

Joanne Wall

From: Loretta Polk <LPolk@NCTA.com>
Sent: Tuesday, March 01, 2016 3:10 PM
To: Jennifer Tatel
Subject: Industry Privacy Framework
Attachments: Wheeler Letter Re Privacy Principles 3 1 16.pdf; BB Privacy Framework 3.1.16.docx

Good afternoon Jennifer,

For your information, I am forwarding a Privacy Framework Discussion Paper and cover letter that was sent to Chairman Wheeler on behalf of five industry associations this afternoon.

If you have any questions, please feel free to contact me. Thank you.

Loretta Polk

Loretta Polk | Vice President and Associate General Counsel
National Cable & Telecommunications Association
25 Massachusetts Avenue, NW | Suite 100 | Washington, DC 20001
202.222.2445 | lpolk@ncta.com

Privacy Framework
Draft Discussion Paper

All entities in the Internet ecosystem should be subject to a consistent privacy framework with respect to consumer information. Consumer information should be protected based upon the sensitivity of the information to the consumer and how the information is used—not the type of business keeping it, how that business obtains it, or what regulatory agency has authority over it. Consumers should have consistent and predictable privacy protections for the information they deem private and sensitive, no matter how or with whom they share it. Consumers also will benefit from a consistent privacy framework that promotes the emergence of new business models and innovative uses of data that foster increased consumer choice and service customization.

The FCC should adopt an approach to privacy and data security for CPNI that is flexible, harmonized with the well-established and successful FTC framework, and backed up by strong but fair enforcement for unfair or deceptive acts or practices (UDAP) that materially harm consumers.¹ This well-tested consumer protection approach is consistent with the FCC’s privacy recommendations in the 2010 National Broadband Plan, the FTC’s and White House’s 2012 Privacy Reports, and the White House’s 2015 Consumer Privacy Bill of Rights, as well as with Chairman Wheeler’s recent testimony before Congress acknowledging the importance of coordination with the FTC and harmonization with its privacy framework.

That approach will benefit consumers by safeguarding privacy interests as it has for years and will ensure that the same privacy and security framework applies to all entities in the Internet ecosystem. By leveraging a tested privacy model, the FCC will avoid inconsistent requirements that could otherwise hamper innovation and reduce competition. Most important, it will minimize consumer confusion as well as other harms associated with disparate privacy regulation across the ecosystem. Indeed, this approach will align with consumers’ expectations that their data would be subject to consistent privacy rules regardless of whether it is used by their Internet Service Provider (ISP), application developers, operating systems, or edge providers.

When adopting a framework, the FCC should keep the following guidelines in mind:

- **Consistent and Coordinated Regulatory Regimes.** The FCC’s rules and principles for regulating and enforcing privacy and security should be as similar as possible to the FTC approach, which will continue to govern other Internet ecosystem players’ use and disclosure of the same or similar data. The consistent application of standards across

¹ This framework is intended for discussion purposes, and we are not conceding that the FCC has authority to adopt privacy and security rules for Broadband Internet Access Services or over data related to consumers’ use of Broadband Internet Access Services. To the extent it is determined that the FCC has such statutory authority, this document is intended to set forth principles for FCC consideration and possible adoption that are harmonized and consistent with the FTC and other government entities’ approach to privacy and security for the same or similar data. Even if courts determine that the FCC’s reclassification of Broadband Internet Access Services is a lawful exercise of authority, any rules must not exceed the text and legislative history of Section 222 of the Act.

sectors would fulfill the following key tenets in the White House Privacy Report: (1) avoid “inconsistent standards for related technologies” that could dampen innovation; (2) foster a “level playing field for companies;” and, most importantly, (3) create “a consistent set of expectations for consumers.” To achieve this end, the FCC’s policies, rules, and enforcement practices should conform to the longstanding limiting principles articulated in the FTC’s Unfairness and Deception Policy Statements. In addition, the FCC and FTC can achieve their recent MOU’s stated goal of avoiding “duplicative, redundant or inconsistent oversight” by developing a new process to ensure that their substantive privacy policies and basis for enforcement are consistent going forward.

- Flexibility. The FCC’s approach should provide a flexible framework within which telecommunications service providers can implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments in this space. Specifically, this framework should identify the privacy or security *goals*, and afford providers flexibility in achieving those goals, rather than dictate the particular *methods* by which providers are expected to achieve those goals. Adopting a flexible approach also will help ensure consistent federal and state requirements governing customer information.
- Application. Consistent with the Communications Act and to eliminate unnecessary duplication of authority with other agencies, the FCC’s framework should only apply when 1) telecommunications service providers are providing telecommunications services and 2) the CPNI is made available by the customer to the telecommunications service provider solely by virtue of the carrier-customer relationship. The framework cannot lawfully apply to:
 - Providers’ non-telecommunications services and products
 - Providers’ non-telecommunications service provider affiliates
 - Information that is not made available to the carrier by the customer solely by virtue of the carrier-customer relationship
- Individually Identifiable. The FCC should carve out from the scope of its new framework any data that is de-identified, aggregated, or does not otherwise identify a known individual. The insights derived from the use of de-identified data can offer great benefits to consumers and society and such use avoids the sensitivities that may be associated with identified data.
- Unfair or Deceptive Conduct. As noted above, the FCC’s policies, rules, and enforcement practices should conform to the FTC’s longstanding limiting principles articulated in its Policy Statements on Unfairness (1980) and Deception (1983). This approach is consistent with the FCC’s commitment to conduct a cost-benefit analysis of its regulatory framework in accordance with President Obama’s Executive Orders 13563 and 13579, which require agencies to “adopt a regulation only upon a reasoned determination its benefits justify its costs” and “tailor its regulations to impose the least burden on society.”

- Unfair Conduct. A provider acts unfairly if its act or practice (1) causes or is likely to cause substantial injury to consumers (2) which is not reasonably avoidable by consumers themselves, and (3) is not outweighed by countervailing benefits to consumers or to competition.
- Deceptive Conduct. A provider acts deceptively if (1) it makes a statement or omission, or engages in a practice, that is likely to mislead a customer, (2) viewed from the perspective of a consumer acting reasonably under the circumstances, and (3) the deceptive statement, omission, or practice is material—meaning that the misrepresentation or practice is likely to affect the consumer’s conduct or decision with regard to a product or service.
- Additional Guidance. In coordination with other privacy regulators, the FCC could, like the FTC and various states like California, provide additional guidance on how it interprets its framework through workshops or reports. The FCC also could encourage and support the development and implementation of industry guidelines.
- Update and Harmonize Existing CPNI Rules. The existing CPNI rules should be revisited in their entirety and modernized to use the same flexible framework for all services subject to Section 222, including traditional voice services. In no event should the prescriptive outdated CPNI rules designed for legacy voice services apply to broadband services. Instead, a common set of flexible policies that allow providers to keep up with their customers’ expectations and evolving technology should apply to both types of services.

With these guidelines in mind, if the courts determine that the FCC has authority to regulate broadband privacy, the FCC could adopt the following principles, which encompass and are consistent with the privacy and security framework that applies to the rest of the industry. Each of these principles and the goals noted above should provide flexibility for providers to implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments:

- Transparency. A telecommunications service provider should provide notice, which is neither deceptive nor unfair, describing the CPNI that it collects, how it will use the CPNI, and whether and for what purposes it may share CPNI with third parties.
- Respect for Context and Consumer Choice. A telecommunications service provider may use or disclose CPNI as is consistent with the context in which the customer provides, or the provider obtains, the information, provided that the provider’s actions are not unfair or deceptive. For example, the use or disclosure of CPNI for the following commonly accepted data practices would not warrant a choice mechanism, either because customer consent can be inferred or because public policy considerations make choice unnecessary: product and service fulfillment, fraud prevention, compliance with law, responses to government requests, network management, first-party marketing, and affiliate sharing where the affiliate relationship is reasonably clear to consumers. Consistent with the flexible choice mechanisms available to all other entities in the Internet ecosystem, telecommunications service providers should give consumers easy-

to-understand choices for non-contextual uses and disclosures of their CPNI, where the failure to provide choice would be deceptive or unfair. The provider should consider the sensitivity of the data and the context in which it was collected when determining the appropriate choice mechanism.

- Data Security. A telecommunications service provider should establish, implement, and maintain a CPNI data security program that is neither unfair nor deceptive and includes reasonable physical, technical, and administrative security safeguards to protect CPNI from unauthorized access, use, and disclosure. Providers' CPNI data security programs should provide reasonable protections in light of the nature and scope of the activities of the company, the sensitivity of the data, and the size and complexity of the relevant data operations of the company.
- Data Breach Notifications. Telecommunications service providers should notify customers whose CPNI has been breached when failure to notify would be unfair or deceptive. Given that breach investigations frequently are ongoing at the time providers offer notice to customers, a notice that turns out to be incomplete or inaccurate is not deceptive, as long as the provider corrects any material inaccuracies within a reasonable period of time of discovering them. Telecommunications providers have flexibility to determine how and when to provide such notice.

The FCC can ensure compliance with the above principles by pursuing reasonable enforcement actions against telecommunications service providers that have clearly violated these principles.

American Cable Association
Competitive Carriers Association
CTIA
National Cable & Telecommunications Association
U.S. Telecom Association

Dated: March 1, 2016



March 1, 2016

The Honorable Tom Wheeler
Chairman
Federal Communications Commission
445 12th St. SW
Washington, D.C. 20554

Dear Chairman Wheeler,

Today, the American Cable Association, Competitive Carriers Association, CTIA, National Cable & Telecommunications Association, and USTelecom offer for the Commission's consideration a detailed proposal for a broadband privacy framework. After significant examination and analysis, these associations have developed the attached consensus Privacy Framework setting forth guidelines and principles to protect consumer privacy in a way that is consistent with other privacy laws that apply to companies providing services online. By adopting these principles, the Commission would establish a regime that protects consumer privacy and security while also providing flexibility for providers to implement and update their practices as consumer expectations and technologies evolve.

If the courts determine that the Commission has authority over broadband privacy, the FCC should focus on four privacy principles: (1) transparency; (2) respect for context and consumer choice; (3) data security; and (4) data breach notification. For each of these principles, the FCC should draw from and harmonize with the longstanding Federal Trade Commission unfairness and deception approach to privacy, which, before the FCC's reclassification decision, governed the privacy practices of all companies in the Internet ecosystem and will continue to apply to non-ISPs going forward.

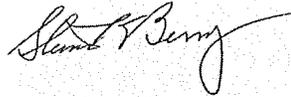
As the Commission develops its approach to broadband privacy, we respectfully request that it seek comment on the entirety of the Privacy Framework we submit today. Because regulation of broadband privacy is a new area for the Commission, it should take the necessary time to build a robust record rather than prejudge the issues by adopting tentative conclusions before there is a public discussion of the consensus Privacy Framework.

We look forward to continuing a conversation with the Commission about the best way to provide privacy and innovation benefits to consumers.

Respectfully submitted,



Matthew M. Polka
President & CEO
American Cable Association



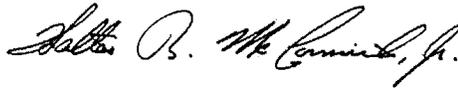
Steven K. Berry
President & CEO
Competitive Carriers Association



Meredith Attwell Baker
President & CEO
CTIA



Michael Powell
President & CEO
National Cable & Telecommunications Association



Walter B. McCormick, Jr.
President & CEO
USTelecom

cc: The Honorable Mignon Clyburn
The Honorable Jessica Rosenworcel
The Honorable Ajit Pai
The Honorable Michael O’Rielly

Privacy Framework

Discussion Paper

All entities in the Internet ecosystem should be subject to a consistent privacy framework with respect to consumer information. Consumer information should be protected based upon the sensitivity of the information to the consumer and how the information is used—not the type of business keeping it, how that business obtains it, or what regulatory agency has authority over it. Consumers should have consistent and predictable privacy protections for the information they deem private and sensitive, no matter how or with whom they share it. Consumers also will benefit from a consistent privacy framework that promotes the emergence of new business models and innovative uses of data that foster increased consumer choice and service customization.

The FCC should adopt an approach to privacy and data security for CPNI that is flexible, harmonized with the well-established and successful FTC framework, and backed up by strong but fair enforcement for unfair or deceptive acts or practices (UDAP) that materially harm consumers.¹ This well-tested consumer protection approach is consistent with the FCC’s privacy recommendations in the 2010 National Broadband Plan, the FTC’s and White House’s 2012 Privacy Reports, and the White House’s 2015 Consumer Privacy Bill of Rights, as well as with Chairman Wheeler’s recent testimony before Congress acknowledging the importance of coordination with the FTC and harmonization with its privacy framework.

That approach will benefit consumers by safeguarding privacy interests as it has for years and will ensure that the same privacy and security framework applies to all entities in the Internet ecosystem. By leveraging a tested privacy model, the FCC will avoid inconsistent requirements that could otherwise hamper innovation and reduce competition. Most important, it will minimize consumer confusion as well as other harms associated with disparate privacy regulation across the ecosystem. Indeed, this approach will align with consumers’ expectations that their data would be subject to consistent privacy rules regardless of whether it is used by their Internet Service Provider (ISP), application developers, operating systems, or edge providers.

When adopting a framework, the FCC should keep the following guidelines in mind:

- **Consistent and Coordinated Regulatory Regimes.** The FCC’s rules and principles for regulating and enforcing privacy and security should be as similar as possible to the FTC approach, which will continue to govern other Internet ecosystem players’ use and disclosure of the same or similar data. The consistent application of standards across sectors would fulfill the following key tenets in the White House Privacy Report: (1) avoid “inconsistent standards for related technologies” that could dampen innovation; (2)

¹ This framework is intended for discussion purposes, and we are not conceding that the FCC has authority to adopt privacy and security rules for Broadband Internet Access Services or over data related to consumers’ use of Broadband Internet Access Services. To the extent it is determined that the FCC has such statutory authority, this document is intended to set forth principles for FCC consideration and possible adoption that are harmonized and consistent with the FTC and other government entities’ approach to privacy and security for the same or similar data. Even if courts determine that the FCC’s reclassification of Broadband Internet Access Services is a lawful exercise of authority, any rules must not exceed the text and legislative history of Section 222 of the Act.

- foster a “level playing field for companies;” and, most importantly, (3) create “a consistent set of expectations for consumers.” To achieve this end, the FCC’s policies, rules, and enforcement practices should conform to the longstanding limiting principles articulated in the FTC’s Unfairness and Deception Policy Statements. In addition, the FCC and FTC can achieve their recent MOU’s stated goal of avoiding “duplicative, redundant or inconsistent oversight” by developing a new process to ensure that their substantive privacy policies and basis for enforcement are consistent going forward.
- Flexibility. The FCC’s approach should provide a flexible framework within which telecommunications service providers can implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments in this space. Specifically, this framework should identify the privacy or security *goals*, and afford providers flexibility in achieving those goals, rather than dictate the particular *methods* by which providers are expected to achieve those goals. Adopting a flexible approach also will help ensure consistent federal and state requirements governing customer information.
 - Application. Consistent with the Communications Act and to eliminate unnecessary duplication of authority with other agencies, the FCC’s framework should only apply when 1) telecommunications service providers are providing telecommunications services and 2) the CPNI is made available by the customer to the telecommunications service provider solely by virtue of the carrier-customer relationship. The framework cannot lawfully apply to:
 - Providers’ non-telecommunications services and products
 - Providers’ non-telecommunications service provider affiliates
 - Information that is not made available to the carrier by the customer solely by virtue of the carrier-customer relationship
 - Individually Identifiable. The FCC should carve out from the scope of its new framework any data that is de-identified, aggregated, or does not otherwise identify a known individual. The insights derived from the use of de-identified data can offer great benefits to consumers and society and such use avoids the sensitivities that may be associated with identified data.
 - Unfair or Deceptive Conduct. As noted above, the FCC’s policies, rules, and enforcement practices should conform to the FTC’s longstanding limiting principles articulated in its Policy Statements on Unfairness (1980) and Deception (1983). This approach is consistent with the FCC’s commitment to conduct a cost-benefit analysis of its regulatory framework in accordance with President Obama’s Executive Orders 13563 and 13579, which require agencies to “adopt a regulation only upon a reasoned determination its benefits justify its costs” and “tailor its regulations to impose the least burden on society.”
 - Unfair Conduct. A provider acts unfairly if its act or practice (1) causes or is likely to cause substantial injury to consumers (2) which is not reasonably avoidable by consumers themselves, and (3) is not outweighed by countervailing benefits to consumers or to competition.
 - Deceptive Conduct. A provider acts deceptively if (1) it makes a statement or omission, or engages in a practice, that is likely to mislead a customer, (2) viewed from the perspective of a consumer acting reasonably under the circumstances, and (3) the deceptive statement, omission, or practice is material—meaning that

the misrepresentation or practice is likely to affect the consumer's conduct or decision with regard to a product or service.

- Additional Guidance. In coordination with other privacy regulators, the FCC could, like the FTC and various states like California, provide additional guidance on how it interprets its framework through workshops or reports. The FCC also could encourage and support the development and implementation of industry guidelines.
- Update and Harmonize Existing CPNI Rules. The existing CPNI rules should be revisited in their entirety and modernized to use the same flexible framework for all services subject to Section 222, including traditional voice services. In no event should the prescriptive outdated CPNI rules designed for legacy voice services apply to broadband services. Instead, a common set of flexible policies that allow providers to keep up with their customers' expectations and evolving technology should apply to both types of services.

With these guidelines in mind, if the courts determine that the FCC has authority to regulate broadband privacy, the FCC could adopt the following principles, which encompass and are consistent with the privacy and security framework that applies to the rest of the industry. Each of these principles and the goals noted above should provide flexibility for providers to implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments:

- Transparency. A telecommunications service provider should provide notice, which is neither deceptive nor unfair, describing the CPNI that it collects, how it will use the CPNI, and whether and for what purposes it may share CPNI with third parties.
- Respect for Context and Consumer Choice. A telecommunications service provider may use or disclose CPNI as is consistent with the context in which the customer provides, or the provider obtains, the information, provided that the provider's actions are not unfair or deceptive. For example, the use or disclosure of CPNI for the following commonly accepted data practices would not warrant a choice mechanism, either because customer consent can be inferred or because public policy considerations make choice unnecessary: product and service fulfillment, fraud prevention, compliance with law, responses to government requests, network management, first-party marketing, and affiliate sharing where the affiliate relationship is reasonably clear to consumers. Consistent with the flexible choice mechanisms available to all other entities in the Internet ecosystem, telecommunications service providers should give consumers easy-to-understand choices for non-contextual uses and disclosures of their CPNI, where the failure to provide choice would be deceptive or unfair. The provider should consider the sensitivity of the data and the context in which it was collected when determining the appropriate choice mechanism.
- Data Security. A telecommunications service provider should establish, implement, and maintain a CPNI data security program that is neither unfair nor deceptive and includes reasonable physical, technical, and administrative security safeguards to protect CPNI from unauthorized access, use, and disclosure. Providers' CPNI data security programs should provide reasonable protections in light of the nature and scope of the activities of the company, the sensitivity of the data, and the size and complexity of the relevant data operations of the company.

- Data Breach Notifications. Telecommunications service providers should notify customers whose CPNI has been breached when failure to notify would be unfair or deceptive. Given that breach investigations frequently are ongoing at the time providers offer notice to customers, a notice that turns out to be incomplete or inaccurate is not deceptive, as long as the provider corrects any material inaccuracies within a reasonable period of time of discovering them. Telecommunications providers have flexibility to determine how and when to provide such notice.

The FCC can ensure compliance with the above principles by pursuing reasonable enforcement actions against telecommunications service providers that have clearly violated these principles.

Privacy Framework

Draft Discussion Paper

All entities in the Internet ecosystem should be subject to a consistent privacy framework with respect to consumer information. Consumer information should be protected based upon the sensitivity of the information to the consumer and how the information is used—not the type of business keeping it, how that business obtains it, or what regulatory agency has authority over it. Consumers should have consistent and predictable privacy protections for the information they deem private and sensitive, no matter how or with whom they share it. Consumers also will benefit from a consistent privacy framework that promotes the emergence of new business models and innovative uses of data that foster increased consumer choice and service customization.

The FCC should adopt an approach to privacy and data security for CPNI that is flexible, harmonized with the well-established and successful FTC framework, and backed up by strong but fair enforcement for unfair or deceptive acts or practices (UDAP) that materially harm consumers.¹ This well-tested consumer protection approach is consistent with the FCC's privacy recommendations in the 2010 National Broadband Plan, the FTC's and White House's 2012 Privacy Reports, and the White House's 2015 Consumer Privacy Bill of Rights, as well as with Chairman Wheeler's recent testimony before Congress acknowledging the importance of coordination with the FTC and harmonization with its privacy framework.

That approach will benefit consumers by safeguarding privacy interests as it has for years and will ensure that the same privacy and security framework applies to all entities in the Internet ecosystem. By leveraging a tested privacy model, the FCC will avoid inconsistent requirements that could otherwise hamper innovation and reduce competition. Most important, it will minimize consumer confusion as well as other harms associated with disparate privacy regulation across the ecosystem. Indeed, this approach will align with consumers' expectations that their data would be subject to consistent privacy rules regardless of whether it is used by their Internet Service Provider (ISP), application developers, operating systems, or edge providers.

When adopting a framework, the FCC should keep the following guidelines in mind:

- **Consistent and Coordinated Regulatory Regimes.** The FCC's rules and principles for regulating and enforcing privacy and security should be as similar as possible to the FTC approach, which will continue to govern other Internet ecosystem players' use and disclosure of the same or similar data. The consistent application of standards across

¹ This framework is intended for discussion purposes, and we are not conceding that the FCC has authority to adopt privacy and security rules for Broadband Internet Access Services or over data related to consumers' use of Broadband Internet Access Services. To the extent it is determined that the FCC has such statutory authority, this document is intended to set forth principles for FCC consideration and possible adoption that are harmonized and consistent with the FTC and other government entities' approach to privacy and security for the same or similar data. Even if courts determine that the FCC's reclassification of Broadband Internet Access Services is a lawful exercise of authority, any rules must not exceed the text and legislative history of Section 222 of the Act.

sectors would fulfill the following key tenets in the White House Privacy Report: (1) avoid “inconsistent standards for related technologies” that could dampen innovation; (2) foster a “level playing field for companies;” and, most importantly, (3) create “a consistent set of expectations for consumers.” To achieve this end, the FCC’s policies, rules, and enforcement practices should conform to the longstanding limiting principles articulated in the FTC’s Unfairness and Deception Policy Statements. In addition, the FCC and FTC can achieve their recent MOU’s stated goal of avoiding “duplicative, redundant or inconsistent oversight” by developing a new process to ensure that their substantive privacy policies and basis for enforcement are consistent going forward.

- Flexibility. The FCC’s approach should provide a flexible framework within which telecommunications service providers can implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments in this space. Specifically, this framework should identify the privacy or security *goals*, and afford providers flexibility in achieving those goals, rather than dictate the particular *methods* by which providers are expected to achieve those goals. Adopting a flexible approach also will help ensure consistent federal and state requirements governing customer information.
- Application. Consistent with the Communications Act and to eliminate unnecessary duplication of authority with other agencies, the FCC’s framework should only apply when 1) telecommunications service providers are providing telecommunications services and 2) the CPNI is made available by the customer to the telecommunications service provider solely by virtue of the carrier-customer relationship. The framework cannot lawfully apply to:
 - Providers’ non-telecommunications services and products
 - Providers’ non-telecommunications service provider affiliates
 - Information that is not made available to the carrier by the customer solely by virtue of the carrier-customer relationship
- Individually Identifiable. The FCC should carve out from the scope of its new framework any data that is de-identified, aggregated, or does not otherwise identify a known individual. The insights derived from the use of de-identified data can offer great benefits to consumers and society and such use avoids the sensitivities that may be associated with identified data.
- Unfair or Deceptive Conduct. As noted above, the FCC’s policies, rules, and enforcement practices should conform to the FTC’s longstanding limiting principles articulated in its Policy Statements on Unfairness (1980) and Deception (1983). This approach is consistent with the FCC’s commitment to conduct a cost-benefit analysis of its regulatory framework in accordance with President Obama’s Executive Orders 13563 and 13579, which require agencies to “adopt a regulation only upon a reasoned determination its benefits justify its costs” and “tailor its regulations to impose the least burden on society.”

- Unfair Conduct. A provider acts unfairly if its act or practice (1) causes or is likely to cause substantial injury to consumers (2) which is not reasonably avoidable by consumers themselves, and (3) is not outweighed by countervailing benefits to consumers or to competition.
- Deceptive Conduct. A provider acts deceptively if (1) it makes a statement or omission, or engages in a practice, that is likely to mislead a customer, (2) viewed from the perspective of a consumer acting reasonably under the circumstances, and (3) the deceptive statement, omission, or practice is material—meaning that the misrepresentation or practice is likely to affect the consumer’s conduct or decision with regard to a product or service.
- Additional Guidance. In coordination with other privacy regulators, the FCC could, like the FTC and various states like California, provide additional guidance on how it interprets its framework through workshops or reports. The FCC also could encourage and support the development and implementation of industry guidelines.
- Update and Harmonize Existing CPNI Rules. The existing CPNI rules should be revisited in their entirety and modernized to use the same flexible framework for all services subject to Section 222, including traditional voice services. In no event should the prescriptive outdated CPNI rules designed for legacy voice services apply to broadband services. Instead, a common set of flexible policies that allow providers to keep up with their customers’ expectations and evolving technology should apply to both types of services.

With these guidelines in mind, if the courts determine that the FCC has authority to regulate broadband privacy, the FCC could adopt the following principles, which encompass and are consistent with the privacy and security framework that applies to the rest of the industry. Each of these principles and the goals noted above should provide flexibility for providers to implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments:

- Transparency. A telecommunications service provider should provide notice, which is neither deceptive nor unfair, describing the CPNI that it collects, how it will use the CPNI, and whether and for what purposes it may share CPNI with third parties.
- Respect for Context and Consumer Choice. A telecommunications service provider may use or disclose CPNI as is consistent with the context in which the customer provides, or the provider obtains, the information, provided that the provider’s actions are not unfair or deceptive. For example, the use or disclosure of CPNI for the following commonly accepted data practices would not warrant a choice mechanism, either because customer consent can be inferred or because public policy considerations make choice unnecessary: product and service fulfillment, fraud prevention, compliance with law, responses to government requests, network management, first-party marketing, and affiliate sharing where the affiliate relationship is reasonably clear to consumers. Consistent with the flexible choice mechanisms available to all other entities in the Internet ecosystem, telecommunications service providers should give consumers easy-

to-understand choices for non-contextual uses and disclosures of their CPNI, where the failure to provide choice would be deceptive or unfair. The provider should consider the sensitivity of the data and the context in which it was collected when determining the appropriate choice mechanism.

- Data Security. A telecommunications service provider should establish, implement, and maintain a CPNI data security program that is neither unfair nor deceptive and includes reasonable physical, technical, and administrative security safeguards to protect CPNI from unauthorized access, use, and disclosure. Providers' CPNI data security programs should provide reasonable protections in light of the nature and scope of the activities of the company, the sensitivity of the data, and the size and complexity of the relevant data operations of the company.
- Data Breach Notifications. Telecommunications service providers should notify customers whose CPNI has been breached when failure to notify would be unfair or deceptive. Given that breach investigations frequently are ongoing at the time providers offer notice to customers, a notice that turns out to be incomplete or inaccurate is not deceptive, as long as the provider corrects any material inaccuracies within a reasonable period of time of discovering them. Telecommunications providers have flexibility to determine how and when to provide such notice.

The FCC can ensure compliance with the above principles by pursuing reasonable enforcement actions against telecommunications service providers that have clearly violated these principles.

American Cable Association
Competitive Carriers Association
CTIA
National Cable & Telecommunications Association
U.S. Telecom Association

Dated: March 1, 2016

Joanne Wall

From: [REDACTED]
Sent: Friday, April 08, 2016 12:21 PM
To: Scott Jordan; Lisa Hone; Jennifer Tatel
Cc: Ruth Milkman
Subject: Fw: IP addresses, domain names and CPNI

(b) (5)

Thx

T

Tom Wheeler
Chairman
Federal Communications Commission
202.418.1000

From: vinton cerf
Sent: Friday, April 8, 2016 10:45 AM
To: [REDACTED]
Subject: IP addresses, domain names and CPNI

Tom,

on the surface this makes no sense to me. IP addresses are not like telephone numbers and domain names are even farther afield - unless they are personal identifiers like joeblow@info and even then they are public information - how can they possibly be CPNI?

this is what I am reacting to:

Here's a link to the docket page: https://apps.fcc.gov/edocs_public/Query.do?numberFld=16-39&numberFld2=&docket=&dateFld=&docTitleDesc=

1. *Internet Protocol (IP) Addresses and Domain Name Information.* We propose to consider both source and destination IP addresses as CPNI in the broadband context.[1] An IP address is the routable address for each device on an IP network,[2] and BIAS providers use the end user's and edge provider's IP addresses to route data traffic between them.[3] As such, IP addresses are roughly analogous to telephone numbers in the voice telephony context, and the Commission has previously held telephone numbers dialed to be CPNI.[4] Further, our CPNI rules for TRS providers recognize IP addresses as call data information.[5] IP addresses are also frequently used in geo-location.[6] As such, we believe that we should consider IP addresses to be "destination" and "location" information under Section 222(h)(1)(A).[7] Similarly, we propose to consider other information in Internet layer protocol headers to be CPNI in the broadband context, because they may indicate the "type" and "amount of use" of a telecommunication service. We seek comment on this proposed interpretation.

