

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

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

**COMMENTS OF THE COMPUTING TECHNOLOGY INDUSTRY
ASSOCIATION (COMPTIA)**

I. Introduction and Summary

The Computing Technology Industry Association (CompTIA) is a non-profit trade association serving as the voice of the information technology industry. With approximately 2,000 member companies, 3,000 academic and training partners and nearly 2 million IT certifications issued, CompTIA is dedicated to advancing industry growth through educational programs, market research, networking events, professional certifications and public policy advocacy.

CompTIA's membership includes ISPs who are directly impacted by these rules, but the NPRM is also of concern to many in the broader IT industry. The concerns we express with the FCC's proposed rules in these comments are founded on the premise that we simply do not believe that a prescriptive list of prohibited behaviors is the appropriate method for regulating an ever-evolving, quickly growing sector of the economy like data collection and use. This approach, and the proposed rules in particular, are out of step with any current federal or state regulations for privacy and data security, and will only serve to stifle innovative business models and deprive consumers of choice. Specifically, we are concerned that these rules, by cutting off current and potential streams of revenue and raising compliance costs, will ultimately result in higher broadband prices and will hinder broadband adoption.

The FTC has been the chief regulator for privacy and data security for decades, and their approach has been to use their authority under Section 5 of the FTC Act to encourage companies to implement strong privacy and data security practices. The FTC's technology-neutral case-by-case approach has proven an effective way to ensure companies implement strong data security and privacy protections without stifling innovation.

Relying on Section 5’s “unfair or deceptive practices” clause and providing guidance through enforcement, the FTC’s approach allows it to adjust its enforcement approach as technology evolves and industry best practices change. Companies are thus free to experiment with new business models and innovations that could positively impact consumers. The FCC’s proposal, on the other hand, would lock in specific, inflexible privacy and security rules, which would not easily adapt to changing technologies.

In place of the privacy and security rules proposed in this NPRM, we ask the Commission to reconsider and instead implement a case-by-case framework mirroring the FTC’s implementation of its Section 5 authority. The FCC’s decision to regulate broadband Internet access service (BIAS) providers differently than how the FTC regulates the rest of the tech industry could result in a number of unintended consequences. For example, the proposed rule that “A BIAS provider *must ensure* the security, confidentiality, and integrity of all customer PI”¹ is inconsistent with the FTC’s sound risk management approach to enforcement that recognizes that “ensuring” customer PI against every threat is not feasible. Such a standard could find companies at risk of violating the rules if their data is accessed, regardless of the efforts taken to protect it.

We also believe that several changes to the proposed rules are needed to ensure they more-closely mirror existing laws governing data protection and privacy. In particular, we are most concerned about the definitions of “personally identifiable information” and “breach,” several aspects of the NPRM’s data breach notification rules, and the scope of the opt-in approval requirement. We hope the Commission carefully considers our suggestions and implements the proposed changes.

II. Definitions

Definition of “Personally Identifiable Information”

The NPRM proposes a problematic definition of “personally identifiable information” that strays from other definitions of the term in statutes used to regulate data security and privacy. It is far too broad in its scope and, in its proposed form, could be interpreted to include just about any customer information, regardless of whether it’s tied to the customer or not. The NPRM claims that “our proposal incorporates this modern understanding of data privacy, which is reflected in our recent enforcement actions, and tracks the FTC and National Institute of Standard and Technology (NIST) guidelines on PII,”² but then proceeds to define PII in a manner that does not comport with any prior definition of the term.

¹ *In re* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, Notice of Proposed Rulemaking, FCC 16-39, at 109 (March 31, 2016) (Broadband Privacy NPRM).

² *In re* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, Notice of Proposed Rulemaking, FCC 16-39, at 21, para. 60 (March 31, 2016) (Broadband Privacy NPRM).

