Executive Summary

The California Attorney General’s Office strongly supports the Federal Communications Commission’s approach to protecting consumers by going beyond the current “notice and choice” regime, which too often takes the form of unnoticeable notices and illusory choices. The proposed privacy rule for Internet service providers (ISPs) is a reasonable regime that is particularly appropriate for a key player in the communications and online ecosystems. Our only concern is regarding the provision on the effect on state laws, which we think should be clarified on the point that a state law that provides greater consumer protection is not per se inconsistent with the rule. We also make some additional recommendations that we think would further strengthen the measure.

Our comments primarily address aspects of the proposed new Subpart GG: Privacy of BIAS Customer Information. On the issue of breach notification, we also address proposed revisions to Subpart U: Customer Proprietary Network Information.

In our comments, we highlight some key provisions and issues: the potential effect on state laws, the definition of covered customer information, collection limitation, improved transparency, data security, and data breach notification. In addition to the first point below, which we believe is essential, we make seven other recommendations for improving the proposed rule:

1. Clarify that state laws providing greater consumer privacy protection are not inconsistent, and thus not preempted, by the proposed privacy rule for that reason.
2. Consider adding a provision that provides consumers with choices on limiting ISPs’ collection of customer personal information.
3. Add a requirement that clarifies the format of the “notice soliciting customer approval.”
4. Add effective date and a description of how customers will be notified of material changes to the “notice of privacy policies.”
5. Add “access” to the unauthorized actions against which customer data must be secured.
6. Add a “good faith employee exception” to the breach notification requirement.
7. Change the timing for notifying customers of a data breach from the proposed 10 days after discovery to “in the most expedient time possible and without unreasonable delay.”

8. Correct an apparent oversight by restoring the subsection on the effect on state law to the proposed new section on breach notification for telecommunications carriers other than ISPs.

Comments

The Federal Communications Commission (Commission) has proposed a privacy rule for Broadband Internet Access Service providers outlining a reasonable privacy regime that is particularly appropriate for a key player in the communications and online ecosystem.

As gatekeepers to the Internet, Broadband Internet Access Service providers (commonly known as Internet service providers or ISPs) are positioned to have a broad and deep view into every aspect of their customers’ online activities. This view will expand even further as more things in our homes are connected to the Internet. Furthermore, unlike some online companies, ISPs are always able to identify data streams with specific customers, whose name, address, and other identifying information the ISPs possess.

Effect on State Laws

The proposed new Subpart GG includes a section on the effect of the entire subpart on state laws.\(^1\) The proposed provisions preempt only inconsistent state law and “only to the extent” that state and federal laws are inconsistent. This is an acknowledgement of the important role the states have played and continue to play in consumer protection and privacy protection in particular. The provision could be improved, however, by clarifying that it serves as a floor and not a ceiling for consumer protection. The Truth in Lending Act’s provision on the applicability of state laws is a good model.\(^2\)

Recommendation 1: We strongly recommend that the provision on the effect on state law be modified to clarify that a state law that provides greater consumer privacy protection is not inconsistent for that reason.

Definition of Covered Customer Information

Recognizing the broad scope of the customer information to which ISPs have access, the proposal appropriately clarifies the “customer proprietary information” (customer PI)\(^3\) to which it applies as including all the personally identifiable information that an ISP acquires through

\(^1\) Proposed 47 CFR § 64.7007. Solely for the purposes of this comment, the California Attorney General assumes that Congress has delegated to the Federal Communications Commission the authority to promulgate a rule concerning preemption.


\(^3\) Proposed 47 CFR § 64.7000(f) defines “customer proprietary information.”
Defaults and Choices

Today’s online economy is fueled by personal information, which contributes to innovation but also raises privacy concerns and harms that threaten innovation. The Fair Information Practice Principles (FIPPs) were formulated more than 40 years ago to address privacy concerns, by balancing the interests of individuals with the potential power of large databases in the hands of organizations. Unfortunately, the FIPPs have devolved in the U.S. to an ineffective “notice and choice” regime. This limited paradigm has become unworkable. While current state and federal laws require posting a privacy policy that discloses company data practices, privacy notices today are often unnoticeable and the choices offered to individuals illusory, frequently amounting to “take it or leave it” or “all or nothing.” As the Internet of Things becomes the Internet of Everything, and some online business models evolve to “collect first, (maybe) explain later,” and data are retained for possible future uses unknown at the time of collection, the shortcomings of the notice and choice regime are inescapable.

