2018

Protecting ISP Customer Proprietary Network Information in Pennsylvania

Samantha Zimmer
Duquesne University School of Law, Class of 2018

Protecting ISP Customer Proprietary Network Information in Pennsylvania

Samantha Zimmer

Table of Contents

I. The Problem

In modern society, technologies evolve and challenge existing legal frameworks regularly. Unfortunately, legislatures do not move as quickly as the tide of technological change when it comes to updating laws to reflect our progression of technology. In order to combat this problem, administrative agencies are often left to bridge the gap by using regulatory power to stretch existing law to encompass new technologies. The Federal Communications Commission ("FCC") has often been at the forefront of this movement, as it tries to regulate internet providers through legislation passed in the 1930s and the 1990s.[1] However, regulatory agencies like the FCC are subject to sudden change depending upon changes in executive administrations.[2] Given the slow nature of the federal legislature and the uncertainty that comes with the promulgation of federal regulations, state legislatures have begun to take up unresolved areas of federal law by creating policy through action at the state level.[3] This was most recently exemplified following the recent repeal of the FCC regulating the use of customer information by Internet service providers. When these regulations were repealed following the change of presidential administrations, bills were proposed in over 20 state legislatures in an effort to maintain the protections of the FCC regulations on the state level.[4] Given the lack of preemption from a federal statute or regulation in this area, states are in a good position to legislate regarding this matter. No such bill has yet been introduced in Pennsylvania, but the state of Pennsylvania has both the need and authority for a statute in this area.

---

[1] *See infra* note 5.
[2] *See, e.g.*, Alexa Lardieri, *Trump Administration to Revamp Title IX*, U.S. NEWS (Sept. 7, 2017 1:46 PM), https://www.usnews.com/news/politics/articles/2017-09-07/betsy-devos-annouces-the-trump-administration-plans-to-revamp-title-ix (discussing the planned roll back of expansive Obama era Title IX regulations); CNBC, *Trump stops hundreds of planned regulations*, (July 20, 2017, 9:00 AM), https://www.cnbc.com/2017/07/20/trump-stops-hundreds-of-planned-regulations.html (explaining the significant decrease in regulatory actions just 6 months into the presidency).
[3] *See infra* note 54.
[4] *See infra* note 55.

A. ISPs as Common Carriers? The Road to Regulating ISP Protection of Customer Data

The Communications Act of 1934 ("Communications Act") created the FCC and gave it the power to regulate "interstate and foreign commerce in communication by wire or radio."[5] This act gave the FCC the broad regulatory authority that allows it to monitor the business and communications practices of landline and telephone providers, radio communications, and various other technologies.[6] Under the Communications Act, there is a distinction made between common carriers and information services.[7] Common carriers are defined entities engaged in interstate communication by radio or wire for hire.[8] In contrast, information services are defined by their capability of "making information available via telecommunications."[9] This distinction is at the core of the Communications Act and past FCC regulations. It follows the traditional idea that public utility providers should be held to a higher standard due to the nature of the service they provide.[10]

As a result of this distinction, telecommunications common carriers are subject to stricter provisions, such as a prohibition on discriminating in services and charges,[11] and a requirement to keep customer proprietary network information confidential.[12] With the Telecommunications Act of 1996 ("Telecommunications Act"), Congress provided that telecommunications services would be regulated as common carriers.[13] Specifically, Congress distinguished between telecommunications carriers and information-service providers.[14] Under

---

[5] 47 U.S.C.A § 151 (Westlaw through P.L. 115-68).
[6] *Id*. § 152.
[7] *Id*. § 153.
[8] *Id*. § 153(11).
[9] *Id*. § 153(24).
[10] Paul R. Gaus, *Only the Good Regulations Die Young: Recognizing the Consumer Benefits of the FCC'S Now-Defunct Privacy Regulations*, 18 MINN. J.L. SCI. & TECH. 713, 726 (2017).
[11] 47 U.S.C.A § 202 (Westlaw through P.L. 115-61).
[12] *Id*. § 222.
[13] *Id*. § 153(51).
[14] Verizon v. F.C.C., 740 F.3d 623, 630 (D.C. 2014). *See also* Sheraz Syed, *Prioritizing Traffic: The Internet Fast Lane*, 25 DEPAUL J. ART, TECH. & INTELL. PROP. L. 151, 157 (2014).

this distinction, telecommunications carriers provided basic services and information-service providers provided an "enhanced service."[15] Companies providing enhanced services were considered to be "more involved in the processing of information than simply its transmission."[16] Following the passage of the Telecommunications Act, the FCC classified Digital Subscriber Line ("DSL") and other broadband Internet services as information services that were not subject to common carrier requirements.[17]

This tension regarding the statutory classification of ISPs was at the center of much debate.[18] This debate over the openness of the internet, commonly referred to as "net neutrality,"[19] culminated in the FCC's Open Internet order in 2015.[20] The Open Internet Order and its subsequent regulations had the effect of establishing that ISPs would be regulated as common carriers, meaning discrimination in provision of services would be prohibited.[21] By settling this classification of ISPs, the FCC established its authority to ensure that ISPs act in compliance with all common carrier provisions set forth in the Communications Act.[22]

Following the reclassification of ISPs, the FCC used its new authority for regulating ISPs as common carriers to implement rules protecting the customer proprietary network information ("CPNI") held by ISPs.[23] Under the Communications Act, CPNI is defined to include

---

[15] *Verizon*, 740 F.3d at 630.
[16] *Id.*
[17] *Id.* at 631.
[18] *See* Nelson Granados, *The Net Neutrality Debate: Why There Is No Simple Solution*, FORBES (May 31, 2017), https://www.forbes.com/sites/nelsongranados/2017/05/31/the-net-neutrality-debate-why-there-is-no-simple-solution/#2379d0215c67 (describing the differing arguments and competing interests on both sides of the net neutrality debate).
[19] Net neutrality refers to the foundational principle of the open Internet, where all consumers and content providers have equal access to receive and provide content, respectively. Mike Snider et al., *What is net neutrality and what would its reversal mean?*, USA TODAY (April 26, 2017, 3:43 PM), https://www.usatoday.com/story/tech/news/2017/04/26/ what-net-neutrality-and-what-would-its-reversal-mean/100930220/.
[20] *See generally* In the Matter of Protecting and Promoting the Open Internet, 30 F.C.C.R. 560 (2016).
[21] *Id.*
[22] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 87274-01, 87277 (Dec. 2, 2016) (to be codified at 47 C.F.R. pt. 64).
[23] *See* 47 C.F.R. § 64.2001 (2017).

information relating to the individual connection to the network along with other information for individual billing.[24] Relying upon its authority under the Open Internet Order, the FCC promulgated regulations to bring ISPs in compliance with § 222 of the Communications Act, a provision that prohibits common carriers from using, disclosing, or permitting access to CPNI.[25]

The 2016 CPNI regulations applied to broadband internet access services ("BIAS" or "ISP"),[26] which were defined as "mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints."[27] The FCC focused on transparency, consumer choice, and data security.[28] At their most basic form, the regulations required ISPs to notify customers of privacy policies, provide opt-in or opt out procedures for consumers, and keep data securely, including data breach procedures.[29]

