



February 26, 2016

The Honorable Tom Wheeler  
Chairman, Federal Communications Commission  
445 12<sup>th</sup> Street, SW  
Washington, D.C. 20554

Dear Chairman Wheeler,

Founded in 2001, Digital Content Next (DCN) is the only trade association that exclusively represents digital content creators. DCN members include many of the Internet's most trusted and respected media brands, collectively reaching an unduplicated audience of 230.6 million unique visitors – or 100% reach of the U.S. online population – monthly. Given the direct and trusted relationships that our members have with consumers, DCN member companies are often viewed as the face of the internet and are in a primary position to feel the consequences of declining consumer trust.

In 1996, Congress added section 222 to the Communications Act. That provision imposed a duty on every telecommunications carrier to protect the confidentiality of its customers' private information. Congress also imposed limitations on the use, disclosure, and access to this information. Congress charged the Federal Communications Commission (Commission) with adopting rules to interpret, implement, and enforce this requirement. In the Open Internet Order adopted in 2015, the Commission made clear that this provision is applicable to broadband Internet access service providers.

In that proceeding, we urged the Commission to focus on the consumer experience by adopting a set of rules that ensure consumers have access to the lawful content of their choosing. The Commission has not yet proposed rules to implement the application of section 222 to broadband, and DCN intends to file substantive comments in response to any Notice of Proposed Rulemaking the Commission adopts. Nevertheless, given the importance of the issues involved, DCN wanted to provide the Commission with its initial and conceptual positions. Most important, as you consider how to apply Section 222 rules to broadband providers, we again urge you to focus on the consumer. In particular, we believe it is important to consider what an average consumer would expect with regard to how their data is collected and used.

**Context Matters.** The importance of context has been adopted by all major recent U.S. privacy frameworks. President Obama’s Privacy Bill of Rights framework advocated seven main principles. The principle of “Respect for Context”, cited as key to matching an average consumer’s expectation of privacy, simply notes that “consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.” To the extent that a consumer’s personal data will be used outside the context where it was collected or for reasons not disclosed at the time of collection, companies should provide transparency and choice to the consumer.

In 2012, the Federal Trade Commission (FTC) also issued a report, entitled “Protecting Consumer Privacy in an Era of Rapid Change.” The FTC’s report noted that certain data collection and use practices do not require consumer choice because they generally meet with a reasonable consumer’s expectations while other practices do require transparency and choice because a reasonable consumer would not expect them. The FTC’s preliminary staff report noted five categories of data collection and use practices that do not require choice. However, the FTC refined the final report to focus on the “context of the interaction.” Specifically, the FTC noted that “whether a practice requires choice turns on the extent to which the practice is consistent with the context of the transaction or the consumer’s existing relationship with the business...”

Current industry best practices require special obligations to provide consumer transparency and choice by service providers that provide services across all or substantially all of the content viewed by a consumer. In the Digital Advertising Alliance (DAA) Self-Regulatory Principles for Online Behavioral Advertising (OBA) (July 2009), a service provider is defined as “an entity that collects and uses data from all or substantially all URLs traversed by a web browser across Web sites for OBA purposes in the course of the entity’s activities as a provider of Internet access service, a toolbar, an Internet browser, or comparable desktop application or client software and not for its other applications and activities.” Under the DAA principles, service providers must obtain consent for the collection and use of data for OBA purposes and provide consumers with an easy to use means to withdraw consent to the collection and use of such data. The Commentary on the DAA’s consent requirement importantly states “the privacy concerns regarding [OBA] are amplified when providers of services can .... potentially gain access to all or substantially all of their customers’ Web surfing behavior.” To address these concerns the DAA’s Choice Principle “holds Service Providers to a high standard” that includes the requirement that “an authorized user take action assenting to the data collection and use of data” – a requirement that does not apply to other participants in the online ecosystem. These DAA consent requirements have been extended in the DAA Application of Self-Regulatory Principles to the Mobile Environment (July 2013) and Application of the DAA Principles of Transparency and Control to Data Used Across Devices (November 2015). As such, a requirement for heightened consent by a broadband provider based on the collection of information about a user’s content consumption or other behaviors for marketing purposes would be consistent with current industry best practices.

Even the Section 222 rules under consideration take context into account with regard to how personal information may be used. Under the existing rules, Customer Proprietary Network

Information (CPNI) data may only be used for marketing the same category of services to which a consumer already subscribes. In order to use this kind of data outside the context in which it was originally collected, a telecommunications provider must provide consumers with an opt-out for marketing other services or an opt-in for broad marketing purposes.