2. Similarly, we propose to consider the domain names with which an end user communicates CPNI in the broadband context. Domain names (e.g., "www.fcc.gov") are common monikers that the end user uses to identify the endpoint to which they seek to connect. Domain names also translate into IP addresses, which we propose to consider CPNI. We therefore propose to treat domain names as destination and location information. We seek comment on this proposed interpretation.

[1] As discussed further below, IP addresses would also fall under our proposed definition of PII. *See infra* para. 62.

[2] *See* Internet Engineering Task Force, The Internet Numbers Registry System, RFC 7020 (2013), <https://tools.ietf.org/html/rfc7020> (discussing non-reserved globally unique unicast IP addresses assigned through the Internet Numbers Registry System).

[3] *See, e.g.*, Kurose & Ross, *supra* n. 65, at 130, 331-63.

[4] *See 2007 CPNI Order*, 22 FCC Rcd at 6931, para. 5.

[5] 47 CFR § 64.5103(c).

[6] A BIAS provider is inherently capable of geo-locating an IP address; in the case of fixed broadband Internet access service, the provider knows the customer's physical address, and in the case of mobile broadband Internet access service, the provider knows the geo-location of the cell towers to which the customer's device connects and can use this to determine the customer's device location.

[7] *See* CDT White Paper.

Joanne Wall

From: [REDACTED]
Sent: Tuesday, April 12, 2016 12:56 PM
To: Scott Jordan; Jessica Almond; Jennifer Tatel; Lisa Hone
Subject: FW: IP addresses, domain names and CPNI

Thank you folks. (b) (5)

T

From: vinton cerf [mailto:(b) (6)]
Sent: Tuesday, April 12, 2016 12:54 PM
To: [REDACTED]
Subject: Re: IP addresses, domain names and CPNI

ah, that's a different interpretation (which IP addresses did the customer visit) - i see how this can be treated as CPNI. I thought the customer's IP address was the target of the policy and that's no longer very precise. The same might be said for the IP addresses the consumer visits but I can see that binding any such list to a particular subscriber seems like a privacy issue.

v

On Tue, Apr 12, 2016 at 12:46 PM, [REDACTED]@fcc.gov> wrote:

Vint –

Sorry to be slow in getting back to you. Things have been popping here.

The issue about which we are asking in the NPRM is what information should be considered CPNI (defined as info related to a telecommunications service that is made available to the carrier by the customer by virtue of the carrier-customer relationship).

The issue is not about whether an IP address or a domain name is public, but rather the confidentiality of the list of IP addresses and domain names that a customer visits. That's the telephone analogy that I use; that currently the list of telephone numbers that a customer calls is treated as CPNI. What the NPRM proposes to do is to treat the list of IP addresses and domain names that a customer visits as CPNI if a broadband ISP collects them from a customer's network traffic.

As always, I appreciate your thoughts. I hope this helps

T

From: vinton cerf [mailto:(b) (6)]
Sent: Friday, April 08, 2016 10:45 AM
To: ** **/@fcc.gov>
Subject: IP addresses, domain names and CPNI

Tom,

on the surface this makes no sense to me. IP addresses are not like telephone numbers and domain names are even farther afield - unless they are personal identifiers like joeblow@info and even then they are public information - how can they possibly be CPNI?

this is what I am reacting to:

Here's a link to the docket page: https://apps.fcc.gov/edocs_public/Query.do?numberFld=16-39&numberFld2=&docket=&dateFld=&docTitleDesc=

1. *Internet Protocol (IP) Addresses and Domain Name Information.* We propose to consider both source and destination IP addresses as CPNI in the broadband context.[1] An IP address is the routable address for each device on an IP network,[2] and BIAS providers use the end user's and edge provider's IP addresses to route data traffic between them.[3] As such, IP addresses are roughly analogous to telephone numbers in the voice telephony context, and the Commission has previously held telephone numbers dialed to be CPNI.[4] Further, our CPNI rules for TRS providers recognize IP addresses as call data information.[5] IP addresses are also frequently used in geo-location.[6] As such, we believe that we should consider IP addresses to be "destination" and "location" information under Section 222(h)(1)(A).[7] Similarly, we propose to consider other information in Internet layer protocol headers to be CPNI in the broadband context, because they may indicate the "type" and "amount of use" of a telecommunication service. We seek comment on this proposed interpretation.

2. Similarly, we propose to consider the domain names with which an end user communicates CPNI in the broadband context. Domain names (e.g., "www.fcc.gov") are common monikers that the end user uses to identify the endpoint to which they seek to connect. Domain names also translate into IP addresses, which we propose to consider CPNI. We therefore propose to treat domain names as destination and location information. We seek comment on this proposed interpretation.

[1] As discussed further below, IP addresses would also fall under our proposed definition of PII. *See infra* para. 62.

[2] *See* Internet Engineering Task Force, The Internet Numbers Registry System, RFC 7020 (2013), <https://tools.ietf.org/html/rfc7020> (discussing non-reserved globally unique unicast IP addresses assigned through the Internet Numbers Registry System).

[3] *See, e.g.,* Kurose & Ross, *supra* n. 65, at 130, 331-63.

[4] *See* 2007 CPNI Order, 22 FCC Rcd at 6931, para. 5.

[5] 47 CFR § 64.5103(c).

[6] A BIAS provider is inherently capable of geo-locating an IP address; in the case of fixed broadband Internet access service, the provider knows the customer's physical address, and in the case of mobile broadband Internet access service, the provider knows the geo-location of the cell towers to which the customer's device connects and can use this to determine the customer's device location.

[7] *See* CDT White Paper.

Joanne Wall

From: **
Sent: Tuesday, April 12, 2016 12:48 PM
To: Scott Jordan; Lisa Hone; Jennifer Tatel; Jessica Almond
Subject: FW: IP addresses, domain names and CPNI

Thanks for your help

T

From: **
Sent: Tuesday, April 12, 2016 12:47 PM
To: 'vinton cerf'
Subject: RE: IP addresses, domain names and CPNI

Vint –

Sorry to be slow in getting back to you. Things have been popping here.

The issue about which we are asking in the NPRM is what information should be considered CPNI (defined as info related to a telecommunications service that is made available to the carrier by the customer by virtue of the carrier-customer relationship).

The issue is not about whether an IP address or a domain name is public, but rather the confidentiality of the list of IP addresses and domain names that a customer visits. That's the telephone analogy that I use; that currently the list of telephone numbers that a customer calls is treated as CPNI. What the NPRM proposes to do is to treat the list of IP addresses and domain names that a customer visits as CPNI if a broadband ISP collects them from a customer's network traffic.

As always, I appreciate your thoughts. I hope this helps

T

From: vinton cerf [mailto:(b) (6)]
Sent: Friday, April 08, 2016 10:45 AM
To: ** * **@fcc.gov>
Subject: IP addresses, domain names and CPNI

Tom,

on the surface this makes no sense to me. IP addresses are not like telephone numbers and domain names are even farther afield - unless they are personal identifiers like joeblow@info and even then they are public information - how can they possibly be CPNI?

this is what I am reacting to:

Here's a link to the docket page: https://apps.fcc.gov/edocs_public/Query.do?numberFld=16-39&numberFld2=&docket=&dateFld=&docTitleDesc=

1. *Internet Protocol (IP) Addresses and Domain Name Information.* We propose to consider both source and destination IP addresses as CPNI in the broadband context.^[1] An IP address is the routable address for each device on an IP network,^[2] and BIAS providers use the end user's and edge provider's IP addresses to route data traffic between them.^[3] As such, IP addresses are roughly analogous to telephone numbers in the voice telephony context, and the Commission has previously held telephone numbers dialed to be CPNI.^[4] Further, our CPNI rules for TRS providers recognize IP addresses as call data information.^[5] IP addresses are also frequently used in geo-location.^[6] As such, we believe that we should consider IP addresses to be "destination" and "location" information under Section 222(h)(1)(A).^[7] Similarly, we propose to consider other information in Internet layer protocol headers to be CPNI in the broadband context, because they may indicate the "type" and "amount of use" of a telecommunication service. We seek comment on this proposed interpretation.

2. Similarly, we propose to consider the domain names with which an end user communicates CPNI in the broadband context. Domain names (e.g., "www.fcc.gov") are common monikers that the end user uses to identify the endpoint to which they seek to connect. Domain names also translate into IP addresses, which we propose to consider CPNI. We therefore propose to treat domain names as destination and location information. We seek comment on this proposed interpretation.

[1] As discussed further below, IP addresses would also fall under our proposed definition of PII. *See infra* para. 62.

[2] *See* Internet Engineering Task Force, The Internet Numbers Registry System, RFC 7020 (2013), <https://tools.ietf.org/html/rfc7020> (discussing non-reserved globally unique unicast IP addresses assigned through the Internet Numbers Registry System).

[3] *See, e.g.,* Kurose & Ross, *supra* n. 65, at 130, 331-63.

[4] *See* 2007 CPNI Order, 22 FCC Rcd at 6931, para. 5.

[5] 47 CFR § 64.5103(c).

[6] A BIAS provider is inherently capable of geo-locating an IP address; in the case of fixed broadband Internet access service, the provider knows the customer's physical address, and in the case of mobile broadband Internet access service, the provider knows the geo-location of the cell towers to which the customer's device connects and can use this to determine the customer's device location.

[7] *See* CDT White Paper.

Joanne Wall

From: Grillo, Kathleen M <kathleen.m.grillo@verizon.com>
Sent: Wednesday, April 06, 2016 4:44 PM
To: Kim Mattos; Ruth Milkman; Jennifer Tatel
Cc: McClure, Lynn B
Subject: RE: Verizon meeting on privacy

That's great. Thanks.

verizon

Kathleen Grillo
Senior Vice President
Public Policy and Government Affairs

1300 I Street, NW, Suite 400W
Washington, DC 20005

O 202.515.2533
kathleen.m.grillo@verizon.com



From: Kim Mattos [<mailto:Kim.Mattos@fcc.gov>]
Sent: Wednesday, April 06, 2016 3:57 PM
To: Ruth Milkman; Grillo, Kathleen M; Jennifer Tatel
Cc: McClure, Lynn B
Subject: [E] RE: Verizon meeting on privacy

Got it.
Hi Lynn: I'll propose times in a bit. -k

From: Ruth Milkman
Sent: Wednesday, April 06, 2016 3:54 PM
To: Grillo, Kathleen M <kathleen.m.grillo@verizon.com>; Kim Mattos <Kim.Mattos@fcc.gov>; Jennifer Tatel <Jennifer.Tatel@fcc.gov>
Cc: McClure, Lynn B <lynn.b.mcclure@verizon.com>
Subject: Re: Verizon meeting on privacy

Thanks Kathy. Kim -- Let's schedule for 45 minutes if that works for the Verizon folks -- we may not need that much time but let's allow for it.

From: Grillo, Kathleen M
Sent: Wednesday, April 6, 2016 3:50 PM
To: Kim Mattos
Cc: Ruth Milkman; McClure, Lynn B
Subject: Verizon meeting on privacy

Kim –

Ruth and I talked yesterday and we would like to schedule a meeting on the privacy NPRM. Attendees on our side would be me, Will Johnson and Karen Zacharia. Ruth mentioned that she would like Jennifer Tatel to attend as well.

I am copying Lynn McClure, who can help with the scheduling on our end.

If possible and if schedules permit, we would like to do this next week because Karen Zacharia and I will both be out of the office from April 18 through April 29.

Thanks very much.

verizon

Kathleen Grillo
Senior Vice President
Public Policy and Government Affairs

1300 I Street, NW, Suite 400W
Washington, DC 20005

O 202.515.2533
kathleen.m.grillo@verizon.com

in

Joanne Wall

From: Jennifer Tatel
Sent: Monday, April 27, 2015 4:24 PM
To: Lisa Hone
Subject: FW: Reporting of telecom data to CRAs

Could you please do this call with me if I schedule it for some time on Wednesday?

From: Kelly, Elizabeth [mailto:Elizabeth_A_Kelly@epic.org] (b)
Sent: Monday, April 27, 2015 10:28 AM
To: Jennifer Tatel
Subject: RE: Reporting of telecom data to CRAs

Jennifer,

Just wanted to follow up and see if you'd have to time to touch base sometime this week about credit reporting of telecom data. My schedule is flexible anytime today, and tomorrow before 2 pm.

Thanks,
Elizabeth

From: Kelly, Elizabeth
Sent: Thursday, April 23, 2015 3:10 PM
To: 'Jennifer.Tatel@fcc.gov'
Subject: Reporting of telecom data to CRAs

Jennifer,

Following up on Ruth and David's conversation, wanted to see if we could connect to discuss perceived barriers to reporting of telecom data to the credit reporting agencies. Would you be free for a quick call on either Monday or Wednesday? My schedule is wide open both days.

Please let me know when would work best for you, and look forward to speaking with you.

Thanks,
Elizabeth

Elizabeth Kelly
Senior Policy Advisor
National Economic Council
ekelly (b) (6)

Joanne Wall

From: Jennifer Tatel
Sent: Thursday, May 14, 2015 9:16 AM
To: 'Kelly, Elizabeth'
Subject: RE: Reporting of telecom data to CRAs

Please call my office at 202.418.1817. Lisa Hone from our Wireline Competition Bureau will join me.

Thanks,
Jennifer

From: Kelly, Elizabeth [mailto:Elizabeth_A_Kelly@fcc.gov] (b) (6)
Sent: Wednesday, May 13, 2015 5:59 PM
To: Jennifer Tatel
Subject: RE: Reporting of telecom data to CRAs

Sorry, meant what number should I call?

From: Kelly, Elizabeth
Sent: Wednesday, May 13, 2015 5:59 PM
To: 'Jennifer Tatel'
Subject: RE: Reporting of telecom data to CRAs

10 am tomorrow works great. What time is best?

From: Jennifer Tatel [mailto:Jennifer.Tatel@fcc.gov]
Sent: Wednesday, May 13, 2015 8:45 AM
To: Kelly, Elizabeth
Subject: RE: Reporting of telecom data to CRAs

Hi Elizabeth. How does 10am tomorrow work for you?

Thanks,
Jennifer

From: Kelly, Elizabeth [mailto:Elizabeth_A_Kelly@fcc.gov] (b) (6)
Sent: Tuesday, May 12, 2015 4:54 PM
To: Jennifer Tatel
Subject: Reporting of telecom data to CRAs

Jennifer,

Is there a time this week that would work for us to discuss perceived barriers to reporting of telecom data to the credit reporting agencies? Please let me know if any of the following times would work for you:

- Wednesday, May 13: after 4 pm
- Thursday, May 14: 9-11 am
- Friday, May 15: 9 am – 2.30 pm

Thanks,
Elizabeth

From: Kelly, Elizabeth
Sent: Tuesday, May 05, 2015 11:46 AM
To: 'Jennifer Tatel'
Subject: RE: Reporting of telecom data to CRAs

Jennifer,

Just wanted to circle back about finding a time to talk. I'm free this afternoon except for 2 to 2.30 pm, or Friday before 11 am, or after 12.30 pm if any of those windows work for you.

Thanks,
Elizabeth

From: Kelly, Elizabeth
Sent: Thursday, April 30, 2015 12:10 PM
To: 'Jennifer Tatel'
Subject: RE: Reporting of telecom data to CRAs

Jennifer,

No worries. Tomorrow is bad, but I'm free from 9-9.30 am, or 1-1.30 pm. Tuesday is also relatively wide open if that works better.

Let me know, and look forward to speaking with you.

Thanks,
Elizabeth

From: Jennifer Tatel [<mailto:Jennifer.Tatel@fcc.gov>]
Sent: Thursday, April 30, 2015 9:00 AM
To: Kelly, Elizabeth
Subject: RE: Reporting of telecom data to CRAs

Elizabeth, with apologies, today no longer works for us. I'm sorry this has been so hard to schedule. Do you have any time tomorrow?

From: Kelly, Elizabeth [<mailto:Elizabeth.A.Kelly@fcc.gov>] (b) (6)
Sent: Wednesday, April 29, 2015 5:51 PM
To: Jennifer Tatel
Subject: RE: Reporting of telecom data to CRAs

That sounds great. Would a call be easiest? If so, what's the best number for you?

From: Jennifer Tatel [<mailto:Jennifer.Tatel@fcc.gov>]
Sent: Wednesday, April 29, 2015 4:26 PM
To: Kelly, Elizabeth
Subject: RE: Reporting of telecom data to CRAs

How about 10:30 tomorrow morning?

From: Kelly, Elizabeth [mailto:Elizabeth.A.Kelly@fcc.gov] (b) (6)
Sent: Tuesday, April 28, 2015 8:27 PM
To: Jennifer Tatel
Subject: RE: Reporting of telecom data to CRAs

Jennifer,

Unfortunately, tomorrow is bad. How does Thursday look for you? I'm free before 11 am or after 5 pm. Alternately, I could do Friday 12-2, or 3-5.

Let me know when is best, and look forward to speaking with you.

Thanks,
Elizabeth

From: Jennifer Tatel [mailto:Jennifer.Tatel@fcc.gov]
Sent: Tuesday, April 28, 2015 9:02 AM
To: Kelly, Elizabeth
Subject: RE: Reporting of telecom data to CRAs

Hi Elizabeth. Apologies for my delay in responding. We are hosting a privacy workshop today, so today is not a good day for a call. Do you have time tomorrow? I could do a call at 1:00pm.

Thanks,
Jennifer

From: Kelly, Elizabeth [mailto:Elizabeth.A.Kelly@fcc.gov] (b) (6)
Sent: Monday, April 27, 2015 10:28 AM
To: Jennifer Tatel
Subject: RE: Reporting of telecom data to CRAs

Jennifer,

Just wanted to follow up and see if you'd have to time to touch base sometime this week about credit reporting of telecom data. My schedule is flexible anytime today, and tomorrow before 2 pm.

Thanks,
Elizabeth

From: Kelly, Elizabeth
Sent: Thursday, April 23, 2015 3:10 PM
To: 'Jennifer.Tatel@fcc.gov'
Subject: Reporting of telecom data to CRAs

Jennifer,

Following up on Ruth and David's conversation, wanted to see if we could connect to discuss perceived barriers to reporting of telecom data to the credit reporting agencies. Would you be free for a quick call on either Monday or Wednesday? My schedule is wide open both days.

Please let me know when would work best for you, and look forward to speaking with you.

Thanks,
Elizabeth

Elizabeth Kelly
Senior Policy Advisor
National Economic Council
[\(b\) \(6\)](mailto:ekelly@b(6))

Kim Mattos

Subject: Meeting with Verizon re. Privacy NPRM (RM) JT,MDN (rescheduled from 4/13)
Location: conf. room #1

Start: Thu 4/14/2016 10:00 AM
End: Thu 4/14/2016 10:45 AM

Recurrence: (none)

Meeting Status: Meeting organizer

Organizer: Kim Mattos
Required Attendees: Ruth Milkman; Jennifer Tatel; Matthew DelNero

4/8-

Hi Ruth:

We've moved Verizon meeting to Thursday (4/14) so that John Frantz, general counsel of new products/business could attend. At your request, Matt has been invited. Thank you. -k

===

4/7

Hi Ruth: per your request. Thank you. -k

Meeting attendees:

Kathleen Grillo, Will Johnson, and Karen Zacharia

PoC:

Lynn McClure

Executive Assistant to Kathy Grillo

O 202-515-2570 | M 703-304-3184

lynn.b.mcclure@verizon.com

Kim Mattos

Subject: Meeting with Verizon (RM) MDN,JT,LH
Location: conf. room #1

Start: Thu 5/5/2016 10:00 AM
End: Thu 5/5/2016 10:30 AM

Recurrence: (none)

Meeting Status: Meeting organizer

Organizer: Kim Mattos
Required Attendees: Ruth Milkman (Ruth.Milkman@fcc.gov); Matthew DelNero; Jennifer Tatal; Lisa Hone
Optional Attendees: Natividad Persaud

5/4-

Updated to add three others, who will also be joining Will. Thank you. -k
Karen Zacharia, Mike Berg, and Maggie McCready

==

4/26-

Dear all:

Per Ruth's request. Thank you. -k

Meeting attendees: tbd

From: Johnson, William H [<mailto:will.h.johnson@verizon.com>]

Sent: Friday, April 22, 2016 6:11 PM

To: Matthew DelNero <Matthew.DelNero@fcc.gov>

Subject: Scheduling

Following up on days that would work for the first meeting we discussed (deeper dive on our programs and practices). The days that work best for us are May 4-6, 11 or 12. Any of those work for you guys?

Will

<image001.png>

William H. Johnson

Senior Vice President, Federal Regulatory & Legal Affairs

Verizon

1300 I St. NW, Suite 400 West

Washington, DC 20005

will.h.johnson@verizon.com

t: (202) 515-2492

c: (202) 805-4321

Robin Colwell

From: Scott Bergmann <SBergmann@ctia.org>
Sent: Tuesday, May 10, 2016 7:15 PM
To: Erin McGrath; Amy Bender; Robin Colwell
Subject: Association Privacy Letter to Judiciary Committee
Attachments: Subcommittee Privacy Letter 5.10.16.pdf

Erin, Amy, Robin,

Just wanted to share with you this multi-association letter that was sent today to the Chair and Ranking Member of the Judiciary Committee's Subcommittee on Privacy, Technology, and the Law. The letter expresses support for a reasonable framework that adheres in all material respects to the successful FTC model that protected the privacy of broadband consumers for years, and applied uniformly to all entities in the broadband ecosystem.

Please let me know if you have any questions. Best,

Scott

Scott Bergmann
Vice President, Regulatory Affairs
1400 16th Street, NW
Washington, DC 20036
202-736-3660 (office)
202-997-3916 (mobile)
sbergmann@ctia.org

Mike Orielly

From: Follansbee, Lynn <lfollansbee@ustelecom.org>
Sent: Tuesday, March 01, 2016 2:21 PM
To: Tom Wheeler; Mignon Clyburn; Jessica Rosenworcel; Ajit Pai; Mike Orielly
Cc: Stephanie Weiner; Louisa Terrell
Subject: Industry Framework Discussion Paper
Attachments: Wheeler Letter Re Privacy Principles 3 1 16.pdf

Chairman Wheeler and Fellow Commissioners;

Please see the attached correspondence.

Thank you,

B. Lynn Follansbee
Vice President, Law & Policy
USTelecom
607 14th Street NW
Suite 400
Washington, DC 20005
Tel: 202-326-7256
Email: lfollansbee@ustelecom.org



Mike Orielly

From: Scott Bergmann <Sbergmann@ctia.org>
Sent: Thursday, August 13, 2015 10:15 AM
To: Mike Orielly
Subject: "Washington Goes Mobile" Agenda at CITA Super Mobility 2015
Attachments: Washington Goes Mobile Agenda.pdf

CTIA
Super Mobility 2015
in partnership with  Microsoft



SEPTEMBER 9 • 10 • 11 | LAS VEGAS | SANDS EXPO

Washington Goes Mobile

We are looking forward to seeing you at CTIA's Washington Goes Mobile regulatory program, which will take place at Super Mobility 2015 at the Sands Expos & Convention Center in Las Vegas, NV on September 9-11, 2015. Attached you will find details on the Washington Goes Mobile agenda, from the CTIA Regulatory Affairs Team. The **attached agenda** provides information on the full schedule of keynotes, policy panels, and social events. Our events kick off on Tuesday evening, September 8th with a welcome reception hosted by Wilkinson Barker Knauer, and the Super Mobility show officially begins on Wednesday, September 9th at 9:00 AM with keynotes on the hottest innovations, best ideas, and toughest challenges in mobile today, featuring Meredith Attwell Baker, CTIA's President and CEO; Tom Wheeler, Chairman of the FCC; and industry leaders from Bluegrass Cellular and Sprint. The packed Washington Goes Mobile agenda for Wednesday includes panels on spectrum, net neutrality, accessibility, cybersecurity, privacy and wireless policy with the FCC Commissioners' Legal Advisors.

On Thursday, September 10th, we will kick off the day with a 9:00 AM keynote featuring industry titans from AT&T, iHeartMedia, and Verizon. Thursday's agenda is loaded with policy panels and engaging speakers, including a lively conversation between Meredith Attwell Baker and the FCC Commissioners, as well as sessions focused on privacy and the 600 MHz Incentive Auction. We will celebrate on Thursday evening with a cocktail reception hosted by Wiley Rein at the Palazzo. The Washington Goes Mobile regulatory program culminates with a special Federal-State Regulatory Dinner sponsored by Samsung and held at Buddy V's in the Grand Canal Shoppes. RSVP is required and can be sent to Emma Prieskorn at

EPrieskorn@CTIA.org. Super Mobility 2015 concludes on Friday morning, September 11th, with keynotes featuring Under Armour and other industry leaders.

We look forward to your participation in this year's Washington Goes Mobile program. If you have any questions, please do not hesitate to contact any member of the Regulatory Affairs team at 202.736.3216 or CTIARegulatoryPolicy@ctia.org.

The CTIA Regulatory Affairs Team

Scott Bergmann, Vice President
Matt Gerst, Director
Brian Josef, Assistant Vice President
Emma Prieskorn, Coordinator
Kara Romagnino, Director
Krista Witanowski, Assistant Vice President

CTIA Super Mobility 2015 Strategic Partners:



This email was sent by CTIA-The Wireless Association, located at 1400 16th Street, NW, Suite 600, Washington, DC 20036 (United States). To receive no further emails, please [click here](#) or reply to this email with "unlist" in the Subject line.

Mike O'Rielly

From: Follansbee, Lynn <lfollansbee@ustelecom.org>
Sent: Tuesday, March 01, 2016 2:21 PM
To: Tom Wheeler; Mignon Clyburn; Jessica Rosenworcel; Ajit Pai; Mike O'Rielly
Cc: Stephanie Weiner; Louisa Terrell
Subject: Industry Framework Discussion Paper
Attachments: Wheeler Letter Re Privacy Principles 3 1 16.pdf

Chairman Wheeler and Fellow Commissioners;

Please see the attached correspondence.

Thank you,

B. Lynn Follansbee
Vice President, Law & Policy
USTelecom
607 14th Street NW
Suite 400
Washington, DC 20005
Tel: 202-326-7256
Email: lfollansbee@ustelecom.org



Mike ORIelly

From: Debbie Matties <dmatties=ctia.org@mail64.suw11.mcdlv.net> on behalf of Debbie Matties <dmatties@ctia.org>
Sent: Friday, December 18, 2015 4:32 PM
To: Mike ORIelly
Subject: ✨Happy New Year and News You Can Use from CTIA Privacy ✨



Dear Friends,

Happy New Year! In an effort to help you relax with family and friends over the holidays, CTIA's Privacy Department brings you all the privacy news you'll need for the rest of the year. We hope you enjoy the holiday season and wish you all the best in 2016!