Utilizing the Congressional Review Act, Congress repealed the 2016 FCC privacy regulations in April of 2017.[30] President Trump signed off on this change and the regulations became ineffective, opening up the door for ISPs to collect, use, and distribute subscriber information to increase their profits.[31]

B. Competing Interests in the ISP CPNI Debate

The FCC's 2016 regulations brought much comment and debate, highlighting the varying competing interests at stake. Interests of ISPs, consumers, the FCC, the Federal Trade Commission ("FTC"), all needed to be accommodated and considered. Based upon two primary

---

[24] 47 U.S.C.A § 222 (2)(h)(1) (Westlaw through P.L. 115-61). Specifically, this includes "information that relates to the quantity, technical configuration, location, and amount of use of a telecommunications service." *Id.*
[25] *Id.* § 222(c)(1).
[26] For the purposes of this paper, ISP and BIAS will be used interchangeably, as the distinction between broadband services and internet services is not relevant for statute applicability.
[27] 47 C.F.R. § 8.2 (2015).
[28] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 87274-01, 87274 (Dec. 2, 2016) (to be codified at 47 C.F.R. pt. 64).
[29] *Id.*
[30] Jeff Dunn, *Trump just killed Obama's internet-privacy rules – here's what that means for you*, BUSINESS INSIDER (April 4, 2017, 10:55 AM), http://www.businessinsider .com/trump-fcc-privacy-rules-repeal-explained-2017-4/#how-did-all-of-this-get-started-1.
[31] *Id.*

arguments, ISPs asserted that these privacy regulations were unnecessary. First, ISPs argued an inherent unfairness to the rules, as edge providers[32] did not fall under the purview of the new regulations. However, ISPs are fundamentally different than edge providers in their function as common carrier telecommunication service providers.[33] Further, while edge providers have significant capability to track browsing habits, ISPs are privileged to even more sensitive customer information, including every aspect of an individual's browsing habits and communications on the Internet.[34] ISPs see 100% of a user's unencrypted Internet traffic,[35] which is significant in light of the typical Internet usage of a consumer and the overall pervasive nature of the Internet.[36]

Second, ISPs contested the regulations based upon the FTC's ability to better regulate this behavior through its monitoring of unfair or deceptive acts.[37] Despite the FTC's past regulation of this type of behavior, the FCC stands in a different position than the FTC and seeks to serve different goals. First, the FCC has a rulemaking ability that the FTC lacks, which allows it to create preventative measures through its regulations.[38] In contrast, the FTC can only step in to provide a remedy after a harm has been done.[39] Moreover, courts have largely blocked the

---

[32] Edge providers include entities that "provide any content, application or service over the Internet." 47 C.F.R. § 8.2(b).
[33] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. at 87277.
[34] *Id.*
[35] *Id.*
[36] As of January 2017, 9 out of 10 American adults use the Internet, and approximately 73% of adults use broadband to connect to the Internet. *Demographics of Internet and Home Broadband Usage in the United States*, PEW RESEARCH CENTER (JAN. 12, 2017), http://www.pewinternet.org/fact-sheet/internet-broadband/.
[37] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. at 87277.
[38] Kate Kaye, *FTC Could Regain ISP Privacy Oversight But it won't be Easy*, ADAGE (March 30, 2017), http://adage.com/article/privacy-and-regulation/ftc-regain-isp-privacy-oversight-easy/308487/.
[39] *Id.*

FTC when it attempts to enforce privacy rules on ISPs.[40] Additionally, the FTC has not specified its expectations regarding data protection and has largely encouraged self-regulation in the industry.[41] Unfortunately, the self-regulation model has not proved successful, and the vague standards set forth from the FTC have left this area in dire need of a clear and permanent solution.[42] As a result, the FCC, or its state counterparts, are in a better position than the FTC to evaluate, accommodate, and regulate the interests at stake with rapidly evolving technology. The FCC is in a unique position to regulate ISPs, as the FCC has the jurisdiction and regulatory authority for this type of technology which the FTC lacks.[43]

Although often unspoken by ISPs and their lobbyists, ISPs have a large profit motive driving their interest in keeping CPNI easily accessible. Due to the continuing integration of technologies and mergers of companies, ISPs are often no longer simply service providers. Rather, ISPs dabble in other communications services. For example, they often also function as content providers or advertisement service providers.[44] If ISPs were able to use and disclose CPNI, they could provide even more detailed targeted advertising that could create substantial profits. [45]

The ISPs profit motive stands at odds with the consumer privacy interests and expectations. Just as ISPs cannot be regulated as edge providers due to their inherent differences, the consumer expectations with regards to both vary as well.[46] When consumers use websites such as Facebook or Google, they expect that their information will be collected for

---

[40] Ernesto Falcon & Karen Gullo, *Selling Out Consumers*, U.S. NEWS (March 31, 2017 6:00 AM), https://www.usnews.com/opinion/articles/2017-03-31/congress-vote-to-repeal-fcc-broadband-privacy-rules-sells-out-consumers.
[41] Gaus, *supra* note 10, at 735.
[42] *Id.*
[43] 47 U.S.C.A § 151 (Westlaw through P.L. 115-68).
[44] *See infra* note 86.
[45] *See* Jeff Dunn, *supra* note 30. For example, Verizon is developing a live-TV streaming service. *Id.* If Verizon could use CPNI to provide significantly personalized advertisements, there becomes "a bigger premium for Verizon's ad space." *Id.*
[46] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 87274-01, 87277 (Dec. 2, 2016) (to be codified at 47 C.F.R. pt. 64).

targeted advertisements.[47] Consumers anticipate providing information in return for free content.[48] Therefore, consumer expectation of privacy with edge providers generating free content is minimal.[49] In contrast, ISP subscribers pay for their service in advance and reasonably expect that personal information transmitted as a result of the service will not be used by the ISPs to make a profit.[50] Further, consumers have reason for concern when CPNI can easily be used and disclosed by ISPs. As soon as CPNI can be bought or sold, the chances of hacking and breaches increases.[51] Given the recent severe data breaches,[52] consumers likely have a viable concern about how their personal information is used and maintained by third parties.[53]

Yet, despite the overall increase in consumer worry about how companies handle their private information, it is important to note that all consumers have different expectations and concerns. While some consumers may desire to keep information private, others may have little reservation about allowing ISPs to use and disclose their information for advertisement purposes. For example, if ISPs provided promotions and lower prices for consumers who opt-in to data collection, some consumers may find that trade-off valuable.[54] Given the various needs and desires of consumers, it is crucial that any regulation or legislation regarding ISP use of CPNI should focus on consumer choice while balancing the competing interests at stake.

