Before the

FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106

COMMENTS OF CALINNOVATES

CALINNOVATES
548 Market St., Ste. 28585
San Francisco, CA 94104
415-570-9303 (phone)

May 26, 2016

INTRODUCTION

The digital era is marked by constant disruption that is changing the world in which we live in remarkable, inspiring ways. In order to enjoy the innovations entering the market at this dizzying pace, consumers are faced with a binary choice to either trust that their data will be safeguarded or forgo the use of certain products or services. Consumers place a significant amount of trust in the products they use, as access to certain services that require the collection of one's personally identifiable information outweighs the costs. Consumers not only want, but demand access to platforms that delight and revolutionize their lives. Innovation is empowering people to take advantage of the new opportunities made available by the new economy. But as the Information Superhighway evolves into the Data Autobahn, consumers know less about how their data is collected, stored and utilized while companies collecting and using the data have come to learn that there is a wealth of value in data. It's the grand bargain that has created such amazing opportunities in our rapidly advancing 21st century digital economy.

But because consumers have little insight into the collection, use and safeguarding of their data, they simply must trust that their data will be protected at the same high level no matter who is collecting, storing and using. And, they must do so despite the fact that consumers cannot easily designate if and how their data is used across the vast array of offerings that exist today, including broadband Internet access services and edge provider platforms. Consumers want to believe that their data should generally be treated with at least a high degree of care no matter who is providing service.

The FCC's foray into privacy regulations complicates consumer choices, rather than clarifying and improving those choices. The Notice of Proposed Rulemaking (NPRM) will diminish innovation and competition in the privacy protection arena, cause great harm to the ongoing yet fragile privacy negotiations with international allies and threatens to expose consumer data to increased risk.

That is why CALinnovates – a coalition of technology leaders, startups, and entrepreneurs – opposes the Commission's plan to enact this proposed rule.

In this instant rulemaking, it may be important for Congress to weigh in as the FCC has misunderstood not only the current market conditions, but also the effects such a rule could have on the future of the innovation economy.

It is with this message that CALinnovates submits its comments to the FCC and looks forward to the ongoing public discussion and debate about the appropriate privacy construct that can protect consumers while fueling the rapid development of the innovation economy that CALinnovates represents.

EXECUTIVE SUMMARY

The startup community for whom we speak is deeply committed to advancing consumer privacy in the digital age. When consumers' believe their privacy is threatened, both our member companies and America's vibrant startup ecosystem suffers. Our community works hard to provide exciting, novel and useful services driven by consumer data that delights consumers. The vast technology ecosystem driving the creation of the 21st century economy is eager to return more value to consumers from the data they receive than they obtain from accessing and using that data. That is one secret to success and growth in technology startups.

As the companies who support CALinnovates are intentionally positioned to gain from increased willingness of consumers to share their personally identifiable information with companies, these companies are also at great risk when consumers' experiences in sharing their data are negative or when their trust that their data is protected, kept private and used prudently is eroded.

The computer engineers and data scientists powering CALinnovates companies and other technology startups take a back seat to no one in their commitment to ensuring and advancing consumer privacy and security. These highly trained experts are laser-focused on the data privacy and security as a critical component of the building of their companies. More so than almost anyone in the United States, these computer engineers know the risks associated with data collection, storage, usage and sharing. They work hard to eliminate or mitigate those risks because their failure to do so could cost them their startups. Their economic interests are, therefore, aligned with being wise and careful stewards of consumer data. CALinnovates encourages the Federal Communications Commission to rely on these engineers' and data scientists' unparalleled expertise to reject this proposed Rule which is fraught with unintended, negative consequences.

CALinnovates views the questions raised by the FCC in this proposed Rule through two interlocking questions: (i) what governmental policies will give innovators clarity to build exciting new products and services using data that will benefit consumers; and, (ii) how can governmental policies maximize consumer trust in data-driven innovations so that consumers will increasingly share their data and reap more than commensurate benefits from that sharing.

