LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Communications Law Practice

November 16, 2016 | Number 2039

FCC Institutes New Privacy Regime for Broadband Providers and Other Telecommunications Carriers

Landmark ruling establishes a variety of new obligations, but long-term effects remain unclear.

On November 2, 2016, the US Federal Communications Commission (FCC) released an order adopting new privacy rules that will govern how broadband Internet access service (BIAS) providers can collect, use, protect and share data about their subscribers.[1] The *2015 Open Internet Order*[2] set the stage for these new privacy rules by reclassifying BIAS as a common carrier telecommunications service governed by Title II of the Communications Act. This reclassification had the effect of exempting BIAS providers from the Federal Trade Commission's (FTC's) privacy requirements (as the FTC Act prohibits the agency from regulating common carriers), while at the same time subjecting BIAS providers for the first time to Section 222 of the Communications Act, which establishes distinct privacy obligations for common carrier telecommunications services. The rules adopted in the FCC's *Broadband Privacy Order* — unless reconsidered by new leadership — will create a new consumer privacy regime for BIAS providers (and other Title II common carriers, including providers of traditional voice services) that will stand in lieu of the FTC's authority. As expected, these rules do not apply to providers of "edge services" (everything from websites, web-based email and streaming services, to mobile applications and search engines).

New Transparency Obligations in the Privacy Context

The *Broadband Privacy Order* starts by requiring that BIAS providers and other telecommunications carriers clearly and accurately disclose to consumers what information is being collected, how and for what purposes that information is used and shared, and the types of entities with which the information is shared.[3] Additionally, BIAS providers must disclose how consumers can exercise their privacy choices, by explaining the opt-in and opt-out rights (discussed further below) that customers have with regard to certain uses and collections of data. In particular, providers must:

- Tell consumers that a customer's exercise of opt-in or opt-out rights will not impact the type or quality of services they receive
- Inform consumers that a customer can change their decision at any time
- Explain the straightforward mechanisms by which consumers can provide or withdraw consent[4]

All privacy disclosures must be immediate (at the time the customer subscribes to the service or when the provider's policy changes) as well as persistently and conspicuously available on the provider's website.[5] The *Broadband Privacy Order* also provides that privacy disclosures must be clear and not misleading, and must be written in plain English that consumers can easily understand.[6] Advance notice of any

material change to a provider's privacy policy must be given in a clear and conspicuous manner, conveying the relevant changes to the policy as well as the consumer's rights.[7]

Bright-Line Consent Requirements for Using and Sharing Data

The *Broadband Privacy Order* establishes new consent requirements relating to using and sharing particular kinds of customer data. First, the rules apply to "customer proprietary network information" (CPNI), a type of data Section 222 of the Communications Act defines as including the quantity, technical configuration, type, destination, location and amount of use of a telecommunications service to which a customer subscribes. For broadband, the FCC declined to provide an "exhaustive" list of data elements that comprise CPNI, but the FCC found that, when collected in connection with providing broadband service, CPNI includes, at a minimum, Internet service plan and pricing, geo-location data, MAC address, Device ID, IP address, traffic statistics, customer premises equipment and device information, and application header, usage and payload information.[8] The *Broadband Privacy Order* also sweeps in so-called "personally identifiable information" (PII), which is defined to include all "linked or reasonably linkable" information about an individual, such as name, date of birth and home address.[9] These two types of data, along with the content of communications, are part of a larger category of data — "customer proprietary information" (customer PI) — that broadband providers and other telecommunications carriers will be required to protect for current and former customers as well as any applicant for service. Notably, the FCC's definition of customer PI also includes all "information that BIAS providers and other telecommunications carriers acquire in connection with their provision of services, which customers have an interest in protecting from disclosure."[10]

The *Broadband Privacy Order* establishes a new hierarchy of opt-in and opt-out privacy practices for BIAS providers that depends on the sensitivity of the information involved. This model of sensitivity-based requirements for data use is consistent with the FTC's approach, and represents a shift from the less granular rules the FCC initially proposed in this proceeding. The most sensitive information, known as "Sensitive Customer PI," includes precise geo-location data, children's information, health information, web browsing and app usage history, and the content of messages (and, for voice services, call detail information).[11] Most notable is the inclusion, following recent FTC guidelines, of web browsing and usage history in the category of "sensitive" information, which could have a significant impact on online advertising services. Sensitive Customer PI cannot be used or shared without the subscriber's express prior opt-in consent. Less sensitive data that is still individually identifiable, or "Non-Sensitive Customer PI," generally can be used or shared unless the customer opts out of that use,[12] though using or sharing that data will require opt-in approval from consumers if the provider proposes a material change in the use or sharing of previously collected information.[13] Once a consumer expresses an opt-in or opt-out choice, the provider must act "promptly" to implement that choice.[14]