---

[47] *Id.*
[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] Falcon, *supra* note 40.
[52] *See* Seth Fiegerman, *The biggest data breaches ever*, CNN (September 7, 2017, 7:37 AM), http://money.cnn.com/2017/09/07/technology/business/biggest-breaches-ever/index.html.
[53] For example, the Pew Research Center recently found that 91% of adults surveyed were concerned about their loss of privacy to third party companies. *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RESEARCH CENTER (Nov. 12, 2014), http://www.pewinternet.org/ files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf.
[54] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 87274-01, 87275 (Dec. 2, 2016) (to be codified at 47 C.F.R. pt. 64). Specifically, the FCC noted that its regulations were not intended as a total prohibition on use of CPNI. *Id.* Rather, the regulations were intended "to protect consumer choice" while also providing flexibility for ISPs. *Id.*

C. Current Proposed State Legislation

Following the repeal of the FCC privacy regulations in April 2017, various state legislatures began to take action, with several states proposing legislation attempting to preserve the FCC regulatory provisions at the state level.[55] Almost all states with pending legislation have identical substantive goals, which is to provide consumer choice regarding use of their individual information.[56] However, the states have taken unique approaches to accomplishing that goal. Specifically, the pending legislation in Vermont, New Jersey, and California highlight three possible approaches to solving this problem on the state level. While Vermont's proposed bill left all rulemaking to a state agency, the proposed bill in California provided a comprehensive and detailed statutory solution. In between these two approaches, New Jersey's proposed bill set forth basic policy and requirements while leaving other specifics to a regulatory agency.

i. Vermont

In April 2017, a bill was introduced in the Vermont Senate with the intent to codify the substance of the former FCC privacy regulations.[57] Vermont's proposed legislation was very general and deferred creation of any rules to the state's Public Service Board.[58] Specifically, the Vermont Senate sought to empower the Public Service Board to promulgate regulations that would be "modeled after, and not more or less restrictive than, the Federal Communications

---

[55] *See* NATIONAL CONFERENCE OF STATE LEGISLATURES, *Privacy Legislation Related to Internet Service Providers*, (August 4, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-internet-service-providers.aspx. As of August 2017, 21 states as well as the District of Columbia introduced legislation specifically targeting protection of consumer privacy with ISPs. *Id.* This does not include legislation that focuses generally upon digital privacy. *Id.*

[56] *See, e.g.*, H.R. 230, 30th Legis., First Sess. (Ala. 2017) (proposing required disclosures by ISPs and the use of CPNI as a violation of the Alaska Unfair Trade Practices and Consumer Protection Act); H.R. 2423, 87th Legis., Reg. Sess. (Kan. 2017) (providing that no state ISP may collect or sell customer information without written consent).

[57] S. 147, 2017 Leg. Sess. (Vt. 2017).

[58] *Id.*

Commission's 2016 Privacy order."[59] The only other requirements specified in the bill were that the rules include disclosure requirements, opt-in and opt-out procedures, and requirements for data security and breach.[60] Through this proposed bill, the Vermont Senate chose to take a simple approach to ensuring these privacy protections within the state by leaving the rule-making function to the state's proper regulatory agency and providing specific intent through its reference to the FCC standards.[61]

ii. New Jersey

In May 2017, a bill intended to protect personally identifiable broadband subscriber information was introduced in the New Jersey General Assembly.[62] New Jersey took a similar approach to the Vermont Senate, but provided a little more detail in its legislation. The bill provided definitions for key terms such as ISP and personally identifiable information.[63] In providing these definitions, the bill was also able to limit the scope of the bill to ensure that the ISPs regulated under the provision would not be ones that were under the jurisdiction of the FCC.[64]

The bill also specifically set forth general mandates that personally identifiable information be kept confidential unless express consent is given, and that proper notice of the statutory requirements be given to each subscriber.[65] After setting forth these basic guidelines, the General Assembly empowered the Director of the Division of Consumer Affairs to promulgate the regulations needed to carry out the provisions of the bill.[66]

---

[59] *Id.*
[60] *Id.*
[61] *Id.*
[62] Gen. Assemb. B. 4819, 217th Gen. Assemb., Gen. Sess. (N.J. 2017).
[63] *Id.*
[64] *Id.* Specifically, the New Jersey bill defined Internet service providers to be businesses qualified to do business in New Jersey that are able to connect subscribers "by wireline or radio frequency to the internet through equipment that is located in this State." *Id.*
[65] *Id.*
[66] *Id.*

iii. California

California's proposed legislation took the most detailed approach in comparison to Vermont and New Jersey. Proposed in February 2017 in the California General Assembly, the bill provides comprehensive definitions and provisions.[67] The expansive definitional section distinguishes between customer network information and customer proprietary network information, between personally identifiable information and sensitive customer information.[68] The bill also sets forth requirements for opt-in and opt-out approval and prohibits discrimination against consumers who do not opt-in or opt-out.[69] Further, the bill specifies that its provisions are only applicable to broadband internet providers operating within the state.[70] Unlike the bills in Vermont or New Jersey, this bill provides its source of authority for such an action, citing to the Communications Act, the Tenth Amendment to the United States Constitution, and the California Constitution.[71]

D. Problem Summary

ISPs hold a wealth of information about their consumers, from personal data to browsing history.[72] Given the increasing presence of the Internet and the profit-driven business model of ISPs, there is the need for a statutory or regulatory solution to balance the interests of consumers and ISPs.[73] The FCC attempted to provide that solution when it used its common carrier regulatory power to create rules allowing consumers to have greater choice in how their information is used and disclosed by ISPs.[74] However, under the current executive branch, these regulations are no longer in effect.[75] Further, because the Republican-majority Congress was the

[67] Assemb. B. 375, 2017 Gen. Assemb., Reg. Sess. (Ca. 2017).
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] *See supra* note 32.
[73] *See supra* note 45 and accompanying text.
[74] *See supra* note 24.
[75] *See supra* note 29.

first to initiate this de-regulation, it is unlikely that a statutory solution on the federal level will be forthcoming.[76] As a result, states have taken it upon themselves to propose statutory solutions to codify the substantive provisions of the defunct FCC regulations.[77] The various proposed state bills provide a template for how to draft a statute properly exercising state authority to protect consumer and ISP interests.[78]

II. Solution

In order to provide consumer choice and protection for personal information within the state, the Pennsylvania legislature should enact a comprehensive statutory solution. A close analysis of the proposed state statutes discussed above indicate some issues that arise in drafting a statute of this nature on the state level. An effective statute in Pennsylvania will combat those issues by grounding its source of authority, balancing competing interests, and blending statutory mandate with regulatory authority.

A. Authority for the Statute

First and foremost, a statutory solution in Pennsylvania should specify its source of authority to create these provisions. Given the broad powers and reach of the FCC, it is crucial that state-centered legislation does not regulate outside of its proscribed jurisdiction. In order to establish the Pennsylvania legislature's authority on this matter, it should rely upon provisions of the Communications Act, the United States Constitution, and the Pennsylvania Constitution. All three of these sources of power give Pennsylvania the authority to act. The Communications Act specifically provides that it does not give the FCC jurisdiction for "charges, classifications, practices, services, facilities, or regulations for or in connection with intrastate communication service by wire or radio of any carrier."[79] This provision has already allowed for the creation of the Pennsylvania Utility Commission ("PUC"), which has the authority to regulate intrastate

[76] *See supra* note 30.
[77] *See supra* note 55.
[78] *See supra* notes 56-66 and accompanying text.
[79] 47 U.S.C. § 152(b) (Westlaw through P.L. 115-68).

telecommunications providers in Pennsylvania.[80] This broad authority is further supported by the Tenth Amendment to the United States Constitution, which reserves to the states any powers not given to the federal government nor prohibited to the states.[81] Further, given the repeal of the regulations that regulated in this area, there is no federal law preempting this type of legislation.[82]

Apart from these federal grants of authority, the Pennsylvania Constitution itself offers a basis upon which the Pennsylvania legislature can rely. Article I Section 8 of the Pennsylvania Constitution provides protection of persons in their "houses, papers, and possessions from unreasonable searches and seizures."[83] The Pennsylvania Supreme Court has long found that this provision of the Pennsylvania Constitution provides a broad right to individual privacy that is more encompassing than its Fourth Amendment counterpart in the federal constitution.[84] As such, Article I Section 8 is considered to "embody a strong notion of privacy, carefully safeguarded in this Commonwealth."[85] Given this interest in individual privacy rooted in state law, Pennsylvania courts have analyzed violations of the right to be left alone by largely depending upon the nature of the information.[86] Due to this strong state history favoring individual privacy rights based on sensitivity of information, Pennsylvania is in a unique position to take up the issue of protecting internet subscriber CPNI through legislation.

