Before the
National Telecommunications and Information Administration
Washington, D.C.

In the Matter of	)	
	)	
Developing the Administration's	)	
Approach to Consumer Privacy	)	Docket No. 180821780–8780–01

COMMENTS OF DIGITAL CONTENT NEXT

Digital Content Next (DCN) appreciates the opportunity to submit comments in the above-captioned proceeding.[1] Founded in 2001 as the Online Publishers Association, DCN is the only trade organization dedicated to serving the unique and diverse needs of high-quality digital content companies which enjoy trusted, direct relationships with consumers and marketers. DCN's members are some of the most trusted and well-respected media brands that, together, have an audience of 256,277,000 unique visitors or 100 percent reach of the U.S. online population[2]. In layman's terms, every person in U.S. who goes online will visit one of our member companies' websites at least one time each month.

DCN supports the passage of comprehensive federal consumer privacy and data security legislation. Federal rules governing the treatment and protection of consumer data will provide certainty and clarity for industry – including both large and small companies and across multiple sectors. In addition, a patchwork of state and international frameworks could create confusion among consumers and potentially lead to loopholes that could be exploited by bad actors. While DCN supports a federal law that would preempt state laws, we believe any federal framework should provide strong protections for consumers. In addition, any federal framework should avoid solidifying the dominance of platform companies.

As the Administration considers the complex public policy issues related to the digital ecosystem and how best to create a workable federal framework to protect consumer privacy, we encourage you to view each issue from the perspective of the consumer and the different relationships consumers have with each company with which they do business in the digital economy.

---

[1] *Request for Comments on Developing the Administration's Approach to Consumer Privacy*, Docket ID: 180821780-8780-01

[2] *comScore Media Metrix Multiplatform Custom Audience Duplication*, December 2017 U.S.

Consumers have a wide variety of places where they can find quality investigative reporting, breaking news, sports, entertainment or comedy. When they visit a site or app, they expect their data may be collected by the site or app owner or a service provider to ensure the service works properly, combat fraud, authorize subscriptions, personalize content or advertising, and recognize a return visitor among other things. These data collection and use cases tend to meet consumer expectations because there is a direct relationship of these activities to the consumer experience and because the consumer's data is collected and used transparently within the same context.

The importance of considering the context in which data is collected and used, and the corresponding relationship to consumer expectations, is artfully explained in the Federal Trade Commission's (FTC) 2012 report entitled "Protecting Consumer Privacy in an Era of Rapid Change.[3]" The report was the product of significant work by FTC staff to build out a framework for respecting consumer privacy in the digital age. The FTC accepted comments from the public and later incorporated and addressed concerns made by commenters. The preliminary staff report "identified five categories of data practices that companies can engage in without offering consumer choice, because they involve data collection and use that is either obvious from the context of the transaction or sufficiently accepted or necessary for technical or security reasons. The categories included: (1) product and service fulfillment; (2) internal operations; (3) fraud prevention; (4) legal compliance and public purpose; and (5) first-party marketing."[4] However, based on comments from the public, the FTC's final report moved away from a concrete list of activities for which consumer choice is unnecessary. Instead, the report refined "the standard to focus on the context of the interaction between a business and the consumer. .... Specifically, 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, or is required or specifically authorized by law."[5] As the FTC astutely noted in 2012, context is key to meeting a consumer's expectations and maintaining consumer trust.

Further, the Digital Advertising Alliance Self-Regulatory Principles[6], the current online industry self-regulatory standard for online advertising, clearly distinguishes the first party context, where a "consumer would reasonably understand the nature of the direct interaction with that entity" from the third-party context where a consumer may not understand or desire that their personal information is collected and used for advertising or other purposes.

---

[3] https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

[4] https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf, page 36.

[5] https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf, pages 36-39.

[6] http://www.aboutads.info/principles

When a consumer's personal data is collected and used within a single context, the consumer can decide whether this value exchange is worth the service provided. If consumers do not like the way their data is being used, they can communicate their dissatisfaction or they can choose to visit a competing site or app. Given the plethora of choices for consumers, publishers are acutely aware that preserving consumer trust is key to building a relationship with the consumer. In short, consumers have choices and leverage with regard to the 1st party websites and apps with which they choose to interact.