The proposed Rule suffers from several debilitating flaws that should cause the FCC to reconsider its objective. The proposed Rule, as currently drafted, is likely neither to increase consumers' trust that their private information is well, and consistently, protected across entities that encounter it nor to increase clarity for producers of cutting edge and emerging digital services. It should, therefore be revisited and the FCC should adopt a set of privacy rules mirroring the time-tested approach that guides the Federal Trade Commission's (FTC) enforcement actions.

In addition to sharing our critiques of this proposed Rule from a customer benefit and startup advancement perspective, we believe the proposed Rule is flawed public policy.

CALinnovates disagrees with the FCC's assertion that this proposed Rule produces the optimal outcome for consumers. It is unlikely that shifting jurisdiction from one agency with longstanding, well-developed, core competency adjudicating whether providers of broadband Internet access service (BIAS) are sufficiently protective of consumer privacy to another with limited-to-no expertise in evaluating privacy matters in this area advances consumer privacy. At best, the FCC could only hope over the next few years to achieve a similar level of consumer privacy protection to that which the FTC has provided consumers over may years. We further disagree with the FCC's assertion that this proposed Rule will not have a negative effect on America's startups and edge providers that make mobile devices and the Internet so beneficial for consumers. In summary, the FCC's proposed Rule will neither produce increased consumer privacy nor increased consumer benefit from their own data and the Internet itself.

FCC PROPOSED RULE IS UNNECESSARY BECAUSE THE FTC SUFFICIENTLY POLICES BIAS PROVIDERS' HANDLING OF CONSUMER DATA

The FTC has repeatedly protected the privacy of consumers' data obtained by taking privacy actions against BIAS providers. Therefore, CALinnovates questions the FCC's justification for seizing this jurisdiction and questions what gap the FCC believes it is attempting to fill. The FTC has acted at least four times previously to police BIAS providers' privacy protections. That history of strong policing of the privacy of Internet customers undercuts the thesis of the FCC's proposal. Given the FTC's focus on ensuring privacy commitments are met by BIAS providers, the FCC's proposed Rule appears unnecessary.

SHIFTING PRIVACY JURISDICTION TO THE FCC WILL DECREASE CONSUMER PRIVACY PROTECTIONS

Given the FTC's repeated enforcement actions to protect BIAS customers' privacy, CALinnovates asserts that it is unreasonable to expect that simply shifting the agency that regulates BIAS customers' privacy will increase consumer privacy. In fact, it may temporarily decrease those customers' privacy. Since customer trust is essential to adoption and continued use of online services, CALinnovates is deeply concerned about the unintended consequences of this proposed shifting of regulatory oversight. The FTC polices more than 50 consumer protection statutes. Like the FCC, it is a resource-constrained agency and if the FCC's proposed Rule is finalized the FTC will redeploy its staff currently reviewing complaints concerning BIAS providers to other functions. In the interim, the FCC – an agency with an historically limited privacy authority – will need to hire and train staff prior to considering alleged privacy violations. Ironically, during this period while the FTC shifts its staff and enforcement focus and the FCC works feverishly to build a new

core competency sufficient to meet its new responsibilities, customers of BIAS should expect to have less, not more, expert privacy resources dedicated to the protection of their data.

INCREASING FCC PRIVACY JURISDICTION OVER BIAS DECREASES LIKELIHOOD OF MULTINATIONAL PRIVACY COOPERATION

The FCC's proposal also lessens the likelihood that the United States and European Union ("EU") governments are able to successfully conclude a pending multinational agreement concerning consumer privacy protection. That will leave both US companies needing to transfer the data of EU citizens to the US and those EU citizens in privacy and legal purgatory. Specifically, the EU has long challenged the US sectoral approach to privacy regulation. In the US federal agencies regulate privacy within specific industries. The FTC serves as the catch-all agency for all data and security commitments made to consumers by companies and for consumer data security protection matters not statutorily committed to another agency.

While the FCC might prefer consideration of only whether to take jurisdiction from the FTC concerning consumer privacy protection by BIAS providers, the FCC's actions have profound international, geopolitical consequences. It is no secret that the EU and the US do not yet agree that the US government's protection of EU citizens' fundamental right to privacy through its regulatory scheme is "adequate" to ensure appropriate protection. A decision by the European Court of Justice[1] in the fall of 2015 invalidated the longstanding US-EU Safe Harbor that allowed for lawful transfer to the US of the personally identifiable information (PII) of EU citizens. Subsequent negotiations to replace the Safe Harbor led to an agreement in principle – dubbed the Privacy Shield – that various Data Protection Authorities throughout the EU continue to deem inadequate.