Warm regards,
Debbie

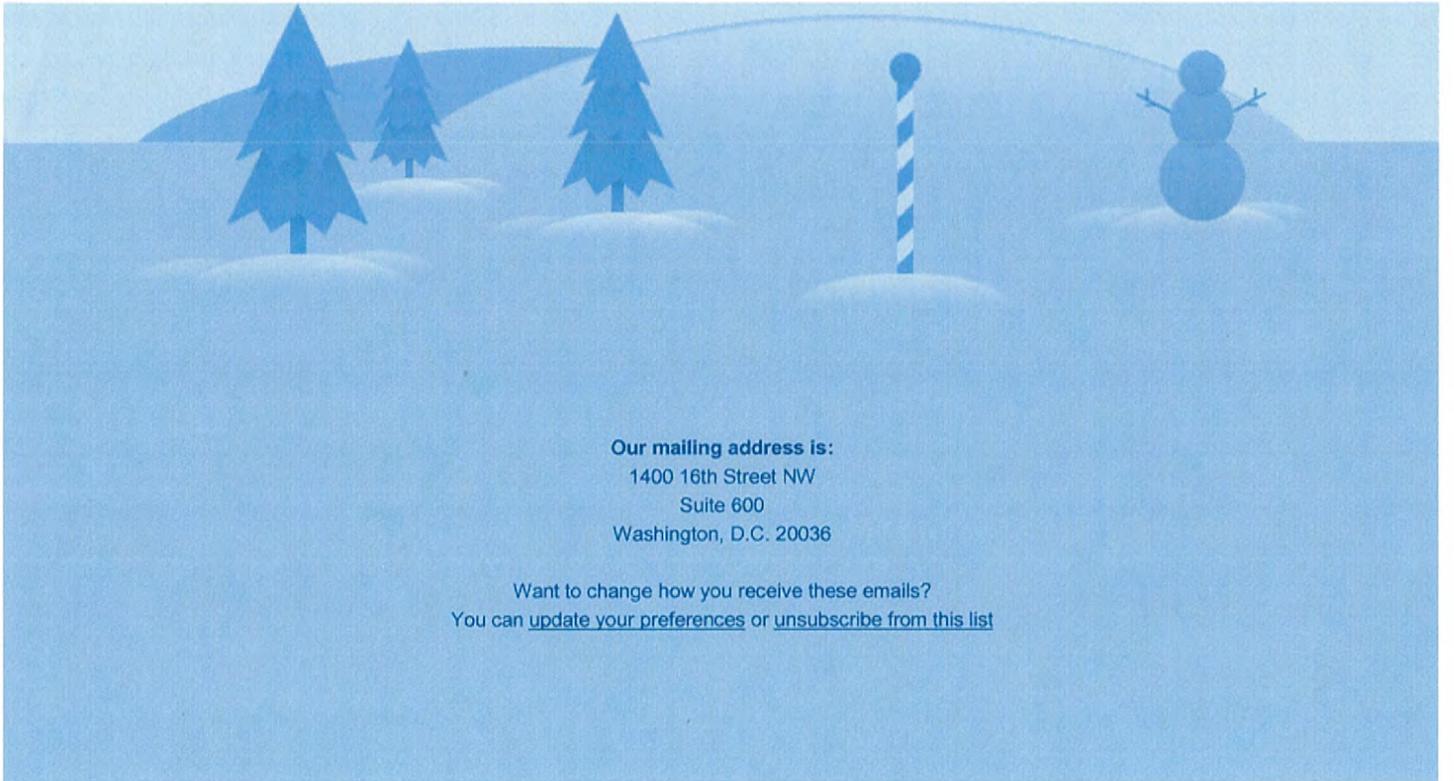
@CTIA_Privacy: North Pole Analytics unveils “Naughty or Nice” API for iOS and Android; misbehaving children decry the lack of opt out choice #HeKnowsWhenYoureSleeping #HeKnowsWhenYoureAwake

@CTIA_Privacy: Reindeer-owned startup launches “KringleKopter” gift-delivery drone service; Santa looks forward to enjoying quality time with Mrs. Claus #HomeFortheHolidays

@CTIA_Privacy: Klaus Ventures leads Series A round for “KringleKopter”, touting company’s widely-praised “privacy by design” high-res camera for navigating narrow chimneys; industry and privacy advocates share rare “Christmas Truce” #ItCouldHappen

@CTIA_Privacy: Report: Mobile users value privacy more after the holidays; cite distant relatives in-depth knowledge of their social media accounts as a determinant #AdjustPrivacySettings

@CTIA_Privacy: CTIA Privacy Working Group adds new “Holiday Privacy Subcommittee” to address unsolicited holiday greeting emails #SorryNotSorry



Our mailing address is:

1400 16th Street NW
Suite 600
Washington, D.C. 20036

Want to change how you receive these emails?
You can [update your preferences](#) or [unsubscribe from this list](#)

This email was sent to Mike.Orielly@fcc.gov
[why did I get this?](#) [unsubscribe from this list](#) [update subscription preferences](#)
CTIA · 1400 16th Street NW · Suite 600 · Washington, DC 20036 · USA



Mike ORIelly

From: CTIA Super Mobility 2016 <conventions@conventions.ctia.org>
Sent: Wednesday, May 18, 2016 11:34 AM
To: Mike ORIelly
Subject: CTIA Awards Call for Entries

Enter to win a CTIA Award today.

ctia Super
Mobility 2016™

September 7, 8 & 9, 2016
Sands Expo | Las Vegas, NV

Attend | Exhibit | Connect



Go ahead, grab the limelight

You're pushing the wireless landscape forward with your cutting-edge, emerging mobile services, solutions and network technology. Every year, **CTIA Emerging Technology Awards (E-Techs)** celebrate innovations like yours—and this year we want to recognize you.

For the 10th year, a select few will be given one of the industry's highest honors by a panel of experts, media and analysts and celebrated at the awards ceremony at **CTIA Super Mobility 2016**. And you don't have to win to get noticed. All entrants will have the opportunity to feature their products in the awards showcase at the event.



Enter by June 20 at 11:59 PM ET
for the 10th Annual 2016 CTIA E-Tech Awards.

Enter the 2016 CTIA E-Tech Awards in one of these categories

Everything Intelligent: celebrating the latest outstanding network developments

Everything Industrial + Enterprise: recognizing excellence in mobile business, software, device management, security, privacy and innovations driving smart cities and industrial connectivity.

Everything Smart: honoring mobile tech that connects consumers with state-of-the-art content, wearables, CE gadgets and accessories

Everything Government: highlighting commitment to wireless innovation in government

Everything Good: showcasing mobile tech that is making a difference in society

> SUBMIT ENTRY

Don't miss seeing the winning products in person.
Register NOW for CTIA Super Mobility 2016 to take
advantage of Early Bird pricing!



THIS EMAIL WAS SENT BY:

CTIA® 1400 16th Street, NW Suite 600 Washington, DC 20036

You have opted-in to receive information about the CTIA® shows, their exhibitors and partners.

Click to [unsubscribe](#).

Susan Fisenne

From: Berkowitz, Ann D (Ann) <aberkowitz@verizon.com>
Sent: Monday, March 14, 2016 8:59 AM
To: Susan Fisenne
Subject: VZ/O'Rielly Mtg re: Privacy

Hi Susan –

I would like to request a meeting with the Commissioner to discuss the upcoming privacy item. The Verizon attendees will be Will Johnson, Senior Vice President-Regulatory Affairs, and Karen Zacharia, Chief Privacy Officer. I'm requesting the meeting be scheduled any time prior to sunshine on 3/24. Thanks and please let me know if you have any questions.

Ann

verizon^v

Ann D. Berkowitz
Federal Regulatory Affairs
(202) 515-2539 (O)
(202) 669-5585 (C)

Susan Fisenne

From: Scott Bergmann <SBergmann@ctia.org>
Sent: Tuesday, August 18, 2015 12:51 PM
To: Susan Fisenne
Cc: Krista Witanowski; Emma Prieskorn; Brian Josef; Erin McGrath
Subject: CTIA Super Mobility Logistics for "Washington Goes Mobile"
Attachments: Washington Goes Mobile Agenda.pdf

Dear Commissioner O'Rielly and Susan,

CTIA Super Mobility 2015 is quickly approaching and we are looking forward to your participation. As we begin the countdown, we wanted to touch base with your team about a few details.

Panel Questions: We will be sending the questions for the "Washington Talks Wireless with Meredith Attwell Baker and FCC Commissioner's" panel the week of August 24th. As a reminder, the panel will take place on Thursday, September 10th from 2:00-3:00pm.

Regulatory Dinner Sponsored by Samsung: Don't forget to send in your RSVP to Emma Prieskorn (EPrieskorn@ctia.org) for the closing "Washington Goes Mobile" dinner. As a reminder, it will be held on Thursday, September 10th at 7:00pm at Buddy V's.

Show Floor Tours: We would be happy to schedule a private tour for Commissioner O'Rielly. If he is interested in a tour, we have a slot available at 12:00pm on Wednesday, September 9th or on Thursday, September 10th we have slots available at 11:00am or 12:00pm. Please let us know what works best for the Commissioner's schedule.

We have attached the most recent "Washington Goes Mobile" agenda, as well as a [promotional video](#) that highlights the policy track at the show. As always, please do not hesitate to contact any member of our team as you finalize your plans for the Show.

Scott and The Regulatory Affairs Team

Scott K. Bergmann
Vice President, Regulatory Affairs
CTIA – The Wireless Association®
Expanding the Wireless Frontier
1400 16th Street, NW Suite 600
Washington, DC 20036
www.ctia.org
Direct: 202.736.3660 Main: 202.785.0081
Mobile: 202.997.3916 Fax: 202.736.3685
Twitter: CTIASbergmann

Susan Fisenne

From: Scott Bergmann <SBergmann@ctia.org>
Sent: Monday, August 24, 2015 5:11 PM
To: Erin McGrath; Susan Fisenne
Cc: Krista Witanowski; Emma Prieskorn
Subject: CTIA Super Mobility Week – Commissioner Panel Questions and Speaker Release Form
Attachments: SM2015 Questions for Commissioner Panel.pdf; Speaker Release Form 2015.docx

Hi Erin and Susan,

I hope this finds you well. As mentioned, we are very excited that Commissioner O’Rielly will be joining us at Super Mobility 2015 and participating on the policy panel with his fellow Commissioners and CTIA President and CEO Meredith Attwell Baker on Thursday, September 10 from 2-3 p.m. at the Sands Expo and Convention Center, Venetian Ballroom.

To help you prepare for the panel, we are enclosing a list of questions that Meredith plans to ask of the Commissioner and his colleagues. As with last year’s panel, we have endeavored to create a lively format that will be both fun and easy for the Commissioners’ participation. The attached document describes the Q&A format and provides the planned questions. Of course, please let us know if you have any questions about the format or substance of the panel.

Additionally, we’re also attaching a Speaker Release Form for the Commissioner’s signature. If you could return a signed copy to us at your convenience, that would be appreciated.

As always, please let us know if you have any questions. We look forward to seeing you in September!

Many thanks,

Scott

Scott K. Bergmann
Vice President, Regulatory Affairs
CTIA – The Wireless Association®
Expanding the Wireless Frontier
1400 16th Street, NW Suite 600
Washington, DC 20036
www.ctia.org
Direct: 202.736.3660 Main: 202.785.0081
Mobile: 202.997.3916 Fax: 202.736.3685
Twitter: CTIASbergmann

CTIA
Super Mobility 2015
in partnership with  Microsoft

September 9, 10 & 11, Las Vegas, Sands Expo
CTIASuperMobility2015.com

It is CTIA’s policy to comply fully with the antitrust laws. To ensure compliance, CTIA’s employees and the representatives of CTIA member companies should follow this Checklist of antitrust “Do’s” and “Don’ts” when participating in CTIA-sponsored activities: http://files.ctia.org/pdf/Antitrust_Checklist_for_CTIA_Meetings.pdf.

Washington Talks Wireless with Meredith Attwell Baker & FCC Commissioners

Thursday, September 10, 2015 – 2:00 PM - 3:00 PM

Location: Sands Expo and Convention Center, Venetian Ballroom

CTIA President and CEO Meredith Attwell Baker sits down with FCC Commissioners to discuss a range of wireless policy issues, including the upcoming 600 MHz Broadcast Incentive Auction, Open Internet regulations and more. Panelists offer insights on how best to ensure the continued growth of and investment in the nation's mobile ecosystem.

Moderator: Meredith Attwell Baker, President & CEO, CTIA

Panelist: Mignon Clyburn, Commissioner, FCC

Panelist: Jessica Rosenworcel, Commissioner, FCC (invited)

Panelist: Ajit Pai, Commissioner, FCC

Panelist: Michael O'Rielly, Commissioner, FCC



Participants and Equipment:

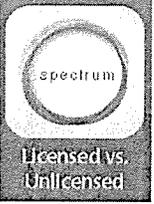
- 4 FCC Commissioners, 1 Moderator, 1 Electronic Board, and 12 Category App Icons

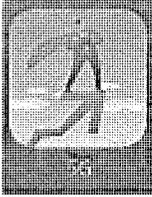
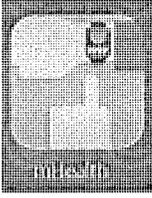
Order of Participants:

- The person with the longest FCC tenure (Commissioner Clyburn) selects a Category App Icon first.

Format:

- The first Commissioner (Commissioner Clyburn) selects a Category App Icon from the electronic board. [Note: The Commissioners will not need to physically select an icon from the board. Our IT folks will handle the electronic components].
- The Category App Icon shows the topic on which the question will be based. For example, if the "mHEALTH" Category App Icon is selected, Meredith will ask the question below about mHealth.
- The question will appear on the electronic board and will be read aloud by Meredith.
- The first asking Commissioner answers the question.
- Any other Commissioner who would like to answer may do so.
- After all Commissioners who want to answer the first question have done so, the second Commissioner in terms of tenure (Commissioner Rosenworcel (invited)) will select a Category App Icon.
- The discussion continues as described above until all questions are answered or time is up.

CATEGORY APP ICON	QUESTION
	<p>600 MHZ AUCTION: We are six months away from the scheduled start of the 600 MHz auction. In your mind, what are the one or two things that still need to happen for a successful auction?</p>
	<p>LIFELINE: 88% of eligible low-income Lifeline subscribers select wireless options today. How can the FCC make sure a modernized Lifeline program continues to reflect low-income consumers' preference for mobile solutions?</p>
	<p>MOBILE VIDEO: Mobile video accounted for 60% of all mobile data traffic at the end of last year, and is projected to grow nearly nine times by the end of the decade. How do you see the marketplace adapting to this shift in consumer behavior?</p>
	<p>LICENSED VS. UNLICENSED: CTIA is a strong advocate for making both licensed and unlicensed spectrum available. How can we best work together to ensure all spectrum users have access to all types of spectrum?</p>
	<p>INFRASTRUCTURE: The Commission has taken a number of important steps to help facilitate wireless siting across the country. As we see the proliferation of more small cell solutions, what else can the government do to promote more mobile broadband deployment?</p>
	<p>MORE SPECTRUM: We need 350 MHz of new licensed spectrum by 2020. What can the FCC do to help re-fill the spectrum pipeline after the 600 MHz auction and shorten the 13 years it takes to re-allocate spectrum?</p>

	<p>5G: The U.S. is the global leader in 4G. What steps can the FCC take to help ensure we retain our lead in 5G?</p>
	<p>mHEALTH: By the end of this year, mHealth could deliver up to \$290 billion in annual healthcare cost savings worldwide. What are biggest challenges to broader mHealth adoption and what role does spectrum play?</p>
	<p>HIGH BAND: As technology improves, more spectrum becomes available for mobile broadband use, including very high band spectrum. New technologies will require a mix of spectrum bands, how do we best preserve that balance?</p>
	<p>COMPETITION: Consumers benefit from the choice of four national wireless operators and multiple resellers and regional providers. How does that high degree of competition factor into your approach to wireless regulation?</p>
	<p>WHAT'S NEXT? You have executives in your office every day pitching what's next. In your mind, what is the next regulatory issues or challenge we don't spend enough time on today and that we should?</p>
	<p>PRIVACY: This fall, the FCC will be releasing an item to address broadband privacy as a result of the Open Internet Order. How do we best safeguard consumers' privacy, end regulatory uncertainty, and not end up with conflicting FTC/FCC mandates setting different rules for different players in our ecosystem?</p>

CTIA Super Mobility 2015

In partnership with  Microsoft



SEPTEMBER 9 • 10 • 11 | LAS VEGAS | SANDS EXPO

Washington Goes Mobile

We are looking forward to seeing you at CTIA's Washington Goes Mobile regulatory program, which will take place at Super Mobility 2015 at the Sands Expos & Convention Center in Las Vegas, NV on September 9-11, 2015. Attached you will find details on the Washington Goes Mobile agenda, from the CTIA Regulatory Affairs Team. The agenda provides information on the full schedule of keynotes, policy panels, and social events. Our events kick off on Tuesday evening, September 8th with a welcome reception hosted by Wilkinson Barker Knauer, and the Super Mobility show officially begins on Wednesday, September 9th at 9:00 AM with keynotes on the hottest innovations, best ideas, and toughest challenges in mobile today, featuring Meredith Attwell Baker, CTIA's President and CEO; Tom Wheeler, Chairman of the FCC; and industry leaders from Bluegrass Cellular and Sprint. The packed Washington Goes Mobile agenda for Wednesday includes panels on spectrum, net neutrality, accessibility, cybersecurity, privacy and wireless policy with the FCC Commissioners' Legal Advisors.

On Thursday, September 10th, we will kick off the day with a 9:00 AM keynote featuring industry titans from AT&T, iHeartMedia, and Verizon. Thursday's agenda is loaded with policy panels and engaging speakers, including a lively conversation between Meredith Attwell Baker and the FCC Commissioners, as well as sessions focused on privacy and the 600 MHz Incentive Auction. We will celebrate on Thursday evening with a cocktail reception hosted by Wiley Rein at the Palazzo. The Washington Goes Mobile regulatory program culminates with a special Federal-State Regulatory Dinner sponsored by Samsung and held at Buddy V's in the Grand Canal Shoppes. RSVP is required and can be sent to Emma Prieskorn at EPrieskorn@CTIA.org. Super Mobility 2015 concludes on Friday morning, September 11th, with keynotes featuring Under Armour and other industry leaders.

We look forward to your participation in this year's Washington Goes Mobile program. If you have any questions, please do not hesitate to contact any member of the Regulatory Affairs team at 202.736.3216 or CTIARegulatoryPolicy@ctia.org.

The CTIA Regulatory Affairs Team

Scott Bergmann, Vice President
Matt Gerst, Director
Brian Josef, Assistant Vice President
Emma Prieskorn, Coordinator
Kara Romagnino, Director
Krista Witanowski, Assistant Vice President

WASHINGTON GOES MOBILE AGENDA

Pre-Show Day: Tuesday, September 8, 2015

Wilkinson Barker Knauer Happy Hour

5:00-7:00pm Press at the Four Seasons Hotel
Notes: Please RSVP to Marc Knox at mknox@wbklaw.com or 202.383.3353.

Day 1: Wednesday, September 9, 2015

Keynotes: 9:00-10:30am

Meredith Attwell Baker, President and CEO, CTIA- The Wireless Association
Ron Smith, President & CEO, Bluegrass Cellular and CTIA Chairman
Tom Wheeler, Chairman, Federal Communications Commission
Marcelo Claude, President & CEO, Sprint

Panel: CTO Roundtable—US Leadership Advancing from 4G to 5G

11:00-12:15pm

Description: U.S. operators led the world in 4G LTE deployment, which is why Americans enjoy some of the largest and most advanced wireless networks. Yet other countries, such as South Korea and Japan, are starting R&D and planning demonstrations of next generation technology they call '5G.' In order for Americans to continue to enjoy state-of-the-art networks, U.S. operators must assume a leadership role in advancing 4G LTE and defining use cases and technical requirements for next generation technology. Chief Technology Officers from leading U.S. operators will share their perspectives on the challenges and opportunities we'll face as the wireless industry advances from 4G LTE to 5G. What is driving the evolving technology? What are some of the key requirements? How will mobile users benefit from 5G?

Moderator: **Tom Sawanobori, CTO, CTIA**

Panelists: **Neville Ray, CTO, T-Mobile**

Roger Gurnani, EVP & Chief Information and Technology Architect, Verizon

Ron Marquardt, VP Technology Innovation and Architecture, Sprint

Tom Keathley, SVP, Wireless Network Architecture and Design, AT&T

Panel: Accessibility Outreach Initiative Forum

11:00-2:00pm

Description: CTIA's annual AOI Forum offers an opportunity for participating member companies to directly engage and learn from leaders in the deaf, hard of hearing, blind/low vision, and older adult communities. This year, CTIA will bring together industry leaders to discuss the ways people with disabilities and older adults will benefit from the Internet of Things and emerging wireless innovations. Participants will also engage in a dialogue to enhance and ensure that CTIA's awareness and outreach efforts reflect the ways that people with disabilities and older adults are utilizing wireless technologies.

Moderator(s): **CTIA External and State Affairs**

Panels: 11:00-12:00pm "What Does the Internet of Things Mean for People with Disabilities and Seniors?"
12:15-1:00pm "Advancing Access to Emergency Communication Technologies for Persons with Disabilities"
1:00-1:45pm "Group Discussion of Content on CTIA's Access Wireless.Org"

Panel: FCC-FTC Privacy Discussion

12:30-1:00pm

Panelists: **FCC Commissioner Michael O'Rielly**
FTC Commissioner Maureen Ohlhausen

*For a full list of Privacy Panels, click [here](#).

Panel: Setting the Record Straight on LTE-U and Wi-Fi Coexistence

Speakers: **Neville Meijers, VP, Business Development, Qualcomm**
Dean Brenner, SVP Government Affairs, Qualcomm
Michael Thelander, President and Founder at Signals Research Group

1:00-3:00pm

Panels: 1:00-1:30pm "What are the Benefits of LTE-U and LAA and MuLTEfire™?"
1:00-2:00pm "A Regulatory Perspective on LTE-U and Wi-Fi Coexistence"
2:00-2:30pm "Wi-Fi/LTE-U Co-existence and the User Experience"

Panel: FCC-NTIA Experts on the Issues

2:00-3:00pm

Description: From spectrum availability and the growth of mobile broadband adoption to public safety, infrastructure deployment and net neutrality, countless regulatory actions are brewing in the wireless space. FCC Commissioners' legal advisors hit on wireless hot topics.

Moderator(s): **Brian Josef, Assistant Vice President of Regulatory Affairs, CTIA**
Matt Gerst, Director in Regulatory Affairs, CTIA

Panelists: **Jessica Almond, Legal Advisor to FCC Chairman Tom Wheeler**
Brendan Carr, Legal Advisor to FCC Commissioner Ajit Pai
Erin McGrath, Legal Advisor to FCC Commissioner Michael O'Rielly
Louis Peraertz, Legal Advisor to FCC Commissioner Mignon Clyburn (Invited)
Johanna Thomas, Legal Advisor to FCC Commissioner Jessica Rosenworcel
Derek Khlopin, Senior Advisor for Spectrum, Office of the Assistant Secretary, NTIA

Panel : Spectrum Regulatory Update: Policy Matters for Your Business

3:00-4:00pm

Moderator(s): **Brian Josef, Assistant Vice President of Regulatory Affairs, CTIA**
Kara Romagnino, Director in Regulatory Affairs, CTIA

Description: Mobile broadband use is exploding, and there is no sign of it slowing down. What are federal agencies and legislators doing to make sure the wireless industry has the spectrum it needs to meet Americans' growing demands? This panel will bring together government and industry representatives who will focus their discussion on efforts to free up more spectrum for licensed and unlicensed use, the prospect of sharing valuable

spectrum resources between federal and commercial stakeholders, and what's in the pipeline for future spectrum auctions and allocations.

Panelists: **Kathy Grillo**, *Senior Vice President, Federal Regulatory and Legal Affairs, Verizon*
Kathleen Ham, *Vice President of Federal Regulatory Affairs, T-Mobile*
David Redl, *Chief Counsel, U.S. House of Representatives Energy and Commerce Committee, Subcommittee on Communications and Technology*
Glenn Reynolds, *Chief of Staff, Office of Assistant Secretary, NTIA*
Roger Sherman, *Chief, Wireless Telecommunications Bureau, FCC*

Panel: Mobile Cybersecurity: New Paradigm, Voluntary Framework vs. Regulation

3:30-5:00pm

Description: Government cybersecurity executives sit down with John Marinho, CTIA, VP Technology, and Cybersecurity for an in-depth discussion about the issues surrounding mobile cybersecurity and the new industry model based on the NIST Framework.

Moderator(s): **John Marinho**, *Vice President, Technology and Cybersecurity, CTIA*

Panelists: **Hala Furst**, *Business Liaison, Private Sector Office U.S. Department of Homeland Security*
Admiral David Simpson, *Chief Public Safety and Homeland Security Bureau, FCC*
Adam Sedgewick, *Senior Information Technology Policy Advisor, NIST*
Josh Goldfoot, *Deputy Chief Cybersecurity, Law and Policy Section, National Security Division, DOJ*

*For a full list of Cybersecurity Panels, click [here](#).

Panel: Net Neutrality: The Impact of the *Open Internet Order* on Innovation and Investment

4:00-5:00pm

Description: Arguably the most high profile release in the FCC's recent history, the 2015 "Open Internet Order" made waves across communications industry sectors, governmental bodies, judicial courts, and the court of public opinion. One thing that is still unknown is how the Order will impact new LTE functionalities, 5G, and other business opportunities. Industry representatives explore these issues and discuss how broad application of Title II to the mobile industry will affect future wireless innovation and investment.

Moderator(s): **Jot Carpenter**, *Vice President of Legislative Affairs, CTIA*

Panelists: **Krista Witanowski**, *Assistant Vice President of Regulatory Affairs, CTIA*
Carl Geppert, *Partner and Telecommunications Practice Leader, KPMG, LLP*
Michael Grendi, *Chief Financial Officer, Bluegrass Cellular*
Bruce Gustafson, *VP Government Affairs, Ericsson*
Brian Hendricks, *Head of Technology and Innovation Policy, Nokia*
Randolph May, *President, The Free State Foundation*

Chairman's Reception

6:00pm Lakeside at the Wynn

Day 2: Thursday, September 10, 2015

Keynotes: 9:00-10:30am

Glenn Lurie, *President & CEO, AT&T Mobility*

Bob Pittman, *Chairman & CEO, iHeartMedia, Inc.*

Marni Walden, *EVP & President of Product Innovation and New Businesses, Verizon*

Briefing: Bidding In Brief: A Walk-Through of the FCC's Incentive Auction Procedures

11:00-12:00pm

Description: FCC Chair and Vice-Chair of the Incentive Auction Taskforce will walk attendees through and answer questions on the Auction Procedures Public Notice for the first ever Incentive Auction scheduled to begin on March 29, 2016.

Hosted by: **Gary Epstein**, *Chair of Incentive Auction Task Force, FCC*
Howard Symons, *Vice Chair of Incentive Auction Task Force, FCC*

Panel: Washington Talks Wireless with Meredith Attwell Baker and FCC Commissioners

2:00-3:00pm

Description: CTIA President and CEO Meredith Attwell Baker sits down with FCC Commissioners to discuss a range of wireless policy issues, including the upcoming 600 MHz Broadcast Incentive Auction, E-911, Open Internet regulations, USF Policy and more. Panelists offer insights on how best to ensure the continued growth of and investment in the nation's mobile ecosystem.

Moderator: **Meredith Attwell Baker**, *CTIA President and CEO*

Panelists: **Commissioner Mignon Clyburn**
Commissioner Michael O'Rielly
Commissioner Ajit Pai
Commissioner Jessica Rosenworcel (*Invited*)

Panel: Incentive Auction Progress Report: To the Bidder End

3:00-4:00pm

Description: Since 2012, the FCC has been working diligently to open the first-of-its-kind 600 MHz broadcast incentive auction and bring new mobile broadband spectrum to market to facilitate innovative wireless use. While the auction will spur wireless broadband's continued growth, its implementation hasn't been without its challenges. FCC and industry stakeholders on this panel will discuss the steps taken so far and the work that still needs to be done to successfully implement the auction.

Moderator(s): CTIA Regulatory Affairs

Panelists: **Gary Epstein**, *Chair of the Incentive Auction Task Force, FCC*
Joan Marsh, *Vice President of Federal Regulatory, AT&T*
Grant Spellmeyer, *Vice President, Federal Affairs and Public Policy, US Cellular*
Lonna Thompson, *Executive Vice President, Chief Operating Officer and General Counsel, Association of Public Television Stations*

Wiley Rein Happy Hour

5:00-7:00pm Table 10 at the Palazzo

Notes: Please RSVP [HERE](#) if you are able to attend.

Federal-State Regulatory Dinner and Dessert Reception Hosted by Samsung

7:00-9:00pm Buddy V's at the Venetian

Notes: Please RSVP to Emma Prieskorn (EPrieskorn@ctia.org) if you are able to attend.

Day 3: Friday, September 11, 2015

Keynotes: 9:30-10:30am

Robin Thurston, *Chief Digital Officer, Under Armour*

Erin McGrath

From: Johnson, William H <will.h.johnson@verizon.com>
Sent: Tuesday, April 05, 2016 6:42 PM
To: Mike Orielly; Robin Colwell; Erin McGrath; Amy Bender
Subject: State of the Market: Internet of Things 2016
Attachments: state-of-the-internet-of-things-market-report-2016.pdf

I wanted to share with you guys the Verizon IoT report that we released earlier today (as well as some related news releases). These detail some of the really cool stuff that we're engaged on in areas like telematics, agriculture, healthcare and smart buildings. I hope you'll find this interesting, and let me know if you'd like more information on any of this.