The Commission’s proposal for ISPs responds to this situation by providing privacy-respectful defaults and more effective user-centric privacy notices, which together enable meaningful customer choices.

The schema for customer choice in the proposed rule is based on alignment with customer expectations, with the greatest control granted for uses\(^5\) of customer PI that are not required for the provision of the broadband service and are thus likely to be unexpected by the customer. This “surprise minimization” approach has been recommended by the California Office of the Attorney General in other contexts as well.\(^6\)

Calibrating appropriate default settings is a key aspect of designing systems for privacy. If an online service begins using and sharing customer information immediately upon initiation, the privacy notice available online comes too late. The Commission’s proposal sets privacy-respectful defaults for three different data use scenarios, on a continuum of alignment with customer expectations.

In the first case, the default is to allow an ISP to use customer PI as necessary to provide the service, because such use is considered to be implied by the customer’s purchase of the service (NO OPTION). Including use for marketing of additional similar services by the customer’s provider in the same default category does not seem unreasonable.

\(^4\) Proposed 47 CFR § 64.7000(g) defines “customer proprietary network information” as having the same meaning as in the Communications Act of 1934, as amended, 47 U.S.C. § 222(h)(1).

\(^5\) In our comments, we use the term “use” to represent the phrase “use, disclosure, or permitting access” to customer PI that is used in the NPRM, at Proposed 47 CFR § 64.7002 and elsewhere.

In the second case, the default is to allow an ISP to use customer PI to market other communications-related services or to share it with affiliates so that they can market their communications-related services—unless the customer says no (OPT OUT).

And in the third case, at the other end of the scale, the default is not to allow customer PI to be used for any other purpose—unless the customer provides affirmative, express consent (OPT IN).\(^7\)

This approach is similar to the choice framework of the California Financial Information Privacy Act of 2003.\(^8\) In that law’s schema, the sharing of customer information is allowed for completing transactions (NO OPTION), sharing with another financial institution for jointly offering a financial product or with certain affiliates is allowed unless the customer objects (OPT OUT), and sharing with unaffiliated third parties requires prior written consent of the customer (OPT IN).

The FCC’s proposed approach is clearly feasible and has been similarly in effect in California for over a decade. Furthermore, compliance with the Commission’s proposed provisions on notice of privacy policies and notice soliciting customer approval rule may simplify compliance with other laws, such as California’s “Shine the Light Law.”\(^9\)

**Collection Limitation**

We note that the Commission’s proposal does *not* provide limitations or offer customer choices on ISPs’ collection of customer PI. The challenges of managing and securing personal information and the risk of privacy harm to individuals are significantly lessened when organizations collect and retain only customer information that is needed to provide the contracted-for service. Consumers *pay* their ISPs for their Internet connection; they do not and should not be expected to also “pay” with their personal information as well.

The customer choice approach that the proposal applies to the use of customer PI might also be applied to collection of the information. Thus, the collection of CPNI might be allowed as the default (NO OPTION), while the collection or retention of additional personally identifiable information would require affirmative express consent (OPT IN).

**Recommendation 2:** We recommend that the Commission consider providing consumers with choices about limiting ISPs’ collection of personally identifiable information.

**Improved Transparency**

Transparency about privacy practices is critical to empowering consumers to make informed decisions. Consumers can only exercise privacy choices when they are aware of them and understand their implications. As we have noted elsewhere, as a best practice, a company should

---

\(^7\) Proposed 47 CFR § 64.7002.

\(^8\) California Financial Code §§ 4050-4060.

\(^9\) California Civil Code § 1798.83; see subsection (c)(2), which relieves of the statute’s other obligations a business that discloses in its privacy policy and provides a notice of a customer’s right to prevent disclosure of personal information to third parties for direct marketing purposes, along with a cost-free means to exercise that right.
alert consumers to potentially unexpected data practices and the choices related to them, in addition to meeting its legal obligations to post a comprehensive privacy policy. The Commission’s proposal seeks to enable consumers to make meaningful choices by requiring enhanced additional notice of data uses not essential for providing the broadband Internet access service.

