

**Before the
Federal Communications Commission
Washington, D.C. 20554**

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

COMMENTS OF PRIVACY RIGHTS CLEARINGHOUSE

Beth Givens, Executive Director
Meghan Land, Staff Attorney
Privacy Rights Clearinghouse
3033 5th Avenue, Suite 223
San Diego, CA 92103
619-298-3396

Filed May 27, 2016

Privacy Rights Clearinghouse (PRC) respectfully submits the following comments in response to the Federal Communications Commission’s (FCC) notice of proposed rulemaking (NPRM) “Protecting the Privacy of Customers of Broadband and Other Telecommunications Services”.

PRC is a nonprofit organization focused on consumer privacy education and advocacy.¹ We serve consumers nationwide and have invited individuals to contact us with their privacy-related questions, concerns, and complaints since 1992. PRC’s mission is to engage, educate, and empower individuals to protect their privacy. In turn, we identify trends and communicate our findings to advocates, policymakers, industry, media, and other consumers. Our point of view is unique due to the fact that we communicate directly with individuals and have a historical understanding of consumer privacy concerns.

PRC supports the FCC’s proposal to apply privacy requirements of the Communications Act to protect broadband users’ privacy and security. The FCC has a robust history of protecting and actively enforcing privacy rights, and is clearly aware of the wide ranging harms that consumers may suffer when their privacy is not protected. PRC fully agrees with the FCC’s characterization of the importance of privacy in the NPRM. “Privacy protects important personal interests. Not just freedom from identity theft, financial loss, or other economic harms but also from concerns that intimate, personal details could become grist for mills of public embarrassment or harassment or the basis for opaque, but harmful judgments, including discrimination.”²

This rulemaking is a vital next step to protect the privacy of telecommunications users. As Internet gatekeepers, broadband Internet access service (BIAS) providers have access to an enormous amount of information about their customers.³ BIAS customers must have meaningful privacy rights and protections, especially as data becomes increasingly valuable and easy to collect, store, disclose, and use in ways that can impact individual lives. FCC rulemaking is necessary because the current legal and regulatory landscape does not provide adequate rights and protections that broadband customers both expect and deserve. Indeed, current protections don’t even meet the expectations of most individuals we speak with who believe, erroneously, there is a comprehensive federal consumer privacy law.

PRC is generally supportive of the FCC’s NPRM. However, as a policy matter, we believe it is important to focus rules on a *complete* set of fair information practice principles (FIPPs) rather than isolating three as being most important: transparency, choice, and data security.⁴ Many areas where the FCC seeks comment are directly related to FIPPs, and we support integrating all FIPPs into the proposed rules. In

¹ Privacy Rights Clearinghouse, <https://www.privacyrights.org> (last visited May 27, 2016).

² Federal Communications Commission, Notice of Proposed Rulemaking: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Apr. 1, 2016, p 3, *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-39A1_Rcd.pdf.

³ Upturn, What ISPs Can See: Clarifying the technical landscape of the broadband privacy debate, Mar. 2016, <https://www.teamupturn.com/static/reports/2016/what-isps-can-see/files/Upturn%20-%20What%20ISPs%20Can%20See%20v.1.0.pdf>.

⁴ For a comprehensive resource on Fair Information Practices, see Robert Gellman, Fair Information Practices: A Basic History, Dec. 2015, *available at* <http://bobgellman.com/rg-docs/rg-FIPShistory.pdf>. *See also* OECD Privacy Principles, <http://oecdprivacy.org/> (last visited May 26, 2016); Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, Appendix A: The Consumer Privacy Bill of Rights, White House, February 2012, *available at* <https://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

addition, PRC believes opt-in consent should be the default by which a customer expresses approval for affiliate and related telecommunications services marketing. Finally, PRC is highly concerned with the concept of pay for privacy.

