, https://digitaladvertisingalliance.org/principles (last visited Nov. 8, 2018).

[vii] Council of Better Business Bureaus, Advertising Self-Regulatory Council, Decisions of the Online Interest-Based Advertising Accountability Program, http://www.asrcreviews.org/category/ap/ (last visited Nov. 8, 2018).

[viii] *See* Council of Better Business Bureaus, BBB EU Privacy Shield, Annual Procedure Reports, https://www.bbb.org/EU-privacy-shield/procedure-report/.