Melissa Newman
Vice President-Federal Regulatory Affairs
1099 New York Avenue NW, Suite 250
Washington, DC 20001
202.429.3120

VIA ECFS

NOTICE OF EX PARTE

September 13, 2016

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street SW
Washington, DC 20554

Re: *In the Matter of Protecting the Privacy of Customers of Broadband and other Telecommunications Services***,** WC Docket No. 16-106

Dear Ms. Dortch:

On September 9, 2016, Bill Hurley, Linda Gardner, Susan Mohr and Melissa Newman, all of CenturyLink, met with Lisa Hone, Daniel Kahn, David Brody and Melissa Kirkel of the Wireline Competition Bureau and Peter Shroyer of the Public Safety and Homeland Security Bureau to discuss the above-captioned proceeding.

The attached document was used as the basis for discussion.

Sincerely,

/s/ Melissa E. Newman

Attachment

Copy via email to:
Lisa Hone
Daniel Kahn
David Brody
Melissa Kirkel
Peter Stryoker

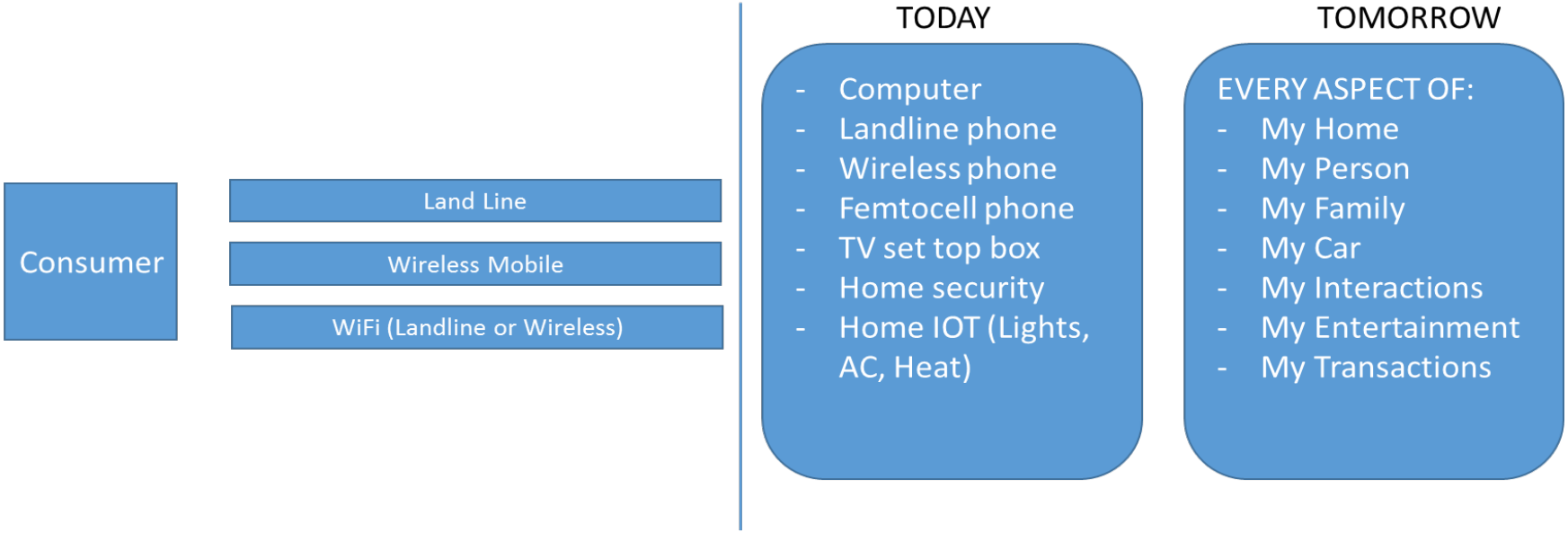
In the Matter of Protecting the Privacy of Customers of Broadband and other Telecommunications Services

WC Docket No. 16-106

September 9, 2016

CenturyLink™

How Consumers Access and Use Broadband Internet Access is Evolving



Consumers expect a "frictionless" online experience when it comes to :

a) **Interactions with others**
b) **Entertainment**
c) **Transactions**

Consumers are looking at the experience – not their broadband service. Adopting new rules that apply only to ISP's threatens the frictionless experience that consumers demand.