Thanks,
Will



William H. Johnson
Senior Vice President, Federal Regulatory & Legal Affairs
Verizon
1300 I St. NW, Suite 400 West
Washington, DC 20005
will.h.johnson@verizon.com
t: (202) 515-2492
c: (202) 805-4321

Is this email not displaying correctly?
[View it in your browser](#)

Verizon Releases Report Showing Growing IoT Market

A new report released today by Verizon highlights how the Internet of Things (IoT) has gone mainstream. The IoT is increasingly connecting citizens to their communities, linking patients to their health services and bringing businesses in closer touch with their customers. As the new report titled "State of the Market: Internet of Things 2016" report shows, Verizon is moving quickly to make the IoT a reality and is committed to bringing the advantages of the IoT ecosystem to consumers and businesses. Real world IoT deployments are driving business revenues across all sectors of the economy, from connected cars to healthcare to energy efficiency.

Please see below for more information and coverage of these exciting IoT developments.



Report: State of the Market: Internet of Things 2016

[Read More](#)

Verizon News Release: Oysters, cars and smart buildings among top highlights in Verizon's new Internet of Things report

[Read More](#)

Verizon News Release: Internet of Things goes mainstream, according to new Verizon report

[Read More](#)

Infographic: How does IoT impact you?

[Read More](#)

FierceWireless: Verizon: IoT 'is now mainstream,' carrier focuses on smart cities by hiring former Cisco exec

[Read More](#)

Light Reading: IoT Already Mainstream, Verizon Claims

[Read More](#)

RCRWireless: Verizon details key IoT market trends

[Read More](#)

Verizon | 1300 I St NW | Washington, DC 20005

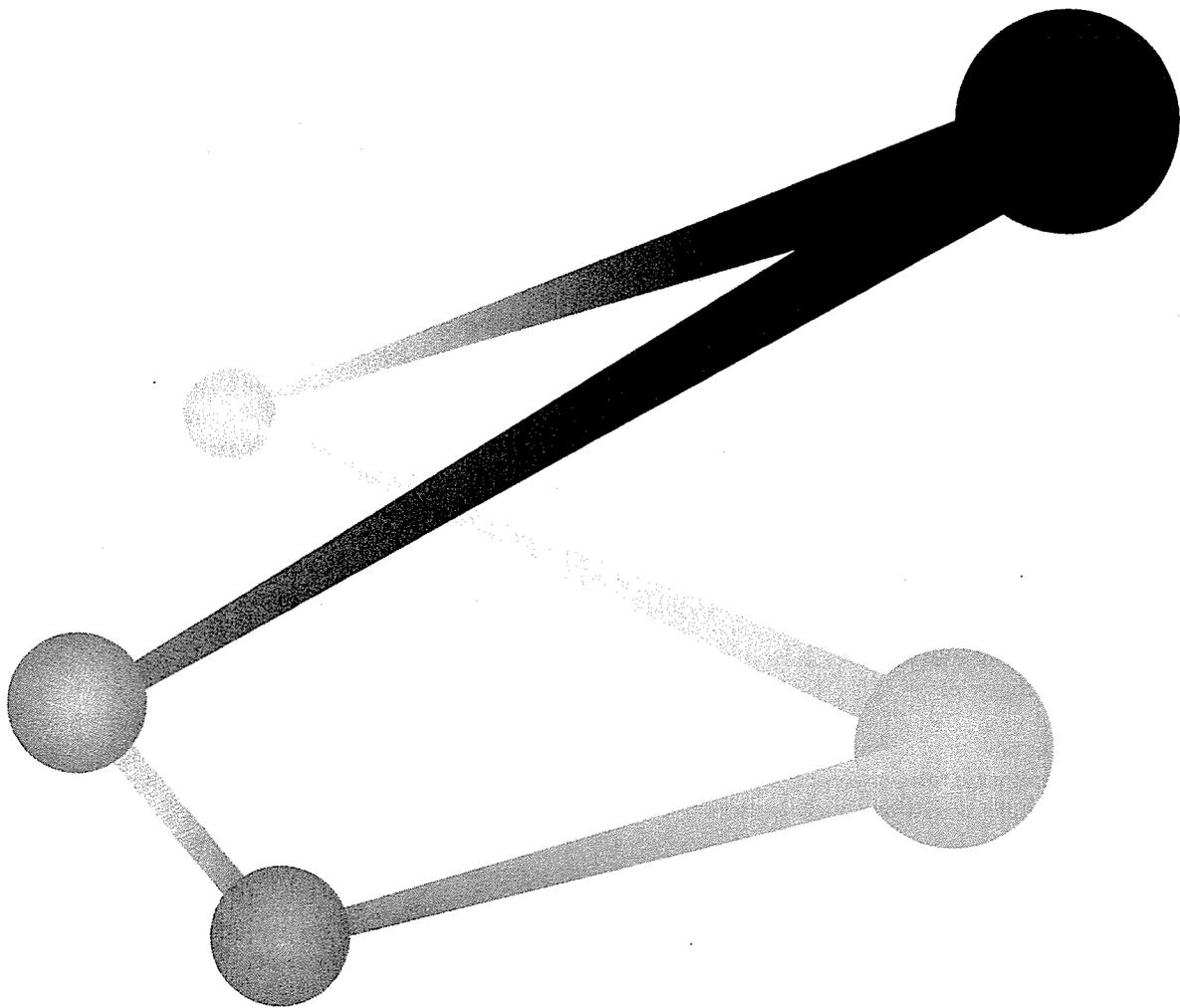
© 2016 Verizon

If you no longer wish to receive future emails, you may unsubscribe [here](#).

State of the Market: Internet of Things 2016

Accelerating innovation, productivity and value.

verizon^v



About this report

The Internet of Things (IoT) is much more than the result of seemingly fragmented and complex technologies smashed together. In the following pages, you'll read about how forward-thinking business and public sector leaders, as well as consumers and developers, are turning to the Internet of Things to address some of society's most pressing social, economic and business challenges.

You'll learn how the combination of five macro trends – data monetization, consumer expectations, the regulatory landscape, network connectivity/IoT platforms and security – are helping to speed IoT adoption and deliver measurable results across several industries and sectors.

We also offer recommendations and insights for how we think large and small businesses, consumers and even our planet can derive the greatest benefit from IoT over the next two years.

Sources for the report

- Verizon usage data, including new IoT connections, from 2015
- Verizon-commissioned research by Oxford Economics
- Interviews with Verizon customers: Insights gleaned from customers working on real IoT projects in the private and public sectors
- Interviews with Verizon subject matter experts
- Third-Party Research: We reference reports from Gartner, IDC, PwC and other authorities. For full citations, see page 24

Why Verizon?

Verizon has been in the IoT space since day one. Millions of IoT devices operate on our network today. We've worked side-by-side with developers in our innovation labs to create connected apps and devices. And we've launched our own utility, transportation and healthcare solutions with products like Networkfleet, GridWide, Verizon Share, hum, and one of our newest products, Intelligent Track and Trace.

So we've done our homework. We have experience across the whole IoT ecosystem, and we know where the pain points are at every link of the value chain – from developer to platform to customer. And we've been working for the last two years on solutions that address the structural barriers that have held back the IoT ecosystem.

Through our ThingSpace platform, we are accelerating adoption of IoT by making it easier, faster and more accessible to develop IoT apps that benefit society.

We believe that no one else in the industry has taken this kind of a holistic approach to IoT. We are scaling the systems required to connect billions of devices. And we are changing the model for IoT. Not just for the CIOs, CTOs and rocket scientists, but for everybody.

We're excited to show you what we're doing and we're even more excited to tell you what comes next.

The Internet of Things goes mainstream.

It's what lets a parent monitor and set driving rules for their newly licensed teenager. It's what enables a working mom with sleep apnea to rest peacefully every night.

It's at work in a California vineyard, measuring soil and moisture conditions to improve plant quality, lower operating costs and increase crop value. It's helping to speed up emergency services and reduce fatalities on the nation's roadways.

The Internet of Things (IoT) is in your home, in your car and phone, and, increasingly, on your body. It's connecting citizens to their cities, linking patients to health services, bringing companies in closer touch with their customers and capturing our imaginations. In-vehicle geofencing and other applications considered novel just a year or so ago are rapidly becoming part of our everyday lives.

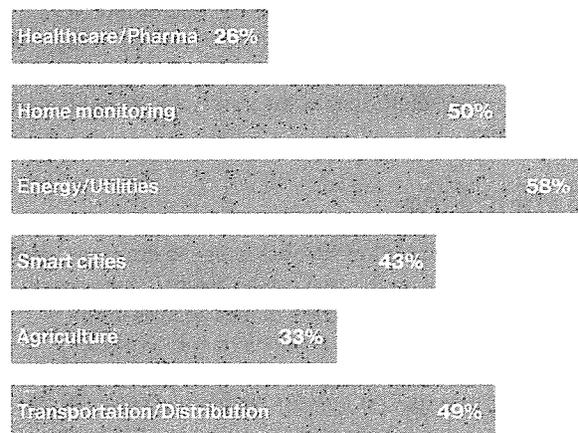
Beyond just a project

In our view, 2015 was the year IoT gained legitimacy. Businesses budged off a "start small think big" mindset. Today, they're building IoT into future strategies and business models. Companies across all industries now have IoT squarely on their radar. The worldwide Internet of Things market spend will grow from \$591.7 billion in 2014 to \$1.3 trillion in 2019 with a compound annual growth rate of 17%. The installed base of IoT endpoints will grow from 9.7 billion in 2014 to more than 25.6 billion in 2019, hitting 30 billion in 2020¹.

And while IoT applications range far and wide, when we think about IoT, we largely focus on the following key areas - smart communities/smart cities, energy, agriculture, transportation, healthcare and home monitoring. We've also seen dramatic increases in activity and innovation on the consumer front as well.

IoT by the numbers

IoT network connections – 2014 vs. 2015 % growth



Source: Verizon data

For example, wearables, which already had a head start with fitness trackers, got an even bigger boost in awareness and adoption as more traditional players brought out connected watch solutions. And we'll continue to see a tremendous amount of innovation in smartwatches and other IoT solutions for the consumer, especially as technologies for the individual, the car and the home become untethered from the phone and increasingly converge with other things around them.

Enterprises to scale from millions to billions of connected devices.

Enterprises view IoT as a new revenue stream. A study we commissioned by Oxford Economics shows that revenue growth is by far the biggest factor driving IoT adoption. Throughout 2016 and beyond, we'll continue to see IoT deployed as a mainstream path to generating higher revenue, thanks largely to the rise of four key trends which have come to an inflection point in the past year; data monetization, core IoT networks and low power devices, platforms as a service, and investment in IoT startups.

Data is king

Although the amount of "things" in use is growing rapidly, IoT services will be the real value drivers in the coming years. We believe companies of all sizes will invest in creating and selling new services based on insights generated by data from IoT-connected devices. Gartner estimates that "the Internet of Things (IoT) will support total services spending of \$235 billion in 2016"². This is in sharp contrast with what we have seen to date. In the past, the push was to collect and use data primarily for the purpose of improving the operational efficiency of the corporation itself.

Yet, despite the huge revenue potential that data monetization presents, our Oxford Economics study found that today only 8% of businesses are actually using more than 25% of their IoT data³. Nearly 50% of businesses already on the IoT journey estimate that in two to three years they will be using more than 25% of their data as companies realize the value in monetizing new products and services, driven by insights from data to drive down costs or increase revenues³.

Networks at the core

Core IoT networks will enable the cost-efficient connection of millions of Category 1 or "Cat 1" devices, which are sensors and devices containing smaller computer chipsets and requiring less power than smartphones and some other mobile devices. This makes them less expensive to deploy in large numbers. Utility meters fall into the Cat 1 classification. Up until now, the cost to connect such devices to a wide-area network has been a major barrier to widespread IoT deployment, but the evolving IoT network and device ecosystem is rapidly changing to remove this barrier.

Moreover, 5G, the next generation of wireless technology, will provide an end-to-end ecosystem to enable a fully mobile and connected society. With speeds measured in multiple gigabits per/second, latency in the single digit milliseconds and the capacity to handle 1,000 times more consumption than current network technologies, 5G promises to deliver on IoT opportunities like robotics, autonomous vehicles and the massive scale expected in a truly connected world.

Revenue growth is the biggest factor driving #IoT.

Only 8% of businesses are using more than 25% of their IoT data³.

² Gartner, Gartner Says 6.4 Billion Connected 'Things' Will Be in Use in 2016, Up 30 Percent From 2015, November 10, 2015, <http://www.gartner.com/newsroom/id/3165317>

Platforms as a service (PaaS)

Creating, implementing and managing IoT applications is a complex process. It involves sensors and mobile devices, secure network connectivity, storage, big data analytics, the ability to scale new services and ongoing integration and fine-tuning. Not surprisingly, most enterprises, regardless of size, do not have all of these capabilities and skills in-house to make IoT a reality.

We see complexity, a fragmented ecosystem and concerns about security and privacy as the key factors that are driving the proliferation of IoT platforms. These platforms are designed to make building and deploying applications easier, faster, secure and more accessible for everyone.

5G promises to deliver on IoT opportunities like robotics and autonomous vehicles.

In 2016, enterprise IoT startups will generate two to three times more funding than their consumer counterparts.

Investment in IoT startups

As a CEO from one of the largest banks in the world famously declared, “Silicon Valley is coming,” confirmation that the explosion of activity among tech start-ups and larger tech companies is posing a serious threat to business as usual. Tech disruption is not unique to financial institutions. A wide range of industries are under competitive pressure from non-traditional players, leading to some interesting mash-ups. For example, amid changing demographic preferences, the auto industry has taken notice of ride-sharing as an immediate threat which has resulted in large-scale investments from top automakers in companies like Uber and Lyft.

The race to usher in new business models and revenue streams through IoT shows no signs of slowing down in the near future. According to analysis conducted by our venture capital (VC) arm, Verizon Ventures, we estimate that consumer IoT startups raised 15% more VC funding than enterprise-focused startups in 2014. However, in 2015, roles seemed to have reversed with enterprise outpacing consumer by around 75%. In 2016, we believe the enterprise will continue that trend, but by a much larger order of magnitude – roughly 2 – 3 times more than consumer. 2016 will see enterprise IoT VC funding considerably dominate that of consumer.

Consistent with these trends, our experts say that the next 18 months will continue to give rise to tech accelerators specifically tailored for a wide range of industries. Think of accelerators as the intersection of IoT innovation meets Industry X. These programs are designed to fuel growth by providing tech startups with funding, proof of concept resources and mentoring. On the flip side, increased participation in accelerator programs as a corporate partner allows enterprises to learn about new IoT technologies that can either be woven into their existing products and services or to create new products and services intended to drive new revenue opportunities.

Factors accelerating adoption

Evolving regulatory landscape

Regulatory compliance is a huge driving factor behind IoT adoption. We've already seen how the Energy Act (2007) in the U.S. accelerated efforts to monitor energy consumption. Nearly a decade later, the installed base of remote-capable meters with smart grid app support is expected to reach 454 million in 2016 and to more than double by 2020, making it a leading IoT device.

Consider the Drug Supply Chain Act. This legislation gives drug manufacturers until late 2017 to electronically transfer and store transaction histories for their prescription drugs, including shipment information across their distribution supply chain. The law is designed to thwart counterfeit drugs which cost the industry \$75 billion annually⁴.

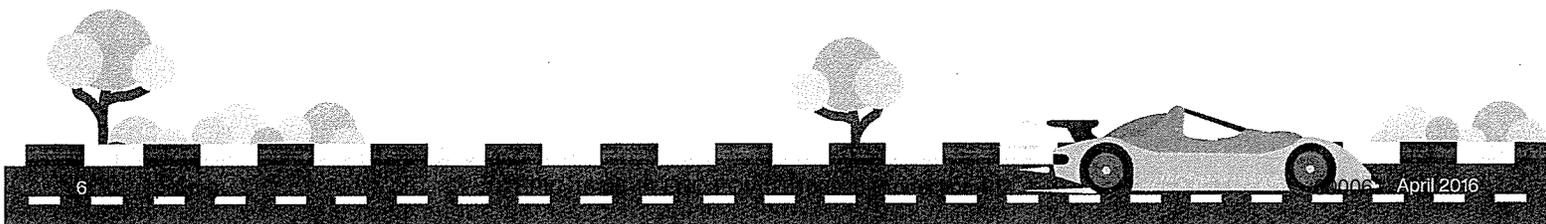
Similar requirements in other sectors such as the beverage and construction industries, where the product can change hands up to 10 times – from manufacturer to consumer – will drive the deployment of millions of sensors to track machines and other assets. IoT will allow small and medium-sized businesses as well as large enterprises to quickly provide critical information to their customers and supply chain partners.

50% of most auto trips are less than three miles⁵.

In the US, the agriculture and food industry is deploying sensors on an ever-widening scale to monitor key production conditions, shipping time and other metrics as a means to comply with a new and comprehensive set of reporting requirements under the 2015 Food Safety Modernization Act.

In the public sector, demand is steadily increasing for intelligent traffic and multimodal transportation solutions such as bikes, scooters and skateboards as alternatives to cars. These efforts are designed to enhance livability for residents and reduce congestion for businesses and other organizations such as colleges and universities. However, considering that many municipalities continue to grapple with aging infrastructure, redesigning streets to accommodate expanded modes of transportation is a huge undertaking. Our experts say that public-private partnerships to make funding viable will be key.

Indeed, more and more “things” – ranging from remotely programmable home thermostats and wearable health and fitness devices to aircraft jet engines and the nation's power grid – will be added to the internet every day. Devices, connectivity, and IT services will make up the majority of the projected \$1.3 trillion IoT market in 2019. Modules and sensors alone will comprise 23% of that total¹.



Growing consumer expectations

I want technology to work for me, not the other way around.

Consumers have grown to appreciate their smartphones, but in an IoT-enabled world, they are starting to understand that their phones can do more. With so much potential at their fingertips, consumers expect to remain constantly connected while also feeling in control of how and when they choose to connect to the people and things that matter to them the most.

Our experts say that consumer expectations fall into three buckets.

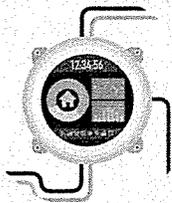
The connected lifestyle defined

Tech Solutionists: These consumers live through mobile and are willing to try new technologies and apps that can introduce a better way of life.

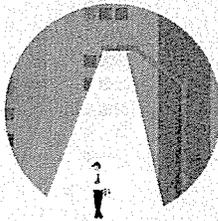
Growing Networks: Whether watching out for an aging parent or beginning to start a family of their own, the network of things they care about continues to change and expand.

Addicted to Improvement: From Fitbits to Facebook Messenger, they crave frequent updates on the people and things they care about and subsequently seek out products and services that can help with this.

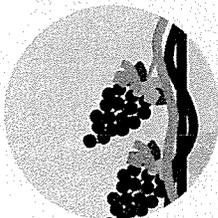
Sizing the IoT market opportunity



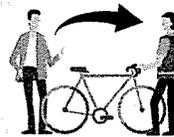
300 million
utility meters



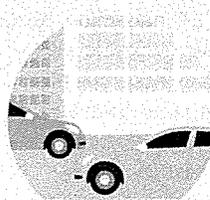
100 million
street lights



1 million
vineyard acres



83.1 million
millennials in the US⁶



150 million
unconnected
passenger cars



\$75 billion
counterfeit drugs

Source: Verizon data

IoT innovation simplified

Apple has HomeKit, Verizon has ThingSpace, Google has Brillo, IBM has Watson and Cisco has Jasper. These and numerous other platforms populating the IoT marketplace promise a secure infrastructure and a set of tools that enable developers to build IoT applications, then manage the vast array of connected devices and the huge volumes of data those endpoints generate.

One-stop shop for developers

In a nutshell, the platforms work to jump-start the development and deployment of IoT apps by radically simplifying the process for building and managing applications. Platforms provide a one-stop shop for development tools, secure network connectivity and everything else needed to launch, scale and manage apps. With IoT, simplicity is a necessary starting point, and platforms like ThingSpace are designed to create zero friction for developers.

For example: with just three mouse clicks, developers working on ThingSpace can access the platform's growing library of application program interfaces (APIs). They also have access to one of the most advanced data and analytics operations of any industry.

Easing innovation for enterprises

Today's IoT platforms address head on the problems of complexity and fragmentation that up until now have been two of the biggest barriers to IoT innovation. Before, developers had to go through multiple channels and cumbersome processes to access and integrate the tools they need to create and launch state-of-the-art applications. The availability of mature platforms not only simplifies the development process, it allows enterprise users to drive the creation of new product and service categories as a foundation for future contextual experiences for consumers, businesses and citizens. Users can also manage their IoT environments and related data, end-to-end, from device to network to application.

Farming for oysters



In his commitment to efficient and sustainable seafood production techniques, Dr. Daniel Ward, an entrepreneur-scientist, established Ward Aquafarms, a 10 acre, 1,000 cage aquaculture farm located in Cape Cod, Massachusetts. Ward's mission is to deliver the freshest seafood possible. The majority of the farm is dedicated to growing Eastern Oysters. Verizon, in collaboration with systems manufacturer Mobotix AG, has enhanced Ward's ability to monitor the safety of its Oyster harvest-to-bag process and predict growth.

Mobotix onboarded its state-of-the-art thermal radiometry sensor enabled-cameras with ThingSpace and was up and running on Verizon's IoT platform in less than an hour. With the help of Verizon's Professional Services team, satellite imaging data has been combined with other complex data such as environmental and sub-tidal water temperature, chlorophyll values, and others. Verizon Professional Services analyzes and contextualizes these inputs and provides specific insights that are valuable for Ward's aquafarming operations.

Mass customization of apps

Platforms also work to democratize the process of app development, which is especially important given that the IoT market is not a single, monolithic market but is instead composed of tens of thousands of small markets.

IoT is not a single, monolithic market but is instead composed of tens of thousands of small markets.

A physician, for example, may have a great idea for an IoT device and app that would help the 400,000 children in the US with juvenile asthma. But amassing the resources necessary to build a solution for such a relatively small market would be challenging. An IoT platform provides the tools necessary to build and launch such a solution in an efficient manner. As one observer put it:

“IoT platforms enable people living a problem to construct solutions and bring them to market cost-effectively.”

Making life more convenient



BuildingLink.com aims to be the gold standard choice for residential property managers looking to upgrade more than 3,200 luxury residential properties. To bring this experience to the next level for residents, BuildingLink used ThingSpace to create a sensor network covering the fitness center and laundry room facilities in a luxury apartment building located in Manhattan. ThingSpace allows residents to check real-time availability of treadmills, stairmasters, washing machines, etc. on a dashboard included in their mobile app. The app provides machine-specific utilization patterns for building management who can then intelligently remove under-utilized machines and add them back in the queue of those most in demand.

Looking ahead, manufacturers and other enterprises will roll out application program interfaces for developers. Developers in turn could create customized applications for say, local and regional markets, adding a new layer of economic value to the IoT ecosystem. The same thing has already happened with the smartphone. Once the platform was opened to the developer community, millions of applications emerged.

We predict a very similar education cycle with IoT. Up until the last year or so, the IoT market didn't fully understand that IoT technologies and apps are just as personal as our homes, our cars and our bodies.

Going forward, as new IoT apps continue to emerge, developers will need to deliver experiences that inform users – whether they're consumers or businesses or citizens – about their world so that they can connect to what matters most, rather than limit those experiences when something goes awry. The takeaway should not be “Oh no, I lost my bag – what happened to that app I installed?” Instead, app experiences in an IoT-enabled world should be more robust and fully integrated in our daily lives.

Wireless networks of the past were designed for smartphones. Most devices today are not as sophisticated as smartphones. Enabling developers to create applications on devices built for IoT using IoT platforms requires transforming wireless networks into a gateway that developers can program themselves. That's the power of ThingSpace.

Connection, convergence, convenience and the connected car.

Many of the technology, data and integration advancements underway with IoT come together in increasingly connected and cognizant cars. Telematics technology has gained momentum largely due to decreasing costs of hardware, software and connectivity and growing ease of use. Gartner has predicted “a huge increase in connected automobiles over the next five years. By 2020, there will be a quarter billion connected vehicles on the road, enabling new in-vehicle services and automated driving capabilities”⁷.

IoT provides opportunities to share information with customers, to improve the customer experience (75%), and to gain insight into customer preferences (74%)⁸.

Data integration and app convergence in the connected car space has worked to streamline and simplify the delivery of solutions that address real-world scenarios and empower consumers in their day-to-day lives. However, retailers note that parents, for example, don't walk into a store and ask for the latest and greatest IoT-enabled gadget. Instead, what they ask for is a way to tell whether their daughter – who just got her driver's license and borrowed the family car – got home safely from school.

On the enterprise front, telematics technology is enabling trucking companies and other fleet operators to comply with regulations requiring them to track and report driving behavior and drivers' hours. Automatic logging and reporting has been tied to reducing highway accidents and fatalities since it alerts drivers when they are nearing their drive time limit. The Federal Motor Carrier Safety Administration is working on rules to require so-called e-logging devices in all interstate trucks and buses as early as 2017.

Verizon Telematics will soon roll out an LTE solution as a standard feature for the OEM automotive market. In recent years, automakers have realized the benefits of having all of their cars and customers connected. For starters, connected cars save lives. In fact, according to our automotive experts, safety continues to rank first in terms of the overall awareness and value that it brings to the connected car. In addition to enhanced safety measures, Verizon's 4G LTE's high bandwidth and low latency will enable features like audio and video streaming as well as over-the-air updates allowing OEMs to deliver an enhanced customer experience. Verizon's all LTE solution is also designed to facilitate global service as OEMs seek to compete in new markets.

Connected cars



Hum by Verizon is a technology designed to make your cars smarter, safer and more connected. The service involves a very simple installation of a plug-in device into a car's on-board diagnostic port. Owners of vehicles manufactured in 1996 or later may gain access to services like boundary and speed alerts, vehicle location and driving history. Especially compelling for consumers is a hum feature that lets subscribers with a car problem talk to a live mechanic via hum's mechanics hotline. Pinpoint roadside and emergency assistance are also included with the service. Consumers also have access for asking questions about where to get the best price on tires or whether a repair estimate is reasonable. For more information about hum, visit www.hum.com.

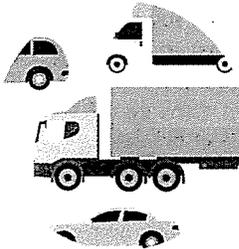
⁷ Gartner, Musings From Def Con 23: Internet of Things Risks Are Bad and Likely to Get Worse 25 September 2015

Big Data streams from connected cars.



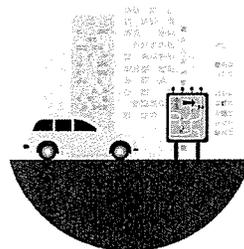
Data source

e.g. Connected car data, network data, contextual data



OEMs & dealerships

e.g. Vehicle diagnostics, in-car service consumption



Smart cities

e.g. Real-time traffic flow, incident alert, parking



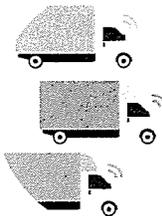
Insurance companies

e.g. Aggregated/anonymized driving data, incident data



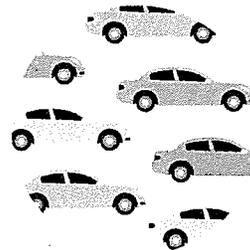
Advertisers

e.g. Customer/passenger demographics



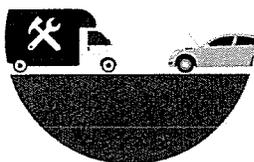
Fleet customers

e.g. Fleet performance, compare against competition



Other B2B

e.g. Content usage, frequency, length, etc



Federal / State DoT

e.g. Breakdown data, accident data, environmental data



Beyond dashboards: the analytics of things.

Consumers and businesses want information they can use to improve their lives and the bottom line. They need not just data but a way to analyze it so they can make better decisions.

The ability to monitor and manage objects in the physical world electronically makes it possible to bring data-driven decision-making to new realms of human activity—to optimize the performance of systems and processes, save time for people and businesses and improve quality of life⁸.

Going forward, companies looking to grow their revenue will exploit the information they collect via “things” to better understand and serve customers, improve products and create customized solutions for individual customers.

Big data will move beyond descriptive data collection to predictive and prescriptive analytics.

Advancing intelligent transportation

Take the app for the city bus on your smartphone that alerts you when the next bus is scheduled to depart for your evening commute home. By combining this data with data on your calendar and your friends’ calendars, predictive analytics could determine when you might need to take an alternate bus route. Imagine receiving a notification on your smartphone that suggests taking bus No. 57 rather than bus No. 10 so that you can stop at your favorite store on the way home and buy a birthday gift for your family member. It can also re-route buses based on passenger needs at various times of the day.