One longstanding complaint that remains unresolved is the EU's insistence that one US federal agency lead the protections of EU citizens' PII. The FCC's attempts to take jurisdiction over privacy matters for BIAS providers – one of the key ways that US companies may encounter EU citizens' data – increases the lack of a central authority leading privacy protection within the US government and further complicates the process for concluding this essential international privacy agreement. The FCC's proposal to expand its jurisdiction over providers of BIAS strips the FTC of an important and central part of its privacy jurisdiction. This weakens the argument made by numerous US government officials that the FTC is **the** lead organization for privacy jurisdiction, a lead organization that negotiators from the EU want to see fully empowered to act.

---

[1] Court of Justice of the European Union. (2015). *The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid* [Press release]. http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

The FCC's proposal also undermines the US position by taking a radically different approach to online privacy than the FTC. The stakes for the US economy could not be greater given that the US leads the world in digital services. Any delay in concluding this multinational agreement sends business to other countries' companies and creates additional regulatory uncertainty that weakens US companies and disproportionately harms innovators and startups who are stuck in limbo in efforts to build products and services to serve EU citizens. The proposed Rule sufficiently complicates the potential of achieving a multinational agreement to facilitate the transfer and processing of EU citizens' data to the US; as such, the FCC proposal should be rejected.

EMPOWERING THE FCC IS INCONSISTENT WITH US PRIVACY REGULATION SINCE NEITHER THE FTC NOR CONGRESS DEEMED BIAS PROVIDERS CONSUMER DATA SENSITIVE

The FCC proposes a different legal standard for evaluating whether providers of BIAS violated consumer privacy than the FTC currently applies. CALinnovates asks: Does the public need a separate and conflicting set of privacy rules? CALinnovates recommends that the FCC adopt the same standard for regulating privacy as the FTC employs utilizing its "unfair and deceptive" trade practices authority springing from §5 of the Sherman Antitrust Act. This regulatory approach serves consumers well. Businesses of all sizes, including startups, know and understand their consumer privacy obligations pursuant to the unfair and deceptive trade practices standard. Businesses also understand the standards by which the FTC and state Attorneys General will evaluate their efforts to satisfy those obligations and the significant consequences, such as lengthy consent decrees, for their failure to protect consumers' privacy.

By proposing an entirely new legal regime rather than adopting the unfair and deceptive trade practices approach, the FCC forces companies to devote scarce time and resources to implement new compliance regimes. These new regulatory burdens will hit startups especially hard. Achieving compliance may divert the startups from growing without meaningfully increasing consumer privacy.

In some cases where a company offers BIAS to customers along with other services the FCC's proposed Rule will force companies to simultaneously satisfy two different sets of privacy rules. CALinnovates believes that applying two privacy schemes to a company based on the services offered – rather than based upon the sensitivity of the data is not beneficial to either startups or consumers. Additional regulatory schemes generally hamper innovation for startups. Sometimes they may be justified if the data in question (health data, financial data or the data of minors/students, for example) is deemed especially sensitive. The US privacy regulatory system is built around the FTC policing corporations' promises with respect to consumer data commitments generally supplemented by Congress granting additional privacy protections by enacting statutes empowering agencies

to police specific types of consumer data deemed especially sensitive. Here, that model is upended as the FCC has not demonstrated that the data at issue is especially sensitive and akin to other types of sensitive data and Congress has not acted to grant the FCC this additional authority.

It is important to note that while the customer data traveling through a BIAS provider is no doubt worthy of protection, the FTC never believed it was deserving of special protection akin to health, educational, financial or children's data. Nor, to date, has Congress enacted a statute elevating data traveling through BIAS providers to the category of sensitive data. It would not make sense to treat online data as sensitive only when it is used by BIAS providers, but not when the same data traveling through BIAS providers is collected and used by other companies. Absent either a Congressional finding or the FTC – the undisputed privacy experts at the federal agency level – determining that this customer data is as sensitive as other data sets that enjoy special protections, it is unclear how the FCC can justify overhauling the American privacy regulatory structure in this manner.

