

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

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

*Balancing Privacy Protection and Access to Network Data*

Comments of<sup>1</sup>

William Lehr, Steve Bauer  
Massachusetts Institute of Technology

and

Erin Kenneally  
University of California, San Diego

May 27, 2016

Table of Contents

1. Introduction.....	1
2. FCC has a valid interest in regulating how BIAS information is shared.....	3
3. Asymmetric, sector-specific regulation can only be part of the solution .....	3
4. Protecting Access to BIAS Data for Network Researchers is Important.....	7
5. Bio Descriptions of Authors .....	9

**1. Introduction**

As academic researchers and advisors engaged in work that touches upon multiple technical, business, and policy aspects of the Internet ecosystem, we are submitting these

---

<sup>1</sup> William Lehr, wlehr@mit.edu, 32 Vassar Street (32-G814), Cambridge, MA 02139 (corresponding author); Steve Bauer, bauer@mit.edu; David Clark, ddc@csail.mit.edu; and Erin Kenneally, erink@icsi.berkeley.edu.org. We are submitting these comments as individuals. The opinions expressed herein are those of the authors alone.

comments in response to the FCC's *Privacy NPRM* which proposes a "framework for applying the traditional privacy requirements of the Communications Act to BIAS" and seeks public input on "the best approach to protecting consumers' privacy when they use broadband services."<sup>2</sup>

The FCC's actions in the *Privacy NPRM* address an important and compelling regulatory concern for the governance of our increasingly Internet-connected world: the need to protect individual consumer privacy. The Internet is valuable precisely because it is a general-purpose platform for electronic communications connecting consumers, ISPs and edge providers. The information that flows across the Internet includes substantial Proprietary Information (PI) that needs to be protected from unauthorized disclosure and use, but which also must be shared appropriately with third parties to enable network management;<sup>3</sup> to enhance cybersecurity and protect critical infrastructure;<sup>4</sup> and to sustain the decentralized resource ownership and control that enables market competition and innovation to thrive. These goals are inextricably linked in the challenge of protecting consumer privacy.

In these comments, we wish to stress several important points.

- First, the FCC has a valid interest in regulating how information is shared via Internet Services that would arise even if there were no regulatory mandate to protect consumer privacy.
- Second, the FCC can be, at best, only part of the regulatory solution needed to protect consumer privacy. The FCC needs to retain authority to act but should be careful in mandating excessive opt-in/out requirements and restrictions on sharing information with third-parties that singles out specific services and actors lest such rules distort

---

<sup>2</sup> See paragraph 14 of *Notice of Proposed Rulemaking*, In the Matter of Protecting the Privacy of Customers or Broadband and Other Telecommunication Services, Before the Federal Communications Commission, WC Docket No. 16-106, released April 1, 2016, available at [https://apps.fcc.gov/edocs\\_public/attachmatch/FCC-16-39A1.pdf](https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-39A1.pdf) (hereafter, "*Privacy NPRM*").

<sup>3</sup> Network management: ISPs, CDNs, and other value-added participants in the end-to-end Internet need to share metadata and traffic data to insure interoperable, high-quality services offering suitable end-to-end Quality-of-Experience (QoE). As we shift to more dynamic cloud-based services (enabled by such things as 5G and or NFV-enabled networks), the range of network-related information that will need to be shared will increase (both with respect to the range of metrics and the data for those metrics). Research on Future Internet Architectures (FIAs) suggests that the Internet is moving toward a world in which much more information (state) will be managed and maintained within the network on a much more granular, dynamic, and automated basis.

<sup>4</sup> To adequately address the growing threats to cybersecurity, more information about threats, vulnerabilities, and attacks needs to be shared. In passing the Cybersecurity Information Sharing Act of 2015 (CISA, see <https://www.congress.gov/bill/114th-congress/senate-bill/754>) Congress demonstrated its recognition of the importance of this. As the principal regulatory of our communications infrastructure, the FCC has an obvious and important role to play with respect to determining what and how information related to cyber threats to the networks may be shared and managed.

market competition, deter incentives for beneficial information sharing, and impede progress toward better, market-based alternatives.