**Notice Soliciting Customer Approval**

The proposal requires ISPs that seek to use or disclose customer PII in a way that is not necessary for providing the basic service to notify the customer on the occasion of the first intention of such use. The notice is to include the details of the intended use, enabling the customer to make an informed decision. In addition to this content, presenting the notice in a required format that enhances readability and highlights the choices to be made would increase its effectiveness, particularly regarding the opt-out choice. Many opt-out choices are buried in privacy policies and notices, with the organization providing the choice having little or no incentive to make it conspicuous. One model for an effective opt-out notice is the Important Privacy Choices for Consumers notice in the California Financial Information Privacy Act, a copy of which is attached hereto.

**Recommendation 3:** We recommend that the notice soliciting customer approval include requirements for a format that would enhance its clarity and effectiveness.

In addition to timely notice, the proposal calls for the provider to offer a “simple, easy-to access method for a customer to provide or withdraw consent at any time.” This might be a dashboard of privacy controls, which should also include a link to the notice of privacy policies discussed below. These two provisions are vital to making the required customer choices actionable.

**Notice of Privacy Policies**

The proposal also requires a more comprehensive notice of privacy policies, which plays an important role in promoting data governance and accountability. Preparing such a notice, requires an organization to consider its data practices and then to ensure that its policies are complied with internally. In addition, a public representation is enforceable and can serve as a catalyst, stimulating changes in practice. Ideally, the required content of the notice will give customers vital details that allow for meaningful choice, such as the provider’s uses of specific types of customer PI collected and the purposes for which any entities with which the provider shares customer PI will use it. Such information would enable current and prospective customers

---


11 The proposal also exempts from the enhanced notice requirement uses of customer PI for billing, protecting the ISP’s rights, protecting against fraud and other abusive or unlawful acts, providing services initiated by the customer, in specified emergency situations, and as otherwise required by law. Proposed 47 CFR § 64.7001(a).

12 In addition to the form provided in the statute as a “safe harbor” for meeting the notice requirements, California Financial Code section 4053(d) sets out the criteria for an alternative form that may be used, including title and headers.

13 Proposed 47 CFR § 64.7002 (c) and (d).

14 Proposed 47 CFR § 64.7001.
to make comparisons among providers and to exercise meaningful privacy choices. The proposal also appropriately requires ISPs to provide advance notice to customers of material changes to the notice of privacy policies by email and other means. Alerting customers to material changes that could lead them to change their privacy choices is much more fair and effective than simply making the changes in the posted privacy policy and leaving it to customers to continually check the policy continually.

**Recommendation 4:** We recommend that the notice of privacy policies be required to include an effective date and a description of how customers will be notified of material changes to it.

**Data Security**

The proposal rightly emphasizes data security as part of the privacy regime.\(^{15}\) As daily reports of data breaches attest, it is vital that organizations be vigilant and proactive in ensuring reasonable security for the personal information entrusted to them. The proposed provision recognizes that security is not a one-time effort but an ongoing process of risk management.

Securing against unauthorized access is the most basic level of data protection. This is reflected in the proposed rule’s definition of “breach of security,” which includes access to, as well as use or disclosure of, customer proprietary information by a person “without authorization or exceeding authorization.”\(^{16}\) Yet the data security provision of the proposed rule omits “access” from the unauthorized actions against which an ISP must secure customer PI.

**Recommendation 5:** We recommend that “access” be inserted after “unauthorized” and before “uses or disclosures,” in proposed 47 CFR § 64.7005 (a).

**Data Breach Notification**

The proposal improves existing Commission regulations governing telecommunications carriers’ notification of affected individuals of a data breach, incorporating many of the provisions that states have added to their breach notification laws to respond to evolving threats. The proposal includes parallel breach notification provisions for ISPs in new subpart GG and for other telecommunications carriers in proposed changes to existing subpart U.\(^ {17}\) Such provisions include streamlining the law enforcement notification procedures, adding helpful content and method requirements to the customer notice, and adding a requirement to notify the Commission as the regulator.

