FCC Releases Broadband Privacy Order with Major Implications for All Telecommunications Carriers

Alysa Z. Hutnik, Jennifer Rodden Wainwright

November 9, 2016

On October 27, 2016, the Federal Communications Commission (FCC or Commission) in a party-line (3-2) vote adopted a Report and Order (the Broadband Privacy Order or Order) that imposes a comprehensive set of privacy and data security regulations for providers of broadband Internet access service (BIAS) and replaces the existing privacy and data security rules for all other telecommunications service providers. The rules represent a significant departure from the Commission's existing privacy and data security framework for customer proprietary network information (CPNI), and as a result may require carriers to make considerable changes to their internal privacy and data security compliance practices, marketing operations, and business plans.

The rules will go into effect on a staggered timeline, beginning 30 days after they are published in the Federal Register. Small providers (i.e., those with 100,000 or fewer subscribers) will have an additional 12 months to come into compliance with some, but not all, of the new rules. Section IX includes an implementation timeline for your reference.

In this client advisory, we provide an overview of the Broadband Privacy Order and the new rules with respect to notice, choice, and data security, and offer key takeaways for clients as they operationalize the rules. The client advisory proceeds in the following sections:

XI. Key Takeaways and Conclusion

I. Background

The Broadband Privacy Order is a product of the 2015 Open Internet Order, which reclassified BIAS as a telecommunications service under Title II of the Communications Act of 1934, as amended (Communications Act or the Act), and imposed the Act's privacy provision – Section 222 – on BIAS providers. While the 2015 Open Internet Order imposed Section 222 on BIAS providers, the FCC declined to impose its voice-centric rules implementing those statutory provisions to broadband, opting instead for a separate rulemaking for broadband-specific privacy rules. On March 31, 2016, the Commission issued a notice of proposed rulemaking (NPRM) to establish specific privacy rules for BIAS providers, and asked whether it should "harmonize" those rules with its existing voice-centric rules for other telecommunications carriers. The Broadband Privacy Order adopts rules based on public input the Commission received in response to the NPRM from scores of interested parties, including the staff of the Federal Trade Commission (FTC).

Section 222 was added to the Telecommunications Act of 1996 to ensure the proper use of information necessary to facilitate the new competitive provider paradigm that replaced monopoly local phone service. As interpreted by the Commission, Section 222 imposes numerous privacy and data security requirements on telecommunications carriers and providers of interconnected Voice over Internet Protocol (VoIP) services.

- **General Standard.** Section 222(a) establishes a general duty "to protect the confidentiality of proprietary information of, and relating to, other telecommunications carriers, equipment manufacturers, and customers, including telecommunications carriers reselling telecommunications service provided by a telecommunications carrier."

- **Carrier Proprietary Information.** Section 222(b) requires a telecommunications carrier that "receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service [to] use such information only for such purpose, and . . . not for its own marketing efforts."

- **Customer Proprietary Network Information (CPNI).** Section 222(c) sets forth the requirements related to CPNI, which is defined as "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information [i.e., information published in a phone book]." Except as required by law or with the approval of the customer, a carrier that receives or obtains CPNI may "only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories." Section 222(c) also requires carriers to disclose CPNI, upon affirmative written request by the customer, to a designee of the customer. Moreover, Section 222(c) permits carriers to use, disclose, or permit access to aggregate customer information (so long as it provides such information to other carriers or persons on reasonable and nondiscriminatory terms).

- **Exceptions.** Section 222(d) includes a number of exceptions from the use, disclosure, and access restrictions above, including "(1) to initiate, render, bill, and collect for telecommunications services; (2) to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services; (3) to provide any inbound telemarketing, referral, or administrative services to the customer for the duration of the call, if such call was initiated by the customer and the customer approves of the use of such information to provide such service; and (4) to provide call location information concerning the user of a commercial mobile service or the user of an IP-enabled voice service [in the event of an emergency]."