A limited set of data can be used with no ability for the subscriber to opt out, so long as the data is used solely to provide the service, issue bills and limit first-party marketing of services within the scope of the provider's relationship with a consumer.[15] A final category of data — that which has been "de-identified" (that is, where the data is no longer associated with the individual to whom the information pertains) — can also be shared outside of the opt-in/opt-out requirements, so long as the de-identification comports with the existing FTC multi-part test (which requires taking reasonable steps to ensure thorough de-identification, commitments not to re-identify the information, and contractual prohibitions on re-identification by parties with whom the information is shared).[16]

These subscriber choice requirements, as well as the transparency obligations discussed above, will go into effect 12 months (or 24 months for small providers) after the *Order* is published in the Federal Register. While opt-in rules are certain to increase the complexity of administering data, they do not

necessarily spell the end for all reasonable uses of data. Well-crafted user interfaces can provide clear, concise and compliant disclosures to customers while simultaneously eliciting a high percentage of subscribers approving data uses. Moreover, these requirements follow a global trend toward obtaining more explicit advanced consent before collecting, using and sharing user information (see, for example, the European Union's draft General Data Protection Regulation).

Restrictions on "Conditional" Privacy

The *Broadband Privacy Order* prohibits BIAS providers from selling services on a "take-it-or-leave-it" basis, such that customers who refuse to agree to less restrictive data privacy protections would be denied service.[17] The *Order* also requires "heightened" disclosures when a provider offers a service with fewer privacy protections in exchange for a lower cost of service.[18] This heightened disclosure regime, along with a case-by-case review of provider practices, is a nod toward FTC practice, which has come to accept that consumers may make reasonable decisions to trade certain privacy rights for improved or lower-cost services. Notably, however, the FCC "reserve[d] the right to take action" against "unreasonable" financial incentive practices, including if "service prices are inflated such that customers are essentially compelled to choose between protecting their personal information and very high prices."[19] Where the FCC would draw that line in an individual case is unclear, so providers likely will be cautious in testing the waters on such arrangements, at least in the near term.

New Data Security Obligations and Data Breach Notification Requirements

The FCC also issued a broad new requirement that BIAS providers take "reasonable measures" to safeguard subscriber data from unauthorized use and disclosure.[20] The reasonableness of security practices depends on the type of information being secured, the size of the provider, and technical feasibility.[21] Moreover, because the *Order* "gives providers broad flexibility to consider costs when determining what security measures to implement over time," the FCC declined to include cost as an enumerated factor in determining the reasonableness of a provider's security practices.[22] While the FCC's approach to data security involves no specific, bright-line requirements (or, for that matter, a safe harbor that could be met by complying with a set of standards),[23] the FCC recommends that providers follow industry best practices; implement strong internal controls; and create customer authentication tools to prevent breaches of consumer data.[24] The *Broadband Privacy Order* also expressly encourages providers to participate in lawful cyber threat information sharing regimes, such as that created by the Cybersecurity Information Sharing Act of 2015.[25] These requirements go into effect 90 days after the *Broadband Privacy Order* is published in the Federal Register.

In addition, the *Broadband Privacy Order* implements new data breach notification rules that are closely aligned with state and federal notification requirements. If a provider determines that a breach of consumer information has a reasonable likelihood of causing harm (financial, emotional or physical), the provider must disclose the breach to consumers and the FCC.[26] The "harm-based trigger" was intended to prevent "excessive notifications" and is supposed to allow providers to "prevent[] and ameliorat[e] breaches, rather than issuing notifications for inconsequential events" — but the threshold for notification is, at best, amorphous (requiring providers to "reasonably determine" whether "harm to customers is reasonably likely to occur").[27] Importantly, the *Order* specifies that the use of encryption is insufficient, in and of itself, to eliminate a reasonable likelihood of harm.[28] Moreover, if the information lost is Sensitive Customer PI, the *Order* establishes a rebuttable presumption that there will be consumer harm and that notification is required.[29] If a breach impacts fewer than 5,000 people, the provider must notify the FCC within 30 calendar days, and if 5,000 or more people are impacted the provider must notify the FCC, the FBI and the US Secret Service within seven business days.[30] Providers must also provide written notice to affected customers within 30 calendar days providing them with information about the timing of the breach; the types of compromised information; contact information for the provider, the FCC and state

regulators; and information about identity theft and credit monitoring.[31] In situations that require law enforcement notice, providers must wait at least three days after giving that notice before notifying affected customers. The *Order* also authorizes providers, at the direction of either the FBI or the Secret Service, to delay customer notification for "as long as necessary" to avoid interference in ongoing law enforcement and national security investigations.[32] In practice, entities that suffer a data breach often choose to work with law enforcement to secure mutually beneficial extensions of notification deadlines. These requirements go into effect (absent reconsideration) six months after the *Order* is published in the Federal Register.