- Third, an important consideration should be to protect and preserve network researchers access to data. To understand the increasingly complex Internet ecosystem so that consumers and value chain participants can make informed decisions requires access to network-related data on traffic, service performance, and market conditions. Access to such data by third party analysts, including academic researchers and others with legitimate research/measurement interests, is important for protecting the competitive process and limiting the need for recourse to more heavy-handed government regulation. The present rules increase the challenges of ensuring such access and should be modified to address this issue.

## **2. FCC has a valid interest in regulating how BIAS information is shared**

We recognize that the FCC has an enduring interest in regulating communications services such as BIAS. From that interest flows a necessary interest in the regulatory framework governing the exchange of consumer PI via the networks and services that support the end-to-end operation of the Internet. That interest exists regardless of one's interpretation of the relevance of Section 222 and the FCC's statutory responsibility for protecting Consumer Privacy. The FCC's interest in promoting appropriate network management, cybersecurity, and Internet competition provide a sufficient basis for the FCC's regulatory interest in the management of what and how consumer PI may be shared with third parties.

Consequently, we applaud the FCC's initiative in promoting an important discussion of the appropriate framework that should be in place to protect consumer PI that arises in the context of providing telecommunication services like BIAS, and how this relates to the Communications Act and other privacy frameworks.

## **3. Asymmetric, sector-specific regulation can only be part of the solution**

The challenge to protecting consumer privacy online is neither limited to BIAS nor solely the responsibility of the FCC. While we do not disagree with the FCC seeking to take action in this area, we hope the comments that this proceeding will engender will result in a beneficial public dialog of what appropriate actions in this space should be.

The emphasis on transparency (consumers should know what consumer PI data BIAS providers have and who they shared it with), choice (consumers should be able to grant informed consent to authorize the use consumer PI), and security (consumer PI should be appropriately secured and mechanisms to address data breaches should be implemented) is appropriate and consistent with other mainstream frameworks to protect consumer PI.

Of these three areas of focus, the one that most concerns us here relates to the rules for ensuring informed consumer choice. More specifically, the rules and standards related to opting in/out of third-party data sharing.

We believe that additional effort is needed to further clarify these frameworks, and that that work should logically precede attempts to standardize transparency and disclosure requirements; and to a lesser extent, efforts to ensure the data is appropriately secured. Clarifying the consumer informed consent rules will be necessary to clarify the definitions of and policies for adequate transparency and disclosure since the sharing rules will set expectations and incentives for strategic behavior with regards to transparency and disclosure reporting.<sup>5</sup> Thus, while we believe efforts to standardize and homogenize reporting obligations are laudable, it would be premature to attempt to do so today.<sup>6</sup>

The FCC's role in preserving consumer privacy is limited in several respects. First, the responsibility to protect consumer privacy and facilitate innovation online is an economy-wide challenge that is hard to compartmentalize in a sharing and interdependent ecosystem. The blurring of industry (sector), market, and firm boundaries – facilitated by the economic changes that the Internet has helped bring -- makes it hard to target regulations to specific actors and risks distorting market incentives.<sup>7</sup> Moreover, the agglomeration of sector-specific (for healthcare, for the financial sector, or for telecommunications) or service-specific (for email or BIAS) privacy regulations creates additional challenges for migrating to a more desirable, technology/market-neutral privacy protection regime in the future.

In issuing the *Privacy NPRM*, the FCC is acting to address a “gap that must be closed” in the federal privacy regime,<sup>8</sup> and justifies its focus on providers of Broadband Internet

---

<sup>5</sup> In Lehr, Kenneally and Bauer (2015), we discussed the challenges and complexity of implementing appropriate disclosure and transparency policies within the context of the Open Internet Order. Briefly, when policymakers require market participants to share information they should anticipate the participants to behave strategically toward that mandate. The same sorts of complexities apply here. (See Lehr, William, Erin Kenneally, and Steve Bauer (2015), *The Road to an Open Internet is Paved with Pragmatic Disclosure & Transparency Policies*,” TPRC2015, Alexandria, VA, September 2015, available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2587718](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2587718).)