INCONSISTENT LEGAL STANDARDS THWART BIAS COMPETITION

Should the FCC proceed to finalize its proposed Rule, if a startup is a BIAS provider and offers other products or services empowered by customer data it will be subject to at least two different privacy regulations regarding the same consumer data depending on the type of product and services it is providing. Thus, the same consumer data collected by the same company could lead to a startup that may be struggling to grow being forced to achieve simultaneous compliance with perhaps inconsistent privacy regulatory schemes. CALinnovates does not understand how this benefits the public as it discourages companies that are startups from entering the BIAS market, thereby decreasing competition. Entrepreneurs, investors and leaders of startup divisions within existing companies will rationally review their chances for successful market entrance and the attendant burdens of regulatory compliance of being a BIAS provider and likely will see greater opportunities offering other products and services due to this thorny regulatory scheme.

If the FCC moves forward with this proposed Rule the better policy approach – and the one that will benefit both consumers and startups – would be for the FCC to shelve this approach and instead consider adopting the general FTC approach while granting greater flexibility for a BIAS providers' collection, storage, sharing, usage and protection of customer data where companies innovate to provide novel but advanced privacy protections. This approach would spur, not thwart competition. The FCC's approach outlined in the proposed Rule will, in contrast, dull privacy protection innovation rather than foster competition over how best to protect consumer data.

INCONSISTENT LEGAL STANDARDS DISCOURAGE PRIVACY INNOVATION

In addition to subjecting any startup innovators offering BIAS services to additional layers of inconsistent, overlapping regulation depending on what services they offer and regarding their collection, storage, usage or sharing of consumer data, the proposed Rule fails to encourage privacy competition and privacy innovation. The proposed Rule is entirely prohibitive; it does not incentivize additional competition. When the same company, especially a startup that may have limited or no in-house legal expertise, must achieve regulatory compliance with multiple privacy schemes despite the data being exactly the same, it slows innovation with customer data. Furthermore, inconsistent legal standards may complicate privacy innovation because while adding novel privacy protections may be permitted by one legal or regulatory scheme they may be forbidden or discouraged by another. This throws a wet blanket over startup engineers building additional, novel systems that may substantially increase consumers' privacy and security.

TREND OF INTRA-INDUSTRY MERGERS UNDERCUTS FCC'S RATIONALE FOR ASSERTING JURISDICTION TO REGULATE BIAS PROVIDERS' PROTECTION OF CONSUMER DATA

Historically, phone companies only offered communications services; Internet companies offered only Internet access services; and content and hardware providers offered programming and technology, respectively. Today, however, those companies are combining with each other across industries with increasing frequency. The silos of tech industry companies being divided by the specific product or service they provide are breaking down, which undercuts the justification for and efficacy of this proposed rule. Rather than failing to appreciate this trend, the FCC should instead recognize the acceleration of cross-industry tech and communication company mergers and acquisitions – many of which it must weigh in on and approve prior to the conclusion of the agreements – and understand that the corporate landscape it seeks to regulate through this proposed Rule is entirely at odds with the actual composition of the communications conglomerates currently in the marketplace. Today, phone companies are buying satellite TV companies. Internet streaming companies are merging with TV networks. Internet edge providers are expanding services and offering broadband Internet access services. These cross industry mergers make it difficult to typify any of the large conglomerates as solely a phone, BIAS, TV, content or edge provider.

The proposed Rule is anachronistic and fails to protect consumer data irrespective of a company's industry or, more likely, industries. It seeks to impose privacy regulations on a world that has either largely vanished or will soon. The practical result of the FCC's proposal is that integrated companies will have to maintain two sets of privacy policies and controls for the same data, depending on whether or not the company collected the data in its capacity as a BIAS provider. Rather than continuing past policies that regulated privacy based on industry sector or type of data the FCC would be wiser to create policy that responds to this dynamic

corporate market and protects consumer data no matter when it is collected, or what affiliate within a conglomerate or type of company undertook the collection to the benefit of both industry and consumers alike.