Respecting context is an important principle to consider with regard to broadband providers. For example, a reasonable consumer would expect a mobile broadband provider to collect data about how a consumer uses their mobile device so the company could make improvements to the broadband service or ensure efficient management of the network. However, consumers would not expect (or even know) if a mobile broadband provider was using this same set of data to tailor advertising to consumers on websites or apps. As several news outlets reported, at least one mobile broadband provider was inserting a unique identification header every time a consumer's mobile browser fetched content from a website. This header was used by advertising partners of the mobile broadband provider to identify individual consumers, track their online behavior and target advertising based on that behavior. However, neither the mobile broadband providers nor their partners meaningfully disclosed to consumers' information about this activity or the ability to opt out. In addition, it was later discovered that the header was being used without the knowledge of the broadband provider by some of their advertising partners to respawn cookies that a consumer had deleted – effectively reversing a consumer's choice for privacy.

**Transparency and Choice Give Consumers Control.** Broadband providers are in a position to collect data about consumers across multiple, distinct contexts and connect them back to large reserves of very personal information, and not just about their own customer: Data about a consumer's friends, browsing history, location and device usage can be combined with information the broadband provider knows about the consumer by virtue of their subscriber relationship. For the record, we have concerns about any company that ubiquitously tracks consumers with little transparency and ineffective choice mechanisms. When companies continue to track consumers outside the context of their relationship on unrelated, unaffiliated sites, those companies undermine consumer trust and denigrate the efforts of good actors to provide safe, trusted environments. While this set of data can be useful to help a broadband provider manage a network, improve a service or combat against fraud, this data collected in a 3<sup>rd</sup> party context can also be used to build profiles about consumers without their knowledge or agreement and may result in compromising trust in DCN members' content. Accordingly, privacy rules that are consistent with existing best practices designed to minimize consumer surprise would be preferred for this context.

Specifically, in light of their access to sensitive information about consumers, we urge the FCC to require broadband providers to provide consumers with transparency and meaningful choice with regard to the collection and use of personal information especially when this data will be used for purposes that fall outside of a consumer's expectation and outside of the context of the interaction where the data was collected. Consumers should have the ability to exercise choice via a mechanism that is easy to use, persistent and universal. The current framework of Section 222 rules may be appropriate for broadband providers where providers must provide an opt-out

for marketing similar services and must obtain opt-in consent for broader marketing or advertising. Broadband providers could potentially provide opt-in or opt-out mechanisms in the account settings for a consumer, or honor opt-out signals sent by a device (i.e. Apple's Limit Ad Tracking signal which is sent with the advertising identifier) or browser (i.e. Do Not Track). In each case, the consumer has clearly expressed a desire to not be tracked. Regardless of the method, broadband providers should provide opt-out or opt-in choice mechanisms that are easy to use, not buried in a privacy policy or the terms and conditions, and persistent. Recognizing the rapidly evolving pace of technology, the FCC could work with self-regulatory bodies to help bring solutions to the marketplace that evolve over time to address consumer concerns with new business practices and changing landscapes. In addition, the FCC should work with the Federal Trade Commission (FTC) to ensure that other entities with similar access to all or substantially all of a consumer's online activity are held to a similarly high standard so that consumers are not confused by different standards across the same ecosystem.

Also, because broadband providers often provide service under a single account for several devices they are in a unique position to potentially offer robust preference mechanisms for consumers across a family of devices. As was discussed at a recent FTC workshop on cross device tracking, many companies engaged in this kind of tracking use probabilistic methods of linking devices. However, broadband providers may be in a position to offer solutions that would help the entire ecosystem. As such, we urge you to engage with broadband providers to explore ways that they could offer consumers ways to extend their preferences across a family of devices.

Transparency and meaningful tools for consumers to express choice will help improve consumer trust in the digital ecosystem. Without consumer trust, broadband services and the digital economy cannot realize its full potential. Thank you for your continued efforts to protect consumers. Please do not hesitate to call upon DCN if you have any questions or if we can be of any help.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Jason Kint', with a stylized flourish at the end.

Jason Kint  
CEO  
Digital Content Next

cc: The Honorable Mignon Clyburn  
The Honorable Jessica Rosenworcel  
The Honorable Ajit Pai  
The Honorable Michael O'Rielly