The Commission proposes that PII is any information that is “linked” or “linkable” to an individual, and states that “the ‘linked or linkable’ standard for determining the metes and bounds of personally identifiable information is well established.”³ Including the vague term “linkable” in the definition vastly expands the scope of what could be considered PII well beyond information that could actually be used to harm customers. Further, there are countless statutes defining PII that do not use the “linked or linkable” standard, and we do not believe it is actually “well established” in this context as the Commission has claimed.

The statutes and regulations the Commission cites as examples for why this definition is well established do not support such a definition when it comes to commercial entities. The scope of the NIST PII guide, for example, is an illustration of how federal agencies, not private companies, should protect their data.⁴ Similarly, FERPA applies to schools that receive federal funds⁵, 32 CFR §§ 310.4 applies to the DOD’s internal data protection practices⁶, 6 CFR § 37.3 applies to “states and territories that choose to issue driver’s licenses and identification cards,”⁷ and 45 CFR § 75.2 and 2 CFR § 200.79 apply to government contractors.⁸ Not a single one of these examples subjects private companies to penalties for failing to adequately protect broadly-defined “linkable” information. Only 17 CFR § 227.305(b), which applies to how companies sell securities, fits that criteria, and largely because the information at issue is almost exclusively highly-sensitive.

In contrast to the FCC’s proposal, the FTC’s Privacy Report, which is voluntary guidance for industry best practices,⁹ provides limits for the term “linkable.” While it recommends the inclusion of “linkable” in its definition of PII, it acknowledges that the term alone could be “overly broad,”¹⁰ includes a reasonableness standard, and offers guidance for determining what “reasonably linkable” means.¹¹ The FCC fails to take any of those steps in its NPRM, leaving a potentially overly broad, and legally enforceable, definition of “linkable,” on the table. Additionally, not a single state data breach or data protection statute uses the “linked or linkable” definition proposed by the FCC.¹²

³ *Id.* at 21, para. 61.

⁴ NIST, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) at § 1.2 (2010), <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>, (NIST PII Guide).

⁵ U.S. Department of Education, Laws & Guidance on Family Educational Rights and Privacy Act (FERPA), <http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>.

⁶ 32 CFR §§ 310.3(a).

⁷ 6 CFR § 37.1.

⁸ See 45 CFR § 75.100 & 2 CFR § 200.100.

⁹ Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers at iii (2012), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> (2012 FTC Privacy Report).

¹⁰ *Id.* at 22.

¹¹ *Id.* at 20-21.

¹² BakerHostetler, Data Breach Charts at 1-8, http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf (BakerHostetler Charts).

Ultimately, based on the facts at hand, it appears that the “linked or linkable” standard is, in fact, not at all “well established” when it comes to regulations on private companies’ protection of their customers’ data and privacy. Holding companies responsible for protecting “linkable” information without further defining the term could lead to severe consequences for a company’s failure to protect seemingly innocuous data. Because the term could be defined so broadly, just about any information could be deemed “linkable” to an individual. We would therefore suggest that the FCC remove the word “linkable” from its definition of PII.

Definition of “Breach”

The NPRM’s definition of the term “breach” as “any instance in which ‘a person, without authorization or exceeding authorization, has gained access to, used or disclosed customer proprietary information’”¹³ is also of concern to our members. Including “access” without any requirement for acquisition of information or a strong harm trigger could lead to overnotification of consumers and lead to unwarranted customer concerns when no information has actually been taken.

Nearly every state with data breach notification laws on the books requires “acquisition of personal information” to be considered a breach of security.¹⁴ The two states in which access to personal information is considered a breach of security, Connecticut¹⁵ and New Jersey,¹⁶ do not require companies to notify customers if they determine there is not a reasonable risk of harm to the customers,¹⁷ meaning access alone does not trigger notification.

While the current FCC rules regarding CPNI only require access to CPNI for a breach to have occurred,¹⁸ the Commission should consider removing the word “access” from its definition of breach due to the vast expansion of information its rules will cover in the future. Additionally, it should adopt a strong harm trigger for notification, as Connecticut and New Jersey have, to ensure that customers are only notified when there is a risk of harm (this will be discussed in further detail below).