CenturyLink Understands the Importance of Meeting Consumer Privacy Expectations

- Sound data privacy protections, including transparency, choice and data security, are critical to assuring consumer confidence in the technologies and companies that drive the digital economy.
- CenturyLink has a strong, independent incentive to meet these expectations– to attract and retain customers.
- Consumers are informed—our privacy policy and related disclosures are carefully crafted, readily available, instructive, and clear so that consumers understand what we collect, how we use or share information and the choices they have.
  - *Consumers can easily find the privacy policy with links from pages frequently visited.*
  - *A series of short videos are available to help consumers understand our privacy and data security practices.*
  - *It is structured to provide an overview or more detail as the consumer desires.*
  - *We also provide answers to frequently asked questions, a "What's New" box, and links to other useful information.*
  - *And, since we want to hear from consumers, readily available contact information for privacy related questions, customer support needs, and to report spam.*

One size does not fit all. Consumers are best served by allowing providers the flexibility to determine how best to communicate privacy practices to its customers.

The Proposed Consent Framework is Unnecessarily Restrictive

Context, Transparency and Choice should guide—not format

- Default "Opt-In" unnecessarily restricts beneficial or necessary uses and sharing of information— for examples, it appears to require opt-in when sharing with:
  - *all* third parties, even those working on our behalf or receiving objectively non-sensitive information
  - affiliates or others such as joint venture partners, or using ourselves, to market services customers desire that complement other services, such as home security, over-the-top video, or connected devices

- Opt-out can be equally, or more, effective than a default opt-in at accurately reflecting the privacy expectations of most consumers
  - Opt-out does not equate to a lack of transparency or choice
  - Consistent with the FTC's guidance, consumers are accustomed to an opt-in only for particularly sensitive information—data about children, financial and health information, SSN and precise geo-location data

CenturyLink recommends the FCC adopt a consent model that more closely tracks what customers are accustomed to and expect—the FTC model that is based on sensitivity of information and context.

New Data Breach Notification Regulations Are Not Needed

- CenturyLink has a trusted relationship with our customers, which includes maintaining reasonable security practices to protect information. CenturyLink already has an incentive to provide prompt notice to customers when a breach of sensitive information occurs that may pose a risk to the customer—it is the right thing to do and necessary to maintain that customer trust.

- Broadband providers, including CenturyLink, are already subject to data breach notification laws in forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands.

- Layering the proposed additional breach notification obligations on providers will result in duplicative and excessive notifications that will confuse customers.

- Customer confusion is further compounded when these obligations do not apply consistently to the same information and across the entire Internet ecosystem.

Customers are already notified when sensitive information is breached without the need for an FCC rule. Additional notices, particularly under circumstances where there is no reasonable likelihood of harm, is not beneficial to customers. If the FCC desires visibility into these instances, it can require broadband providers to provide notice to the agency when we report a breach under state law.

State Laws Provide the Proper Guidance for a Breach Notification Framework

Proportionate Notice is Good: Excessive Notice is Not

- Triggers are important. Too broad leads to over-notification and notice fatigue.
- Notice should only be required where
  - Information is actually acquired and the information is objectively sensitive
- But not, for example, if it involves
  - Unsuccessful attempts, the exposure of encrypted or otherwise unreadable information, or it amounts to a "breach" that poses no reasonable likelihood of harm

Premature Notice is Detrimental to Consumers

- Investigations are complex; suppositions change to facts which could show no breach at all, less information or fewer customers involved than originally suspected
- Notice is most effective and beneficial when you have those facts, can reassure of steps taken to further protect the information, and have completed the preparation necessary to promptly and accurately respond to customer concerns
  - 7 or 10 days from "discovery" will not only lead to incomplete, inaccurate, and multiple notices, but consumer frustration

Any new requirement should require notice only where there has been a determination, after investigation, that a breach of sensitive information has occurred. Notice should not be required where there is no real likelihood of harm from the breach and not provided until the investigation is completed, remediation identified, scope of the information and affected individuals determined, and the communication structure is in place to timely address customer questions and concerns. Our incentive is already to do this as quickly as possible, as the complexity allows.