BIAS Customers Deserve Meaningful Notice of Privacy Practices

Online privacy notices are standard practice. They are also notoriously lengthy, vague, and exceedingly complex.⁵ While privacy notices in their current state can be helpful tools for regulators and privacy advocates, there is a disconnect between consumer expectations and actual data practices.⁶ At least one study has shown that a significant number of consumers think that a privacy policy's mere presence means that websites cannot sell personal information to third parties.⁷ BIAS providers' data practices are largely invisible to customers and data is becoming increasingly valuable and easy to collect, store, and share. This highlights the need for clear, conspicuous, and easy-to-understand privacy notices.

Standardized Notices

We advocate for the FCC to require a standardized notice to help bring consumer expectations closer to reality, make services easier to compare, and help consumers become familiar with recognizable formats. While not mandated, entities subject to the Gramm-Leach-Bliley Act may use a model privacy notice form as a safe harbor to comply with notice requirements.⁸ We believe the model notice provides consumers with an easy way to better understand a financial institution's practices and better highlights options for consumers to control their information. Standardized short form notices could also be used as a consumer-facing supplement to longer and more complex privacy notices.

Required Disclosures

The FCC asks whether it should consider adopting a requirement similar to California's Shine the Light law. As an organization with a long history in California advocacy work, we fully support the idea and intent behind Shine the Light. However, over the years it has become apparent that there is substantial non-compliance and there are major loopholes.⁹ A similar requirement could be incredibly beneficial for broadband customers, but FCC must take steps to avoid the flaws that currently exist in California's law.

⁵ See e.g. Aleecia McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, I/S: A Journal of Law and Policy for the Information Society (2008), available at <http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf>.

⁶ See Ashwini Rao, Alessandro Acquisti, Florian Schaub, Ruogu Kang, & Norman Sadeh, *Expecting the Unexpected: Understanding Mismatched Privacy Expectations Online*, October 2015, available at https://www.ftc.gov/system/files/documents/public_comments/2015/10/00081-99936.pdf.

⁷ See Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus*, 49 Wake Forest Law Review 261, 281 (2014), available at <http://ssrn.com/abstract=2434800> (describing a 2009 survey and quiz).

⁸ See Model Privacy Form, https://www.ftc.gov/system/files/documents/rules/privacy-consumer-financial-information-financial-privacy-rule/privacymodelform_optout.pdf (last visited on May 26, 2016).

⁹ See ACLU of California, *Losing the Spotlight: A Study of California's Shine the Light Law*, Nov. 2013, <https://www.aclunc.org/sites/default/files/Losing%20the%20Spotlight%20-%20A%20Study%20of%20California's%20Shine%20the%20Light%20Law%20final.pdf>; Chris Jay Hoofnagle & Jennifer King, *Consumer Information Sharing: Where the Sun Still Don't Shine* (Dec. 17, 2007), available at

Timing and Placement of Privacy Notices

PRC fully supports the FCC's proposal to require BIAS providers to give customers clear, conspicuous, and understandable information about their privacy practices and make the notice easily accessible prior to purchase at point of sale and on an on-going basis. We do not believe that the frequency with which users are presented notice (for instance annual or bi-annual) is relevant as long as privacy notices are easy to access from all devices, notices are written in a clear and comprehensible manner, customers receive notice when privacy practices have changed, and customers are given meaningful control and are able to express meaningful opt-in consent.¹⁰

BIAS Customers Must Have the Ability to Control their Information and Provide Affirmative Opt-In Consent to Data Practices

BIAS customers must be able to exercise meaningful choice so that they can exercise control over their information. Just because there is a privacy notice present or agreed to as a condition of service does not mean that the consumer has made an informed privacy tradeoff or exercised choice.¹¹

Privacy Dashboard

We strongly endorse the idea of providing BIAS users with a dashboard where they may view, change, and select privacy preferences. A dashboard with granular controls would allow customers to better understand BIAS providers' data practices and make informed choices about how their information is shared. A dashboard should be accessible at minimum through the BIAS provider's homepage, mobile application, and any functional equivalent. In addition, as Internet usage shifts increasingly to mobile devices it is important for any notices and tools to be developed with mobile in mind. We agree with the FCC's proposal to provide such a mechanism through a user interface that is readily apparent, easy to comprehend, and made available to customers at no cost.