Similarly, we believe that unauthorized access should have to be intentional to qualify as a breach. Without a strong harm trigger in place, requiring customer notification for innocuous inadvertent breaches will lead to overnotification and possibly so-called “breach fatigue” from customers. Customers should only be notified of breaches when there is a risk of actual harm resulting from the breach, and inadvertent breaches, particularly internal ones, are not likely to result in harm to the customer. The Commission should thus adopt an intent requirement in the definition of a breach.

¹³ Broadband Privacy NPRM at 26-27, para. 75.

¹⁴ BakerHostetler Charts at 8.

¹⁵ Conn. Gen Stat. § 36a-701b.

¹⁶ NJ Rev Stat § 56:8-161.

¹⁷ BakerHostetler Charts at 9-11.

¹⁸ 47 CFR § 64.2011(e).

III. Data Breach Notification

Notification Timeframe

Our members have some strong concerns about the proposed Data Breach Notification Requirements,¹⁹ particularly in regards to the requirement to notify affected customers no later than 10 days after the discovery of the breach.²⁰ The proposed 10-day notification window is unprecedented for data breach notification requirements and is so short that it may put both ISPs and their customers at additional risk.

After a breach, companies must have an adequate amount of time to conduct a risk assessment to determine the type of data that has been accessed and the risk that potential use of the data could entail. Further, companies must be able to identify the vulnerability responsible for the breach and resolve that vulnerability before notifying customers or else risk subjecting themselves to additional breaches by publicly disclosing details of the breach before fixing its cause. If a company does not have adequate time to complete a risk assessment, it may not be able to properly assess the scope of the breach or the damage it caused. This could lead to incomplete or inaccurate notifications to consumers that will later have to be corrected by further notices. Sending multiple unnecessary, potentially inaccurate, breach notifications to customers is costly to companies, and is likely to result in customers ignoring or missing meaningful notifications where their information could actually be at risk. Overnotification would thus undermine the primary goal of data breach notifications: encouraging customers to take steps to protect themselves.

Ultimately, we believe that ensuring the notification to customers is accurate is more beneficial than rushing to notify with potentially erroneous and harmful information. For that reason, we ask the Commission to reconsider its proposal to require customer notification within 10 days of the discovery of the breach and instead implement a flexible standard that allows for adequate assessment and resolution of the breach.

None of the current data breach laws in states today contain a time frame that is even comparable to the Commission's proposed 10-day window. 39 of the 47 states with data breach notification laws do not specify a time frame for notification at all, instead using language such as "in the most expedient time and manner possible" and "without unreasonable delay."²¹ Eight states, however, do require customers to be notified within a specific timeframe, but allow significantly more time or flexibility: Connecticut requires notification "no later than 90 days after discovery of a breach;" Ohio, Rhode Island, Vermont, Washington and Wisconsin require notification within 45 days after discovery; and Florida requires notification within 30 days after discovery.²² Maine uses a slightly different mechanism, requiring notification within 7 days after the completion of a

¹⁹ Broadband Privacy NPRM at 75-82, para. 233-255.

²⁰ *Id.* at 76, para. 234.

²¹ BakerHostetler Charts at 15.

²² *Id.* at 16.

“prompt investigation to determine the likelihood that personal information has been or will be misused,” and after law enforcement “determines that the notification will not compromise a criminal investigation.”²³

Compared to the data breach notification laws currently on the books, the FCC’s proposal for notification within 10 days is unreasonable and diverts from any pre-established norms. We would instead encourage the Commission to adopt a flexible standard that allows for proper completion of a risk assessment prior to notification.