A statute in Pennsylvania should provide for this statutory authority both through a specific section and carefully crafted definitions. First and foremost, a statute should set forth

---

[80] *See generally* 66 Pa. C.S.A. § 101 (Westlaw through Reg. Sess. Acts 1-41) (establishing the PUC and excluding interstate communications from its jurisdiction).
[81] U.S. CONST. amend. X.
[82] *See supra* note 30.
[83] PA. CONST. art. I, § 8.
[84] *See also* Commonwealth v. Murray, 223 A.2d 102, 109-1o (Pa. 1966) (finding Article 1 Section 8 to be "dedicated to the right to be let alone" as part of the "inherent and indefeasible rights" protected by the Pennsylvania Constitution).
[85] Commonwealth v. Edmunds, 586 A.2d 887, 897 (Pa. 1991).
[86] Seth F. Kreimer, *The Right to Privacy in the Pennsylvania Constitution*, 3 WIDENER J. PUB. L. 77, 96 (1993).

where the Pennsylvania legislature derives its authority to regulate the behavior of ISPs through federal grants of authority and its independent state grounds. Aside from that, however, the definitions section must define ISPs and subscribers to ensure that the statute does not encompass regulation of interstate telecommunications carriers or other persons outside of the Commonwealth. For this purpose, ISPs should be carefully defined to include only the providers that are already under the authority of the PUC.[87] The definition should reference the public utilities already under the PUC's jurisdiction and further clarify that the affected ISPs are those using wireline or radio equipment in the state.[88] Through these definitions and a source of authority section, the Pennsylvania statute will clarify that it is regulating only an area where there is no existing federal preemption.

B. Balancing Competing Interests

Given the various interests at stake in this issue, proposed legislation should focus on balancing those interests to ensure that consumers and ISPs are both given the opportunity to thrive. When it comes to use and disclosure of CNPI, ISPs are motivated by profit potential.[89] While consumers and privacy advocates may not approve of that motive, ISPs should be given the opportunity to expand their businesses into advertisement services if they see fit.[90]

Standing in contrast to the ISPs are the consumers, who are often left without options or control over how their information is compiled and used. Under the current law, ISP collection of CPNI is governed solely by the service agreement between the ISP and the consumer.[91] Internet service agreements typically favor only the interests of the ISPs, leaving consumers to

---

[87] *See supra* note 78.
[88] *See* Gen. Assemb. B. 4819, 217th Gen. Assemb., Gen. Sess. (N.J. 2017).
[89] *See supra* note 30.
[90] *See generally* Verizon Selects, VERIZON, https://www.verizonwireless.com/support/verizon-selects-faqs/ (last visited Nov. 27, 2017). The Verizon Selects program is a typical example of the expansion of ISPs into advertising services through use of subscriber information.
[91] Justin S. Brown, *Broadband Privacy Within Network Neutrality: The FCC's Application & Expansion of the CPNI Rules*, 11 U. ST. THOMAS J. L. & PUB. POL'Y 45, 49 (2017).

either consent to the ISPs use of their information or forego the service entirely.[92] Given the necessity of the Internet in modern society and the lack of competition in the ISP market, consumers are often required to consent to these terms, as there is no meaningful choice or opportunity to bargain.[93] Notwithstanding the lack of control that consumers currently have over their own information at the hands of ISPs, it is also important to note that consumer privacy expectations will often vary. While some consumers may not want any personal information disclosed, others may not mind allowing ISPs to gather some personal information for advertising purposes.[94]

Because the consumer's information is at the center of the battle, any proposed legislation should put the power to decide into the consumer's hands.[95] This can be done by requiring opt-in and opt-out procedures, as this will restore consumers' ability to determine how their information is used and what the terms governing their service agreement will entail.[96] Further, such an approach is aligned with the Pennsylvania Utility Commission's mission statement, which provides that it seeks to "[balance] the needs of consumers and utilities . . . protect the public interest, . . . [and educate] consumers to make independent and informed utility choices."[97] The opt-out procedures should be with regards to a subscriber's personal information, whereas the opt-in procedures should be for consumer information that is less sensitive.

---

[92] *Id.*
[93] *Id.*
[94] *See* Privacy and Information Sharing: Scenarios, PEW RESEARCH CENTER (Jan. 14, 2016), http://www.pewinternet.org/interactives/privacy-scenarios/. Specifically, the Pew Research Center found that consumer expectations of privacy vary widely depending on circumstances. *Id.*
[95] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 87274-01, 87275 (Dec. 2, 2016) (to be codified at 47 C.F.R. pt. 64).
[96] *See* Gaus, *supra* note 10, at 741.
[97] *About the PUC*, PENNSYLVANIA UTILITY COMMISSION, http://www.puc.state.pa.us/about_puc.aspx (last visited Nov. 27, 2017).

This sensitivity-based framework in combination with anti-discrimination provisions will continue to serve the purpose of balancing interests. By prohibiting discrimination on the basis of exercising the opt-out feature, the statute leaves open the possibility for ISPs to provide discounts to customers who do use opt-in features.[98] This allows ISPs to continue to expand their business models and profits while still ultimately leaving the decision with the consumer. Further, opt-in and opt-out procedures based on the sensitivity of the information ensure customer choice.[99] Opt-out procedures should be required for disclosure and use of CPNI, whereas opt-in procedures should be used for any information that does not fall within this category. Further, the definitions section of the statute should define CPNI in a manner understandable to the consumer by terming it personally identifiable information and defining it with examples of information with which consumers are familiar. This ensures that the statute is consumer-focused, as it avoids terminology that is technical in nature or familiar only to ISPs.

Disclosure notice requirements also serve the goal of a consumer-centered statute. ISPs should be required to provide notice to consumers when they contract for the service and whenever the privacy policy changes.[100] These notices should be conspicuous and written in language understandable to the average consumer, detailing the consumer's rights under the statute, what constitutes personally identifiable information, and circumstances of use and disclosure of the information.[101] This requirement will put the burden on the ISP to ensure that the consumers not only have the choice, but have the information available to make the informed choice regarding how their information is used.

---

[98] *See supra* note 91.
[99] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. at 87275.
[100] *Id.*
[101] *See* 47 C.F.R. § 64.2003 (2017) (explaining the FCC's promulgated disclosure requirements to include similar elements of conspicuousness and comprehensible language).