Customer Approval Required for Use and Disclosure of Customer PI for Marketing Communications-Related Services

The FCC currently proposes that a BIAS provider give a customer notice and an opportunity to opt out before it uses customer proprietary information or shares it with an affiliate that provides communications-related services to market communications-related services to that customer. Customers deserve the right to opt in to the use and disclosure of their information in all but the narrowest of circumstances. It is tenuous at best to assume that a customer has approved use or sharing merely because she has not opted out of a practice. This is especially true if an opt-out choice is buried deep in a privacy notice, and is in no way in line with customers' expectations.

We also find the proposed definition of "affiliate" problematic. We oppose conditioning affiliate status on an equity ownership percentage for practical reasons. In many, if not most, cases a consumer will have

<http://ssrn.com/abstract=1137990>; Lauren Thomas & Chris Jay Hoofnagle, *Exploring Information Sharing through California's 'Shine the Light' Law* (Aug.13, 2009), available at <http://ssrn.com/abstract=1448365>.

¹⁰ See e.g., Consumer Financial Protection Bureau, CFPB Finalizes Rule to Promote More Effective Privacy Disclosures, October 20, 2014, <http://www.consumerfinance.gov/about-us/newsroom/cfpb-finalizes-rule-to-promote-more-effective-privacy-disclosures/>.

¹¹ See generally Joseph Turow, Michael Hennessy & Nora Draper, *The Tradeoff Fallacy*, Annenberg School for Communication, University of Pennsylvania, June 2015, available at https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.

a difficult time determining a BIAS provider's affiliates as well as the extent to which affiliate sharing occurs.¹² As the FCC notes, affiliates may have completely different branding and provide completely different services from the BIAS provider with whom the customer has a relationship. We strongly believe that the FCC should treat all affiliates as third parties and require opt-in consent from consumers for any sharing with affiliates.

The FCC Must Account for the Possibility of Re-identification of Aggregate Customer PI

The burden of proving that aggregate customer information is not reasonably identifiable or linkable to an individual should lie with the BIAS provider. However, we do have concerns that existing de-identification standards fail to sufficiently protect individuals' privacy. It is becoming increasingly clear that true de-identification is extremely complex if not a misnomer. Multiple studies have shown that seemingly singular, non-identifying data points can be used in combination with publicly available information or other seemingly innocuous information to identify individuals.¹³

BIAS Customers Deserve a Right to Access and Correct their Data

The right to access and correct personal data is a principle that is critical to any FIPPs-based framework to protect personal data. For instance, the White House Consumer Privacy Bill of Rights states, "Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate."¹⁴ We support building this principle into proposed rules, but also advocate implementing a meaningful audit mechanism and process by which BIAS providers may be held accountable for noncompliance.

BIAS Providers Must Secure Customer Proprietary Information and Provide Notice When it is Breached

Data Minimization

Also embodied in FIPPs, data minimization is crucial to protecting privacy,¹⁵ and PRC strongly recommends that the FCC require data minimization practices when possible. In the absence of data minimization requirements, BIAS providers have incentive to collect any and all information about their customers regardless of the sensitivity or utility of the data gathered. This is not only counter to privacy best practices, it also increases harmful effects of a potential data breach.

¹² For extensive information about ISP data practices, see Jeffrey Chester, *Big Data is Watching: Growing Digital Data Surveillance of Consumers by ISPs and Other Leading Video Providers*, Mar. 23 2016, available at <https://www.democraticmedia.org/article/big-data-watching-growing-digital-data-surveillance-consumers-isps-and-other-leading-video>.

¹³ See the work of Latanya Sweeney for more in-depth information, <http://latanyasweeney.org/publications.html> (last visited May 27, 2016).

¹⁴ Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, Appendix A: The Consumer Privacy Bill of Rights, White House, Feb. 2012, available at <https://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

¹⁵ The Consumer Privacy Bill of Rights states, "Consumers have a right to reasonable limits on the personal data that companies collect and retain." The OECD FIPPs articulate this right as a collection limitation principle stating, "There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."