Breach Notification Trigger

We appreciate the Commission’s proposal to “adopt a trigger to limit breach notification,”²⁴ and would encourage it to adopt a standard based on the risk of consumer harm. Most states use some variation of a “reasonable likelihood of harm” standard as their trigger, where harm is often defined as financial harm, bodily harm, identity theft, or fraud.²⁵ Given that this standard (or some slight variation of it) is used in most states already, it would make sense for the FCC to adopt such a standard in their rules as well. There does not appear to be any demonstrated reason to divert from what is already being used in practice across the country.

The NPRM goes on to ask a number of more-detailed questions about how the harm trigger should function such as “how would broadband providers, and the Commission, determine the likelihood of misuse or harm?” and “how much time should the providers have before they need to make their determination?”²⁶ We think that these questions do not necessarily need to be answered at this time because the answers will likely vary from breach-to-breach and may evolve as technology progresses. Instead of specifically outlining answers to these questions in the rules, the Commission should simply adopt a reasonability standard and develop these answers through enforcement actions on a case-by-case basis.

IV. Opt-in Approval

We are concerned that the scope of the proposed rules for opt-in approval is too broad and should be narrowed to more specific uses and types of data. The NPRM claims that the Commission’s proposal for opt-in approval is “consistent with . . . other privacy frameworks,”²⁷ and yet fails to cite any other such frameworks. It also generally cites the FTC’s 2012 Privacy Report for its framework of privacy choices, but that report makes a much narrower recommendation for when consumers should have to opt-in, suggesting that customers should have to opt-in before companies “(1) us[e] consumer data in a materially different manner than claimed when the data was collected; or (2) collect

²³ Me. Rev. Stat. tit. 10 § 1348.

²⁴ Broadband Privacy NPRM at 76, para. 236.

²⁵ BakerHostetler Charts at 8-12.

²⁶ Broadband Privacy NPRM at 77, para. 237-238

²⁷ *Id.* at 45, para. 127.

sensitive data for certain purposes.”²⁸ Further, according to Commissioner Ohlhausen, the FTC’s approach of only “requir[ing] opt in for specific, sensitive uses” is consistent with widely held consumer preferences.²⁹

To align with the FTC’s practices, the FCC should only require opt-in approval for the use and sharing of sensitive information such as health, financial and geolocation information. Further, as Commissioner Ohlhausen has pointed out, requiring opt-in approval for such a broad set of circumstances “prevent[s] unanticipated beneficial uses of data.”³⁰ The FCC’s proposed rules very clearly delineate specific uses of data that do not require opt-in approval, leaving all other uses of data to be subject to the opt-in requirement.³¹ This approach fails to account for potential new, innovative uses of data that could prove beneficial to consumers, leaving them subject to the opt-in regime by default. The Commission should, instead, outline specific situations for which opt-in consent is necessary and not presume that any use it has not considered is inherently harmful to consumers and therefore subject to an opt-in requirement.

V. Conclusion

With this NPRM, the Commission has shown a strong indication that it plans to regulate ISPs’ data security and privacy practices under ex ante rules more prescriptive than any existing federal or state requirements. These rules, as proposed, will only serve to stifle innovation, raise broadband costs, and deprive consumers of choice. They could also be used as a model for states and other entities to impose the same stifling regulations on the broader IT industry. We thus ask the Commission to reconsider its proposal and instead align its rules with the FTC’s current case-by-case approach, and to make significant changes to the definitions of “personally identifiable information” and “breach,” as well as its proposed data breach and opt-in requirements. Such changes would harmonize data security and privacy rules across the IT industry and would better serve an ever-changing sector of the economy than the FCC’s rules as proposed.

²⁸ 2012 FTC Privacy Report at viii.

²⁹ Remarks of FTC Commissioner Maureen K. Ohlhausen, Free State Foundation Eight Annual Telecom Policy Conference, March 23, 2016, p. 9, https://www.ftc.gov/system/files/documents/public_statements/941643/160323fsf1.pdf.

³⁰ *Id.* at 8.

³¹ Broadband Privacy NPRM at 45.