<sup>6</sup> See paragraphs 88-93 in *Privacy NPRM*.

<sup>7</sup> Either because of changes in the way productive activities are organized into firms, markets, or industries because of the rapid changes in the Internet ecosystem, or because firms restructure so as to avoid regulation, the ability to target specific actors is increasingly challenging in the Internet. The architecture of the Internet, as evidenced by the softwarization of operator networks (e.g., deployment of SDN and NFV technology to allow finer-grained dynamic control of network resources), the rise of cloud services (content-delivery networks, on-demand computing resources, and data centers), and the convergence of fixed/mobile networks makes it easier to shift functionality across firm and traditional industry boundaries; or, distinguishing between edge and access providers, service or application/content providers, etcetera. Asymmetric regulations that target firms based on legacy notions of how functionality is organized distort incentives for how to structure Internet functionality and favor one set of competitors over another.

<sup>8</sup> See paragraph 2 of *Privacy NPRM*.

Access Services (BIAS), in part, because it views such providers as having an “ability to capture a breadth of data” that is unmatched by any edge provider.<sup>9</sup> By framing its actions in this way, the FCC is explicitly acknowledging that BIAS providers are not unique in posing a potential risk to consumer privacy; and that the FCC is not the only government entity with responsibility for protecting privacy.<sup>10</sup>

For example, edge providers and other value-added Internet service providers all play a role in enabling end-to-end Internet services, and may pose a threat to consumer privacy.<sup>11</sup> While it is not unreasonable to conclude that providers of BIAS may be better placed than many edge providers or other actors in the Internet ecosystem, the risks to privacy are a question of degrees. It is far from clear that a Comcast or Verizon BIAS provider has the ability to capture more consumer private information than a Google or Facebook. The fact that consumers may find it easier to switch search engines than to switch broadband access providers today does little to mitigate concerns about the potential ability of edge-providers like Google, Facebook, or Twitter to pose a significant threat to consumer privacy.

The FCC acknowledges the importance of the FTC’s role in protecting online privacy through its assertion of its general authority (i.e., not sector-specific) to “prohibit ‘*unfair or deceptive acts or practices in or affecting commerce.*’”<sup>12</sup> Certainly, the FTC’s efforts to audit and hold-to-account edge providers on-line promises to protect customer privacy are important regulatory actors in the overall federal policy regime. Indeed, the fact that the FTC’s focus is not limited to a single sector or class of actors is attractive from the perspective of addressing the drawbacks associated with sector-specific regulatory frameworks noted above.

Although in an ideal world, we might hope for a harmonized and symmetric privacy protection regime that is not based on a mélange of overlapping and potentially conflicting sector-specific regulations, the U.S. approach to date has been substantially reliant on sector-specific rules (e.g., for healthcare, for financial data, etc.).<sup>13</sup> Viewed

---

<sup>9</sup> See paragraph 4 of Privacy NPRM.

<sup>10</sup> The FCC interprets Section 222 – Privacy of Customer Information of the Communications Act (47 U.S.C. § 222), which states “Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier.” (see <https://www.law.cornell.edu/uscode/text/47/222>).

<sup>11</sup> Edge providers include providers of applications, content, and devices. Others that may not be explicitly identified as edge providers may also pose a threat to consumer privacy. This includes ISPs that provide transit and peering services that BIAS connect to, as well as providers of services such as cloud storage and computing, content-delivery services, and other ancillary services that support the Internets basic functionality.

<sup>12</sup> See paragraph 8 of Privacy NPRM. Italics in the original.

