



DATE: July 10, 2017

TO: Members of the Senate Business, Professions, and Economic Development Committee

FROM: DMA – Data & Marketing Association
4A’s – American Association of Advertising Agencies
AAF – American Advertising Federation
ANA – Association of National Advertisers
IAB – Interactive Advertising Bureau
NAI – Network Advertising Initiative

**SUBJECT: AB 375 (Chau) INTERNET SERVICE PROVIDERS: CUSTOMER PRIVACY
OPPOSE AS AMENDED JUNE 19, 2017
SCHEDULED FOR HEARING – July 17, 2017**

The above-signed associations representing the advertising and marketing industry write to respectfully **oppose AB 375** because it is unnecessary and unreasonably restrictive. Internet Service Providers (“ISPs”) are already regulated by federal law, which is complimented by enforceable self-regulation.

This bill, if passed, would create serious unintended consequences and negatively impact consumers, business, and the Internet. It would foster a complicated regulatory structure at the state level for a sector that is best addressed via a national approach. AB 375 would make California a far more difficult place to innovate on the Internet, ultimately hurting consumers and the information economy that has become an important part of the state’s economy.

Consumers and Businesses Can Rely on the Federal Approach to Privacy. The recent repeal of the Federal Communication Commission’s (“FCC”) Broadband Privacy Rules does not mean that consumers will be left unprotected. In fact, Internet Service Providers (“ISPs”) have been and will continue to be substantially regulated at the federal level. Prior to the FCC’s decision to adopt the Broadband Privacy Rules, it issued a wide-ranging enforcement advisory opinion, making it clear that the Communications Act (Section 222) applies to ISPs. This guidance continues to apply today. The recent action by Congress and the President does not change or alter the obligations of ISPs under Section 222, or the FCC’s ability to enforce noncompliance. Nor does the recent repeal of the Broadband Privacy Rules create new rights or powers for ISPs because the new FCC rules never went into effect. ISPs continue to operate under the same laws in place before the rules were adopted. As such, consumers continue to be protected under existing FCC authority.

AB 375’s Definition of Customer Personal Information Is Overly Broad. The proposed definition of “customer personal information” (“CPI”) would impose requirements on data beyond that which is used to identify an individual. This proposed definition is well outside the bounds of what other states and the federal government have designated as “personal information” under the law. The bill defines

“personal information” to include “[d]emographic information, such as date of birth, age, gender, race, ethnicity, nationality, religion, or sexual orientation”; “[i]nformation from the use of the service, such as Web browsing history, application usage history, content of communications, and origin and destination Internet Protocol (IP) addresses of all traffic”; and “[d]evice identifiers, such as media access control (MAC) address or Internet mobile equipment identity (IMEI).” These data elements alone do not identify an individual and should not be subjected to the rigid restrictions contained in AB 375.

AB 375 Is Unreasonably Restrictive. AB 375 would require opt-in consent for almost all uses of CPI, including marketing uses. Opt-in consent has not been the historical standard for advertising and marketing, and is not the appropriate standard for advertising and marketing going forward in any medium. If adopted, such a standard could heavily restrict beneficial uses of data and stands in contrast with the privacy framework developed by the Federal Trade Commission (“FTC” or “Commission”).

The FTC’s 2012 Privacy Report determined that opt-in consent was appropriate only in limited circumstances, such as the collection or use of sensitive information.¹ For first-party marketing, the Commission found consumer choice to be unnecessary as first-party marketing practices are “consistent with consumer’s relationship with the business.”² Permitting ISPs to use CPI for their own marketing purposes without explicit customer approval adequately protects customer privacy in the broadband context because of the direct relationship between the consumer and the first-party. Consumers appreciate that collecting data for advertising and marketing purposes is an inherent aspect of their relationship with ISPs.

Advocates for AB 375 and similar bills in other states have failed to identify a single, concrete harm that would be remedied through it. Instead, proponents of AB 375 have offered a speculative “parade of horrors” without justification or evidence.

In the advertising and marketing world, where no record of consumer harm exists to justify a restrictive opt-in standard, the above-signed associations maintain that consumer privacy preferences with respect to advertising and marketing may best be expressed through implied consent or an opt-out standard.

Enforceable Voluntary Self-Regulation Effectively Regulates Web-Viewing and Application Use Data. In a rapidly evolving technological environment, existing voluntary self-regulatory regimes present the appropriate tool for governing web-viewing and application use data in the dynamic and interrelated data and marketing ecosystem. In contrast to the rigid statutory restrictions that AB 375 would impose, self-regulatory programs have successfully allowed data advancements to flourish responsibly because they govern practices or functions instead of imposing standards based on specific types of entities.