Moreover, the FCC should take this opportunity to recognize that no matter what products or services are offered by a company – especially one that merged with a company providing a product or service outside of its core market – every company is now dependent on its consumer data. Therefore, to advance the public interest and match the realities of the emerging corporate marketplace the FCC should fundamentally rethink its approach so that its proposed Rule encourages all types and sizes of companies, to protect their customers' data. Failure to account for this new set of conglomerates risks obviating the protections the FCC seeks before the proposed Rule is finalized.

A rethinking of the purpose behind the proposed Rule is also necessary because these conglomerates face few, if any, limitations on sharing consumer data collected by one of their brands or products with other affiliated but perhaps unrelated brands within the same holding company. Since the FCC could only extend privacy protections to customers of the providers of BIAS, its proposed Rule will not limit sharing of customer data to a BIAS division within a diversified company. While CALinnovates is not proposing the FCC regulate inter-corporate data sharing, we believe the FCC's attempts to regulate privacy by type of company or service is inconsistent with marketplace realities and unlikely to be successful. It regulates a marketplace that no longer exists. The unmistakable trend of intra-industry mergers, combinations and consolidations supports centralizing jurisdiction for privacy protection with the FTC rather than shifting a piece of enforcement authority to the FCC.

While CALinnovates believes this dynamic marketplace of conglomerates undercuts the thesis of these privacy rules, if the FCC finalizes its proposed Rule the focus should be on protecting consumer data rather than by imposing industry-specific privacy rules. A focus on the type of company rather than on the need to protect consumer data misconstrues what consumers need, which is protection for their data wherever and whenever the consumer data would be obtained and irrespective of the type of company.

CONSUMER DATA SHOULD BE PROTECTED AT ALL TIMES, NO MATTER WHICH COMPANIES ENCOUNTER IT

Most companies now recognize both the values and risks of the consumer data they collect. Corporations now understand that the consumer data they ingest is, in and of itself, a highly valuable commodity that can produce significant streams of revenue. In this sense, every company is now a data company in addition to producing whatever other products or services it may provide. The FCC and other policymakers should recognize this reality as the FCC considers how to improve this proposed Rule. If companies are regulated regarding privacy by the type of

products or services they provide rather than based upon a focus on the data they collect, however it is collected, shared, stored, protected and used, the FCC's proposed Rule is likely to provide only limited protections to consumers. The FCC cannot and should not ignore the emerging reality that data is a new type of commodity that fundamentally alters how business is conducted.

Because the landscape of communications companies merging with Internet service and other digital service providers has changed dramatically and remains dynamic, the FCC's proposed Rule, if finalized, is likely to have an additional, negative, market distorting effect. Because consumer data is so valuable, savvy companies will naturally engage in strategic efforts to find the optimal level of privacy regulation so that they can maximize their use of customer data as an asset. The companies that maximize their ability to use customer data are likely to be the most successful and profitable companies in the future. CALinnovates worries about several, unintended and counterintuitive consequences that would distort and disrupt the market should the proposed Rule be finalized. We believe savvy companies might alter their strategic direction to avoid altogether entering the market to provide broadband Internet access services so as to escape any FCC privacy regulation. Alternatively, existing providers may exit that market and provide alternative technologies to be able to maximize their profitability and their freedom to use customer data. If a company can decrease its legal and regulatory costs, increase its flexibility to introduce new products and services driven by customer data, or increase its ability to use customer data by steering away from the FCC's proposed privacy regulatory scheme the FCC should expect it might do so. Discouraging the offering of broadband services should not be the price of advancing consumer privacy over the Internet. Rather, the FCC should foster both a healthy BIAS provider market and competition over privacy to maximally benefit consumers.

THE PROPOSED RULE FAILS TO INCENTIVIZE COMPETITION OVER PRIVACY THEREBY LIMITING ITS BENEFIT TO THE PUBLIC

The proposed Rule may actually lead to companies not grappling with how to provide BIAS while at the same time providing sufficient privacy protections for their customers and their data. The FCC can advance consumer privacy best by promoting policies that spur competition between companies over advancing consumer privacy as a competitive market differentiator. Policies that would do so would grant companies, including these new conglomerates, greater freedom to innovate with consumer data the more thoroughly they protect their customers' data. The FCC's proposed Rule does the opposite; it imposes limitations and requirements on companies without offering any marketplace advantage to advance consumer protection.