<sup>13</sup> This is at variance with the European approach, where policymakers have sought to establish a comprehensive general privacy protection framework. It is arguable whether that

from that perspective, the FCC's efforts to reinterpret Section 222 in the Communications Act for the new world of the Internet – which was not mentioned in the Telecommunications Act of 1996, when Section 222 was added – may be seen as rationally consistent with its actions in the Open Internet Order that defined BIAS.<sup>14</sup>

Moreover, because the FCC needs to be involved in defining the rules for third-party sharing of consumer PI that is needed to facilitate the secure operation of the Internet (for network management, cybersecurity, and to provide end-to-end services across a network of networks) and those needs are inextricably bound up with privacy concerns, it is not reasonable to simply delegate responsibility for privacy protection to the FTC. While some segmentation of responsibilities is certainly desirable, it does not seem advisable to rely on a segmentation that assigns and limits FCC oversight solely to BIAS providers and oversight of edge providers to the FTC. It will remain necessary and complex to coordinate and manage their dual oversight roles, and those of other regulatory actors with responsibilities in this area (e.g., SEC, Homeland Security, etc.).

Thus, the need to manage multiple regulatory agencies as part of the fabric of the federal privacy protection framework is both unavoidable and continuing. Furthermore, frameworks for protecting privacy are continuing to evolve. For example, it is becoming increasingly clear just how difficult it is to appropriately anonymize data to allow it to be shared without risking that the data could be re-identified later. This makes it difficult to define frameworks for sharing aggregate or anonymized data, which otherwise might provide a good solution in many contexts.<sup>15</sup> Meanwhile, efforts are underway in the case of healthcare, where the Health Insurance Portability and Accountability Act (HIPAA) has established a strong foundation for privacy protection and where standards for what constitutes acceptable practices for de-identifying data are more developed than in other sectors, for extending an auditable framework for ensuring the privacy protection of data shared with third parties. Under HIPAA, third-party data recipients (“business associates”) inherit the same data security and privacy obligation as first party data controllers (“covered entities”), whose liability is expanded if they do not implement transitive responsibility via business agreements with third-party data recipients. Such a chain of oversight is needed to address data leakage problems and induce appropriate incentives to protect and use the healthcare equivalent of consumer PI as authorized.

---

approach will actually prove more effective in practice, and in any case, circumstances in the U.S. are now different.

<sup>14</sup> See *Report and Order on Remand, Declaratory Ruling, and Order*, In the Matter of Preserving the Open Internet, GN Docket No. 14-28, adopted February 26, 2015, available at [https://apps.fcc.gov/edocs\\_public/attachmatch/FCC-15-24A1.pdf](https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf) (hereafter, "FCC 2015 OIO").

<sup>15</sup> See paragraph 154 of the *Privacy NPRM* for a discussion of the proposed framework for sharing aggregate or anonymized data. The *Privacy NPRM* proposes allowing BIAS providers to share anonymized or aggregate data with third-parties if the provider does a number of things, including “determines that the aggregated customer PI is not reasonably linkable to a specific individual or device” and “exercise reasonable monitoring to ensure those contracts are not violated.” In both of these, the question of how “reasonable” may be interpreted and evolve over time renders the implementation of this framework inherently uncertain, but such regulatory uncertainty – while unfortunate – is not avoidable.

Of course, not all consumer PI is equally as sensitive and as amenable to corrective action if breached,<sup>16</sup> and a one-size-fits-all approach is unlikely to be appropriate for all data sources and for all sectors. Actors in the healthcare space have been long accustomed to the need for relatively high standards for data protection. It is uncertain whether consumer PI in other domains will be deemed as worthy of high-cost privacy protection measures as healthcare or certain financial information; or indeed, what those costs might be in a more comprehensive privacy protection regime. Nevertheless, as the FCC suggests the best practices being implemented for sensitive healthcare and financial data may provide valuable lessons for informing a framework that may be extended more generally.<sup>17</sup>

On the narrower question of whether it makes sense for the framework to distinguish between fixed and mobile broadband services, we agree with the FCC's preliminary conclusion that separate frameworks are not warranted.<sup>18</sup> While there may be valid reasons for why either mobile or fixed BIAS providers should not be required to comply with the framework as proposed in the *Privacy NPRM*,<sup>19</sup> it would make little sense to have substantively separate frameworks for mobile and fixed BIAS providers. The world is increasingly moving to a world in which mobile broadband will be an ever-increasing mode for how subscribers will access the Internet and subjecting this to a (presumably) weaker framework would tilt the competitive landscape, and in any case, would be unlikely to result in better overall protection of consumer privacy. If the framework needs to be relaxed to accommodate either mobile or fixed BIAS providers, then those modifications should apply to both symmetrically to the greatest extent possible.