Once consumer data enters the stream of commerce, there are few to no options to limit further access to and use of that data. This leaves consumers especially vulnerable to uses of their data that do not conform to their expectations, with little to no ability to regain control or even know how their data is being used and shared.¹⁶

Equally concerning to PRC is that institutions prove themselves incapable of sufficiently securing their sensitive and valuable data almost daily. In the eleven years that PRC has been tracking data breaches, we have seen an overall increase in the number of records breached and individuals impacted.¹⁷ The more data a company holds, the more attractive it is to criminals. To reduce the negative effects of almost inevitable data breaches, we urge the FCC to institute data minimization rules requiring BIAS providers to only collect personal data that is directly relevant and necessary to accomplish specified purposes and only retain such information for as long as is necessary to fulfill the specified purposes.

Data Breach Notification Requirements

Data breach notices are an important tool for consumers to use to help protect their personal information. When notices are clear and contain easy-to-understand information about the incident and types of information compromised, actionable tips, and useful resources, we do not believe that “overnotification” is an issue. Breach incidents vary, but it is rarely beneficial for a victim to be left in the dark. This is especially true because information that one victim may not consider sensitive, another may find highly sensitive and want to take action.

The PRC supports much of the FCC’s proposal regarding data breach notification requirements. However, with respect to the question of whether the FCC should condition notification on a risk of harm, we are strongly opposed. PRC has consistently advocated against conditioning breach notification on a trigger based on risk of harm.¹⁸ Such a trigger relies on the judgment of the breached entity and rarely takes into account any harm that falls outside of financial loss or the risk of identity theft. Privacy harms are broad and nuanced, and breach victims often suffer or are at risk of suffering harms that can’t be qualified as financial or economic in nature.

The FCC Must Prohibit Pay-for-Privacy Business Models that Force Individuals to Choose Between their Rights and Using Broadband Internet Service

PRC is fundamentally opposed to and concerned about the potential effects of pay-for-privacy scenarios on all consumers and particularly vulnerable populations. Under no circumstances should any consumer, especially those who are members of vulnerable communities, have to choose between their rights to privacy and foregoing broadband service.

The FCC Must Take a Careful Approach to Using Multi-Stakeholder Processes

¹⁶ See generally, Federal Trade Commission, *Big Data, A Tool for Inclusion or Exclusion?*, *Understanding the Issues*, FTC Report, January 2016, <https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf>.

¹⁷ See Privacy Rights Clearinghouse, *Chronology of Data Breaches, Security Breaches 2005 – Present*, <http://www.privacyrights.org/data-breach> (last visited May 26, 2016).

¹⁸ See e.g., Privacy Rights Clearinghouse, *Federal Data Breach Legislation – A Step Backward for Consumers*, Mar. 25, 2015, <https://www.privacyrights.org/Federal-Data-Breach-Legislation>.

Should the FCC decide to utilize multi-stakeholder processes, it must take a very careful approach. We believe that multi-stakeholder processes are prone to significant flaws that can prevent them from producing meaningful consensus documents, tools, and solutions.

After watching multiple National Telecommunications and Information Administration privacy-based multi-stakeholder processes over recent years, we have major concerns with using such processes on an ongoing basis without making fundamental changes. One of the most basic flaws is that the process is conducted entirely in Washington, D.C. even though many relevant stakeholders are based elsewhere. Organizations and even small companies without trade associations or a DC-based lobbyist must travel to every meeting or participate remotely, which is far less effective. In addition, it is not always clear who participants represent, and all participants must be required to make it explicitly clear who he or she represents in every meeting and perhaps every time he or she speaks. Many such processes also minimize the voice of the minority in the room. It is important to recognize that the civil society and consumer advocate community is small, and many organizations have little bandwidth. Finally, participants must have an incentive to participate in good faith. In most cases this means the end product must be meaningful, binding, and/or enforceable.

Conclusion

PRC believes this is an important rulemaking and a major potential step forward for consumer privacy protections. In addition to these comments, we have also signed on to comments opposing forced arbitration clauses and comments articulating the importance of this rulemaking.