Over the last twenty years, the FCC has adopted a complicated suite of rules implementing Section 222, including notice and consent requirements, safeguards against pretexters, annual certification requirements, and data security breach notification obligations. Recently, the Commission significantly increased its enforcement efforts against providers for alleged violations of Section 222 and the Commission's privacy rules. In addition, the Commission has used Section 201(b) of the Act, which prohibits "unjust and unreasonable" practices, to impose strong data security requirements on carriers. The Commission also has imposed significant privacy and data security requirements on carriers through consent decrees, creating a "common law of privacy" similar to the enforcement mechanisms that the FTC has employed under Section 5 of the FTC Act. Apart from its traditional telecommunications privacy rules under Section 222, the Commission also has authority over the privacy and data security practices of cable (Section 631) and satellite (Section 338(i)) providers.

II. Scope of the Broadband Privacy Order

In the Order, the Commission adopts a uniform suite of privacy and data security rules for all telecommunications carriers – including BIAS providers, traditional voice providers, and other providers of telecommunications service – and providers of interconnected VoIP services. The rules apply to customer proprietary information (customer PI), which includes both personally identifiable information (PII), CPNI, and the content of communications. The rules exclude de-identified information, provided carriers take steps to prevent the information from being re-identified.

The rules apply to all telecommunications carriers

The rules apply to all telecommunications carriers and providers of interconnected VoIP services. The Commission adopts a single definition of "telecommunications carrier" for Section 222 purposes – those providing telecommunications services subject to Title II including BIAS – in order to harmonize the privacy and data security rules for both voice and broadband telecommunications carriers. As with its existing privacy rules for voice providers, the Commission also applies its new privacy and data security regime to interconnected VoIP services.

The rules cover all customer proprietary information

The rules apply to customer PI, an umbrella term that includes nearly all information acquired in connection with the provision of telecommunications service. More specifically, customer PI includes three types of information:

- **Individually identifiable Customer Proprietary Network Information (CPNI)**has the statutory definition in Sec. 222 (h): "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship." For voice

providers, CPNI also includes information contained in subscriber bills. For BIAS providers, the statutory phrase "made available to the carrier by the customer solely by virtue of the carrier-customer relationship" is interpreted to mean any information that falls within a CPNI category that the BIAS provider collects in connection with providing the service, but not through independent means. Types of information considered CPNI in the BIAS context include broadband service plans; geo-location information; MAC addresses and other device identifiers; IP addresses and domain name information; traffic statistics; port information; application header; application usage; application payload; and customer premises equipment (CPE) and device information.

- **Personally identifiable information (PII)** is any information that is linked or reasonably linkable to an individual or device. Examples of PII include, but are not limited to, name, Social Security number, date of birth, mother's maiden name, government-issued identifiers, physical address, email address (or other online contact information), phone numbers, MAC addresses (or other unique device identifiers), IP addresses, and persistent online or unique advertising identifiers.
- **Content of communications** means any part of a communication that is highly suggestive of the substance, purpose, or meaning of a communication. Examples of content for BIAS providers are email contents, social media communications, search terms, website comments, shopping cart items, input on web-based forms, and consumer documents, photos, videos, books read, and movies watched.

The rules cover the customer PI of telecommunications carrier customers. The Commission defines "customers" as current and former subscribers as well as applicants for telecommunications service. Thus, a carrier's duty to protect a customer's information will extend beyond the period of the contractual relationship. The Commission notes that a carrier can limit the scope of this duty by minimizing data collection and destroying applicant and former customer information as soon as practicable, consistent with any other legal requirements.

The Order designates the subscriber to the telecommunications service as the party responsible for all privacy choices for a particular subscription, regardless of whether the particular account is shared between multiple users. However, if a provider normally treats each user differently and the subscriber allows those users to control their privacy and data security settings, the provider should give each user individualized privacy controls.

Consistent with the Commission's earlier ruling on mobile device CPNI, the Order clarifies that information that a BIAS provider causes to be collected or stored on a customer's device, including CPE, is CPNI.