In summary, therefore, we are cautiously supportive of the FCC's efforts to redefine Section 222 in order to address BIAS, but are concerned about ways in which this asymmetric regulation may inappropriately distort market protection and add costs, without significantly enhancing the federal framework for protecting consumer PI. We look forward to what we hope will be a fruitful detailed examination of the many questions and issues raised in the *Privacy NPRM*.

#### **4. Protecting Access to BIAS Data for Network Researchers is Important**

---

<sup>16</sup> For example, healthcare PI is permanently associated with an individual, whereas financial data like credit card numbers can be replaced if breached.

<sup>17</sup> See paragraphs 171, 181-184.

<sup>18</sup> See paragraph 310 in *Privacy NPRM*.

<sup>19</sup> We have not sufficiently considered the *Privacy NPRM* to offer an opinion on the suitability of the framework for mobile versus fixed BIAS providers.

Strong privacy protection rules make it more difficult to share data with third-parties, including academics, network researchers, and application developers.<sup>20</sup> Ensuring adequate access to network data is important to enable and sustain academic research and a viable and vigorous ecosystem of third-party analysts and sustaining market competition across the value chain (which includes in edge provider markets). In a number of papers, we have explained why third-party access to Internet performance metrics and data helps sustain competition and complements and enhances trust in other regulatory mechanisms.<sup>21</sup>

Unfortunately, adequate data about network performance is often not available to third-party researchers, including academics, who are doubly challenged since they rely on scarce research funding to cover their data acquisition and research costs. Moreover, in most cases, network researchers are heavily dependent on the voluntary cooperation of participants in the Internet ecosystem, including BIAS providers, to acquire the data needed to conduct important research on the technical and market performance of broadband and other Internet services. The incentives for BIAS providers to support such research, especially when directed toward studies that will be made generally available to the public instead of proprietary consultancy-based studies, is already tenuous.

The privacy rules promulgated in the *Privacy NPRM* are likely to make it more difficult for academics to acquire BIAS performance data.

While we recognize that academics are not immune from needing oversight to protect access to and use of PI, we encourage the FCC to consider formally recognizing the importance of enabling sharing with academic and other third-party network researchers. In most cases, aggregate or otherwise de-identified data may be sufficient. For example,

---

<sup>20</sup> For example, ISPs do not currently expose an API for users or their applications to access basic service parameters such as upload and download speeds which is some of the sort of information that one might expect to be included in CPNI. Accessing such information could allow users to better diagnose network performance problems (e.g., on their home networks) and applications to conduct performance tests to improve the end-to-end quality of experience on the user's behalf. While we believe ensuring adequate access to information for application developers is important, it is not the main focus of our comments here, and we recognize engages additional considerations that would need to be addressed.

<sup>21</sup> See for example, Bauer, Steve, William Lehr, and Shirley Hung (2015), "Gigabit Broadband, Interconnection Propositions, and the Challenge of Managing Expectations," TPRC2015, Alexandria, VA, September 2015, available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2586805](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2586805); Clark, D., S. Bauer, W. Lehr, K. Claffy, A. Dhamdhere, B. Huffaker, and M. Luckie (2014), "Measurement and Analysis of Internet Interconnection and Congestion" *Journal of Information Policy*, Vol 4; Lehr, W., D. Clark, and S. Bauer (2013), "Measuring Performance when Broadband is the New PSTN," *Journal of Information Policy*, Vol. 3 (2013), pg. 411-441; or, Bauer, Stephen, David Clark, and William Lehr (2013), "Broadband Micro Foundations: the Need for Traffic Data," in *Beyond Broadband Access: Developing Data-based Information*, edited by Richard Taylor and Amit Schejter, Fordham University Press, 2013.

such language might be included in the discussion of Permissible Uses and Disclosures of customer PI for which Customer Approval is Implied or Unnecessary.<sup>22</sup>

In addition, we recommend that the FCC consider instituting an exception process for data sharing with third-party network researchers. We believe in most cases that such sharing is likely to fit within the category of data that needs to be shared to sustain the safe operation of the end-to-end Internet. For example, data about the configuration of services, technical performance and traffic statistical data – appropriately de-identified in most cases, is needed to inform research directed at designing better Internet technologies and evaluating market performance.