Let’s say that you arrive back at the bus stop near your home late one night, but still need to walk home, which is approximately one mile away. Prescriptive analytics goes a step further, by offering alternate modes of transportation such as a bike or ride-share so that you don’t have to walk home alone in the dark which might help prevent an unsafe situation.

This requires a convergence of IoT data and analytics capabilities that can scale to handle the massive volumes of data generated by millions of sensors.

IoT promises to enhance the way you live rather than expecting you to adapt.

Descriptive analytics:

Answers:
“What has happened?”

Data aggregation and data mining to provide insight into the past.

Predictive analytics:

Answers:
“What could happen?”

Statistical and models and forecasting techniques to understand the future.

Prescriptive analytics:

Answers:
“What should we do?”

Optimization and simulation algorithms to advise on outcomes and machine automation.

The supply chain reimaged

Consider, for example, the massive number of touch points in the pharmaceutical supply chain, from plant materials to packaged products on a store shelf. Today, companies widely use RFID technology to track the movement of products, but the technology is limited. It can tell when and where an item was scanned, but there is little to no visibility into what happened between two scanned points.

IoT devices enable companies to track heat, light and other relevant factors. By integrating this data with say, weather and traffic data, the company can make better decisions because it has a more holistic view that is tied to the business.

Companies also can set up rules to govern shipments based on real-time conditions. If it's raining, take Highway 10 because the usual Highway 5 route floods in rainy weather. The ability to collect, integrate and act on data from multiple sources is what enables predictive and prescriptive analytics.

The role of domain experts

Without question, virtually all industries will be inundated with a deluge of IoT data. Contextualizing that data for different kinds of businesses is imperative. Along with analytics capability, subject matter expertise will be an increasingly critical component of IoT platforms and the overall IoT ecosystem.

Agronomists, public health experts, structural engineers and other experts will bring their expertise to data modeling and the creation of algorithms that go into predictive and prescriptive analytics, benefiting the food, health and building industries.

In the event of a power outage, for example, a power company could receive an automatic notification from the meters of every home and business without power—thus helping to detect the source of the power problem—plus have access to a map showing where each of its technicians are located and get prescriptive advice for dispatching them in the most efficient manner.

Up until now, the world of IoT has been a pretty geeky place. Yes, gadgets could learn behaviors but each gadget came with its own software, set up and variations. Now, the platform's capabilities enable apps to learn enough about human behavior around multiple devices so a parent or homeowner does not have to create a set of rules for each and every device. Instead, the platform will automatically ensure that relevant data generated by a thermostat, for example, is communicated to appropriate appliances and adjust them accordingly.

Helping the patient on the go



Verizon is currently working with industry experts like AMC Health that delivers mobile patient monitoring solutions via smart phones and tablets. Customers may continue using services from their home and anywhere the Verizon mobile network is available. For example, by using AMC Health's mobile patient monitoring solution, an active pregnant woman who needs to track her blood sugar can use a mobile device to communicate readings from her glucometer at any time and any place she chooses, and that information is stored securely in the cloud. Her care provider has 24/7 access to her information and can determine whether she, her baby or both are at risk. Using this information, the woman's health care provider can provide more timely and appropriate care for the benefit of both mother and baby.

IoT security and privacy

The sheer volume of IoT devices constantly producing communications, require careful security and privacy considerations. There is no current IoT protection framework that's ahead of the implementation of this technology. The industry is keeping up with the development of technology by looking to the rising threat vectors – some old, some new – that will impact deployments and ongoing operations. Authentication of critical data, and baseline triggers for action are the emerging security focus.

How devices will mutually authenticate to a reliable degree of authenticity to prevent rogue commands and communications or data leakage is a priority consideration. Communications could be interrupted given a variety of factors and unless there is an assurance that corresponding devices are legitimate, there is no basis for secure operations.

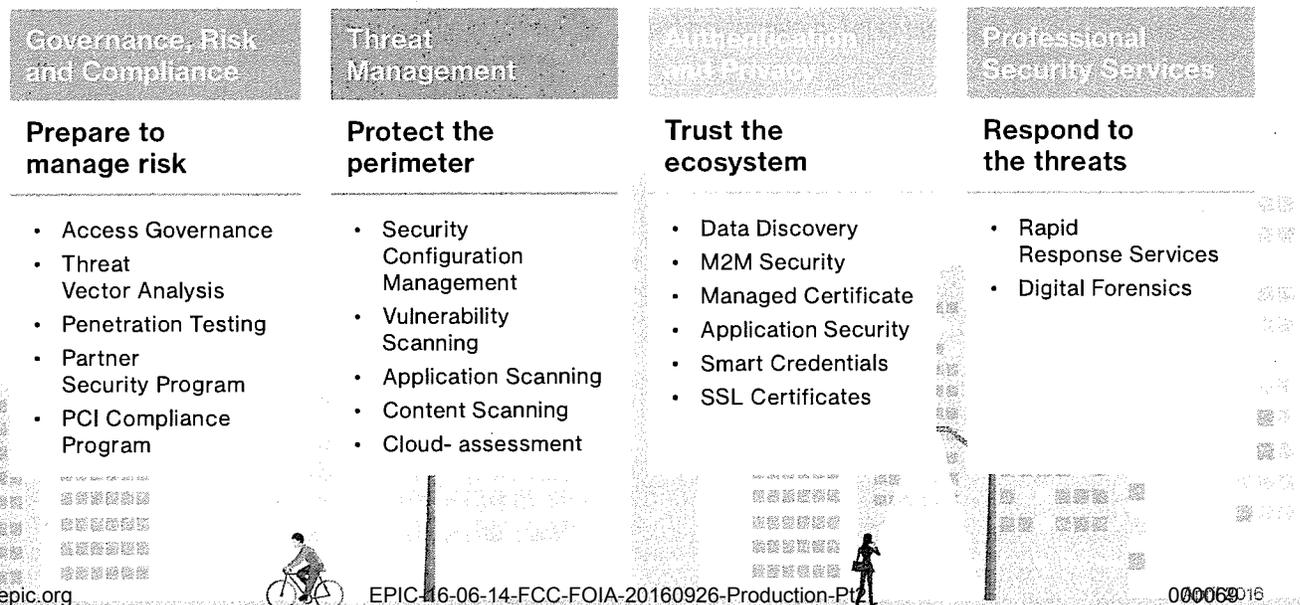
The scale of data being communicated within specific ranges or environments is a factor for maintaining consistent operations, but critical data that can be traced and identified requires a privacy technique known as "pseudonomization" of the data – that is, assigning an

obscured identifier to the data so that it doesn't readily map to a known person, address, etc. This is not one process, but a series of interactive pieces that will be a priority to test, protect and defend.

Communications between devices that trigger activity is of the highest concern to validate and secure. The timing of response ultimately is what creates the beneficial experience when the technology is functioning as designed, it is always the unintended, overlooked, or malicious capabilities that have to continue to inform security and privacy design, and implementation.

According to our Oxford Economics study, security and privacy concerns are long-standing issues. Respondents noted that success depends on developing systems, policies and procedures for managing the information that IoT generates³. Changes to ways of working and new skills are key opportunities.

Security involves multiple layers



Farming with precision.

Industry experts have quipped that the agriculture industry is proof that soon, every company will be an IoT business. Why? Because the benefits that growers are reaping by deploying IoT technologies to their fields – namely bigger crop yields, overall operational efficiencies and reduced costs – are too valuable to ignore.

One of the biggest trends in farming today is precision agriculture, the practice of sensing and responding to variable soil, moisture, weather and other conditions across different plots. Farmers are deploying wireless sensors and weather stations to gather real-time data about things such as how much water different plants need and whether they require pest management or fertilizer. (See page 17 sidebar on Hahn Family Wines.)

The total market size for digital precision agriculture services is expected to grow at a compound annual growth rate of 12.2% between 2014 and 2020, to reach \$4.55 billion⁹.

Using this data, growers can customize growing processes. Indeed, one of the biggest benefits IoT offers farmers is the ability to gather much more granular data about smaller parcels of land. With site-specific data, growers can then optimize growing conditions on a plot-by-plot basis, boosting yields, improving quality and cutting costs in the process.

The agriculture industry is proof that soon, every company will be an IoT business.

In the wine industry, for example, the amount of water that different grape plants require depends on the kind and quality of wine that will be produced from them. Pinot Noir grapes have different soil and moisture requirements than Chardonnay grapes, yet a grower may be cultivating both kinds of vines in adjacent plots. Collecting and analyzing real-time data from different plots enables farmers to fully optimize growing conditions for all plants under cultivation.

Verizon's agriculture IoT solution is designed to gain insights and provide actionable intelligence at a block level. On a multi-acre farm, block level is defined as adjacent acres with unified conditions. Growers can collect sensor data for each block and then calibrate watering or the spraying of herbicides or fungicides for each block.

Site-specific data can also help farmers satisfy the demands of 21st-century consumers who want to know more than ever before about where their food comes from and how it was grown.

According to the United States Department of Agriculture, consumer demand for organically produced goods continues to show double-digit growth, providing market incentives for U.S. farmers across a broad range of products. Organic products are now available in nearly 20,000 natural food stores and nearly 3 out of 4 conventional grocery stores. Organic sales account for over 4 percent of total U.S. food sales, according to recent industry statistics.

To meet organic standards, farmers can't use synthetic pesticides, growth hormones or antibiotics and instead must find other methods to improve soil quality. One alternative being explored is the use of pheromones which could work to disrupt the mating patterns of pests harmful to crops. In this scenario, wireless sensor networks would monitor pest counts and when a dangerous level is detected, a pheromone delivery system would be activated.

IoT-enabled agriculture makes good business sense. But there is an even bigger factor driving adoption across the farming industry.

The Internet of Things is also poised to play a key role in helping farmers comply with anticipated regulatory reporting requirements around issues like water usage. Sensors will automatically monitor irrigation activity and aggregate data at the block level to allow for accurate reporting. More broadly, IoT will help promote the efficient use of resources and will result in high-quality products while preserving the Earth.

- With the world's population expected to grow by 2 billion, to 9.7 billion in 2050¹⁰, and with a limited amount of arable land, finding better methods to feed the planet has become a global imperative.

Precision agriculture relies on IoT

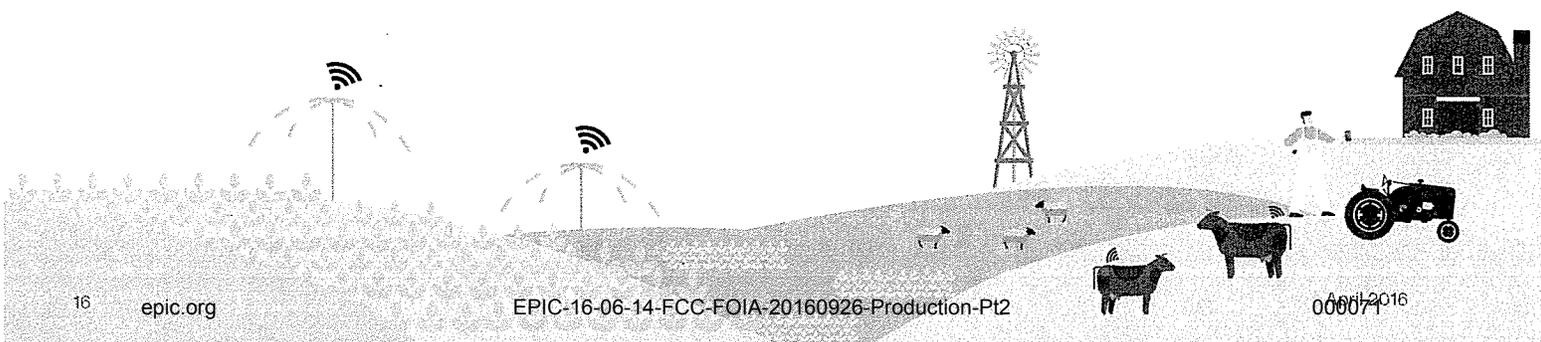
It makes seeding, irrigation and the application of fertilizers and pesticides more accurate. It monitors livestock for location and movement, so injury, illness or theft can be instantly detected. And it brings new levels of automation to crop harvesting.

A new generation of technology-savvy farmers is embracing digital agriculture. As a result, big data analytics is expected to play an expanded role in food production.

IoT platforms are already becoming populated with agriculture-specific applications developed by university-based agronomy researchers. This will enable even small and mid-sized farmers to share in the benefits of precision agriculture going forward.

Feeding a growing population

IoT is transforming agriculture and enabling farmers to overcome challenges such as water shortages, escalating costs and the limited availability of land, all of which are critical in meeting the food needs of a global population. The demand for food is expected to grow by 70% by 2050¹¹.



Fine-tuning grape growing at Hahn Family Wines.

Hahn Family Wines, a family-owned winery based in the Santa Lucia Highlands in California's Monterey County, has launched a pilot project with Verizon that uses sensor data and analytics to conserve resources and add precision to watering and fertilizing five six-acre blocks at the company's 1,000-acre vineyard. IoT technology promises to increase yields plus improve the quality of the harvest by targeting irrigation and customizing fertilizer applications to specific plots.

"Water is one of the most important tools we have as vineyard managers," says Andy Mitchell, director of viticulture at Hahn. "With this technology, instead of a 50-, 60- or 100-acre sampling site, we'll be able to micro-manage and get very specific on certain blocks. This will help us get to the next level in approaching world-class status."

Hahn has equipped each block in the pilot with a water flowmeter at the water pump, a battery-operated moisture probe that measures four different levels of soil where the grapes are growing, and a weather station to measure air temperature and other conditions. An IoT gateway continuously monitors data from the various sensors and transmits it wirelessly to Verizon's Ag tech solution on ThingSpace.

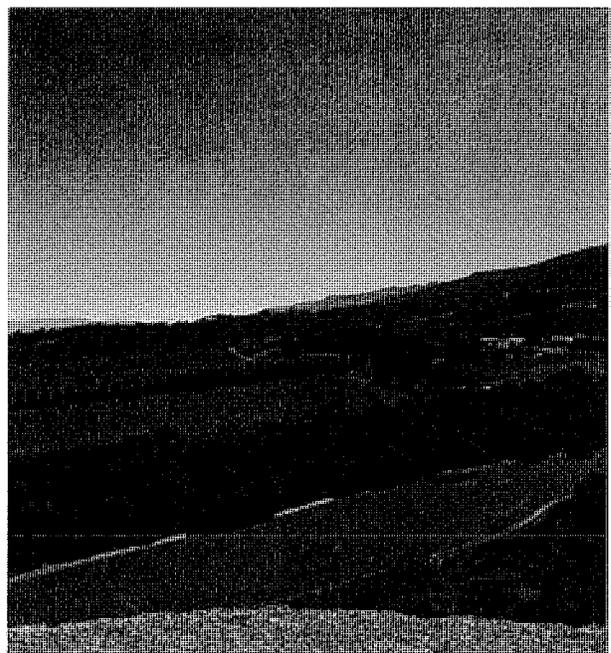
Having all of this information will help the company in applying chemicals to different blocks, Mitchell says. The Santa Lucia Highlands has ideal growing conditions for Pinot Noir and Chardonnay wines, but unfortunately, also for mildew.

"We're prone to mildew, so we have to stay vigilant. This additional information will help us be more efficient with sprays," he explains, adding that in the absence of site-specific data, vineyards have used single spraying across their acreage.

In the pilot, Hahn is using the weather station to monitor solar radiation, wind velocity, humidity and temperature in the air above the vine-canopy. Using this data, the company can time and target its use of fungicide sprays to prevent disease and rotting, which can be caused by heavy condensation.

Verizon's Ag tech solution makes data available on a dashboard, and Hahn can check the information in real-time and adjust growing processes accordingly.

"We're really looking forward to getting more and more precise, and we're already looking at variable frequency motors that will let us put out different levels and different pressures of spray to different blocks," Mitchell says.



Making communities smart and sustainable.

The world's population is migrating to cities. Already, 54% of the world's people live in urban areas, with an estimated 180,000 more moving to cities each day¹². The World Health Organization estimates that by 2050, approximately two-thirds of the global population will be city dwellers¹³.

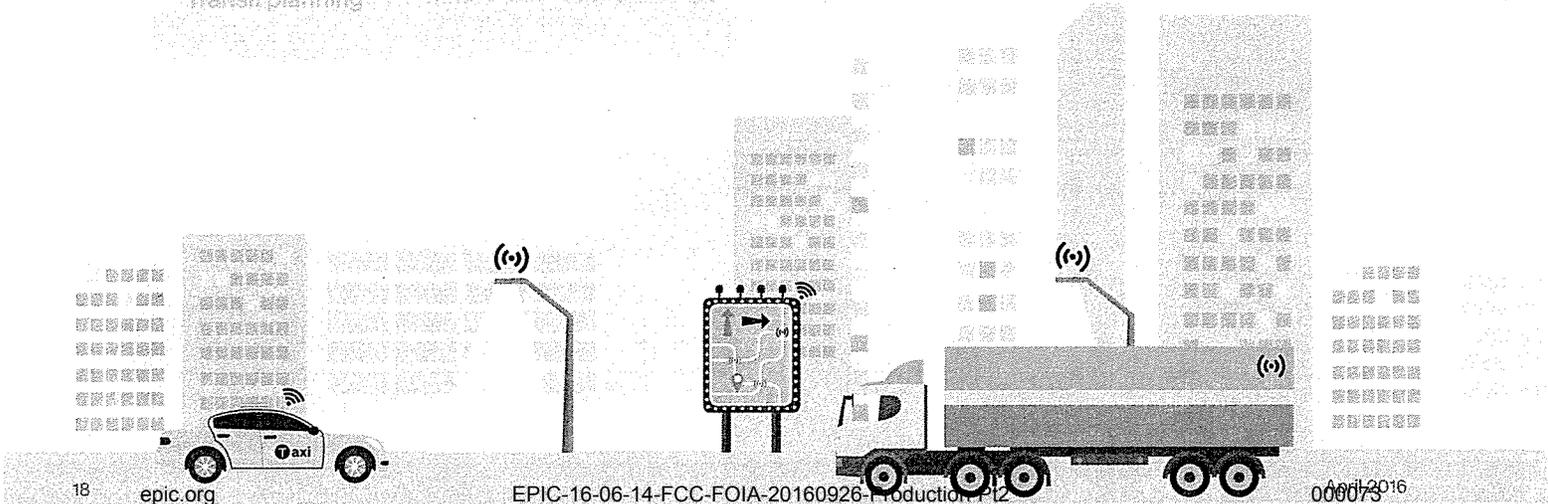
Rapid urbanization is putting a huge strain on city services not to mention aging infrastructure that supports fire and emergency services, public transportation, lighting, sewer and sanitation systems.

And while IoT is providing the way forward, focusing on smart cities alone is only scratching the surface. Realizing the vision of smart cities requires effectively addressing the needs of even smaller communities including neighborhoods, industrial parks, venues, multi-dwelling units, colleges and universities.

IoT technology is providing a way forward. Smart streetlights equipped with sensors are saving cities energy and money by detecting pedestrians, cyclists and vehicles so that lights brighten and dim when they sense movement. Cities can analyze this data for other useful information about traffic patterns, parking spaces and public safety requirements. At least one smart lighting manufacturer, for example, is exploring technology that would detect gunfire and, with real-time data analysis, pinpoint the location of shots and notify emergency dispatchers to send police officers to the area¹⁴.

In Charlotte, North Carolina, a public-private partnership known as Envision Charlotte has been measuring and continually displaying energy used by uptown buildings, a move the city says has helped to reduce the city's energy use by 16% and keep 220,999 metric tons of greenhouse gases from being emitted¹⁵.

What makes a smart community?



76%

76% of IoT adopters in public sector institutions say that an organizational structure that encourages flexibility and cross-functional work is important for improving performance around IoT³.

Now, a spinoff group called Envision America has taken the energy conservation and efficiency program to several other cities, broadening it to include water, waste and air as well. Both programs reinforce the adage that "what gets measured, gets done."

San Diego, California, and Jacksonville, Florida both have trials underway that use LED streetlight technology to collect real-time data not only to manage lighting, but also to manage parking, locate and identify potholes and keep track of repairs to municipal streets.

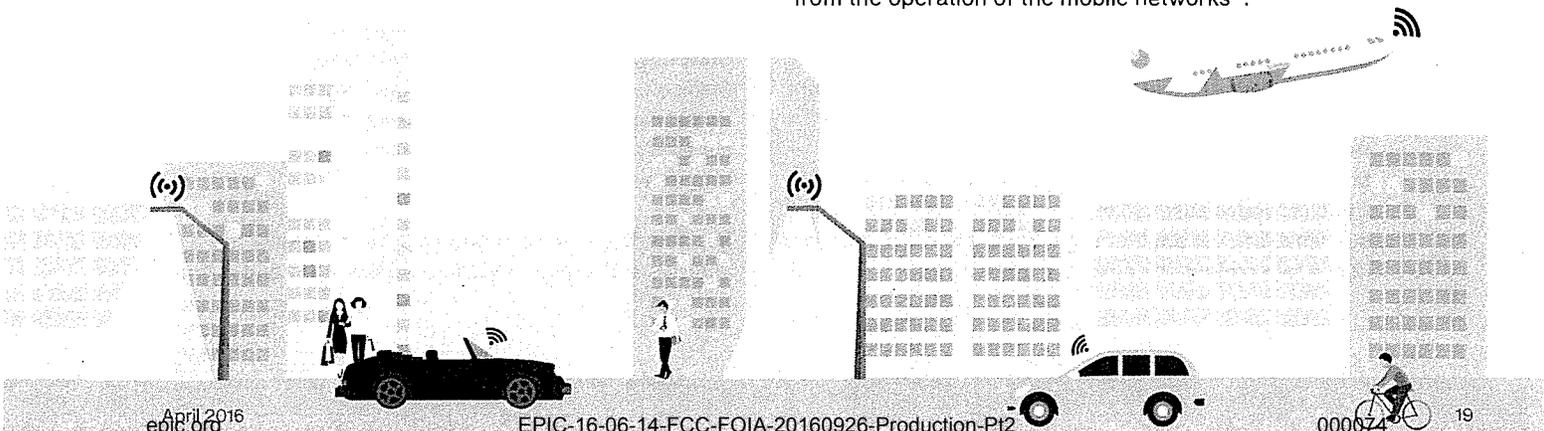
Yet to deliver value to citizens and ensure sustainability, municipalities must do more than monitor and measure. This is where the power of analytics comes in to play. Analytics can integrate and analyze data in new ways to make innovative municipal services possible.

81%

81% of IoT early movers in the public sector believe their citizens increasingly expect them to offer enhanced services using data from IoT³.

The vision is that of a citywide information network composed of connected, sensor-equipped streetlights that will both save energy costs and enable new city services. Imagine motorists receiving a text message when a parking space becomes available in the vicinity where they want to shop.

Mobile technology is making a considerable contribution to action on climate change according to Mobile Carbon Impact, a report released by the Global e-Sustainability Initiative (GeSI), authored by the Carbon Trust. The analysis found that the use of mobile in the US and Europe alone is already enabling a saving of more than 180 million tonnes of carbon emissions a year, an amount greater than the total annual emissions of the New York State. This abatement, or reduction impact, is approximately 5 times greater than the emissions emitted from the operation of the mobile networks¹⁶.



Bedford Park, Illinois

Forward-thinking city officials like Mayor David R. Brady view smart cities as a means to attract new businesses, a younger workforce and a re-energized tax base to urban areas like Bedford Park, Illinois.

Located immediately south of Chicago's Midway Airport, Bedford Park is an ideal business location. 90% of its land area is devoted to industry and it is home to 380 companies¹⁷.

"Traditionally, we're more of an industrial and commercial area, and we think a smart city will help us compete for more diversified and tech-oriented businesses," Brady says. "It sets us up for the future."

Bedford Park is home to 200 residences and 600 residents, all of which have been equipped with fiber-optic connections to provide residents with internet speeds that are 20 times faster than average. "We did that to attract Millennials," Brady explains. The strategic goal is to make Bedford Park a showcase Smart City Municipal Innovation District that integrates multiple smart village services that benefit the village's businesses and residents.

In the year ahead, analysts expect to see many new use cases, such as renting large equipment and power tools on a self-service basis.

Bedford Park isn't alone. Municipalities nationwide are working to attract start-ups, new businesses, jobs, and a new generation of workers, homeowners and taxpayers. A critical success factor is a strong digital infrastructure enabling a sharing economy. Millennials are driving a transformational shift away from ownership of cars, homes and other assets. Instead, the overwhelming trend is toward asset sharing, which increases overall sustainability, yet another area where the IoT is poised to play a huge role in the next 18 months or so.

Of those who have tried the sharing economy, 72% say they envision themselves being a consumer in the sharing economy by the end of 2016. Young adults aged 18 – 24 are most excited by the sharing economy¹⁸.



say they envision themselves being a consumer in the sharing economy by the end of 2016¹⁸.

Innova UEV

Verizon is partnering with Innova UEV on a university campus-based car sharing program to provide 4G LTE wireless connectivity within Innova's all-electric Dash vehicles. Innova UEV is also using Verizon's Share IoT solution via ThingSpace to ensure a friendly experience between driver, application and vehicle.

The Innova EV Car Share app powered by Verizon enables the student to locate, reserve, access, utilize, then return the car, using their smartphone or tablet. It also displays how much carbon emissions are saved for each ride. Innova UEV's Founder and CEO, Roman M. Kuropas says that Verizon's Share solution enabled Innova to reduce its development time by two years.

Currently, Innova is running pilot programs at the University of Pittsburgh, the University of Wisconsin-Madison, Colorado State and Washington State. The companies are collecting data from more than 40 vehicle sensors and cameras and analyzing it to enable further program innovations.

For now, the sharing economy pertains largely to vehicles and accommodations – think Uber and Airbnb.

Providing real-time energy insight.

Energy and utility companies are regulated and must modernize their aging infrastructures, all while increasing efficiency and keeping costs down.

IoT is already playing a role in addressing these challenges, and moving forward, its role is likely to expand significantly.

At the center of this ecosystem is data which can be remotely collected from meters, pipes and other equipment and assets, then analyzed to enable a better understanding of not only power usage but also power quality, the location of outages and the condition of critical infrastructure.

New low-power, low-cost grid sensors enable electricity providers to sense environmental events like trees interfering with power lines. With this data, utility crews can schedule foliage maintenance before an accident occurs.

By monitoring voltage, for example, power providers can determine whether a transformer is running too hot and needs to be fixed or replaced. Or, they may have too many users on a particular line and thus need to add other elements to optimize the grid. Right now, power providers don't know exactly how the grid is performing at any endpoint.

The advent of newer "as a service" network models, under which companies pay only when they transmit data, are breaking down certain industry barriers to modernization. Because utilities need to go before public utilities commissions to ask for a rate increase to pay for new technology, they have been slow to move forward. Instead, they tend to ride out existing investments, depreciating them over 10 to 15 years.

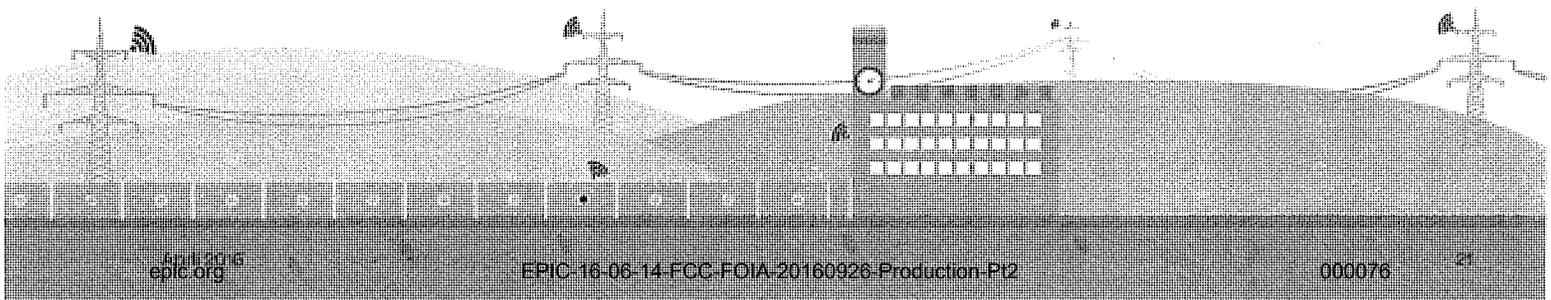
By contrast, with "as a service" models, utilities don't have to swap out the entire meter population at once. They can put in remote readers at say, difficult to reach places and pay only for service to and from those remotely located meters.