Against that backdrop, we are concerned that Outcome #2 identified by the NTIA does not accurately reflect the different relationships that consumers have with different entities in the digital economy. Outcome #2 reads "Users should be able to exercise **control** over the personal information they provide to organizations." We agree with the general principle that consumers should have control. As noted above, consumers do currently enjoy fundamental choice over which websites or apps they choose to visit. However, to require choice mechanisms for "all" data collection and use practices, including benign activities such as combatting fraud or personalizing content, would undermine the effectiveness of the framework. We believe any federal framework for protecting consumer privacy should provide robust, persistent and easy-to-use mechanisms for consumers to exercise choice over data collection and use that falls outside of a consumer's expectation based on the context of the transaction and the consumer's relationship with the business.

Consumers' trust can be eroded when their data is collected in one context but used in another without transparency or an opportunity to exercise choice. The ongoing scandal involving Facebook and Cambridge Analytica is a good example. In that case, Facebook allowed an outside company to collect data about Facebook users and their friends for what consumers expected was a benign purpose and solely within the confines of the Facebook service. However, the data was ultimately shared with multiple parties and used for unexpected secondary purposes. Also, it is important to note that, in contrast to the initial, promised use of the data, the secondary data use was not transparent and provided no benefit to the consumer. In general, non-transparent secondary uses of data outside of context tend to run afoul of consumer expectations. Notice and control should be required for such uses.

In June, DCN commissioned[7] a survey of consumers to better understand consumer expectations with regard to how Facebook collects and uses data. The results underscore that consumers generally expect their data to be collected and used within the same context. However, our survey found that 72% of consumers do not expect Facebook to collect data about a person's online activities on a non-Facebook webpage if a person does not click the 'Like' button, which is at odds with Facebook's reported practices[8].

[7] http://www.niemanlab.org/2018/04/jason-kint-here-are-5-ways-facebook-violates-consumer-expectations-to-maximize-its-profits/

[8] https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html

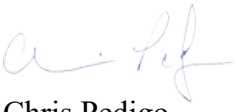
Similarly, Google is in a unique position to collect massive amounts of data about consumers practically anywhere they go on the Internet. Google collects this data from multiple points – Chrome (#1 browser), Android (#1 mobile operating system) and Google Search (#1 search engine) in addition to Google Analytics and the various ad serving technologies which enable Google to dominate the ad-serving supply chain. While consumers may expect Google to collect some data to provide a service, consumers are not likely to expect that Google collects data about consumers as they navigate across the Internet. According to research[9] conducted by Vanderbilt Professor Douglas Schmidt, two-thirds of the consumer data collected by Google is done through "passive" means which consumers would not be likely to know about or expect, especially in the absence of notice and control.

While these examples highlight data collection and use practices that do not meet consumer expectations, it is also important to note that in some cases consumers have no way to avoid data collection by an entity or to exercise meaningful choice over how their data is used. Indeed, the aforementioned 2012 FTC report expressed concerns about the unique role of large platform providers when it noted "even if a company has a first-party relationship with a consumer in one setting, this does not imply that the company can track the consumer for purposes inconsistent with the context of the interaction across the Internet, without providing choice."[10] The FTC was rightly concerned about companies with the ability to track consumers, beyond just across affiliated sites, but across the entire web and across different devices. Companies that dominate the digital landscape and have the ability to track consumers on virtually every site or app they visit are in a unique and privileged position. In the case of this kind of ubiquitous data collection by a single entity, there should be a higher bar. Consumers should be provided with meaningful transparency and control mechanisms.

In closing, we appreciate the opportunity to provide comments in this proceeding and we look forward to working with you to protect consumers in the digital age.

Sincerely,

Jason Kint
CEO
Digital Content Next



Chris Pedigo
SVP, Government Affairs
Digital Content Next

---

[9] https://digitalcontentnext.org/blog/2018/08/21/google-data-collection-research/

[10] https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf, pages 55 – 57.