The rules permit use and sharing of de-identified information, with safeguards

Carriers may rely on de-identification as a means to enable use and sharing of customer PI without obtaining customer consent. The Order adopts a three-part test, grounded in FTC guidance, to establish a baseline for deeming information as de-identified. Customer PI will be considered de-identified if the carrier:

1. determines the information is not *reasonably linkable* to an individual or device;
2. publicly commits to maintain and use the information in a non-individually identifiable manner and not attempt to re-identify the data; and

3. contractually forbids any entity that it gives access to the de-identified data from trying to re-identify the data.

The standard for assessing reasonableness will depend on how easy it is to re-identify the data, not how much it costs to initially de-identify it. The Commission emphasizes that it will not prohibit particular de-identification practices, but rather will analyze de-identification practices on a case-by-case basis.

III. New Customer Notice Requirements

The Order requires telecommunications carriers to provide clear privacy notices informing customers about the type of information they collect and to explain how and for what purposes carriers will use or share that information. Carriers must also notify customers about their rights to opt in or out of sharing customer PI.

The privacy notice must be provided to customers at the point of sale and made persistently available and accessible on a provider's website, app, and any functional equivalent. The notice must include the following information:

- the types of customer PI the carrier collects just by providing its services and how that information will be used;
- when a carrier discloses or allows access to each type of customer PI, the types of entities it shares that information with, and the purposes for which that customer PI will be used by each type of entity; and
- how consumers can exercise their privacy choices.

Telecommunications carriers must also provide an additional notice in the event of *material changes* to their privacy and data security practices. The Commission explains that a change to a privacy policy is considered material if a reasonable customer would find it important to his or her decisions about privacy. Notification of such a material change must be provided through a form of active communication agreed to by the customer, such as email, and must describe (1) the changes being made and (2) the customer's rights with respect to the material change as it relates to his or her customer PI. The Commission eliminates existing periodic notice requirements for voice CPNI from the rules.

All notices must be clear, conspicuous, and not misleading, and must be conveyed in a language other than English if the telecommunications carrier transacts business with the customer in that other language.

The Order also tasks the Commission's Consumer Advisory Committee with creating a standardized privacy notice that will serve as a "safe harbor" for those carriers that choose to adopt it. The proposed notice standard is to be developed no later than June 1, 2017.

IV. Customer Consent Framework

The Broadband Privacy Order adopts a modified three-tiered consent framework governing the collection, use, and sharing of customer PI, based on the sensitivity of the information at issue. This new framework replaces the existing entity-and-use-based framework for other telecommunications services and interconnected VoIP services. As explained below, the new framework requires opt-in consent for uses and sharing of sensitive customer PI, requires opt-out consent for uses and sharing

non-sensitive customer PI, and permits certain uses and sharing of customer PI for specific purposes enumerated in the statute without obtaining additional customer consent.

When opt-in consent is required

The new rules require express informed consent (opt-in approval) from customers for the use of sensitive customer PI. Specifically, the Order states that the following categories of information qualify as "sensitive customer PI":

- Precise geo-location information (excluding customer postal or billing address)
- Health information
- Financial information
- Children's information
- Social Security numbers
- Contents of communications
- Web browsing and application usage histories and their functional equivalents
- Call detail information (for voice providers)

The Order also requires BIAS and voice providers to obtain opt-in consent for material retroactive changes to the use of both sensitive and non-sensitive information.

When opt-out consent will suffice

The Order requires BIAS providers and other telecommunications carriers to obtain customer opt-out consent before using, disclosing, or allowing access to non-sensitive customer PI. The Commission defines opt-out approval as a means of obtaining customer consent based on a customer's failure to object to the carrier's request for consent.

The Order eliminates the existing 30-day waiting period before carriers may deem opt-out consent effective. Now, carriers must wait for an amount of time that would give a reasonable customer the opportunity to view the opt-out solicitation. The Order also eliminates the requirement for telecommunications carriers to refresh opt-out approval every two years.

Exceptions to customer approval requirements

The Commission recognizes certain exceptions to the requirements for customer consent for use and sharing of customer PI.