C. Blending Statutory Mandate with Regulatory Authority

In addition to a focus on balancing consumer interests, the statute must detail whether it will rely solely upon regulatory rulemaking authority or if it will take a hybrid approach. Although regulatory agencies are in a good position to quickly adapt rules for changing circumstances, this can also mean that regulations are often in flux and lack the concrete longevity of a statute.[102] Additionally, broad policy mandates, such as the one in the proposed Vermont legislation, may result in agency misinterpretation of congressional intent.[103] On the other hand, legislation that does not delegate to a regulatory authority at all, like the proposed California legislation, lacks flexibility for agencies to respond to evolving business practices and technology.

While there are benefits to leaving statutory detail and enforcement solely to the proper regulatory agency, the best solution for Pennsylvania would be to provide a detailed statutory mandate and delegate to an agency certain specific enforcement provisions. Pennsylvania should take an approach similar to New Jersey and enact legislation that details what information is protected, who is protected, and the procedures for disclosure and opting in or out.[104] However, it should then delegate to the PUC to enforce the provisions by promulgating rules. By delegating this authority, the legislature can allow the PUC to determine and alter the specifics regarding violations of the statutory provisions and managing consumer complaints.[105] The PUC already has under its regulatory authority telecommunications providers that own or

---

[102] *See supra* note 2.
[103] *See* Daniel J. Gifford, *The Emerging Outlines of a Revised Chevron Doctrine: Congressional Intent, Judicial Judgment, and Administrative Autonomy*, 59 ADMIN. L. REV. 783, 797 (2007) (discussing the shift to deference to regulatory actions carrying out broad congressional policy mandates).
[104] *See supra* note 62.
[105] Specifically, the PUC should create procedures for consumers to report suspected violations of their rights. However, the PUC should not be the only source of remedy for consumers. Rather, the statute should also allow consumers to bring a private cause of action when a breach of the statute results in harm.

operate equipment in the state for conveying communications through wire or radio, so it will be able to efficiently carry out this regulatory function.[106]

Under this statutory scheme, it will be the responsibility of the PUC to respond to changes in the market through its provisions enforcing the statute. The PUC will determine what constitutes a violation and what financial penalties should be assessed for ISPs. Because these determinations should be detailed and require consideration of interests and operations of ISPs and consumers, the PUC is in a better position to handle this enforcement than the legislature could. Additionally, the PUC can establish grievance procedures for consumers who believe their rights under the statute have been violated by an ISP. Although the PUC should establish grievance procedures, the statute should also provide consumers with the right to institute a private cause of action against ISPs when their rights are violated in a way that results in damages to the consumer.

III. Conclusion

Broadband internet usage continues to rise in the United States, and consumers continue to have little bargaining power when it comes to choosing the terms of their service. Although the FCC attempted to regulate this area to provide for consumer choice regarding how their personal data was used, these regulations are no longer in effect. Given this gap in the regulatory and statutory framework, Pennsylvania has the ability to enact a statute regulating conduct of ISPs in the state to ensure that consumer data is not used or disclosed without consent.

[106] 66 Pa. C.S.A. § 102 (Westlaw through 2017 Reg. Sess. Acts 1-41). Additionally, the PUC has recently been entrusted with promulgating regulations to carry out the statutory mandate to increase access to Broadband Internet across the commonwealth. *See* 66 Pa. C.S.A. § 3011 (Westlaw through 2017 Reg. Sess. Acts 1-41).

Appendix A
Original Statutes Used

Cited Sources:
Gen. Assemb. B. 4819. 217th Gen. Assemb., Gen. Sess. (N.J. 2017).
Assemb. B. 375, 2017 Gen. Assemb., Reg. Sess. (Ca. 2017).
47 C.F.R., Part 64, Subpart U.

Source of authority

1. California adopts this chapter pursuant to all inherent state authority under the Tenth Amendment of the United States Constitution and all relevant authority granted and reserved to the states by Title 47 of the United States Code, including the authority to impose requirements necessary to protect public safety and welfare, safeguard the rights of consumers, manage public rights-of-way, and regulate franchises. California further adopts this law pursuant to the inalienable right of privacy granted under the authority of Article I, Section 1 of the California Constitution.

Section 22556 of Assemb. B. 375, 2017 Gen. Assemb., Reg. Sess. (Ca. 2017).

Definitions

1. "Internet service provider" means a person, business, or organization qualified to do business in this State that provides individuals, businesses, or other entities with the ability to connect by wireline or radio frequency to the Internet through equipment that is located in this State. **Section 1 of Gen. Assemb. B. 4819. 217th Gen. Assemb., Gen. Sess. (N.J. 2017).**
    a. (2) "Broadband Internet access service" does not include a premises operator, including a coffee shop, bookstore, airline, private end-user network, or other business that acquires BIAS from a BIAS provider to enable patrons to access the Internet from its respective establishment. **Section 22551(2) of Assemb. B. 375, 2017 Gen. Assemb., Reg. Sess. (Ca. 2017).**
2. "Subscriber" means a residential or business subscriber located in this State that subscribes with an Internet service provider to receive access to the Internet on equipment located in the State. **Section 1 of Gen. Assemb. B. 4819. 217th Gen. Assemb., Gen. Sess. (N.J. 2017).**
3. Personally Identifiable information: "Personally identifiable information" means any information that personally identifies, describes, or is able to be associated with a subscriber or users of a subscriber's account, including, but not limited to:
    a. name, address, precise geolocation, social security number, or telephone number;
    b. requests for specific materials or services from an Internet service provider;
    c. online service use history;
    d. Internet websites visited during use of a subscriber's account; or
    e. the contents of a subscriber's communications or data-storage devices. **Section 1 of Gen. Assemb. B. 4819. 217th Gen. Assemb., Gen. Sess. (N.J. 2017).**
4. Opt-out approval: means a method for obtaining customer consent to use, disclose, or permit access to the customer's proprietary information. Under this approval method, a customer is deemed to have consented to the use or disclosure of, or access to, the customer's proprietary information if the customer has failed to object to that use, disclosure, or access after the customer is provided appropriate notification of the communications BIAS provider's request for consent, consistent with the requirements of this chapter. **Section 22551 (2)(j) of Assemb. B. 375, 2017 Gen. Assemb., Reg. Sess. (Ca. 2017).**

5. Opt-in approval: means a method for obtaining customer consent to use, disclose, or permit access to the customer's proprietary information. This approval method requires that the communications BIAS provider obtain from the customer affirmative, express consent allowing the requested usage, disclosure, or access to the customer proprietary information after the customer is provided appropriate notification of the BIAS provider's request, consistent with the requirements of this chapter. **Section 22551(2)(i) of Assemb. B. 375, 2017 Gen. Assemb., Reg. Sess. (Ca. 2017).**

Disclosure Requirements – 47 C.F.R. 64.2003.