While CALinnovates concedes that the FCC could impose privacy prohibitions as a means of claiming to advance consumer privacy, it would better achieve its stated objectives by fostering a virtuous cycle of privacy innovation and competition among companies that further enhances the value of the customer data a company

has collected rather than diminishing its value. The likely result of the proposed Rule, in contrast, is that rather than spurring innovation for how companies may simultaneously collect, store, share or use data responsibly and in a manner that ensures it is protected, companies likely will seek to achieve minimal compliance with the proposed Rule to avoid regulatory liability. Startups particularly will assume there are easier paths to profitability that do not involve undertaking the privacy responsibilities that would be incurred by being a provider of BIAS. That would miss an opportunity to benefit consumers and US startups.

The privacy policy that should be pursued by the FCC is the one that encourages startups to devote innovation cycles and resources to achieving increased consumer privacy and marketplace advantage over competitors. The startup culture for which CALinnovates speaks responds best to rules and regulations that incentivize behavior rather than those that forbid or limit opportunities. Startups, after all, rise or fall on their ability to pivot quickly and undertake new efforts to build and offer new services or products. The proposal that will, therefore, produce the most protection of customer data is the one that leads companies to compete over privacy rather than one that flatly limits certain data practices without providing new avenues for corporate advancement and growth.

STATUTES, NOT REGULATIONS, WOULD REMOVE STARTUPS' LEGAL UNCERTAINTY AND SPUR GREATER PRIVACY PROTECTIONS

CALinnovates would prefer the FCC seek this enhanced privacy jurisdiction through enactment of a statute whereby Congress grants the FCC clear authority to regulate the consumer privacy practices of BIAS providers. The FCC's proposed Rule rests on its premise that the Open Internet Order will be upheld despite legal challenges. Whether the FCC's supposition is correct, the innovation ecosystem needs and deserves clarity so that it can efficiently build their businesses and privacy protective systems and be certain it can achieve compliance with all regulatory burdens. CALinnovates recommends the FCC set aside this proposed Rule and instead create draft legislation it would present to Congress to clarify its proposed expansion of its privacy jurisdiction.

On behalf of startups everywhere, CALinnovates seeks legal clarity that benefits consumers and innovators alike and increases trust from the former in the latter. We understand that the FCC based this proposed Rule on the authority it granted itself through the Open Internet Order. Given the pending legal challenges the FCC faces to that Order and the likelihood of subsequent direct challenges to this proposed Rule if it is finalized, any proposed privacy rule that is dependent on that Order being upheld is endangered. Innovators need clarity and legal stability in order to build their businesses. CALinnovates asks: What will happen to this proposed Rule if the Open Internet Order or this Rule are struck down in whole or in part? While large companies can absorb the costs of compliance, startups will face significant burdens if they are forced to divert from building their products and services and growing their businesses to devote scarce time and resources to

ensuring compliance with this Rule and whatever successor Rule it may be replaced with if any legal challenge is successful.

CONCLUSION: THE FCC SHOULD WITHDRAW THIS PROPOSED RULE AND REVISE IT SUBSTANTIALLY TO INCREASE CONSUMER PRIVACY TRUST AND INNOVATORS' FLEXIBILITY

CALinnovates is troubled by inconsistencies in governmental policies regulating data based on industry or product rather than recognizing that data that is PII is worthy of protection no matter how it is collected or by whom it is used.

CALinnovates is further concerned that corporate behavior will be altered because of the FCC further complicating, not clarifying, privacy regulation. We anticipate that companies will spin off divisions, merge with or acquire other companies solely to maximize their consumer privacy regulatory flexibility rather than doing so based on other compelling market efficiency justifications.

The FCC's NPRM is unjustified, slows agreement with the European Union, misunderstands the changed and dynamic corporate marketplace it seeks to regulate and will produce policy disincentives that distort markets and leave consumers' data inconsistently protected. CALinnovates encourages the FCC to withdraw its proposed Rule, revise it to produce positive corporate competition regarding protection of consumers' data and seek legislation to cement its privacy authority.