At the outset, we support the proposed definition of “breach of security” for both ISPs and other telecommunications carriers, as it is similar to the definition in the California breach law.\(^ {18}\) The proposed definition makes the trigger for notification access to, use of, or disclosure of customer PI by an unauthorized person. This is similar to California’s trigger of acquisition by an unauthorized person. The California provision is based on the assumption that personal

---

\(^ {15}\) Proposed 47 CFR § 64.7005.

\(^ {16}\) Proposed 47 CFR § 64.7000(b).

\(^ {17}\) Proposed 47 CFR § 64.7006(a) and § 64.2011(a).

\(^ {18}\) Proposed 47 § 64.2003(b) and § 64.7000(b). Cf. California Civil Code § 1798.82(g).
information in the hands of an unauthorized person constitutes a risk of harm. Some state breach laws allow the breached entity to decide whether or not a specific breach creates a risk of harm. The weakness of such a provision lies in the difficulty in determining enough facts to enable an estimation of the likelihood of harm in many situations and in the breached organization’s general inclination to avoid notification.

We suggest one improvement to the provisions. The California breach law, like nearly all state breach laws, contains an exception to the notification requirement for the good faith acquisition of personal information by an employee or agent, provided that the information is not used or subject to further unauthorized disclosure. This provision accommodates situations where an employee inadvertently acquires information that he or she is not authorized to have. Notifying the data subjects in such situations would serve no purpose and could needlessly alarm them.

Recommendation 6: We recommend adding a “good faith employee exemption” provision to the definition of “breach of security” in both proposed 47 CFR § 64.7006(a) and § 64.2011(a).

There are additional lessons that can be drawn from a dozen years of experience with state breach laws. With respect to the timing of customer notification, the proposal extends the present requirement to notify customers within seven days of discovery to ten days. Based on four years of California data, breached entities notify affected individuals on an average of forty days, with a median notification time of thirty days. We believe that setting a specific time limit here is not in the best interests of consumers.

Both prompt notification and accurate information are critical to ensure that data breach notifications are helpful to consumers. The challenge is to find the right balance of speed and accuracy. California, like all but seven of the 47 states with breach laws, requires notification “in the most expedient time possible and without unreasonable delay.” This standard allows for achieving an appropriate balance. A specific deadline, while expressed as an outer bound, risks becoming the standard. And because the time it takes from discovery to notification is very fact-specific, a deadline of ten days would be too short in some cases, such as large breaches in which the logistics of conducting the notification can be daunting and the forensic investigation to determine which data and whose data was involved can demand more time. Allowing more time, say thirty or forty-five days, may be too long in many cases (and might be too short in others). Furthermore, what constitutes a reasonable time for notification today might be unreasonable tomorrow, as technological improvements allow for faster forensic analysis, cheaper and more effectively targeted notice, and an improved ability by companies to provide consumers with remedies promptly.

We also note that the proposed provision requires notification of the Commission no later than seven days after discovering a breach. This requirement provides an additional incentive to expedient notification of customers and enables the Commission to assess the reasonableness of any delay.

---

19 California Civil Code § 1798.82(g).


21 Five states provide an outer limit of 45 days, one allows up to 30 days, and one up to 90 days. See one of the compendia of state breach laws, those available online from Mintz Levin or Baker Hostetler.
Recommendation 7: We recommend that the breach notification provision proposed for both ISPs and for other telecommunications carriers be modified to provide for notifying customers in the most expedient time possible and without unreasonable delay, rather than within ten days, after discovery of the breach.

The existing breach notification section for telecommunications carriers includes a subsection providing that the section only supersedes state laws to the extent that a law is inconsistent with the section and then only to the extent of that inconsistency.\(^\text{22}\) In the proposed revision of this section, there is no language about its relation to state law. Given the Commission’s stated intention “to preempt state laws only to the extent that they are inconsistent with any rules adopted by the Commission,” we surmise that this omission is an oversight.\(^\text{23}\)

Recommendation 8: We recommend that the existing language on its effect on state laws be restored to § 64.2011, with the modification described in Recommendation 1 above.

\(^{22}\) Existing 47 CFR § 64.2011(f).

\(^{23}\) NPRM, paragraph 276.