1. (a) A telecommunications carrier must notify its customers of its privacy policies. Such notice must be clear and conspicuous, and in language that is comprehensible and not misleading.
2. (b) Contents. A telecommunications carrier's notice of its privacy policies under paragraph (a) must:
    a. (1) Specify and describe the types of customer proprietary information that the telecommunications carrier collects by virtue of its provision of telecommunications service and how it uses that information;
    b. (2) Specify and describe under what circumstances the telecommunications carrier discloses or permits access to each type of customer proprietary information that it collects;
    c. (3) Specify and describe the categories of entities to which the carrier discloses or permits access to customer proprietary information and the purposes for which the customer proprietary information will be used by each category of entities;
    d. (4) Specify and describe customers' opt-in approval and/or opt-out approval rights with respect to their customer proprietary information, including:
        i. (i) That a customer's denial or withdrawal of approval to use, disclose, or permit access to customer proprietary information will not affect the provision of any telecommunications services of which he or she is a customer; and
        ii. (ii) That any grant, denial, or withdrawal of approval for the use, disclosure, or permission of access to the customer proprietary information is valid until the customer affirmatively revokes such grant, denial, or withdrawal, and inform the customer of his or her right to deny or withdraw access to such proprietary information at any time.
    e. (5) Provide access to a mechanism for customers to grant, deny, or withdraw approval for the telecommunications carrier to use, disclose, or provide access to customer proprietary information as required by § 64.2004;
    f. (6) Be completely translated into a language other than English if the telecommunications carrier transacts business with the customer in that language.

Use of Personally Identifiable Information

1. (b) Opt-out approval required. Except as otherwise provided in this section, a telecommunications carrier must obtain opt-out approval from a customer to use, disclose, or permit access to any of the customer's non-sensitive customer proprietary information. If it so chooses, a telecommunications carrier may instead obtain opt-in approval from a customer to use, disclose, or permit access to any of the customer's non-sensitive customer proprietary information.
2. (c) Opt-in approval required. Except as otherwise provided in this section, a telecommunications carrier must obtain opt-in approval from a customer to:

a. (1) Use, disclose, or permit access to any of the customer's sensitive customer proprietary information;

47 C.F.R. 64.2004.

3. (d) Notice and solicitation required.
    a. (1) Except as described in paragraph (a) of this section, a telecommunications carrier must at a minimum solicit customer approval pursuant to paragraph (b) and/or (c), as applicable, at the point of sale and when making one or more material changes to privacy policies. Such solicitation may be part of, or the same communication as, a notice required by § 64.2003.
    b. (2) A telecommunications carrier's solicitation of customer approval must be clear and conspicuous, and in language that is comprehensible and not misleading. Such solicitation must disclose:
        i. (i) The types of customer proprietary information for which the carrier is seeking customer approval to use, disclose, or permit access to;
        ii. (ii) The purposes for which such customer proprietary information will be used;
        iii. (iii) The categories of entities to which the carrier intends to disclose or permit access to such customer proprietary information; and
        iv. (iv) A means to easily access the notice required by § 64.2003(a) and a means to access the mechanism required by paragraph (e) of this section.
    c. (3) A telecommunications carrier's solicitation of customer approval must be completely translated into a language other than English if the telecommunications carrier transacts business with the customer in that language.

47 C.F.R. 64.2004.

4. "..if the customer has failed to object to that use, disclosure, or access after the customer is provided appropriate notification of the communications BIAS provider's request for consent, consistent with the requirements of this chapter." **Section (2)(j) of Assemb. B. 375, 2017 Gen. Assemb., Reg. Sess. (Ca. 2017).**
5. Opt out approval is not required for:
    a. (2) A BIAS provider may use, disclose, or permit access to customer proprietary information without customer approval for any of the following purposes:
        i. (A) In its provision of the communications BIAS service from which the information is derived, or in its provision of services necessary to, or used in, the provision of the service.
        ii. (B) To initiate, render, bill, and collect for communications service. BIAS.
        iii. (C) To protect the rights or property of the BIAS provider, or to protect users of the communications service BIAS and other BIAS providers from fraudulent, abusive, or unlawful use of the service.
        iv. (D) To provide any inbound marketing, referral, or administrative services to the customer for the duration of a realtime interaction, if the interaction was initiated by the customer. interaction.
        v. (E) To provide location information or nonsensitive customer proprietary information to any of the following:
            1. (i) A public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's request for emergency services.

2. (ii) The user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm.
3. (iii) Providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency.

vi. (F) To generate an aggregate customer information dataset using customer personal information, or using, disclosing, or permitting access to the aggregate customer information dataset it generated.

vii. (G) For any other lawful purpose if the BIAS provider ensures the customer proprietary information is not individually identifiable by doing all of the following:
1. (i) Determining that the information is not reasonably linkable to an individual or device.
2. (ii) Publicly committing to maintain and use the data in a non-individually identifiable fashion and to not attempt to reidentify the data.
3. (iii) Contractually prohibiting any entity to which it discloses or permits access to the de-identified data from attempting to re-identify the data

Section 22552(2) of Assemb. B. 375, 2017 Gen. Assemb., Reg. Sess. (Ca. 2017).

b. BIAS provider shall not do either of the following:
i. (a) Refuse to provide broadband Internet access service, BIAS, or in any way limit that service, to a customer who does not waive his or her privacy rights guaranteed by law or regulation, including this chapter.
ii. (b) Charge a customer a penalty, penalize a customer in any way, or offer a customer a discount or another benefit, as a direct or indirect consequence of a customer's decision to, or refusal to, waive his or her privacy rights guaranteed by law or regulation, including this chapter.

Section 22553 of Assemb. B. 375, 2017 Gen. Assemb., Reg. Sess. (Ca. 2017).

Enforcement

1. This portion was not adapted from an existing statute.

Appendix B
Proposed Statute Redlined

Source of authority[1]

1. ~~California~~ Pennsylvania adopts this ~~chapter~~ section pursuant to ~~all inherent state~~ its authority under:
    a. the Tenth Amendment of the United States Constitution;
    b. ~~and all~~ the relevant authority granted and reserved to the states by Title 47 of the United States Code, including the authority to impose requirements necessary to protect public safety and welfare, ~~safeguard the rights of consumers, manage public rights-of-way,~~ and regulate franchises; and
    c. ~~California further adopts this law pursuant to the inalienable right of privacy granted under the authority of~~ Article I, Section 8 of the ~~California~~ Pennsylvania Constitution, as it has been interpreted by the Pennsylvania Supreme Court.

Definitions[2]

6. "Internet service provider" ~~means~~ - ("ISP") a ~~person, business, or organization qualified to do business in this State~~ public utility as defined in 66 Pa. C.S. § 102 that provides ~~individuals, businesses, or other entities~~ subscribers with the ability to connect ~~by wireline or radio frequency~~ to the Internet through wireline or radio equipment ~~that is~~ located in this State.
    a. ~~(2) "Broadband Internet access service"~~ It does not include a ~~premises operator, including a coffee shop, bookstore, airline, private end-user network, or other business that acquires BIAS from a BIAS provider~~ businesses or institutions that enable patrons to access the Internet from its ~~respective~~ establishment.
7. "Subscriber" ~~means~~ – a ~~residential or business subscriber located in this State that~~ person subscribed ~~with~~ to an Internet service provider as defined in this ~~section to receive access to the Internet on equipment located in the State~~ for the purpose of connecting to the Internet.
8. Personally Identifiable information: ~~"Personally identifiable information" means any~~ – information that personally identifies, describes, or is able to be associated with a subscriber ~~or users of~~ or the subscriber's account, including~~, but not limited to~~:
    a. name, address, ~~precise geo~~location, social security number, or telephone number;
    ~~b. requests for specific materials or services from an Internet service provider~~;
    ~~c. online service use history~~ subscriber requests for information from the ISP;
    d. Internet websites visited ~~during use of a~~ under the subscriber's account; or
    e. ~~the~~ contents of a ~~subscriber's~~ communications ~~or data-storage devices~~, including messages and content sent or received by the subscriber.
9. Opt-out approval~~: means~~ – ~~a method for obtaining~~ when an ISP obtains ~~customer~~ a subscriber's express consent for the ISP to use, disclose, or permit access to the ~~customer's~~ subscriber's ~~proprietary information~~ personally identifiable information. ~~Under this approval method, a customer is deemed to have consented to the use or disclosure of, or access to, the customer's proprietary information if the customer has failed to object to that use, disclosure, or access after the customer is provided appropriate notification of the communications BIAS provider's request for consent, consistent with the requirements of this chapter.~~