With an addressable market of more than 300 million electric, water and gas meters in service in the US today, the opportunity for intelligent solutions and services in the utilities market is massive.

The water industry also needs to know about conditions in the water grid. As is the case with power utilities, manual meter reading is expensive. Water utilities are realizing that wireless networks, with their extensive coverage, reliability and security, offer a cost-effective and efficient alternative.

Visibility into energy consumption and efficiency is also gaining importance as states enact legislation requiring monitoring. Nearly 50 states have efficiency requirements specifically for state-owned or funded public buildings. Additionally, legislation regarding energy efficiency in all public buildings was enacted in 13 states in 2015.

IoT core networks coupled with new Cat 1 devices enable water and other utilities to more easily and less expensively monitor pipes and other hard-to-access infrastructure. Prior to these advancements, utilities have been essentially limited to using their own wireless networks to monitor infrastructure. Unfortunately, private networks are expensive to develop, operate and manage.



What does it all mean?

Greater automation for consumers

Over the next 18 months, IoT adoption will grow significantly, thanks largely to falling costs, the continuing convergence of data and services and ever-increasing IoT technology simplification – a factor of utmost importance to consumers in particular. Homeowners can look forward to a simplified user interface to address a range of everyday issues, from controlling and monitoring home security and environmental conditions to monitoring their teenagers' driving habits.

The cost efficiency, convenience, simplicity and security of connecting things will drive wider societal changes. The sharing economy will grow and flourish, expanding to personal vehicles and household gear. Neighbors will check online to see whose car might be available for use, or borrow a chainsaw from the local home store and pay only for the time they use the tool. Eventually, the ability to track usage will create new service categories. Rates for insurance and healthcare will be based on usage and behavior, which can be tracked through IoT.

In three to five years' time, consumers will experience a much higher level of automation and efficiency in daily life, thanks largely to the ability to customize "if-then" scenarios via a streamlined IoT interface.

If the outside temperature reaches 80 degrees, turn the home air-conditioning unit on when my car signals I am 20 minutes from home.

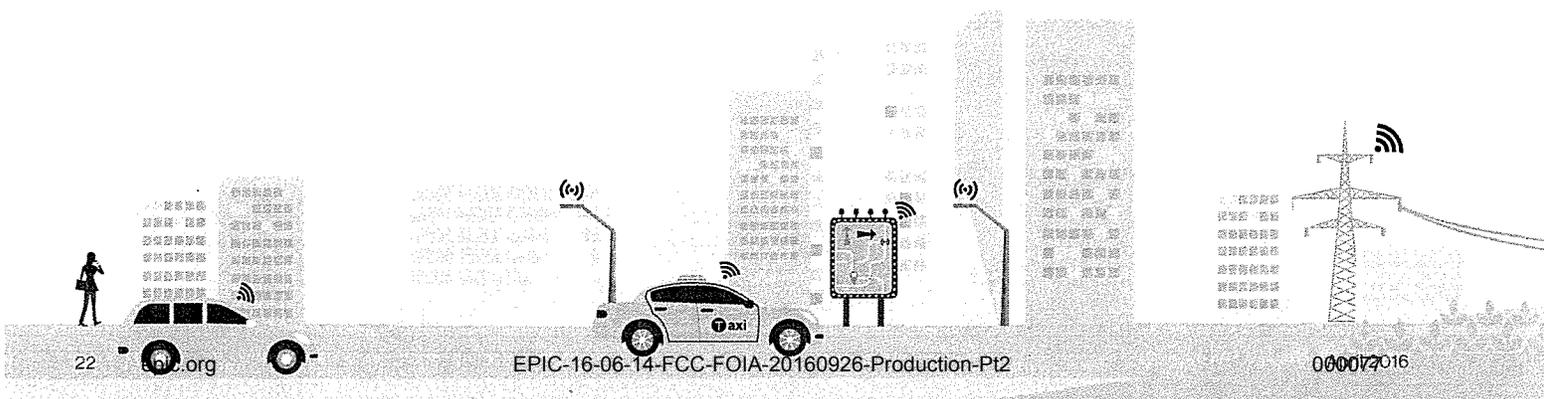
Overall, average consumers – and not just the gadget geeks – will become increasingly willing to try new ideas and services as ease of use and increased efficiencies become apparent. As people begin to experience tangible benefits, IoT adoption will expand quickly, just as cell phone usage did.

IoT usage at home will be less fragmented as well. Companies and services developing products and services will collaborate, enabling users to engage with a variety of IoT applications through a single interface, likely voice, virtual reality and augmented reality, which we see among the major points of interaction in 2016 and beyond.

More tools for developers

Developers can expect to see platforms host a growing library of APIs. Deeper industry-specific expertise will be available to apps they're developing on IoT platforms, which will continue to improve existing services such as device management, integration, security, protocols for data collection and data analytics. This will trigger a proliferation of new IoT use cases as well as greater integration across existing use cases. For example, autonomous cars will interact with smart metering and traffic and lighting systems.

Developers can also look to new edge-computing capabilities in the network, which will become increasingly important as more data from more devices and apps floods the network. Edge-computing capabilities will filter IoT data, sending only relevant bits to central processing platforms for deeper analysis.



New opportunities for enterprise

The same factors driving change among consumers will enable new efficiencies at the enterprise level. New devices – think drones – will proliferate, creating an order of magnitude increase in information – think aerial data, which can be used across a broad array of new use cases across multiple industries. Mining companies, for example, might use aerial data collected by unmanned drones to assess stockpiles or conduct volumetric analyses of supplies stored in remote locations.

New environmental and safety regulations will expand beyond nation-state borders as the economy becomes ever more global, and sustainability issues like carbon emissions and overall planetary health are tackled on a global basis. IoT technologies will enable enterprises to comply with new tracking and monitoring and data reporting and analyses requirements.

New focus for policy makers

Regulators themselves will become more tech savvy as the number of IoT and wearable products and services increase. The head of the US Federal Trade Commission predicted recently that 10 years from now, technologists will need to comprise the bulk of the commission's staff, which is now comprised largely of lawyers and economists. Further advances in consumer-facing technology will demand that this knowledge gap be filled.

Greater potential for society

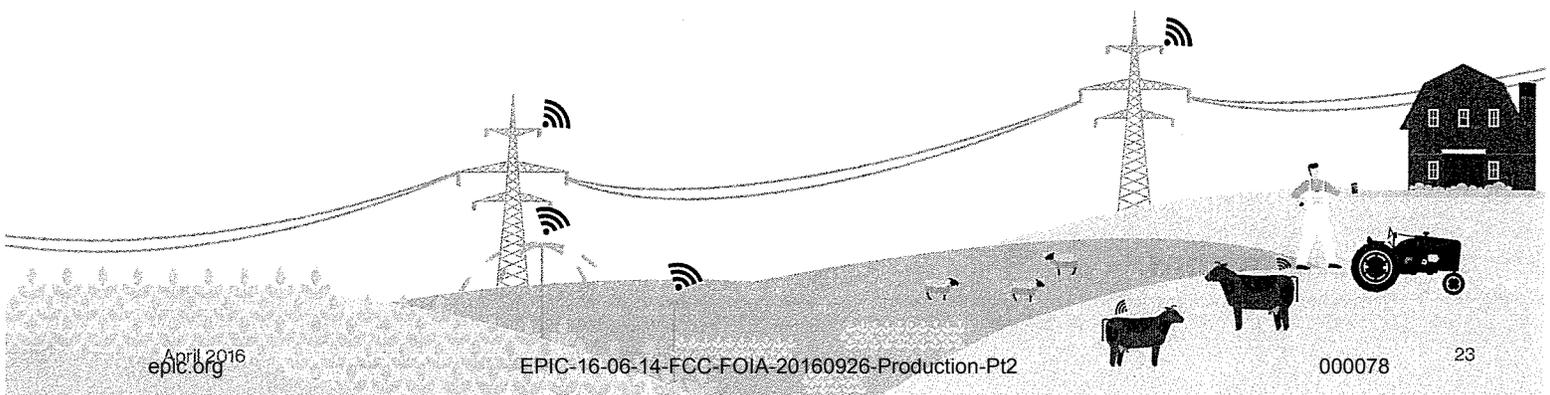
The sharing economy will grow and flourish, producing the “Uberization” of a wide range of new services. Asset tracking will steadily morph into asset sharing. Rates for services such as insurance and healthcare will be based on usage and behavior, which can be tracked through the IoT.

The bottom line

Innovation, productivity and value will thrive as private companies and the public sector both come to the inevitable conclusion that IoT is imperative to delivering the integrated, easy to use and sustainable products and services demanded by an increasingly mobile, tech-savvy 21st-century society.

No single company or country can realize the full promise of IoT on its own. We believe collaboration, experimentation and openness will:

- Create cleaner cities
- Deliver better healthcare
- Make transportation systems safer
- Conserve water
- Boost productivity
- And make the digital world work better for consumers and citizens.



1. IDC, Worldwide Internet of Things Forecast Update: 2015 – 2019, February 2016
2. Gariner, Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015, November 10, 2015, <http://www.Gartner.com/newsroom/id/3165317>
3. Survey of IoT adopters conducted by Oxford Economics, sponsored by Verizon, 2015
4. World Health Organization (WHO), Growing Threat from Counterfeit Medicines, Bull World Health Organ, 2010;98(4):247-8
5. Swiftmile.com, March 2016
6. US census, <https://www.census.gov/newsroom/press-releases/2015/cb15-113.html>
7. Gartner, Musings From Def Con 23: Internet of Things Risks Are Bad and Likely to Get Worse, 25 September 2015
8. McKinsey & Company, The Internet of Things: Mapping the Value Beyond the Hype, June 2015
9. [Accenture, Digital Agriculture: Improving Profitability, 2015](#)
10. United Nations Dept.of Economic and Social Affair, World population projected to reach 9.7 billion by 2050, July 2015
11. Population Institute, FAO says Food Production must Rise by 70%, 2009
12. Citymetric.com, "Three million people move to cities every week": so how can cities plan for migrants?, December 2015
13. The Dawn of an Urban World, In: Hidden cities: unmasking and overcoming health inequities in urban settings, World Health Organization, The WHO Centre for Health Development, Kobe, and United Nations Human Settlements Programme (UN-HABITAT), 2010
14. Smart Cities Council, Smart street lights shine spotlight on violent crimes, October 2015
15. Charlotte Business Journal, September 2015
16. Carbon Trust, Mobile Carbon Impact, December 2015
17. Village of Bedford Park website, March 2016
18. PWC, The Sharing Economy, 2015

verizon.com

© 2016 Verizon. All Rights Reserved. The Verizon logo and the Verizon shield are trademarks of Verizon Wireless. All other trademarks are the property of their respective owners. All other trademarks are the property of their respective owners.

Erin McGrath

From: Rath, Charla <charla.rath@verizon.com>
Sent: Monday, March 14, 2016 8:53 AM
To: Erin McGrath
Subject: Fwd: [E] FCC workshop demonstrates the 5G future

Hi Erin - Wanted to make sure you saw the attached. Charla

Charla Rath
202-515-2574

----- Forwarded Message -----

From: Verizon Public Policy <public.policy@verizon.com>
Date: Mar 11, 2016 3:29:35 PM
Subject: [E] FCC workshop demonstrates the 5G future
To: "Rath, Charla" <Charla.Rath@one.verizon.com>

Yesterday's FCC workshop previewed a future powered by 5G.

[View this email in your browser](#)



FCC workshop demonstrates the 5G future

By Charla Rath

While many in Washington were enjoying a perfect spring day yesterday, several technology leaders convened inside the Federal Communications Commission (FCC) offices for a [workshop](#) to discuss and demonstrate some early developments in fifth generation "5G" mobile technology. If there's one key message to take away from the workshop, it's that the race to 5G is on, and its future potential is unbounded.

FCC Chairman Tom Wheeler and Commissioner Michael O'Rielly kicked off the workshop by reiterating the agency's commitment to jumpstarting 5G deployment. Beyond making more spectrum available to "let innovators innovate," the Chairman highlighted another essential component of 5G – infrastructure. For that, "more than just good spectrum policy is required" he said, citing the need for local governments to implement policies that facilitate the infrastructure deployments necessary to support 5G and noting that "the wireless future depends on wired

connectivity in so many ways". Commissioner O'Rielly echoed the need to reduce burdens on infrastructure siting... ([MORE](#))

Read more about the 5G possibilities on display at yesterday's workshop at the [Verizon News Center](#).

5G is coming. Learn more.

Verizon Policy

1,974 followers
2,243 tweets
following 862 people

[follow](#)

Latest Tweets

- Yesterday, FCC officials saw a demonstration of a future powered by #5G: <https://t.co/HBpCLjJlLc> 3:05PM
- #FF: @NeoNneka @Daedyo @SanjayUdani @DonnaEppsVZ @mgtye @RichYoung810:15AM
- RT @daedyo: My colleague @NeoNneka speaking at the @TIAonline Policy Summit! <https://t.co/huEvod7CFL> 2:56PM
- Unique Identifier Headers (UIDH) are more sensitive to privacy concerns than ad IDs used by other Internet companies <https://t.co/bxHuvFwLsE> 12:10PM
- Verizon believes in showing kids how to be not just a technology user, but a technology #maker. <https://t.co/2c3QYhnhQg> by @DonnaEppsVZ10:15AM

[About Verizon](#) [News Center](#) [Careers](#) [Responsibility](#)

For media inquiries, please contact richard.j.young@verizon.com or elizabeth.iacobson@verizon.com

Copyright © 2016 Verizon, All rights reserved.

[unsubscribe from this list](#) [update subscription preferences](#)

Erin McGrath

From: Brian Josef <BJosef@ctia.org>
Sent: Tuesday, September 01, 2015 4:16 PM
To: Jessica Almond; Brendan Carr; Derek Khlopin; Erin McGrath; Louis Peraertz; Johanna Thomas
Cc: Matthew Gerst
Subject: RE: CTIA Super Mobility "FCC-NTIA Experts on the Issues" Panel Questions
Attachments: 150901 - Revised (Redline) Legal Advisors Panel Questions.docx; 150901 - Revised Legal Advisors Panel Questions (Clean).docx

All:

We are looking forward to seeing you next week in Las Vegas! We received some feedback regarding a few of the questions that we circulated last week. Accordingly, we made some minor changes to the panel questions in the attached (redline and clean versions attached) that are intended to facilitate your answers and accompanying preparation. Of course, please let us know if you have further questions.

Best regards,

Brian and Matt

From: Brian Josef
Sent: Wednesday, August 26, 2015 6:21 PM
To: Jessica.Almond@fcc.gov; Brendan Carr <Brendan.Carr@fcc.gov>; Derek Khlopin <DKhlopin@ntia.doc.gov>; Erin.McGrath@fcc.gov; Louis Peraertz <Louis.Peraertz@fcc.gov>; Johanna Thomas <Johanna.Thomas@fcc.gov>
Cc: Matthew Gerst <MGerst@ctia.org>
Subject: CTIA Super Mobility "FCC-NTIA Experts on the Issues" Panel Questions

Hi all,

Matt and I want to thank you again for agreeing to participate on our policy panel, "*FCC-NTIA Experts on the Issues*" at CTIA's Super Mobility 2015 show, located at the Sands Expo & Convention Center in Las Vegas, Nevada, on Wednesday, September 9th from 2:00-3:00 pm in the Mobile Intelligence Conference Center-Venetian Ballroom on the "Washington Goes Mobile" stage. We are looking forward to a great discussion with you all.

I have pasted below the description and panelists for our panel, and have attached questions that we plan to ask during the panel. Please feel free to email me and let me know if there are any questions you are not comfortable addressing or if I have missed any areas of discussion you would like to cover.

In terms of format, we will briefly introduce you all and then move immediately to question and answer, so no need to prepare any presentations or opening remarks.

FCC-NTIA Experts on the Issues

Wednesday, September 9, 2015 – 2:00 pm - 3:00 pm

Mobile Intelligence Conference Center-Venetian Ballroom, "Washington Goes Mobile" Stage

From spectrum availability and the growth of mobile broadband adoption to public safety, infrastructure deployment and net neutrality, countless regulatory actions are brewing in the wireless space. FCC Commissioners' and NTIA legal advisors hit on wireless hot topics.

Moderator(s): Brian Josef, Assistant Vice President of Regulatory Affairs, CTIA
Matt Gerst, Director in Regulatory Affairs, CTIA

Panelists: Jessica Almond, Legal Advisor to FCC Chairman Tom Wheeler
Brendan Carr, Legal Advisor to FCC Commissioner Ajit Pai
Derek Khlopin, Senior Advisor for Spectrum, Office of the Assistant Secretary, NTIA
Erin McGrath, Legal Advisor to FCC Commissioner Michael O'Rielly
Louis Peraertz, Legal Advisor to FCC Commissioner Mignon Clyburn
Johanna Thomas, Legal Advisor to FCC Commissioner Jessica Rosenworcel

Finally, you will also find attached a speaker release form for your signature. Please email me a signed .pdf copy at your earliest convenience.

Again, thank you for agreeing to participate, and please feel free to let us know if you have any questions.

Many thanks,

Brian and Matt

Brian M. Josef

Assistant Vice President, Regulatory Affairs

CTIA-The Wireless Association®

Expanding the Wireless Frontier

Twitter: @CTIAbmj

www.ctia.org

Direct: 202.736.3253 Mobile: 202.445.6000

It is CTIA's policy to comply fully with the antitrust laws. To ensure compliance, CTIA's employees and the representatives of CTIA member companies should follow this Checklist of antitrust "Do's" and "Don'ts" when participating in CTIA-sponsored activities: http://files.ctia.org/pdf/Antitrust_Checklist_for_CTIA_Meetings.pdf.

Washington Goes Mobile: Why Policy Matters

FCC-NTIA Experts on the Issues

Wednesday, September 9, 2015 – 2:00 pm - 3:00 pm

Mobile Intelligence Conference Center-Venetian Ballroom, “Washington Goes Mobile” Stage

From spectrum availability and the growth of mobile broadband adoption to public safety, infrastructure deployment and net neutrality, countless regulatory actions are brewing in the wireless space. FCC Commissioners’ and NTIA legal advisors hit on wireless hot topics.

Moderator(s): Brian Josef, Assistant Vice President of Regulatory Affairs, CTIA
Matt Gerst, Director in Regulatory Affairs, CTIA

Panelists: Jessica Almond, Legal Advisor to FCC Chairman Tom Wheeler
Brendan Carr, Legal Advisor to FCC Commissioner Ajit Pai
Derek Khlopin, Senior Advisor for Spectrum, Office of the Assistant Secretary, NTIA
Erin McGrath, Legal Advisor to FCC Commissioner Michael O’Rielly
Louis Peraertz, Legal Advisor to FCC Commissioner Mignon Clyburn
Johanna Thomas, Legal Advisor to FCC Commissioner Jessica Rosenworcel

1. Priorities: Turning the corner into election season next Fall brings into focus an evaluation of the Commission’s and NTIA’s goals over the next 12-18 months. Please spend a few minutes discussing your office’s priorities.
2. Incentive Auction: The 600 MHz Broadcast Television Incentive Auction will be critical to the wireless industry because it represents the last scheduled auction for wireless broadband and has the potential to make available much-needed spectrum to meet consumer demand. Of course, it also is unprecedented for its complexity.
 - a. What is left for the FCC to do between now and the FCC’s stated March 29th, 2016 auction start date to make this auction a reality and which of these issues are your bosses most focused on?
3. Spectrum Pipeline: Earlier this summer The Brattle Group, using the same formula and approach the FCC used to formulate the National Broadband Plan in 2010 and taking into account technical efficiencies and infrastructure investment, issued a paper estimating that we need to increase our existing supply of licensed spectrum by over 350 MHz by the end of this decade.
 - a. How can we unlock more licensed and unlicensed spectrum while improving federal agency incentives to refuel the spectrum pipeline?

4. Infrastructure: Wireless infrastructure has been – and will remain – a key component of reliable wireless service.
 - a. What are the key Commission and Administration infrastructure policies that can help to expedite wireless broadband infrastructure deployment?
5. Open Internet: It's no secret that CTIA challenged the FCC's Open Internet rules.
 - a. From the Commission's and Administration's perspectives, what will have the greatest impact on how consumers are able to access content from mobile broadband providers?
6. Privacy: Over the last few years, the regulatory agencies have taken a more aggressive approach to privacy and data security issues while carriers and manufacturers, in turn, have focused on protecting consumer privacy and complying with broad federal and state privacy laws. Recently, CTIA challenged the FCC's authority to expand its privacy authority under 222(a) of the Communications Act, which is limited to CPNI.
 - a. Given the existing scope of privacy protections and industry actions, how does your office view recent efforts and potential actions to consider more expansive privacy regulations?
7. Wireless Adoption: Over the years, the Commission has used many different tools to assist the rapid deployment of wireless services.
 - a. From your offices' perspectives, how would you describe the ways that wireless is meeting the diverse needs of consumers, whether low-income, people with disabilities, minorities, and small business owners?
 - b. What Commission policies have enabled the ability to meet these demands or could be further refined to help meet these demands?
8. FCC Process and Procedure: Are the FCC's processes, including equipment authorization or legacy regulation evaluations, capable of keeping up with the rapid pace of innovation that is the hallmark of the wireless industry?
 - a. In the context of spectrum policy, how do your offices think the FCC should achieve actions that protect against harmful interference while enabling "permission-less innovation," in the interests of consumers?
9. Voluntary Agreements: The FCC has looked to the wireless industry for voluntary commitments on several consumer and public safety-related issues. In recent instances, the industry has responded with good faith commitments – in some cases even formally amending the CTIA Wireless Consumer Code – even as the Commission ultimately adopted rules around these approaches.

- a. How should the Commission and Administration consider the impact that adopting rules based on voluntary commitments may have on the collaborative spirit for future voluntary commitments?
 - b. Does the voluntary commitment process allow agencies to address policy priorities without locking in specific mandates in perpetuity?
10. Lifeline: The FCC is taking a hard look at the Lifeline program, which provides direct support to low-income consumers. How does your office believe the FCC can modify the Lifeline program while maintaining low-income consumer choice and preference for wireless?

Washington Goes Mobile: Why Policy Matters

FCC-NTIA Experts on the Issues

Wednesday, September 9, 2015 – 2:00 pm - 3:00 pm
Mobile Intelligence Conference Center-Venetian Ballroom, “Washington Goes Mobile” Stage

From spectrum availability and the growth of mobile broadband adoption to public safety, infrastructure deployment and net neutrality, countless regulatory actions are brewing in the wireless space. FCC Commissioners’ and NTIA legal advisors hit on wireless hot topics.

Moderator(s): Brian Josef, Assistant Vice President of Regulatory Affairs, CTIA
Matt Gerst, Director in Regulatory Affairs, CTIA

Panelists: Jessica Almond, Legal Advisor to FCC Chairman Tom Wheeler
Brendan Carr, Legal Advisor to FCC Commissioner Ajit Pai
Derek Khlopin, Senior Advisor for Spectrum, Office of the Assistant Secretary, NTIA
Erin McGrath, Legal Advisor to FCC Commissioner Michael O’Rielly
Louis Peraertz, Legal Advisor to FCC Commissioner Mignon Clyburn
Johanna Thomas, Legal Advisor to FCC Commissioner Jessica Rosenworcel

1. Priorities: Turning the corner into election season next Fall brings into focus an evaluation of the Commission’s and NTIA’s goals over the next 12-18 months. Please spend a few minutes discussing your office’s priorities.
2. Incentive Auction: The 600 MHz Broadcast Television Incentive Auction will be critical to the wireless industry because it represents the last scheduled auction for wireless broadband and has the potential to make available much-needed spectrum to meet consumer demand. Of course, it also is unprecedented for its complexity.
 - a. What is left for the FCC to do between now and the FCC’s stated March 29th, 2016 auction start date to make this auction a reality and which of these issues are your bosses most focused on?
3. Spectrum Pipeline: Earlier this summer The Brattle Group, using the same formula and approach the FCC used to formulate the National Broadband Plan in 2010 and taking into account technical efficiencies and infrastructure investment, issued a paper estimating that we need to increase our existing supply of licensed spectrum by over 350 MHz by the end of this decade.
 - a. How can we unlock more licensed and unlicensed spectrum while improving federal agency incentives to refuel the spectrum pipeline?

4. Infrastructure: Wireless infrastructure has been – and will remain – a key component of reliable wireless service.

a. What are the key Commission and Administration infrastructure policies that can help to expedite wireless broadband infrastructure deployment?

~~5. Open Internet: It's no secret that CTIA challenged the FCC's Open Internet rules. While the appeal process will run its course, the Commission in the meantime has plans to take a number of next steps in the future, including a new Ombudsman, the potential for a broadband consumer disclosure box, a new privacy regime, enforcement procedures, and more.~~

~~5.~~
a. From the Commission's and Administration's perspectives, what will have the greatest impact on how consumers are able to access content from mobile broadband providers?

6. Privacy: Over the last few years, the regulatory agencies have taken a more aggressive approach to privacy and data security issues while carriers and manufacturers, in turn, have focused on protecting consumer privacy and complying with broad federal and state privacy laws. Recently, CTIA challenged the FCC's authority to expand its privacy authority under 222(a) of the Communications Act, which is limited to CPNI.

a. Given the existing scope of privacy protections and industry actions, how does your office view recent efforts and potential actions to consider more expansive privacy regulations?

~~7. Lifeline Wireless Adoption: Over the years, the Commission has used many different tools to assist the rapid deployment of wireless services.~~

~~a. From your offices' perspectives, how would you describe the ways that wireless is meeting the diverse needs of consumers, whether low-income, people with disabilities, minorities, and small business owners?~~

~~b. What Commission policies have enabled the ability to meet these demands or could be further refined to help meet these demands?~~

~~7. The FCC is taking a hard look at the Lifeline program, which provides direct support to low-income consumers. Wireless providers' impact on the Lifeline program is undeniable, with most eligible low-income consumer choosing wireless.~~

~~a. How does your office believe the FCC can modify the Lifeline program while maintaining low-income consumer choice and preference for wireless?~~

~~b. What kind of program reforms would need to be in place to reach levels of subscribership consistent with other low-income government assistance programs?~~

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.75"

Formatted: Indent: Left: 0.75", No bullets or numbering

Formatted

Formatted: Indent: Left: 1", No bullets or numbering

Formatted

Formatted: No bullets or numbering

Formatted: Indent: Left: 0"

Formatted: No bullets or numbering

8. FCC Process and Procedure: Are the FCC's processes, including equipment authorization or legacy regulation evaluations, capable of keeping up with the rapid pace of innovation that is the hallmark of the wireless industry?
 - a. In the context of spectrum policy, how do your offices think the FCC should achieve actions that protect against harmful interference while enabling "permission-less innovation," in the interests of consumers?

9. Voluntary Agreements: The FCC has looked to the wireless industry for voluntary commitments on several consumer and public safety-related issues. In recent instances, the industry has responded with good faith commitments – in some cases even formally amending the CTIA Wireless Consumer Code – even as the Commission ultimately adopted rules around these approaches.
 - a. How should the Commission and Administration consider the impact that adopting rules based on voluntary commitments may have on the collaborative spirit for future voluntary commitments?
 - b. Does the voluntary commitment process allow agencies to address policy priorities without locking in specific mandates in perpetuity?

10. Lifeline: The FCC is taking a hard look at the Lifeline program, which provides direct support to low-income consumers. How does your office believe the FCC can modify the Lifeline program while maintaining low-income consumer choice and preference for wireless?
 - b.

- Formatted: List Paragraph, No bullets or numbering
- Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.75"
- Formatted: No underline
- Formatted: Underline
- Formatted: Indent: Left: 1", No bullets or numbering

Erin McGrath

From: Scott Bergmann <SBergmann@ctia.org>
Sent: Monday, August 24, 2015 5:11 PM
To: Erin McGrath; Susan Fisenne
Cc: Krista Witanowski; Emma Prieskorn
Subject: CTIA Super Mobility Week – Commissioner Panel Questions and Speaker Release Form
Attachments: SM2015 Questions for Commissioner Panel.pdf; Speaker Release Form 2015.docx

Hi Erin and Susan,

I hope this finds you well. As mentioned, we are very excited that Commissioner O’Rielly will be joining us at Super Mobility 2015 and participating on the policy panel with his fellow Commissioners and CTIA President and CEO Meredith Attwell Baker on Thursday, September 10 from 2-3 p.m. at the Sands Expo and Convention Center, Venetian Ballroom.

To help you prepare for the panel, we are enclosing a list of questions that Meredith plans to ask of the Commissioner and his colleagues. As with last year’s panel, we have endeavored to create a lively format that will be both fun and easy for the Commissioners’ participation. The attached document describes the Q&A format and provides the planned questions. Of course, please let us know if you have any questions about the format or substance of the panel.