Classifying the data shared with legitimate researchers in this way would allow researchers access without requiring costly explicit “opt-in” approval from each subscriber. Requiring such opt-in approval for the sorts of large data sets typically engaged by network researchers would be impractical and likely to pose an insurmountable cost burden, rendering the data inaccessible. Moreover, any additional costs- whether operational or viz legal risk- imposed on BIAS providers associated with their efforts to share data with network researchers would weaken their already weak incentives to share.

Finally, we believe that it is reasonable to afford subscribers the ability to have a simple and automated way to acquire machine-readable information about their service configuration. There are a number of ways this might be accomplished. In Lehr, Kenneally, and Bauer (2015), we suggested one approach that we refer to as “Net.Info,” which is a proposal for creating a secure distributed channel for sharing information regarding BIAS service and an end-user.<sup>23</sup>

## 5. Bio Descriptions of Authors

[William Lehr](#) is a telecommunications/Internet industry economist and policy analyst with over twenty years of experience in academic research and industry consulting. He is currently a research scientist in the Computer Science and Artificial Intelligence Laboratory (CSAIL) at the Massachusetts Institute of Technology (MIT). Dr. Lehr's research focuses on the economic and policy implications of broadband Internet access, next generation Internet architecture, and the evolution of wireless technology. In addition to his academic research, Dr. Lehr regularly advises senior executives and policymakers in the U.S. and abroad on business strategy and policy matters of relevance to the communications and information technology industries. Dr. Lehr holds a PhD in

---

<sup>22</sup> See paragraph 111 and following in *Privacy NPRM*.

<sup>23</sup> See pages 16-17, 22-23 in Lehr, William, Erin Kenneally, and Steve Bauer (2015), “The Road to an Open Internet is Paved with Pragmatic Disclosure & Transparency Policies,” TPRC2015, Alexandria, VA, September 2015, available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2587718](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2587718).

Economics from Stanford, an MBA in Finance from the Wharton School, and MSE, BA, and BS degrees from the University of Pennsylvania.

[Erin Kenneally](#) is a Program Manager in the Cyber Security Division for the Homeland Security Advanced Research Projects Agency (HSARPA) with the DHS Science & Technology Directorate. Her portfolio comprises trusted data sharing, privacy, cyber analytics, and information communications technology ethics. She manages the IMPACT (Information Marketplace for Policy and Analysis of Cyber-risk and Trust) and Cyber Economics/Analytics programs. Prior to joining CSD, Kenneally was Founder and CEO of Elchemy, Inc., and served as Technology-Law Specialist at the International Computer Science Institute (ICSI) and the Center for Internet Data Analysis (CAIDA) and Center for Evidence-based Security Research (CESR) at the University of California, San Diego. Erin is a licensed Attorney specializing in information technology law, including privacy technology, data protection, trusted information sharing, technology policy, cybercrime, data ethics, and emergent IT legal risks. She holds Juris Doctorate and Masters of Forensic Sciences degrees, and is a graduate of Syracuse University and The George Washington University.

Dr. Steven Bauer is a Research Affiliate at the Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory. Bauer's research focuses on the architectures and economics of Internet-scale networks. He has been involved in many measurement projects entailing the collection and analysis of very large corpuses of network data. He has collaborated on research initiatives with the FCC, Google, Akamai and some of the largest broadband providers around the world. Bauer was the recipient of the Department of Defense National Science and Engineering Fellowship and the National Science Foundation Fellowship. He is also a Harry S. Truman Scholar and Barry Goldwater Scholar.