The Order permits use and sharing of non-sensitive customer PI without customer consent for the provision and marketing of services that are part of, necessary to, or used in the provision of telecommunications. This exception includes the provision and marketing of communications services commonly bundled with the subscriber's telecommunications service, CPE, and adjunct-to-basic services (such as caller ID and call forwarding for voice and DNS for BIAS). The exception also includes the provision of inside wiring and technical support, reasonable network management, and network enhancement and security research.

Moreover, pursuant to Section 222(d) of the Communications Act, carriers do not need to seek

approval to use or share customer PI to:

- initiate, render, bill, and collect for service;
- protect the rights and property of the carrier or protect their customers from unwanted abuses, including to protect against spam, malware, and other harmful traffic (e.g., robocalls);
- provide inbound services to customers (such as when a customer initiates contact with a carrier's customer service division); and
- provide certain customer PI in emergency situations.

The rules do not alter carrier obligations under existing laws and regulations affecting collection, use, or disclosure of communications, such as the Electronic Communications Privacy Act (ECPA), the Communications Assistance for Law Enforcement Act (CALEA), and the Cybersecurity and Information Sharing Act (CISA).

Requirements for soliciting opt-out and opt-in approval

The Order requires carriers to solicit customer approval for the use and sharing of customer PI at the point of sale (which may be in person, by phone, or electronic), and permits carriers to solicit approval at any time after the point of sale. Carriers making material changes to their privacy policies must solicit customer approval before implementing such changes.

Carriers' solicitations must "clearly and conspicuously" inform customers of:

- the types of customer PI they seek to use, disclose, or permit access to;
- how such information will be used or shared; and
- the types of entities with which such information will be shared.

Solicitations must be "comprehensible and not misleading," must be translated into a language other than English if the carrier transacts business with the customer in another language, and must provide a means to easily access (1) the carrier's privacy policy and (2) a mechanism which will enable the customer to adjust privacy settings (more on that below).

How customers may exercise privacy choices

Carriers must provide customers with access to a choice mechanism that is "simple, easy-to-use, clear and conspicuous, in language that is comprehensible and not misleading, and made available at no additional cost to the customer." This mechanism must be persistently accessible on or via the carrier's website, app (if the carrier provides one for purposes of account management), or the functional equivalents of either.

The Commission recommends, but does not require, a customer-facing dashboard for controlling privacy settings.

Out of concern for the compliance costs for small businesses, the Commission will allow carriers flexibility in implementing choice mechanisms. For example, if a carrier does not maintain a website, it could provide a 24-hour toll-free number for changing privacy settings.

The Commission does not establish a bright-line rule about how quickly carriers must give effect to a customer's grant, denial, or withdrawal of approval, but indicates that customer choices must be

implemented “promptly,” and that customer choices must remain in effect indefinitely absent revocation.

Importantly, the Order eliminates the specific periodic compliance recordkeeping and annual certification requirements that previously applied to voice providers.

V. Reasonable Data Security Standard

In the Order, the Commission requires telecommunications carriers to adopt reasonable data security practices. The reasonable data security standard requires that carriers “take reasonable measures to protect customer PI from unauthorized use, disclosure, or access.” The Commission finds that carriers’ data security practices should be oriented around principles of “confidentiality, integrity, and availability.” Confidentiality means protecting customer PI from unauthorized access and disclosure; integrity means protecting information from unauthorized modification or destruction; and availability means providing authorized users with access to information on an as-needed basis.

In assessing whether or not their security practices comply with the reasonable data security standard, carriers must take into account the following four factors:

1. The nature and scope of the carrier’s activities;
2. The sensitivity of the collected data;
3. The size of the carrier; and
4. Technical feasibility.

These factors will be assessed in light of the totality of the circumstances, and no single factor is independently outcome determinative.