The Digital Advertising Alliance (“DAA”) administers the Self-Regulatory Principles for Online Behavioral Advertising, Self-Regulatory Principles for Multi-Site Data, Application of Self-Regulatory Principles to the Mobile Environment, and Application of the DAA Principles of Transparency and Control to Data Used Across Devices (collectively, “Self-Regulatory Principles”). The Self-Regulatory Principles provide actionable, robustly enforced, principles for entities engaged in the collection and

¹ FTC, *Protecting Consumer Privacy in an Era of Rapid Change* 57 (Mar. 2012), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

² *Id.* at 40.

use of data in online, mobile, and across devices. These Self-Regulatory Principles are designed to provide consumers with enhanced notice and control over the collection and use of Multi-Site, Cross-App, Precise Location, and Personal Directory Data. AB 375 is unnecessary and would add confusion to this established, successful framework.

In addition, DMA's Guidelines for Ethical Business Practice ("Guidelines") provide meaningful transparency, controls, and accountability to help ensure the responsible use of data in marketing. For more than four decades, DMA has proactively enforced its Guidelines against both DMA members and non-member companies across industries. Such enforcement of the Guidelines by the DMA has occurred in hundreds of data-driven marketing cases concerning deception, unfair business practices, personal information protection, and other ethical issues.

The self-regulatory regimes outlined above align with the FTC's approach to non-sensitive data and provides a flexible, innovative, and independently enforceable framework that keeps pace with the marketplace.

AB 375 Has Not Undergone Adequate Review or Analysis. AB 375 is attempting to regulate in a complicated, highly technical area despite the fact that it has not received sufficient analysis. AB 375, however, is merely a reaction to the decision to repeal the FCC's Broadband Privacy Rules, and is not the product of a deliberative, thoughtful legislative process.

AB 375 Would Stifle Economic Growth and Innovation. According to the [Value of Data](#) report³ commissioned by the DMA, the Data-Driven Marketing Economy in California alone generated \$26.8 billion in revenue and generated 128,000 jobs in 2014. Similarly, the Interactive Advertising Bureau ("IAB") commissioned a [study](#)⁴, which revealed that the advertising supported Internet ecosystem generated \$1.121 trillion for the U.S. economy in 2016, accounting for 6% of U.S. GDP, double its contribution in 2012. The IAB study also noted the advertising-supported Internet ecosystem created 10.4 million jobs in the United States, a 104% increase from 2012. Further, a recent Zogby Analytics poll⁵ commissioned by the DAA shows that consumers assign a value of almost \$1,200 a year to ad-supported online content. 86% of respondents to the same poll suggested that they prefer an ad-supported internet to paying for online content. The same poll showed Ad-supported online content is the backbone upon which the Internet as we know it is built.

The regulatory landscape for the Internet that existed prior to the FCC's rules helped facilitate these significant economic developments. AB 375 would stifle that growth and would be very harmful to the Internet's role as an economic engine for the California and American economy.

The unprecedented growth and success of the Internet over the past two decades, and the high rate of consumer adoption that goes along with it, demonstrates that consumers are pleased with the Internet that has developed under current law. They are increasingly relying on the free and low-cost access to entertainment, news, and financial services, and other useful content that the Internet offers. By destabilizing the ecosystem, AB 375 threatens the "free Internet" that has become part of the daily lives of millions of American consumers.

³ <https://thedma.org/advocacy/data-driven-marketing-institute/value-of-data/>

⁴ <https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf>

⁵ <http://digitaladvertisingalliance.org/press-release/zogby-poll>

We have already seen the disruptive effects of restrictive requirements for the Internet in other regions, including Europe. It is no coincidence that the major Internet and technology companies in the world were developed in the United States, under the privacy regime that existed before the FCC's Broadband Privacy Rules were adopted. A state-by-state approach on privacy, such as the one set forth in AB 375 would put the United States in an inferior competitive position, harm the American economy, and deprive consumers of a vast array of digital benefits as a result.

Because it is unnecessary for consumers as they already receive significant protections under federal and state rules, unduly burdens California's businesses (both small and large), and negatively impacts California's tech and data-driven economy, the above-signed associations respectfully **oppose AB 375**.

cc: The Honorable Ed Chau
Tom Dyer, Office of the Governor
Bill Gage, Senate Business Professions, and Economic Development Committee
Kayla Williams, Assembly Republican Caucus