Additionally, we’re also attaching a Speaker Release Form for the Commissioner’s signature. If you could return a signed copy to us at your convenience, that would be appreciated.

As always, please let us know if you have any questions. We look forward to seeing you in September!

Many thanks,

Scott

Scott K. Bergmann

Vice President, Regulatory Affairs
CTIA – The Wireless Association®
Expanding the Wireless Frontier
1400 16th Street, NW Suite 600
Washington, DC 20036
www.ctia.org
Direct: 202.736.3660 Main: 202.785.0081
Mobile: 202.997.3916 Fax: 202.736.3685
Twitter: CTIASbergmann



September 9, 10 & 11, Las Vegas, Sands Expo
CTIASuperMobility2015.com

It is CTIA’s policy to comply fully with the antitrust laws. To ensure compliance, CTIA’s employees and the representatives of CTIA member companies should follow this Checklist of antitrust “Do’s” and “Don’ts” when participating in CTIA-sponsored activities: http://files.ctia.org/pdf/Antitrust_Checklist_for_CTIA_Meetings.pdf.

Washington Talks Wireless with Meredith Attwell Baker & FCC Commissioners

Thursday, September 10, 2015 – 2:00 PM - 3:00 PM

Location: Sands Expo and Convention Center, Venetian Ballroom

CTIA President and CEO Meredith Attwell Baker sits down with FCC Commissioners to discuss a range of wireless policy issues, including the upcoming 600 MHz Broadcast Incentive Auction, Open Internet regulations and more. Panelists offer insights on how best to ensure the continued growth of and investment in the nation's mobile ecosystem.

Moderator: Meredith Attwell Baker, President & CEO, CTIA

Panelist: Mignon Clyburn, Commissioner, FCC

Panelist: Jessica Rosenworcel, Commissioner, FCC (invited)

Panelist: Ajit Pai, Commissioner, FCC

Panelist: Michael O'Rielly, Commissioner, FCC



Participants and Equipment:

- 4 FCC Commissioners, 1 Moderator, 1 Electronic Board, and 12 Category App Icons

Order of Participants:

- The person with the longest FCC tenure (Commissioner Clyburn) selects a Category App Icon first.

Format:

- The first Commissioner (Commissioner Clyburn) selects a Category App Icon from the electronic board. [Note: The Commissioners will not need to physically select an icon from the board. Our IT folks will handle the electronic components].
- The Category App Icon shows the topic on which the question will be based. For example, if the "mHEALTH" Category App Icon is selected, Meredith will ask the question below about mHealth.
- The question will appear on the electronic board and will be read aloud by Meredith.
- The first asking Commissioner answers the question.
- Any other Commissioner who would like to answer may do so.
- After all Commissioners who want to answer the first question have done so, the second Commissioner in terms of tenure (Commissioner Rosenworcel (invited)) will select a Category App Icon.
- The discussion continues as described above until all questions are answered or time is up.

CATEGORY APP ICON	QUESTION
	<p>600 MHZ AUCTION: We are six months away from the scheduled start of the 600 MHz auction. In your mind, what are the one or two things that still need to happen for a successful auction?</p>
	<p>LIFELINE: 88% of eligible low-income Lifeline subscribers select wireless options today. How can the FCC make sure a modernized Lifeline program continues to reflect low-income consumers' preference for mobile solutions?</p>
	<p>MOBILE VIDEO: Mobile video accounted for 60% of all mobile data traffic at the end of last year, and is projected to grow nearly nine times by the end of the decade. How do you see the marketplace adapting to this shift in consumer behavior?</p>
	<p>LICENSED VS. UNLICENSED: CTIA is a strong advocate for making both licensed and unlicensed spectrum available. How can we best work together to ensure all spectrum users have access to all types of spectrum?</p>
	<p>INFRASTRUCTURE: The Commission has taken a number of important steps to help facilitate wireless siting across the country. As we see the proliferation of more small cell solutions, what else can the government do to promote more mobile broadband deployment?</p>
	<p>MORE SPECTRUM: We need 350 MHz of new licensed spectrum by 2020. What can the FCC do to help re-fill the spectrum pipeline after the 600 MHz auction and shorten the 13 years it takes to re-allocate spectrum?</p>

	<p>5G: The U.S. is the global leader in 4G. What steps can the FCC take to help ensure we retain our lead in 5G?</p>
	<p>mHEALTH: By the end of this year, mHealth could deliver up to \$290 billion in annual healthcare cost savings worldwide. What are biggest challenges to broader mHealth adoption and what role does spectrum play?</p>
	<p>HIGH BAND: As technology improves, more spectrum becomes available for mobile broadband use, including very high band spectrum. New technologies will require a mix of spectrum bands, how do we best preserve that balance?</p>
	<p>COMPETITION: Consumers benefit from the choice of four national wireless operators and multiple resellers and regional providers. How does that high degree of competition factor into your approach to wireless regulation?</p>
	<p>WHAT'S NEXT? You have executives in your office every day pitching what's next. In your mind, what is the next regulatory issues or challenge we don't spend enough time on today and that we should?</p>
	<p>PRIVACY: This fall, the FCC will be releasing an item to address broadband privacy as a result of the Open Internet Order. How do we best safeguard consumers' privacy, end regulatory uncertainty, and not end up with conflicting FTC/FCC mandates setting different rules for different players in our ecosystem?</p>

Amy Bender

From: Hilke, Catherine Michelle <catherine.hilke@verizon.com>
Sent: Friday, April 01, 2016 12:08 PM
To: Amy Bender
Subject: RE: Commissioner O'Rielly Statement - Privacy

Thanks!



Catherine M. Hilke
O 202.515.2438 | M 202.407.0592
catherine.hilke@verizon.com

From: Amy Bender [mailto:Amy.Bender@fcc.gov]
Sent: Friday, April 01, 2016 12:07 PM
To: Hilke, Catherine Michelle
Subject: [E] Fw: Commissioner O'Rielly Statement - Privacy

Just wanted to pass along his full written dissent on the privacy NPRM. Hope you are well.

From: Robert Bukowski <Robert.Bukowski@fcc.gov>
Sent: Friday, April 1, 2016 10:56 AM
To: Robert Bukowski
Cc: Robin Colwell; Erin McGrath; Amy Bender; Susan Fisenne
Subject: RE: Commissioner O'Rielly Statement - Privacy

Good morning,

Please see Commissioner O'Rielly's written statement on the Privacy NPRM attached. The full written statement on Lifeline will follow early next week.

Thank you,

Robert

From: Robin Colwell
Sent: Thursday, March 31, 2016 5:53 PM
To: Erin McGrath <Erin.McGrath@fcc.gov>; Amy Bender <Amy.Bender@fcc.gov>
Cc: Susan Fisenne <Susan.Fisenne@fcc.gov>; Robert Bukowski <Robert.Bukowski@fcc.gov>
Subject: Commissioner O'Rielly Statements

Good evening,

Attached please find some of Commissioner O'Rielly's statements from today's Open Meeting. Please note that the Lifeline statement (along with the two slides) is the spoken version as delivered today. His more substantive written dissent, along with his statement on the Privacy NPRM, will be available shortly.

-Robin

Robin Colwell
Chief of Staff and Legal Advisor, Media
Office of Commissioner Mike O'Rielly
Federal Communications Commission
202.418.2300

Amy Bender

From: Jennifer McKee <JMckee@NCTA.com>
Sent: Tuesday, March 01, 2016 3:08 PM
To: Amy Bender
Subject: Industry Associations Privacy Framework
Attachments: Industry Associations Principles for Broadband Privacy 3-1-16.pdf

Follow Up Flag: Follow up
Flag Status: Completed

Amy,

Attached is a copy of the letter that the associations are sending to the chairman today submitting a broadband privacy framework that we are hoping to have considered as part of any upcoming NPRM on the issue. If you have any questions or if you would like to discuss this further please feel free to give me a call. Thank you.

Jennifer McKee

Vice President and Associate General Counsel
National Cable & Telecommunications Association
25 Massachusetts Avenue, NW - Suite 100
Washington DC, 20001
Phone: 202-222-2460
Fax: 202-222-2446
Email: jmckee@ncta.com



March 1, 2016

The Honorable Tom Wheeler
Chairman
Federal Communications Commission
445 12th St. SW
Washington, D.C. 20554

Dear Chairman Wheeler,

Today, the American Cable Association, Competitive Carriers Association, CTIA, National Cable & Telecommunications Association, and USTelecom offer for the Commission's consideration a detailed proposal for a broadband privacy framework. After significant examination and analysis, these associations have developed the attached consensus Privacy Framework setting forth guidelines and principles to protect consumer privacy in a way that is consistent with other privacy laws that apply to companies providing services online. By adopting these principles, the Commission would establish a regime that protects consumer privacy and security while also providing flexibility for providers to implement and update their practices as consumer expectations and technologies evolve.

If the courts determine that the Commission has authority over broadband privacy, the FCC should focus on four privacy principles: (1) transparency; (2) respect for context and consumer choice; (3) data security; and (4) data breach notification. For each of these principles, the FCC should draw from and harmonize with the longstanding Federal Trade Commission unfairness and deception approach to privacy, which, before the FCC's reclassification decision, governed the privacy practices of all companies in the Internet ecosystem and will continue to apply to non-ISPs going forward.

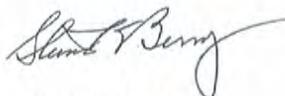
As the Commission develops its approach to broadband privacy, we respectfully request that it seek comment on the entirety of the Privacy Framework we submit today. Because regulation of broadband privacy is a new area for the Commission, it should take the necessary time to build a robust record rather than prejudge the issues by adopting tentative conclusions before there is a public discussion of the consensus Privacy Framework.

We look forward to continuing a conversation with the Commission about the best way to provide privacy and innovation benefits to consumers.

Respectfully submitted,



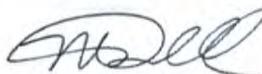
Matthew M. Polka
President & CEO
American Cable Association



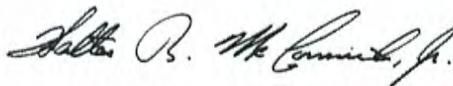
Steven K. Berry
President & CEO
Competitive Carriers Association



Meredith Attwell Baker
President & CEO
CTIA



Michael Powell
President & CEO
National Cable & Telecommunications Association



Walter B. McCormick, Jr.
President & CEO
USTelecom

cc: The Honorable Mignon Clyburn
The Honorable Jessica Rosenworcel
The Honorable Ajit Pai
The Honorable Michael O'Rielly

Privacy Framework

Discussion Paper

All entities in the Internet ecosystem should be subject to a consistent privacy framework with respect to consumer information. Consumer information should be protected based upon the sensitivity of the information to the consumer and how the information is used—not the type of business keeping it, how that business obtains it, or what regulatory agency has authority over it. Consumers should have consistent and predictable privacy protections for the information they deem private and sensitive, no matter how or with whom they share it. Consumers also will benefit from a consistent privacy framework that promotes the emergence of new business models and innovative uses of data that foster increased consumer choice and service customization.

The FCC should adopt an approach to privacy and data security for CPNI that is flexible, harmonized with the well-established and successful FTC framework, and backed up by strong but fair enforcement for unfair or deceptive acts or practices (UDAP) that materially harm consumers.¹ This well-tested consumer protection approach is consistent with the FCC's privacy recommendations in the 2010 National Broadband Plan, the FTC's and White House's 2012 Privacy Reports, and the White House's 2015 Consumer Privacy Bill of Rights, as well as with Chairman Wheeler's recent testimony before Congress acknowledging the importance of coordination with the FTC and harmonization with its privacy framework.

That approach will benefit consumers by safeguarding privacy interests as it has for years and will ensure that the same privacy and security framework applies to all entities in the Internet ecosystem. By leveraging a tested privacy model, the FCC will avoid inconsistent requirements that could otherwise hamper innovation and reduce competition. Most important, it will minimize consumer confusion as well as other harms associated with disparate privacy regulation across the ecosystem. Indeed, this approach will align with consumers' expectations that their data would be subject to consistent privacy rules regardless of whether it is used by their Internet Service Provider (ISP), application developers, operating systems, or edge providers.

When adopting a framework, the FCC should keep the following guidelines in mind:

- Consistent and Coordinated Regulatory Regimes. The FCC's rules and principles for regulating and enforcing privacy and security should be as similar as possible to the FTC approach, which will continue to govern other Internet ecosystem players' use and disclosure of the same or similar data. The consistent application of standards across sectors would fulfill the following key tenets in the White House Privacy Report: (1) avoid "inconsistent standards for related technologies" that could dampen innovation; (2)

¹ This framework is intended for discussion purposes, and we are not conceding that the FCC has authority to adopt privacy and security rules for Broadband Internet Access Services or over data related to consumers' use of Broadband Internet Access Services. To the extent it is determined that the FCC has such statutory authority, this document is intended to set forth principles for FCC consideration and possible adoption that are harmonized and consistent with the FTC and other government entities' approach to privacy and security for the same or similar data. Even if courts determine that the FCC's reclassification of Broadband Internet Access Services is a lawful exercise of authority, any rules must not exceed the text and legislative history of Section 222 of the Act.

foster a “level playing field for companies;” and, most importantly, (3) create “a consistent set of expectations for consumers.” To achieve this end, the FCC’s policies, rules, and enforcement practices should conform to the longstanding limiting principles articulated in the FTC’s Unfairness and Deception Policy Statements. In addition, the FCC and FTC can achieve their recent MOU’s stated goal of avoiding “duplicative, redundant or inconsistent oversight” by developing a new process to ensure that their substantive privacy policies and basis for enforcement are consistent going forward.

- Flexibility. The FCC’s approach should provide a flexible framework within which telecommunications service providers can implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments in this space. Specifically, this framework should identify the privacy or security *goals*, and afford providers flexibility in achieving those goals, rather than dictate the particular *methods* by which providers are expected to achieve those goals. Adopting a flexible approach also will help ensure consistent federal and state requirements governing customer information.
- Application. Consistent with the Communications Act and to eliminate unnecessary duplication of authority with other agencies, the FCC’s framework should only apply when 1) telecommunications service providers are providing telecommunications services and 2) the CPNI is made available by the customer to the telecommunications service provider solely by virtue of the carrier-customer relationship. The framework cannot lawfully apply to:
 - Providers’ non-telecommunications services and products
 - Providers’ non-telecommunications service provider affiliates
 - Information that is not made available to the carrier by the customer solely by virtue of the carrier-customer relationship
- Individually Identifiable. The FCC should carve out from the scope of its new framework any data that is de-identified, aggregated, or does not otherwise identify a known individual. The insights derived from the use of de-identified data can offer great benefits to consumers and society and such use avoids the sensitivities that may be associated with identified data.
- Unfair or Deceptive Conduct. As noted above, the FCC’s policies, rules, and enforcement practices should conform to the FTC’s longstanding limiting principles articulated in its Policy Statements on Unfairness (1980) and Deception (1983). This approach is consistent with the FCC’s commitment to conduct a cost-benefit analysis of its regulatory framework in accordance with President Obama’s Executive Orders 13563 and 13579, which require agencies to “adopt a regulation only upon a reasoned determination its benefits justify its costs” and “tailor its regulations to impose the least burden on society.”
 - Unfair Conduct. A provider acts unfairly if its act or practice (1) causes or is likely to cause substantial injury to consumers (2) which is not reasonably avoidable by consumers themselves, and (3) is not outweighed by countervailing benefits to consumers or to competition.
 - Deceptive Conduct. A provider acts deceptively if (1) it makes a statement or omission, or engages in a practice, that is likely to mislead a customer, (2) viewed from the perspective of a consumer acting reasonably under the circumstances, and (3) the deceptive statement, omission, or practice is material—meaning that

the misrepresentation or practice is likely to affect the consumer's conduct or decision with regard to a product or service.

- Additional Guidance. In coordination with other privacy regulators, the FCC could, like the FTC and various states like California, provide additional guidance on how it interprets its framework through workshops or reports. The FCC also could encourage and support the development and implementation of industry guidelines.
- Update and Harmonize Existing CPNI Rules. The existing CPNI rules should be revisited in their entirety and modernized to use the same flexible framework for all services subject to Section 222, including traditional voice services. In no event should the prescriptive outdated CPNI rules designed for legacy voice services apply to broadband services. Instead, a common set of flexible policies that allow providers to keep up with their customers' expectations and evolving technology should apply to both types of services.

With these guidelines in mind, if the courts determine that the FCC has authority to regulate broadband privacy, the FCC could adopt the following principles, which encompass and are consistent with the privacy and security framework that applies to the rest of the industry. Each of these principles and the goals noted above should provide flexibility for providers to implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments:

- Transparency. A telecommunications service provider should provide notice, which is neither deceptive nor unfair, describing the CPNI that it collects, how it will use the CPNI, and whether and for what purposes it may share CPNI with third parties.
- Respect for Context and Consumer Choice. A telecommunications service provider may use or disclose CPNI as is consistent with the context in which the customer provides, or the provider obtains, the information, provided that the provider's actions are not unfair or deceptive. For example, the use or disclosure of CPNI for the following commonly accepted data practices would not warrant a choice mechanism, either because customer consent can be inferred or because public policy considerations make choice unnecessary: product and service fulfillment, fraud prevention, compliance with law, responses to government requests, network management, first-party marketing, and affiliate sharing where the affiliate relationship is reasonably clear to consumers. Consistent with the flexible choice mechanisms available to all other entities in the Internet ecosystem, telecommunications service providers should give consumers easy-to-understand choices for non-contextual uses and disclosures of their CPNI, where the failure to provide choice would be deceptive or unfair. The provider should consider the sensitivity of the data and the context in which it was collected when determining the appropriate choice mechanism.
- Data Security. A telecommunications service provider should establish, implement, and maintain a CPNI data security program that is neither unfair nor deceptive and includes reasonable physical, technical, and administrative security safeguards to protect CPNI from unauthorized access, use, and disclosure. Providers' CPNI data security programs should provide reasonable protections in light of the nature and scope of the activities of the company, the sensitivity of the data, and the size and complexity of the relevant data operations of the company.

- Data Breach Notifications. Telecommunications service providers should notify customers whose CPNI has been breached when failure to notify would be unfair or deceptive. Given that breach investigations frequently are ongoing at the time providers offer notice to customers, a notice that turns out to be incomplete or inaccurate is not deceptive, as long as the provider corrects any material inaccuracies within a reasonable period of time of discovering them. Telecommunications providers have flexibility to determine how and when to provide such notice.

The FCC can ensure compliance with the above principles by pursuing reasonable enforcement actions against telecommunications service providers that have clearly violated these principles.

Amy Bender

From: Scott Bergmann <SBergmann@ctia.org>
Sent: Tuesday, May 10, 2016 7:15 PM
To: Erin McGrath; Amy Bender; Robin Colwell
Subject: Association Privacy Letter to Judiciary Committee
Attachments: Subcommittee Privacy Letter 5.10.16.pdf

Erin, Amy, Robin,

Just wanted to share with you this multi-association letter that was sent today to the Chair and Ranking Member of the Judiciary Committee's Subcommittee on Privacy, Technology, and the Law. The letter expresses support for a reasonable framework that adheres in all material respects to the successful FTC model that protected the privacy of broadband consumers for years, and applied uniformly to all entities in the broadband ecosystem.

Please let me know if you have any questions. Best,

Scott

Scott Bergmann
Vice President, Regulatory Affairs
1400 16th Street, NW
Washington, DC 20036
202-736-3660 (office)
202-997-3916 (mobile)
sbergmann@ctia.org



May 10, 2016

The Honorable Jeff Flake
Chairman
Subcommittee on Privacy, Technology, and the Law
Committee on the Judiciary
413 Russell Senate Office Building
Washington, D.C. 20510

The Honorable Al Franken
Ranking Member
Subcommittee on Privacy, Technology, and the Law
Committee on the Judiciary
309 Hart Senate Office Building
Washington, D.C. 20510

Dear Chairman Flake and Ranking Member Franken:

We write to commend the Subcommittee for its examination of the issues, and potential impact on consumers, competition, and innovation, arising from the Federal Communications Commission's recently proposed privacy rules for Internet Service Providers (ISPs).

The Internet has thrived under a single, unified privacy framework applicable to all entities collecting and using consumer data. Accordingly, we believe the FCC's primary objective should be to closely harmonize any ISP privacy rules it adopts with the existing FTC framework. There is nothing inherent in the FCC's decision to reclassify broadband as a Title II service that warrants departure from the FTC's successful approach to privacy based on effective notice to consumers and a meaningful choice as to how their data is used. Nothing has changed in the way ISPs collect and use data. The only thing that has changed is that the FCC's action in reclassifying broadband service has negated the FTC's power to apply its well-accepted framework to ISPs.

ISPs have strong incentives to earn and maintain their customers' loyalty by safeguarding their personal data, and considerable experience in meeting the requirements of the FTC privacy regime. As the FCC itself noted in its March 31 Notice of Proposed Rulemaking (NPRM), "[t]he importance of privacy protection is certainly not new to the nation's largest broadband providers, all of which have publicly available privacy policies, describing their use and sharing of confidential customer information."

Informed by this experience, a broad coalition urged the FCC to take the straightforward step of adopting a flexible, principles-based privacy regime that hews closely to the FTC's notice-and-choice framework applicable to the rest of the broadband ecosystem. The attached comprehensive privacy proposal includes important privacy principles such as transparency, respect for context, and choice. These concepts are at the core of the FTC framework that effectively balances the need to safeguard consumers' personal information and gives them choices over how their data is used with the benefits of enabling companies to use data in ways that foster innovation, competition, new services, and new capabilities. Adoption of this approach would be less disruptive for the broadband ecosystem, minimize consumer confusion, subject all Internet entities to comparable privacy regimes, and protect consumer privacy in a manner that provides the flexibility the marketplace needs in order to innovate and evolve.

The privacy regime proposed by the FCC in the NPRM departs from the FTC framework in significant and material respects. The FTC prudently has found that an opt-out approach should govern use of consumer data in most instances, with opt-in reserved for uses of the most sensitive consumer data. The FCC framework, however, would make opt-in the default consent mechanism for virtually all uses of customer data. This would lead to absurd results, such as restricting an ISP's ability to market accessories that work with a consumer's device. It also would make it difficult for consumers to have access to discounted offers from their providers. This broad opt-in requirement, irrespective of the sensitivity of data, would be inconsistent with common Internet practice and would harm consumer welfare. More important, it would be confusing to require consumers to opt-in to ISP data use and sharing because consumers would likely not understand how the opt-in regime would apply.

We appreciate the diligence shown by the members of the Subcommittee in examining the important issues surrounding the FCC's NPRM. We support a reasonable framework that adheres in all material respects to the successful FTC model that protected the privacy of broadband consumers for years, and applied uniformly to all entities in the broadband ecosystem. We are hopeful that your interest in, and oversight of, these issues will help to re-align the FCC's proposal more closely with the proven and effective approach administered by the FTC.

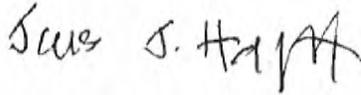
Sincerely,



Matthew M. Polka
President & CEO
American Cable Association



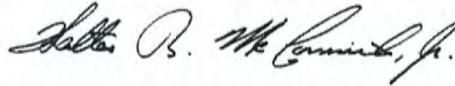
Meredith Attwell Baker
President & CEO
CTIA



Jim Halpert
President & CEO
Internet Commerce Coalition



Michael Powell
President & CEO
National Cable & Telecommunications Association



Walter B. McCormick, Jr.
President & CEO
USTelecom

cc: The Honorable Orrin G. Hatch
The Honorable David Perdue
The Honorable Mike Lee
The Honorable Thom Tillis
The Honorable Lindsey Graham
The Honorable Dianne Feinstein
The Honorable Charles E. Schumer
The Honorable Sheldon Whitehouse
The Honorable Christopher A. Coons

Privacy Framework

Discussion Paper

All entities in the Internet ecosystem should be subject to a consistent privacy framework with respect to consumer information. Consumer information should be protected based upon the sensitivity of the information to the consumer and how the information is used—not the type of business keeping it, how that business obtains it, or what regulatory agency has authority over it. Consumers should have consistent and predictable privacy protections for the information they deem private and sensitive, no matter how or with whom they share it. Consumers also will benefit from a consistent privacy framework that promotes the emergence of new business models and innovative uses of data that foster increased consumer choice and service customization.

The FCC should adopt an approach to privacy and data security for CPNI that is flexible, harmonized with the well-established and successful FTC framework, and backed up by strong but fair enforcement for unfair or deceptive acts or practices (UDAP) that materially harm consumers. This well-tested consumer protection approach is consistent with the FCC's privacy recommendations in the 2010 National Broadband Plan, the FTC's and White House's 2012 Privacy Reports, and the White House's 2015 Consumer Privacy Bill of Rights, as well as with Chairman Wheeler's recent testimony before Congress acknowledging the importance of coordination with the FTC and harmonization with its privacy framework.

That approach will benefit consumers by safeguarding privacy interests as it has for years and will ensure that the same privacy and security framework applies to all entities in the Internet ecosystem. By leveraging a tested privacy model, the FCC will avoid inconsistent requirements that could otherwise hamper innovation and reduce competition. Most important, it will minimize consumer confusion as well as other harms associated with disparate privacy regulation across the ecosystem. Indeed, this approach will align with consumers' expectations that their data would be subject to consistent privacy rules regardless of whether it is used by their Internet Service Provider (ISP), application developers, operating systems, or edge providers.

When adopting a framework, the FCC should keep the following guidelines in mind:

- **Consistent and Coordinated Regulatory Regimes.** The FCC's rules and principles for regulating and enforcing privacy and security should be as similar as possible to the FTC approach, which will continue to govern other Internet ecosystem players' use and disclosure of the same or similar data. The consistent application of standards across sectors would fulfill the following key tenets in the White House Privacy Report: (1) avoid "inconsistent standards for related technologies" that could dampen innovation; (2) foster a "level playing field for companies;" and, most importantly, (3) create "a consistent set of expectations for consumers." To achieve this end, the FCC's policies,

rules, and enforcement practices should conform to the longstanding limiting principles articulated in the FTC's Unfairness and Deception Policy Statements. In addition, the FCC and FTC can achieve their recent MOU's stated goal of avoiding "duplicative, redundant or inconsistent oversight" by developing a new process to ensure that their substantive privacy policies and basis for enforcement are consistent going forward.

- Flexibility. The FCC's approach should provide a flexible framework within which telecommunications service providers can implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments in this space. Specifically, this framework should identify the privacy or security *goals*, and afford providers flexibility in achieving those goals, rather than dictate the particular *methods* by which providers are expected to achieve those goals. Adopting a flexible approach also will help ensure consistent federal and state requirements governing customer information.
- Application. Consistent with the Communications Act and to eliminate unnecessary duplication of authority with other agencies, the FCC's framework should only apply when 1) telecommunications service providers are providing telecommunications services and 2) the CPNI is made available by the customer to the telecommunications service provider solely by virtue of the carrier-customer relationship. The framework cannot lawfully apply to:
 - Providers' non-telecommunications services and products
 - Providers' non-telecommunications service provider affiliates
 - Information that is not made available to the carrier by the customer solely by virtue of the carrier-customer relationship
- Individually Identifiable. The FCC should carve out from the scope of its new framework any data that is de-identified, aggregated, or does not otherwise identify a known individual. The insights derived from the use of de-identified data can offer great benefits to consumers and society and such use avoids the sensitivities that may be associated with identified data.
- Unfair or Deceptive Conduct. As noted above, the FCC's policies, rules, and enforcement practices should conform to the FTC's longstanding limiting principles articulated in its Policy Statements on Unfairness (1980) and Deception (1983). This approach is consistent with the FCC's commitment to conduct a cost-benefit analysis of its regulatory framework in accordance with President Obama's Executive Orders 13563 and 13579, which require agencies to "adopt a regulation only upon a reasoned determination its benefits justify its costs" and "tailor its regulations to impose the least burden on society."
 - Unfair Conduct. A provider acts unfairly if its act or practice (1) causes or is likely to cause substantial injury to consumers (2) which is not reasonably avoidable by consumers themselves, and (3) is not outweighed by countervailing benefits to consumers or to competition.
 - Deceptive Conduct. A provider acts deceptively if (1) it makes a statement or omission, or engages in a practice, that is likely to mislead a customer, (2) viewed from the perspective of a consumer acting reasonably under the circumstances, and (3) the deceptive statement, omission, or practice is material—meaning that the misrepresentation or practice is likely to affect the consumer's conduct or decision with regard to a product or service.