Exemplary reasonable data security practices

In the Order, the Commission abandons its NPRM proposal to mandate specific minimum security standards in favor of a general reasonableness standard and recommended “exemplary practices.” Those practices include:

- **Engagement with industry best practices and risk management tools.** Carriers may consider adopting the NIST Cybersecurity Framework, examining FTC guidance, reviewing implementation guides for security requirements under existing sectoral privacy laws, and examining best practices recommended by the FCC’s Communications Security, Reliability, and Interoperability Council (CSRIC).
- **Strong accountability and oversight.** The Commission recommends that carriers develop comprehensive, written data security programs. Carriers may also consider hiring chief privacy and data security officers, conducting employee training on handling customer PI, and obtaining data security commitments from third parties as a condition of disclosure.
- **Robust customer authentication.** Carriers may consider stronger alternatives to customer authentication than customer-generated passwords or routine security questions. They may heighten authentication requirements before disclosing information that could cause serious harm to customers if improperly disclosed. Carriers could also give customers notice of attempted account changes, but should avoid inducing “notice fatigue.”

- **Other practices.** Carriers may benefit from implementing data minimization procedures spanning the entire data lifecycle (from collection to deletion/disposal), utilizing strong data encryption technologies, and appropriately sharing cyber threat information with law enforcement officials.

While the reasonable data security standard applies to both BIAS and other telecommunications services, the Commission clarified that the above exemplary practices "may be implemented differently depending on the services an entity provides."

VI. Data Breach Notification Requirements

The Broadband Privacy Order requires BIAS providers and other telecommunications providers to notify affected customers and certain government agencies of data breaches unless the provider reasonably determines that no harm to customers is likely to occur.

The Order defines a breach as "any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information." This definition includes unintentional data breaches and breaches involving a carrier's vendors and contractors.

Harm-based notification trigger

The Commission will require breach notification "unless the carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach." Under this rule, carriers have an obligation to take the necessary investigative steps to determine whether harm is reasonably likely. The Order defines "harm" broadly to include "financial, physical, and emotional harm." As a result, breach notification will be required in circumstances that could lead to reputational damage, personal embarrassment, or loss of control over the exposure of intimate personal details.

The rules also establish a rebuttable presumption that any breach involving sensitive customer PI poses a reasonable likelihood of customer harm and hence would require customer notification. The Order notes that the harm-based trigger applies even if the breached data had been encrypted.

Notification to the Commission and federal law enforcement

Under the Broadband Privacy Order, providers must notify the FCC of all breaches that meet the harm-based trigger, and, if a breach affects 5,000 or more customers, the provider must notify the FBI and Secret Service.

The breach notifications must occur within the following timeframe:

- **Breaches affecting 5,000 or more customers.** Carriers must notify the FCC, FBI, and Secret Service within 7 business days from when they reasonably determined a breach occurred, and at least 3 days before notifying customers.
- **Breaches affecting fewer than 5,000 customers.** Carriers must notify the FCC without unreasonable delay and within 30 calendar days from the reasonable determination that a breach occurred.

The Commission will create a centralized portal for reporting breaches to the FCC and federal law enforcement agencies, and will issue a public notice with details on how to access the portal once it

has been set up.

Customer notification requirements

Carriers must notify affected customers of reportable breaches within 30 calendar days following the carriers' reasonable determination that a breach occurred, unless the FBI or Secret Service requests a further delay. The FBI or Secret Service can direct a provider to delay notifying customers and the general public of a breach for as long as necessary to avoid interference with an ongoing criminal or national security investigation.

The Commission notes that carriers have a continuing obligation to supplement their breach notifications if they determine that a breach affects additional customers than those initially notified.

Data breach notifications to affected customers must contain the following information:

- the date, estimated date, or estimated date range of the breach;
- a description of the customer PI breached or reasonably believed to have been breached;
- information the customer can use to contact the carrier to inquire about the breach and the customer PI that the carrier maintains about that customer;
- information about how to contact the FCC and any pertinent state regulatory agencies; and
- if the breach creates a risk of financial harm, information about national credit-reporting agencies and steps customers can take to guard against identity theft, as well as any credit monitoring, credit reporting, credit freezes, or other consumer protections the carrier is offering affected customers.

Customer notifications must occur by means of written notification to the customer's address or email address, or by other electronic means of communications agreed to by the customer for such purposes. Former customers must be notified at their last known postal address determinable on the basis of commonly available sources.