---

[1] *See supra* notes 76-86 and accompanying text.
[2] *See supra* notes 87-88 and accompanying text.

10. Opt-in approval~~: means~~ – ~~a method for obtaining~~ when an ISP obtains ~~customer~~ a subscriber's consent to use, disclose, or permit access to the ~~customer's~~ subscriber's ~~proprietary~~ information that is not personally identifiable as defined by this statute. ~~This approval method requires that the communications BIAS provider obtain from the customer affirmative, express consent allowing the requested usage, disclosure, or access to the customer proprietary information after the customer is provided appropriate notification of the BIAS provider's request, consistent with the requirements of this chapter.~~

Disclosure Requirements[3]

3. (a) ~~A telecommunications carrier must~~ An ISP shall notify ~~its customers~~ subscribers of its privacy ~~policies~~ policy. The notice shall be given at the time the contract for service begins and whenever the policy is altered. ~~Such~~ The notice ~~must~~ shall be clear ~~and~~, conspicuous, and in language that is comprehensible ~~and not misleading~~.
4. (b) Contents. ~~A telecommunications carrier's~~ The ~~notice of its privacy policies under paragraph (a)~~ must specify:
    a. ~~(1) Specify and describe~~ The types of ~~customer proprietary~~ subscriber information that the ~~telecommunications carrier~~ ISP collects by virtue of its provision of ~~telecommunications~~ service and how it ~~uses~~ discloses that information;
    b. ~~(2) Specify and describe under what~~ The circumstances under which the ~~telecommunications carrier~~ ISP discloses personally identifiable and non-personally identifiable information ~~or permits access to each type of customer proprietary information~~ that it collects;
    c. ~~(3) Specify and describe the categories of entities to which the carrier discloses or permits access to customer proprietary information and the purposes for which the customer proprietary information will be used by each category of entities~~;
    ~~d. (4) Specify and describe~~ The details of disclosures that do not require ~~customers' opt-in approval and/or~~ opt-out approval by the subscriber under section (4)(b) of this statute. ~~rights with respect to their customer proprietary information, including:~~
        ~~i. (i) That a customer's denial or withdrawal of approval to use, disclose, or permit access to customer proprietary information will not affect the provision of any telecommunications services of which he or she is a customer; and~~
        ii. ~~(ii) That any grant, denial, or withdrawal of approval for the use, disclosure, or permission of access to the customer proprietary information is valid until the customer affirmatively revokes such grant, denial, or withdrawal, and inform the customer of his or her right to deny or withdraw access to such proprietary information at any time.~~
    e. The subscriber's opt-in and opt-out approval rights as specified in this statute.
    f. (5) ~~Provide~~ Instructions regarding how to access to a simple mechanism ~~for customers to grant, deny, or withdraw approval for the telecommunications carrier to use, disclose, or provide access to customer proprietary information as required by § 64.2004~~ to exercise the opt-in and opt-out rights;
    ~~g. (6) Be completely translated into a language other than English if the telecommunications carrier transacts business with the customer in that language.~~

[3] *See supra* notes 89-101 and accompanying text.

Use of Personally Identifiable Information[4]

6. (b) Opt-out approval required. ~~Except as otherwise provided in this section, a telecommunications carrier must~~ An ISP shall obtain opt-out approval from a ~~customer~~ subscriber to use, disclose, or permit access to any of the ~~customer's~~ subscriber's ~~non-sensitive customer proprietary~~ personally identifiable information.
7. ~~If it so chooses, a telecommunications carrier may instead~~ An ISP shall obtain opt-in approval from a ~~customer~~ subscriber to use, disclose, or permit access to ~~any of the customer's non-sensitive customer proprietary~~ a subscriber's non-personally identifiable information.

~~8. (c) Opt-in approval required. Except as otherwise provided in this section, a telecommunications carrier must obtain opt-in approval from a customer to:~~

- ~~a. (1) Use, disclose, or permit access to any of the customer's sensitive customer proprietary information;~~

~~9. (d) Notice and solicitation required.~~

- ~~a. (1) Except as described in paragraph (a) of this section, a telecommunications carrier must at a minimum solicit customer approval pursuant to paragraph (b) and/or (c), as applicable, at the point of sale and when making one or more material changes to privacy policies. Such solicitation may be part of, or the same communication as, a notice required by § 64.2003.~~
- b. ~~(2) A telecommunications carrier's solicitation of customer approval must~~ The opt-out and opt-in notice shall be clear and conspicuous, and in language that is comprehensible ~~and not misleading. Such solicitation must disclose~~. It must specify:
  - i. The definition of personally identifiable information;
  - ii. The subscriber's rights and duties under this section, including the validity of the use and disclosure of personally identifiable information until the subscriber affirmatively exercises the opt-out rights by these procedures;
  - iii. That a subscriber's exercise of the opt-out or opt-in rights will not affect the subscriber's provision of service by the ISP;
  - iv. Instructions regarding how to access a simple mechanism to exercise the opt-in and opt-out right;
  - ~~v. (i) The types of customer proprietary information for which the carrier is seeking customer approval to use, disclose, or permit access to;~~
  - ~~vi. (ii) The purposes for which such customer proprietary information will be used;~~
  - ~~vii. (iii) The categories of entities to which the carrier intends to disclose or permit access to such customer proprietary information; and~~
  - viii. ~~(iv) A means to easily~~ instructions regarding how to access ~~the notice required by § 64.2003(a) and a means to access the~~ a simple mechanism to exercise the opt-in and opt-out right ~~required by paragraph (c) of this section~~.
- ~~c. (3) A telecommunications carrier's solicitation of customer approval must be completely translated into a language other than English if the telecommunications carrier transacts business with the customer in that language.~~

10. ~~"..if the customer has failed to object to~~ a subscriber is deemed to have consented to ~~that~~ the use~~,~~ and disclosure~~, or access~~ of personally identifiable information ~~after the~~

[4] *See supra* notes 89-101 and accompanying text.