Future Review of Mandatory Arbitration Provisions

Finally, while there were reports that the FCC would ban the use of mandatory arbitration agreements in the broadband privacy context, the *Broadband Privacy Order* stops short of adopting such a prohibition. Instead, the FCC expressed its "concern" about such arrangements and contemplates a rulemaking in 2017 to address them.[33] The *Order* points out that "the Consumer Financial Protection Bureau (CFPB) — which has extensive experience with consumer arbitration agreements and dispute resolution mechanisms — issued a report last year on mandatory arbitration clauses and is currently engaged in a rulemaking on the subject in the consumer finance context," and notes that the FCC "expect[s] that many of the lessons the CFPB learns and the conclusions it draws in its rulemaking will be informative and useful."[34]

Conclusion

The *Broadband Privacy Order* certainly is a landmark FCC ruling that establishes a variety of new obligations for broadband providers and other telecommunications carriers. Nevertheless, the long-term effect of the *Order* is somewhat unclear. Broadband providers may seek agency reconsideration of the *Order* or could challenge it in court, which could stoke a prolonged legal battle similar to the one over the FCC's adoption of the *2015 Open Internet Order*. Moreover, if the FCC's decision in the *2015 Open Internet Order* to reclassify broadband as a Title II common carrier service is set aside — by a court, future FCC (which Republicans will control after the inauguration of President-elect Trump) or future legislation — then the legal underpinning of the *Broadband Privacy Order* likely would vanish. The broadband privacy space thus will be a source of continuing interest in the months and years ahead.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Matthew A. Brill
matthew.brill@lw.com
+1.202.637.1095
Washington, D.C.

Jennifer C. Archie
jennifer.archie@lw.com
+1.202.637.2205
Washington, D.C.

James H. Barker
james.barker@lw.com
+1.202.637.2200
Washington, D.C.

John P. Janka
john.janka@lw.com
+1.202.637.2289
Washington, D.C.

Matthew T. Murchison
matthew.murchison@lw.com
+1.202-637-2136
Washington, D.C.

Amanda E. Potter
amanda.potter@lw.com
+1.202.637.2192
Washington, D.C.

Alexander L. Stout
alexander.stout@lw.com
+1.202.637.2158
Washington, D.C.

You Might Also Be Interested In

5 Preventative Steps to Manage Cybersecurity Breach Risk

New EU Data Protection Rules Move the M&A Goalposts

European Commission Unveils New Digital Single Market Proposals

FCC Proposes Sweeping Broadband Privacy Rules

Endnotes

1 *See, generally*, *Protecting the Privacy of Customers of Broadband and Other Telecommunication Services*, Report and Order, WC Docket No. 16-106, FCC 16-148 (rel. Nov. 2, 2016) (*Broadband Privacy Order* or *Order*).

2 *See, generally*, *Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601 (2015) (*2015 Open Internet Order*).

3 *Broadband Privacy Order* ¶ 125–26.

4 *Id.* at ¶¶ 132-34.

5 *Id.* at ¶¶ 137-43.

6 *Id.* at ¶¶ 147-51.

[7] *Id.* at ¶¶ 156-63.
[8] *Id.* at ¶ 53.
[9] *Id.* at ¶¶ 89, 95-96.
[10] *Id.* at ¶ 85.
[11] *Id.* at ¶¶ 166-67.
[12] *Id.* at ¶ 167.
[13] *Id.* at ¶ 195.
[14] *Id.* at ¶ 231.
[15] *Id.* at ¶¶ 203, 204.
[16] *Id.* at ¶¶ 106-07.
[17] *Id.* at ¶ 294.
[18] *Id.* at ¶ 297.
[19] *Id.* at ¶ 303.
[20] *Id.* at ¶ 242.
[21] *Id.*
[22] *Id.* at ¶ 244.
[23] *Id.* at ¶ 245.
[24] *Id.* at ¶¶ 250-53.
[25] *Id.* at ¶ 246.
[26] *Id.* at ¶¶ 261-66.
[27] *Id.* at ¶¶ 71, 264.
[28] *Id.* at ¶ 269.
[29] *Id.*
[30] *Id.* at ¶¶ 278-79.
[31] *Id.* at ¶¶ 288-92.
[32] *Id.* at ¶ 281.
[33] *Id.* at ¶¶ 304-05.
[34] *Id.* at ¶ 305.