Record retention and harmonization

Providers must keep records of the dates on which they determine that reportable breaches have occurred, the dates of customer notification, and written copies of all customer notifications for two years from the date a breach was reasonably determined to have occurred. This retention requirement does not extend to breaches that fall short of requiring notice to the FCC.

VII. Particular Practices that Raise Privacy Concerns

The Order addresses two practices that the Commission has deemed particularly concerning for consumer privacy: so-called "take-it-or-leave-it" offers, and programs that provide financial incentives to consumers in exchange for allowing providers to use, disclose and/or permit access to customer PI.

"Take-it-or-leave-it" offers

The Order prohibits BIAS providers from "conditioning the provision of broadband service on a customer surrendering his or her privacy rights" or from "terminating service or otherwise refusing to provide BIAS due to a customer's refusal to waive any such privacy rights." The Order finds that

such practices are harmful to consumers, particularly lower-income consumers, and that "prohibiting such practices will ensure that consumers will not have to trade their privacy for broadband services."

In support of its decision, the Commission states that so-called "take-it-or-leave-it" offers are inconsistent with the requirements under Section 222(a) for telecommunications carriers to protect the confidentiality of customer PI and notes that "a 'take-it-or-leave-it' customer acceptance" does not constitute "approval" to use, disclose or permit access to CPNI as required by Section 222(c)(1). The Order further concludes that a take-it-or-leave-it approach is both an unjust and unreasonable practice under Section 201(b) and violates Section 202(a)'s prohibition against unreasonable discrimination.

Financial incentive programs

The Order adopts heightened disclosure and affirmative consent requirements for "BIAS providers offering financial incentives in exchange for consent to use, disclose, and/or permit access to customer PI."

Unlike "take-it-or-leave-it" offers, the Commission finds that certain financial incentive practices can be beneficial to both BIAS providers and consumers, and that "it is not unusual for business[es] to give consumers benefits in exchange for their personal information." However, in order to prevent BIAS providers from engaging in "coercive or predatory" practices in connection with a financial incentive offer, the Order requires providers to "provide a clear and conspicuous notice of the terms of any financial incentive program that is explained in a way that is comprehensible and not misleading."

Such notices must comply with the general notice requirements adopted in Section 64.2003 of the Commission's rules and must, at a minimum, include the following information: (1) what customer PI the provider will collect; (2) how the customer PI will be used; (3) the types of entities with which the customer PI will be shared; and (4) the purposes for which the customer PI will be shared. The Order requires that such a notice "must be provided both at the time the program is offered and at the time a customer elects to participate in the program" and must be "easily accessible and separate from any other privacy notifications."

Additionally, the notice must be translated into other languages through which the BIAS provider transacts business with its customers. Moreover, BIAS providers must "provide at least as prominent information to customers about the equivalent plan without exchanging personal information" when marketing a financial incentive program.

BIAS providers must obtain opt-in consent for consumers to participate in financial incentive programs and "must provide a simple and easy-to-use mechanism that enables customers to change their participation in such programs at any time."

The Commission will review financial incentive practices on a case-by-case basis.

VIII. Other Issues

Dispute resolution

The Order maintains the Commission's current informal dispute resolution process through which customers can file informal complaints against a provider for alleged violations of the Commission's rules, and reminds carriers that they may not "require customers to waive, or otherwise restrict their

ability to file complaints with or otherwise contact the Commission regarding violations of their privacy rights."

The Order also addresses the practice of requiring customers to arbitrate disputes with the carrier. The Commission notes that it has "serious concerns" about the inclusion of mandatory arbitration clauses in contracts for communications services, which it will address in a notice of proposed rulemaking in February 2017.

Privacy and data security exemption for enterprise voice customers

The Order broadens an existing exemption from the Commission's Section 222 rules for enterprise voice customers. Specifically, the Order establishes that "a carrier that contracts with an enterprise customer for telecommunications services other than BIAS need not comply with the other privacy and data security rules" adopted in the Order if the contract meets certain conditions.

In particular, the contract must "[address] the issues of transparency, choice, data security, and data breach; and [provide] a mechanism for the customer to communicate with the carrier about privacy and data security concerns." Notably, "the contract at issue need not be a fully negotiated agreement, but can take the shape of standard order forms."