~~customer~~ if the subscriber fails to object to the ISP's request for consent. ~~is provided appropriate notification of the communications BIAS provider's request for consent, consistent with the requirements of this chapter."~~

11. Opt out approval is not required for:
    a. ~~(2) A BIAS provider may~~ use~~, disclose, or permit access to customer proprietary information without customer approval~~ personally identifiable information for ~~any of~~ the following purposes:
        i. ~~(A) In its~~ provision ~~of the communications BIAS~~ of service ~~from which the information is derived, or in its provision of services necessary to, or used in, the provision of the service~~.
        ii. ~~(B) To initiate~~, rendering~~,~~ bills~~, and collect for communications service. BIAS.~~
        iii. ~~(C) To~~ protecting ~~the rights or property of the BIAS provider, or to protect users of the communications service BIAS and other BIAS providers~~ the ISP from fraudulent, abusive, or unlawful use of the service.
        ~~iv. (D) To provide any inbound marketing, referral, or administrative services to the customer for the duration of a realtime interaction, if the interaction was initiated by the customer. interaction.~~
        v. (E) To provide location information or ~~nonsensitive customer proprietary~~ non-personally identifiable information ~~to any of the following~~~~:~~
            1. ~~(i) A public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or~~ law enforcement ~~official, or hospital emergency or trauma care facility,~~ in order to respond to the ~~user's~~ subscriber's request for emergency services
            2. ~~(ii) The user's legal guardian or members of the user's immediate family of the user's location~~ or aid in an emergency situation ~~that~~ involv~~es~~ing the risk of death or serious physical harm.
            ~~3. (iii) Providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency.~~
        ~~vi. (F) To generate an aggregate customer information dataset using customer personal information, or using, disclosing, or permitting access to the aggregate customer information dataset it generated.~~
        ~~vii. (G) For any other lawful purpose if the BIAS provider ensures the customer proprietary information is not individually identifiable by doing all of the following:~~
            ~~1. (i) Determining that the information is not reasonably linkable to an individual or device.~~
            ~~2. (ii) Publicly committing to maintain and use the data in a non-individually identifiable fashion and to not attempt to reidentify the data.~~
            ~~3. (iii) Contractually prohibiting any entity to which it discloses or permits access to the de-identified data from attempting to re-identify the data~~
    ~~b. BIAS provider shall not do either of the following:~~
        ~~i. (a) Refuse to provide broadband Internet access service, BIAS, or in any way limit that service, to a customer who does not waive his or her privacy rights guaranteed by law or regulation, including this chapter.~~
        ii. ~~(b) Charge a customer a penalty, penalize a customer in any way, or offer a customer a discount or another~~ An ISP must provide the same service at

the same charge for subscribers who choose to opt-out. This includes not offering a subscriber a benefit~~, as a direct or indirect consequence of a customer's decision to, or refusal to, waive his or her privacy rights guaranteed by law or regulation, including this chapter~~ for failing to exercise the subscriber's opt-out rights.

1. This provision does not prevent ISPs from offering a benefit to subscribers who choose to exercise opt-in rights.

Enforcement[5]

1. This portion was not adapted from an existing statute.

[5] *See supra* notes 102-106 and accompanying text.

Appendix C
Proposed Statute Clean Copy

1. **Authority**
    a. Pennsylvania adopts this section pursuant to its authority under:
        i. The Tenth Amendment of the United States Constitution;
        ii. The relevant authority granted to the states by Title 47 of the United States Code, including the authority to safeguard the rights of consumers and regulate franchises; and
        iii. Article I, Section 8 of the Pennsylvania Constitution, as it has been interpreted by the Pennsylvania Supreme Court.
2. **Definitions**
    a. Internet Service Provider – ("ISP") a public utility as defined in 66 Pa. C.S. § 102 that provides subscribers with the ability to connect to the Internet through wireline or radio equipment located in this state. It does not include businesses or institutions that enable customers to access the Internet from their establishment.
    b. Subscriber – a person subscribed to an Internet service provider as defined in this section for the purpose of connecting to the Internet.
    c. Personally identifiable information – information that personally identifies, describes, or is able to be associated with a subscriber and the subscriber's account. It includes:
        i. Name, address, location, Social Security number, or telephone number;
        ii. Internet websites visited under the subscriber's account;
        iii. Subscriber requests for information from the ISP;
        iv. Content of communications, including messages and content sent or received by the subscriber.
    d. Opt-out approval – When an ISP obtains a subscriber's express consent for the ISP to use, disclose, or permit access to the subscriber's personally identifiable information.
    e. Opt-in approval – When an ISP obtains a subscriber's express consent for the ISP to use, disclose, or access the subscriber's information that is not considered personally identifiable as defined by this statute.
3. **Disclosure Requirements**
    a. An ISP shall notify subscribers through mail or electronic mail of its privacy policy. The notice shall be given at the time the contract for service begins and whenever the privacy policy is altered. The notice shall be clear, conspicuous, and in language that is comprehensible.
        i. The notice must specify:
            1. The types of subscriber information that the ISP collects by virtue of its provision of service and how it collects and discloses that information;
            2. The circumstances under which the ISP discloses personally identifiable information and non-personally identifiable information that it collects;
            3. The details of disclosures that do not require opt-out approval by the subscriber under (4)(b) of this statute;
            4. The subscriber's opt-in and opt-out approval rights as specified in this statute;
            5. Instructions regarding how to access a simple mechanism to exercise the opt-in and opt-out right.

4. Uses of personally identifiable information

a. Opt-out Procedures
    i. An ISP shall obtain opt-out approval from a subscriber to use, disclose, or permit access to the subscriber's personally identifiable information.
    ii. An ISP shall obtain opt-in approval from a subscriber to use, disclose, or permit access to a subscriber's non-personally identifiable information.
    iii. The opt-out and opt-in notice shall be clear, conspicuous, and comprehensible. It must specify:
        1. The definition of personally identifiable information;
        2. The subscriber's rights and duties under this section, including the validity of the use and disclosure of personally identifiable information until the subscriber affirmatively exercises the opt-out right by these procedures;
        3. A subscriber's exercise of the opt-out or opt-in rights will not affect the subscriber's provision of service by the ISP;
        4. Instructions regarding how to access a simple mechanism to exercise the opt-in and opt-out right;
    iv. A subscriber is deemed to have consented to the use and disclosure of the personally identifiable information if the subscriber fails to object to the ISP's request for consent.

b. Opt-out approval is not required for use of personally identifiable information for the following purposes:
    i. Provision of service;
    ii. Rendering bills;
    iii. Protecting the ISP from fraudulent, abusive, or unlawful use of the service;
    iv. Providing location information or non-personally identifiable information to law enforcement in order to respond to the subscriber's request for emergency services or aid in an emergency situation involving the risk of death or serious physical harm.

c. An ISP must provide the same service at the same charge for subscribers who choose to opt-out. This includes not offering a subscriber a benefit for failing to exercise the subscriber's opt-out rights.
    i. This provision does not prevent ISPs from offering a benefit to subscribers who choose to exercise opt-in rights.

5. Oversight of this statute

a. The Pennsylvania Utility Commission shall prescribe any rules and regulations it deems necessary for enforcement of these provisions, including:
    i. Standards for determining violations of these provisions;
    ii. Procedures for subscribers to report suspected violations of these provisions; and
    iii. A scale of fines levied for violations of these provisions.

b. When a subscriber's rights are violated under this statute and result in a breach of personal data that causes substantial financial harm to the subscriber, the subscriber may pursue a cause of action against the ISP.