The Order acknowledges that enterprise customers often have different privacy needs and expectations than individual consumers, and that these sophisticated customers should be permitted to negotiate privacy and data security protections with their carriers to meet their own unique needs. However, the Commission reminds carriers that even with this exemption, they remain subject to the statutory requirements of Section 222.

IX. Implementation

As explained in more detail below, in recognition that "carriers will need some time to update their internal business processes as well as their customer-facing privacy policies and choice mechanisms," the Order provides a staggered timeline by which carriers must implement the new privacy and data security rules. It also provides guidance on how carriers should treat customer approvals and share customer PI received before the new rules are effective. Finally, the Order extends the timeline for small carriers to implement the transparency and customer choice rules.

Effective dates and implementation schedule for privacy rules

Effective Date	Rule Section(s)	Summary of Rule
30 Days After Publication of a Summary of the Order in the Federal Register	47 C.F.R. § 64.2001	Basis and purpose of the rules
	47 C.F.R. § 64.2002	Definitions
	47 C.F.R. § 64.2011(a)	Prohibition on "take-it-or-leave-it" broadband service offerings
	47 C.F.R. § 64.2010	Business customer exemption
	47 C.F.R. § 64.2012	Preemption of state law

90 Days After Publication of a Summary of the Order in the Federal Register	47 C.F.R. § 64.2005	Requirement to employ reasonable data security practices
6 Months After Publication of a Summary of the Order in the Federal Register or Upon PRA Approval,* whichever is later *After PRA approval, the WCB must release a public notice indicating that the rule is effective, and giving carriers a time period to come into compliance with the rule that is the later of (1) eight weeks from the date of the public notice, or (2) six months after the Commission publishes a summary of the Order in the Federal Register.	47 C.F.R. § 64.2006	Requirement to provide notification of data breaches to customers, the FCC and law enforcement (depending on the size and nature of the breach)
12 Months After Publication of a Summary of the Order in the Federal Register or Upon PRA Approval,* whichever is later** *After PRA approval, the WCB must release a public notice indicating that the rule is effective, and giving carriers a time period to come into compliance with the rule that is the later of (1) eight weeks from the date of the public notice, or (2) twelve months after the Commission publishes a summary of the Order in the Federal Register. **The Order provides small carriers an additional 12 months to comply with the new notice and approval rules	47 C.F.R. § 64.2003	Requirements for providing notice to customers of privacy policies
	47 C.F.R. § 64.2004	Requirements for customer approval to use, disclose or permit access to customer PI (this includes inferred, opt-out and opt-in approval)
	47 C.F.R. § 64.2011(b)	Notice requirements for financial incentive programs

Uniform timeline for BIAS and voice services

The Order clarifies that the new rules will be implemented simultaneously for both BIAS providers and providers of other telecommunications services. It also cautions that until the new rules are effective and implemented, the existing rules for voice services remain in place, and that all providers of telecommunications services, including BIAS providers, remain subject to Section 222.

Customer consent obtained prior to effective and implementation date of new rules

The Order provides that for BIAS providers, including small BIAS providers, the Commission will "treat as valid or 'grandfather' any consumer consent that was obtained prior to the effective date of [the new] rules" so long as such consent is "consistent with [the] new requirements," meaning that the notice provided the consumer with adequate notice regarding his or her privacy rights. In so doing, the Order states that the Commission's goal is to "minimize disruption to carriers' business practices." The Order further directs the Consumer and Governmental Affairs Bureau to work with the industry to engage in a voluntary consumer education campaign about the new rules.

With respect to providers of other telecommunications services, the Order determines that a proper customer consent "subject to the legacy rules remains valid for the time during which it would have remained valid under the legacy rules," but the scope of such consent remains unchanged. It further specifies that "opt-out consent obtained before the release date of this order remains valid for two

years after it was obtained, after which a carrier must conform to the new rules" and "[o]pt-in consent that is valid under the legacy rules remains valid."

Limited extension of implementation period for small carriers

In recognition that some of the new rules may constrain the limited resources available to smaller carriers, the Order provides a 12-month extension for small carriers to implement the new notice and customer approval rules. The small carrier extension will be available to "small BIAS providers . . . with 100,000 or fewer broadband connections and small voice providers with 100,000 or fewer subscriber lines as reported on their most recent Form 477, aggregated over all the providers' affiliates."

The Commission declines to provide an extension of the other rule changes (e.g., data breach notification and "take-it-or-leave-it" prohibition) because they "should not be costly for small carriers that generally collect less customer information and use customer information for narrower purposes."

X. Preemption of State Law

The Order adopts a proposal from the NPRM to "preempt state privacy laws, including data security and breach laws, *only* to the extent that they are inconsistent with any rules adopted by the Commission." The Order acknowledges that states play a key role in protecting consumer privacy, and as such directs that "[w]here state privacy laws do not create a conflict with federal requirements, providers must comply with federal law and state law."

The Commission will "take a fact-specific approach" to determine if a conflict between state and federal law exists, and the Order instructs providers to notify the Commission in an "appropriate petition" if they believe that they are "unable to comply simultaneously with the Commission's rules and with the laws of another jurisdiction."

Additionally, to address concerns about customer notice fatigue, the Commission invites providers that may be required to send out multiple customer notices in order to comply with both state and federal law to "come to the Commission with a proposed waiver that will enable them to send a single notice that is consistent with the goals of notifying consumers of their data breach."

Finally, the Order clarifies that the same preemption standard will apply for both voice and BIAS providers.

XI. Key Takeaways and Conclusion

The Broadband Privacy Order is the arguably most consequential and comprehensive FCC privacy rulemaking since the 1996 Telecommunications Act, which codified Section 222. Not only does the Order impose new rules for broadband providers, it also "harmonizes" these new rules with its existing rules for other telecommunications service providers. The practical impact and reach of the rules will not be known for some time, but at this point we can offer a few of our key takeaways from the Order:

- **All carriers must prepare and maintain public-facing privacy notices.** The Commission's new notice rules will require all telecommunications carriers to draft and post public-facing privacy policies that describe their collection, use, and sharing of customer PI. Formerly, this obligation only applied to BIAS providers (through the Commission's transparency rule). We

expect that disclosures in these privacy policies will be a significant area of enforcement, similar to the Commission's enforcement of annual CPNI certifications.

- **The sensitivity-based consent framework upends the existing CPNI approval framework.** The Commission's adopted rules fundamentally reshape the consent framework for telecommunications carriers, focusing on the sensitivity of the information, rather than on the particular uses and recipients of the information (as the voice CPNI rules did). As a result, all carriers should carefully review and revise their policies, procedures, and systems for obtaining and tracking customer approval.
- **The Order leaves a significant interpretive role for FCC's Enforcement Bureau with respect to data security.** Unlike the existing voice CPNI rules and the Commission's proposed data security rules, which mandated specific data security compliance practices, the new rules simply require carriers to adopt "reasonable" data security practices. By focusing on the "reasonableness" of carriers' privacy and data security practices, the Commission leaves significant room for its Enforcement Bureau to interpret whether particular practices are reasonable, in a manner similar to the FTC's approach to privacy and data security enforcement. For this reason, providers should carefully review the Commission's "exemplary" data security practices and Enforcement Bureau consent decrees in order to gauge which practices the Commission expects of providers.
- **Now is the time to begin reviewing contracts with vendors.** In the Order, the Commission makes clear that carriers will be held responsible for the acts of their agents, vendors, and other third parties with whom they share customer PI. As a result, carriers should take the opportunity now to review contracts with those third parties to determine whether they include specific terms addressing privacy and security. This is particularly important for non-BIAS telecommunications carriers serving enterprise customers, who will be able to take advantage of the Commission's expanded business customer exemption.

Kelley Drye's Communications and Privacy & Information Security practice groups are well-versed in privacy law at the federal and state level, and stand ready to help interested parties understand the scope of these rules and how to operationalize them. Should you have any questions, please contact any of the attorneys listed in the margin.