- Additional Guidance. In coordination with other privacy regulators, the FCC could, like the FTC and various states like California, provide additional guidance on how it interprets its framework through workshops or reports. The FCC also could encourage and support the development and implementation of industry guidelines.
- Update and Harmonize Existing CPNI Rules. The existing CPNI rules should be revisited in their entirety and modernized to use the same flexible framework for all services subject to Section 222, including traditional voice services. In no event should the prescriptive outdated CPNI rules designed for legacy voice services apply to broadband services. Instead, a common set of flexible policies that allow providers to keep up with their customers' expectations and evolving technology should apply to both types of services.

With these guidelines in mind, if the courts determine that the FCC has authority to regulate broadband privacy, the FCC could adopt the following principles, which encompass and are consistent with the privacy and security framework that applies to the rest of the industry. Each of these principles and the goals noted above should provide flexibility for providers to implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments:

- Transparency. A telecommunications service provider should provide notice, which is neither deceptive nor unfair, describing the CPNI that it collects, how it will use the CPNI, and whether and for what purposes it may share CPNI with third parties.
- Respect for Context and Consumer Choice. A telecommunications service provider may use or disclose CPNI as is consistent with the context in which the customer provides, or the provider obtains, the information, provided that the provider's actions are not unfair or deceptive. For example, the use or disclosure of CPNI for the following commonly accepted data practices would not warrant a choice mechanism, either because customer consent can be inferred or because public policy considerations make choice unnecessary: product and service fulfillment, fraud prevention, compliance with law, responses to government requests, network management, first-party marketing, and affiliate sharing where the affiliate relationship is reasonably clear to consumers. Consistent with the flexible choice mechanisms available to all other entities in the Internet ecosystem, telecommunications service providers should give consumers easy-to-understand choices for non-contextual uses and disclosures of their CPNI, where the failure to provide choice would be deceptive or unfair. The provider should consider the sensitivity of the data and the context in which it was collected when determining the appropriate choice mechanism.
- Data Security. A telecommunications service provider should establish, implement, and maintain a CPNI data security program that is neither unfair nor deceptive and includes reasonable physical, technical, and administrative security safeguards to protect CPNI from unauthorized access, use, and disclosure. Providers' CPNI data security programs should provide reasonable protections in light of the nature and scope of the activities of the company, the sensitivity of the data, and the size and complexity of the relevant data operations of the company.
- Data Breach Notifications. Telecommunications service providers should notify customers whose CPNI has been breached when failure to notify would be unfair or

deceptive. Given that breach investigations frequently are ongoing at the time providers offer notice to customers, a notice that turns out to be incomplete or inaccurate is not deceptive, as long as the provider corrects any material inaccuracies within a reasonable period of time of discovering them. Telecommunications providers have flexibility to determine how and when to provide such notice.

The FCC can ensure compliance with the above principles by pursuing reasonable enforcement actions against telecommunications service providers that have clearly violated these principles.

cc: The Honorable Mignon Clyburn
The Honorable Jessica Rosenworcel
The Honorable Ajit Pai
The Honorable Michael O'Rielly

Amy Bender

From: Scott Bergmann <SBergmann@ctia.org>
Sent: Thursday, February 11, 2016 8:51 AM
To: Amy Bender
Subject: Fwd: Joint Association Letter on Privacy
Attachments: image001.png; ATT00001.htm; Privacy Letter Final 523pm.pdf; ATT00002.htm

Hi Amy, as mentioned. I am at an appointment this morning but will give you a call later to catch up. If you have any urgent questions, just call my mobile.

Scott

Begin forwarded message:

From: Scott Bergmann <SBergmann@ctia.org<mailto:SBergmann@ctia.org>>
Date: February 11, 2016 at 7:36:51 AM EST
To: Scott Bergmann <SBergmann@ctia.org<mailto:SBergmann@ctia.org>>
Subject: Joint Association Letter on Privacy

Attached please find a joint association letter filed today calling on the FCC, to the extent that it initiates a proceeding addressing broadband privacy, to develop a framework that offers consumers robust privacy protection, while at the same time allowing broadband providers to continue to innovate and compete. The letter - filed by ACA, CCA, CTA, CTIA, ICC, NCTA, and US Telecom - recommends that any FCC framework be consistent with the successful FTC approach, grounded on prohibiting unfairness and deception.

Please let me know if you have any questions. Best,

Scott



February 11, 2016

The Honorable Tom Wheeler
Chairman
Federal Communications Commission
445 12th St. SW
Washington, D.C. 20554

Dear Chairman Wheeler,

As associations representing a large cross-section of the technology companies that make up today's vibrant Internet economy, our collective members are committed to providing consumers with innovative products and services and are equally committed to earning consumer trust and respecting privacy. If the courts determine that the FCC has authority to regulate broadband privacy, we encourage you to develop a framework that offers consumers robust privacy protection, while at the same time allowing broadband providers to continue to innovate and compete. We recommend that any FCC framework be consistent with the successful FTC approach, which is grounded on prohibiting unfairness and deception. The FTC's time-tested framework has accomplished two important goals—it provides consumers with meaningful privacy protection and helps to enable a dynamic marketplace that supports the emergence of innovative new business models. By developing a consistent framework, the FCC will further these important goals.

Our member companies recognize that ensuring robust privacy protection is important and have devoted substantial capital, resources and personnel to develop, maintain, and enhance meaningful data privacy and security programs. Indeed, our companies have strong incentives to earn and maintain their customers' loyalty by protecting their data. In the rapidly evolving online marketplace, our companies want to ensure that they can continue to provide such protections while meeting consumers' expectation of continued access to new innovations that enhance their experience.

All companies in the Internet ecosystem, including Internet service providers, have long operated under the FTC regulatory regime for protecting consumer privacy. The aim of this well-tested approach is to combine strong protections for consumers with flexibility that allows for rapid innovation. Under the FTC regime, all companies in the Internet ecosystem must ensure that

their privacy and data security practices are neither deceptive nor unfair. As a result, consumers are protected and all companies that collect consumer data should be able to innovate and adapt to the inevitable changes in technology and the market for online services.

We understand the FCC is considering initiating a proceeding to consider how Section 222 of the Communications Act, which governs Customer Proprietary Network Information (“CPNI”), should apply to broadband Internet access service. The applicability of Section 222 in this context is currently subject to judicial review. If the Commission nonetheless moves forward in this space, consumers would be best served by an approach to privacy and data security for CPNI that is harmonized with the FTC’s established privacy protection framework based on enforcement against unfair and deceptive acts or practices.

You have recognized that the FTC has a longstanding, thoughtful, and rational approach to privacy, and you have committed to working closely with the FTC and to developing a consistent privacy framework for Internet service providers. Ensuring consistency with this effective consumer protection approach would be in accordance with statements supporting the FTC’s privacy regime and endorsing the benefits of a consistent privacy framework for the Internet in the 2010 National Broadband Plan, the FTC’s and White House’s 2012 Privacy Reports, and the White House’s 2015 Consumer Privacy Bill of Rights.

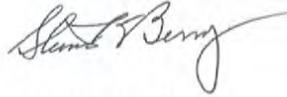
We believe it is important to maintain a consistent privacy framework for the Internet. Such an approach will protect consumers and avoid entity-based regulation that would create consumer confusion and stifle innovation. Consumers expect their data will be subject to consistent privacy standards based upon the sensitivity of the information and how it is used regardless of which entity in the Internet ecosystem uses that data. To achieve parity across the Internet ecosystem, any FCC framework for Internet service providers should be reflective of the deception and unfairness standard, consistent with the existing protections consumers receive when they engage with other companies in the Internet ecosystem.

A consistent privacy framework for the Internet also will continue to provide Internet service providers with the flexibility to update their practices in ways that meet the evolving privacy and data security needs of their customers and ensure they can provide their customers new products and customized services. Such a framework would identify privacy or security goals, and afford providers, including smaller providers with limited resources, flexibility in achieving those goals. Rules dictating specific methods quickly become out of date and out of step with constantly changing technology, and will only hamper innovation and harm consumers.

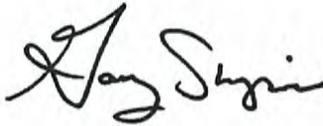
In short, if you seek to initiate a proceeding under Section 222, we respectfully urge you to ensure that the FCC acts in a manner consistent with the strong current national privacy framework applied by the FTC to other companies in the Internet ecosystem. This flexible approach would meet consumers’ privacy needs while allowing them to take advantage of innovative products and services, and would avoid inconsistent oversight. We look forward to continuing a conversation with the FCC about the best way to provide privacy and innovation benefits to consumers.



Matthew M. Polka
President & CEO
American Cable Association



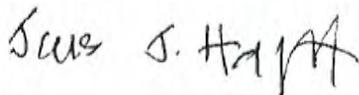
Steven K. Berry
President & CEO
Competitive Carriers Association



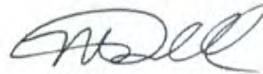
Gary Shapiro
President & CEO
Consumer Technology Association



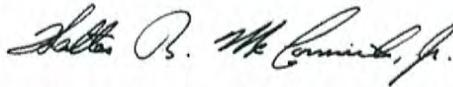
Meredith Attwell Baker
President & CEO
CTIA



Jim Halpert
President & CEO
Internet Commerce Coalition



Michael Powell
President & CEO
National Cable & Telecommunications Association



Walter B. McCormick, Jr.
President & CEO
U.S. Telecom Association

cc: The Honorable Mignon Clyburn
The Honorable Jessica Rosenworcel
The Honorable Ajit Pai
The Honorable Michael O'Rielly

Amy Bender

From: Emma Prieskorn <EPrieskorn@ctia.org>
Sent: Wednesday, March 09, 2016 3:45 PM
To: Robert Bukowski
Cc: Scott Bergmann; Debbie Matties; Amy Bender
Subject: CTIA Meeting Request: Broadband Privacy NPRM

Hi Robert,

I'm reaching out (again) to schedule a meeting with Amy Bender to discuss the FCC's upcoming Broadband Privacy NPRM. Attending the meeting from CTIA will be Scott Bergmann and Debbie Matties. We are hoping to schedule the meeting sometime during the week of March 14th.

Feel free to let me know if you have any questions.

Many thanks,

Emma



Emma (Keech) Prieskorn

Coordinator, Regulatory Affairs

1400 16th Street, NW

Washington, DC 20036

202-736-3671 (office)

Amy Bender

From: Scott Bergmann <SBergmann@ctia.org>
Sent: Wednesday, February 10, 2016 5:28 PM
To: Amy Bender
Subject: Message

Hi Amy, just left you a detailed message on your voicemail about a joint trade association filing that will happen tomorrow concerning broadband privacy. I'd be happy to talk in more detail tonight if you like (just call my mobile – 2-2.997.3916), and I will send the letter tomorrow as soon as final. Best,

Scott



Scott Bergmann

Vice President, Regulatory Affairs

1400 16th Street, NW

Washington, DC 20036

202-736-3660 (office)

202-997-3916 (mobile)

sbergmann@ctia.org

Erin McGrath

From: Debbie Matties <DMatties@ctia.org>
Sent: Wednesday, September 09, 2015 1:19 PM
To: Erin McGrath
Subject: Re: FCC/FTC privacy session today at 12:30

Great! Let me know if I can do anything to help get you situated. We've not met before, when we meet you'll recognize me by my plum dress. And thanks for putting the Commissioner's correct email address on the message.

From: Erin McGrath <Erin.McGrath@fcc.gov>
Sent: Wednesday, September 9, 2015 1:07 PM
To: Debbie Matties; Ohlhausen, Maureen; 'morielly@fcc.gov'; Robin Colwell; Chilson, Neil; Mike O'Rielly
Subject: Re: FCC/FTC privacy session today at 12:30

We just landed.

Sent from my BlackBerry 10 smartphone on the Verizon Wireless 4G LTE network.

Original Message
From: Debbie Matties
Sent: Wednesday, September 9, 2015 9:54 AM
To: Ohlhausen, Maureen; 'morielly@fcc.gov'; Robin Colwell; Chilson, Neil; Erin McGrath; Mike O'Rielly
Subject: Re: FCC/FTC privacy session today at 12:30

Great. Adding Erin McGrath from Commissioner O'Rielly's office - sorry I didn't include you earlier. And I'm not sure that I had Commissioner O'Rielly's email correct; I added another version.

From: Ohlhausen, Maureen <mohlhausen@ftc.gov>
Sent: Wednesday, September 9, 2015 12:46 PM
To: Debbie Matties; 'morielly@fcc.gov'; 'robin.colwell@fcc.gov'; Chilson, Neil
Subject: Re: FCC/FTC privacy session today at 12:30

I'll be there by 12:10. Thanks Debbie.

Maureen

----- Original Message -----

From: Debbie Matties [mailto:DMatties@ctia.org]
Sent: Wednesday, September 09, 2015 12:43 PM
To: Ohlhausen, Maureen; morielly@fcc.gov <morielly@fcc.gov>; Robin Colwell <robin.colwell@fcc.gov>; Chilson, Neil
Subject: FCC/FTC privacy session today at 12:30

Hello Commissioners O'Rielly and Ohlhausen, Robin and Neil,

Checking in to make sure everyone is hear and will be ready to go at 12:30. You will be on the "Washington Goes Mobile" stage in the Venetian Ballroom. The Venetian Ballroom is on the right as you're walking into the Sands Convention Center from the Palazzo/Venetian. The entrance is before you get to the keynote ballroom.

I will plan to get there by about 12:10, and I will have paper copies of the attached session notes and questions.

In the meantime, if there's anything I can do for you, please don't hesitate to email or call - my number is 202-758-7697.

See you soon!

Debbie

Debbie Matties
Vice President, Privacy
CTIA-The Wireless Association®
1400 16th Street, NW Suite 600
Washington, DC 20036
www.ctia.org
Direct: 202.736.3654
Wireless: 202.758.7697

Erin McGrath

From: Chilson, Neil <nchilson@ftc.gov>
Sent: Thursday, August 27, 2015 5:46 PM
To: Erin McGrath
Subject: RE: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel

Sounds good! Thank you.

From: Erin McGrath [mailto:Erin.McGrath@fcc.gov]
Sent: Thursday, August 27, 2015 5:18 PM
To: Chilson, Neil; Scott Bergmann
Cc: Robin Colwell; Debbie Matties
Subject: RE: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel

We will run this by the boss as soon as possible. The Commissioner and Robin are (b) (6), so there may be a delay in our response.

Erin

From: Chilson, Neil [mailto:nchilson@ftc.gov]
Sent: Thursday, August 27, 2015 5:12 PM
To: Erin McGrath <Erin.McGrath@fcc.gov>; Scott Bergmann <SBergmann@ctia.org>
Cc: Robin Colwell <Robin.Colwell@fcc.gov>; Debbie Matties <DMatties@ctia.org>
Subject: RE: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel

Erin,

Thanks! I had pinged Robin just to chat about the upcoming panel (Sorry to disturb (b) Robin!), but of course I'm glad to work with you. About the proposed format: Debbie suggested, and Maureen agreed, that it would maximize the use of the 30 minutes if there was no moderator. Instead, we thought that it would be fun if the two commissioners "interviewed" each other, perhaps even swapping chairs half way through the session. Maureen likes this idea, and Robin said she thought that sounded ok but I'm not sure she was able to run it past Commissioner O'Rielly. Could you see if that works for him?

Assuming so, my understanding is that we need to 1) draft a summary of the panel (my crack at it below) and 2) swap "interview" questions (i.e., I would write questions for Mike to ask Maureen, and you would write questions for Maureen to ask Mike) and then add edits or drop questions. I can get started on those questions right away.

Glad to talk about any of this!

FTC Commissioner Maureen K. Ohlhausen and FCC Commissioner Michael P. O'Rielly recently joined forces in the pages of the Wall Street Journal to explain how the FCC's Net Neutrality order may create tension between the FTC and FCC over privacy and data security issues, ultimately harming consumers. Come watch as they interview each other about privacy and data security initiatives at their respective agencies and how regulatory humility and process reform could improve consumer privacy and security outcomes in the year ahead.

From: Erin McGrath [<mailto:Erin.McGrath@fcc.gov>]
Sent: Thursday, August 27, 2015 4:44 PM
To: Scott Bergmann; Chilson, Neil
Cc: Robin Colwell; Debbie Matties
Subject: RE: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel

Thanks. Robin has been on (b) (6) so I wanted to make sure that there wasn't anything that you needed from us. I will be traveling with the Commissioner at CTIA, so please feel free to contact me if anything is needed.

Erin

From: Scott Bergmann [<mailto:Sbergmann@ctia.org>]
Sent: Thursday, August 27, 2015 4:41 PM
To: Erin McGrath <Erin.McGrath@fcc.gov>; Nchilson@ftc.gov
Cc: Robin Colwell <Robin.Colwell@fcc.gov>; Debbie Matties <DMatties@ctia.org>
Subject: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel

Hi Erin and Neil,

I wanted to make a virtual introduction for you both, and to thank you once again for your commissioners' participation at Super Mobility 2015. My understanding is that Neil and Robin have been coordinating on the Commissioners' joint panel, but we wanted to loop in Erin who also staffs Commissioner O'Rielly.

I am also copying my colleague, Debbie Matties, who is our CTIA POC for this panel. Of course, please let me know if there is any assistance I can provide as you prepare for the show and panel. Best regards,

Scott

Scott K. Bergmann
Vice President, Regulatory Affairs
CTIA – The Wireless Association®
Expanding the Wireless Frontier
1400 16th Street, NW Suite 600
Washington, DC 20036
www.ctia.org
Direct: 202.736.3660 Main: 202.785.0081
Mobile: 202.997.3916 Fax: 202.736.3685
Twitter: CTIASbergmann

From: Debbie Matties
Sent: Thursday, July 30, 2015 10:54 PM
To: Robin.Colwell@fcc.gov; Neil Chilson (Nchilson@ftc.gov)
Cc: Kathryn Dall'Asta (KDallasta@ctia.org); Heather Lee
Subject: CTIA 2015 SuperMobility - government privacy panel on Sept. 9 - new time and details

Dear Robin and Neil,

We're delighted that Commissioners Ohlhausen and O'Reilly will be participating at the CTIA show in September. This email contains some information that will be useful. Heather Lee from our convention team, copied here, will arrange for you to get additional logistical information, including registration if you haven't already registered.

As noted in the subject line, we've had one more change of time for this panel. My apologies for any inconvenience this may cause. The panel is now on **Wednesday, September 9 at 12:30 – 1:00pm**. Please confirm that this new time is acceptable for you.

Neil has agreed to take on the task of providing a title and description for your slot, and I trust he will work with Robin to ensure that both Commissioners are comfortable with it. When you have that ready to go, please send it to us. If you would prefer to provide some bullets or topics, we can draft the title and description for you. In any event, our conventions team may need to edit the title and description for clarity, length, or style.

I will be out of town (b) (6) starting next week, returning the week of the 24th. If you should have any questions in my absence, my colleague Kathryn Dall'Asta is a good point of contact in addition to Heather in our conventions office.

We look forward to seeing you in September in Las Vegas!

Best regards,

Debbie Matties

Vice President, Privacy
CTIA-The Wireless Association®
1400 16th Street, NW Suite 600
Washington, DC 20036
www.ctia.org
Direct: 202.736.3654
Wireless: 202.758.7697

Erin McGrath

From: Debbie Matties <DMatties@ctia.org>
Sent: Friday, August 28, 2015 9:49 AM
To: Chilson, Neil; Erin McGrath
Cc: Robin Colwell; Scott Bergmann
Subject: RE: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel

Thanks Neil and Erin – we really appreciate your work in putting this great session together. I would be happy to assist as needed on the substance – we could jump on the phone today or sometime next week if that would be helpful.

We're working on finalizing materials for the educational programs, so the sooner we can get the description for the session taken care of the better. What Neil has below looks good to me. We also need a title – I propose "FTC Commissioner Ohlhausen and FCC Commissioner O'Reilly: A Conversation about Data Security and Privacy" but I welcome revisions.

From: Chilson, Neil [mailto:nchilson@ftc.gov]
Sent: Thursday, August 27, 2015 5:12 PM
To: 'Erin McGrath'; Scott Bergmann
Cc: Robin Colwell; Debbie Matties
Subject: RE: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel

Erin,

Thanks! I had pinged Robin just to chat about the upcoming panel (Sorry to disturb (b) Robin!), but of course I'm glad to work with you. About the proposed format: Debbie suggested, and Maureen agreed, that it would maximize the use of the 30 minutes if there was no moderator. Instead, we thought that it would be fun if the two commissioners "interviewed" each other, perhaps even swapping chairs half way through the session. Maureen likes this idea, and Robin said she thought that sounded ok but I'm not sure she was able to run it past Commissioner O'Rielly. Could you see if that works for him?

Assuming so, my understanding is that we need to 1) draft a summary of the panel (my crack at it below) and 2) swap "interview" questions (i.e., I would write questions for Mike to ask Maureen, and you would write questions for Maureen to ask Mike) and then add edits or drop questions. I can get started on those questions right away.

Glad to talk about any of this!

FTC Commissioner Maureen K. Ohlhausen and FCC Commissioner Michael P. O'Rielly recently joined forces in the pages of the Wall Street Journal to explain how the FCC's Net Neutrality order may create tension between the FTC and FCC over privacy and data security issues, ultimately harming consumers. Come watch as they interview each other about privacy and data security initiatives at their respective agencies and how regulatory humility and process reform could improve consumer privacy and security outcomes in the year ahead.

From: Erin McGrath [mailto:Erin.McGrath@fcc.gov]
Sent: Thursday, August 27, 2015 4:44 PM
To: Scott Bergmann; Chilson, Neil
Cc: Robin Colwell; Debbie Matties
Subject: RE: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel

Thanks. Robin has been (b) (6) so I wanted to make sure that there wasn't anything that you needed from us. I will be traveling with the Commissioner at CTIA, so please feel free to contact me if anything is needed.

Erin

From: Scott Bergmann [<mailto:SBergmann@ctia.org>]
Sent: Thursday, August 27, 2015 4:41 PM
To: Erin McGrath <Erin.McGrath@fcc.gov>; Nchilson@ftc.gov
Cc: Robin Colwell <Robin.Colwell@fcc.gov>; Debbie Matties <DMatties@ctia.org>
Subject: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel

Hi Erin and Neil,

I wanted to make a virtual introduction for you both, and to thank you once again for your commissioners' participation at Super Mobility 2015. My understanding is that Neil and Robin have been coordinating on the Commissioners' joint panel, but we wanted to loop in Erin who also staffs Commissioner O'Rielly.

I am also copying my colleague, Debbie Matties, who is our CTIA POC for this panel. Of course, please let me know if there is any assistance I can provide as you prepare for the show and panel. Best regards,

Scott

Scott K. Bergmann
Vice President, Regulatory Affairs
CTIA – The Wireless Association®
Expanding the Wireless Frontier
1400 16th Street, NW Suite 600
Washington, DC 20036
www.ctia.org
Direct: 202.736.3660 Main: 202.785.0081
Mobile: 202.997.3916 Fax: 202.736.3685
Twitter: CTIASbergmann

From: Debbie Matties
Sent: Thursday, July 30, 2015 10:54 PM
To: Robin.Colwell@fcc.gov; Neil Chilson (Nchilson@ftc.gov)
Cc: Kathryn Dall'Asta (KDallasta@ctia.org); Heather Lee
Subject: CTIA 2015 SuperMobility - government privacy panel on Sept. 9 - new time and details

Dear Robin and Neil,

We're delighted that Commissioners Ohlhausen and O'Reilly will be participating at the CTIA show in September. This email contains some information that will be useful. Heather Lee from our convention team, copied here, will arrange for you to get additional logistical information, including registration if you haven't already registered.

As noted in the subject line, we've had one more change of time for this panel. My apologies for any inconvenience this may cause. The panel is now on **Wednesday, September 9 at 12:30 – 1:00pm**. Please confirm that this new time is acceptable for you.

Neil has agreed to take on the task of providing a title and description for your slot, and I trust he will work with Robin to ensure that both Commissioners are comfortable with it. When you have that ready to go, please send it to us. If you would prefer to provide some bullets or topics, we can draft the title and description for you. In any event, our conventions team may need to edit the title and description for clarity, length, or style.

I will be out of town on leave starting next week, returning the week of the 24th. If you should have any questions in my absence, my colleague Kathryn Dall'Asta is a good point of contact in addition to Heather in our conventions office.

We look forward to seeing you in September in Las Vegas!

Best regards,

Debbie Matties

Vice President, Privacy
CTIA-The Wireless Association®
1400 16th Street, NW Suite 600
Washington, DC 20036
www.ctia.org
Direct: 202.736.3654
Wireless: 202.758.7697

Erin McGrath

From: Chilson, Neil <nchilson@ftc.gov>
Sent: Friday, September 04, 2015 6:46 PM
To: Robin Colwell; Erin McGrath
Cc: Debbie Matties (DMatties@ctia.org)
Subject: RE: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel
Attachments: WASHINGTON GOES MOBILE - Questions and Stage Directions.docx

Hello, all!

Attached are draft questions and stage directions for the two Commissioners. We're glad to tweak, obviously, but I wanted to circulate now as this event is coming up quickly! Please let me know if you have any questions or thoughts.

Have a great weekend.

-Neil

From: Chilson, Neil
Sent: Thursday, September 03, 2015 7:09 PM
To: 'Robin Colwell'; Erin McGrath
Subject: RE: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel

Robin and Erin,

Below are the questions we suggest would be good for Mike to ask Maureen at their co-interview next week. Of course, you should feel absolutely free to inject Mike's own voice and any new questions. Let me know if I can help with formulating the questions Maureen should ask Mike.

Thanks!

- Here at CTIA, many people are intimately familiar with the FCC. But they may be less familiar with the FTC's enforcement authority and its actions on privacy and data security specifically. Can you please snapshot the Commission's legal authority and general agency process?
- What is the FTC's role in U.S. privacy and data security? Can you give some recent examples of FTC enforcement actions and policy initiatives in the privacy and data security sphere?
- Under the FTC Act, the FTC is precluded from bringing enforcement actions against "common carriers." How does this exemption work? What does it cover? And how does the FCC's recent reclassification of broadband as a Title II service interact with the FTC's common carrier exemption?
- As we've discussed, FCC staff is investigating how to apply CPNI rules, designed to protect specific types of telephone data, to broadband ISPs. How important is it that these rules, if established, are compatible with the privacy approach of the FTC?
- How is the FTC's track record on protecting consumer privacy while promoting the innovation that ultimately improves consumers' lives? What agency structures have contributed to this track record? What could the FCC learn from the FTC on this?

From: Robin Colwell [<mailto:Robin.Colwell@fcc.gov>]
Sent: Wednesday, September 02, 2015 3:48 PM
To: Debbie Matties; Chilson, Neil; Erin McGrath; Scott Bergmann
Subject: RE: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel

Hello all, sorry for the delay on our end but the description looks good to us. Looking forward to it!
-Robin

From: Debbie Matties [<mailto:DMatties@ctia.org>]
Sent: Wednesday, September 02, 2015 3:14 PM
To: Chilson, Neil <nchilson@fcc.gov>; Erin McGrath <Erin.McGrath@fcc.gov>; Scott Bergmann <SBergmann@ctia.org>
Cc: Robin Colwell <Robin.Colwell@fcc.gov>
Subject: RE: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel

Thanks for following up, Neil. Erin and Robin, can you please let us know by **COB tomorrow, Thursday, September 3**, whether you have any objections to the description below?

From: Chilson, Neil [<mailto:nchilson@fcc.gov>]
Sent: Wednesday, September 02, 2015 9:04 AM
To: 'Erin McGrath'; Scott Bergmann
Cc: Robin Colwell; Debbie Matties
Subject: RE: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel

Erin and Robin,

Hi! Hope everyone's (b) (6) was great. We're creeping up on the panel next week and CTIA needs the OK to publish the blurb below. Of course, any changes are welcome. Just let us know.

Thanks,
-Neil

From: Erin McGrath [<mailto:Erin.McGrath@fcc.gov>]
Sent: Thursday, August 27, 2015 5:18 PM
To: Chilson, Neil; Scott Bergmann
Cc: Robin Colwell; Debbie Matties
Subject: RE: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel

We will run this by the boss as soon as possible. The Commissioner and Robin are (b) (6) until Monday, so there may be a delay in our response.

Erin

From: Chilson, Neil [<mailto:nchilson@fcc.gov>]
Sent: Thursday, August 27, 2015 5:12 PM
To: Erin McGrath <Erin.McGrath@fcc.gov>; Scott Bergmann <SBergmann@ctia.org>
Cc: Robin Colwell <Robin.Colwell@fcc.gov>; Debbie Matties <DMatties@ctia.org>
Subject: RE: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel

Erin,

Thanks! I had pinged Robin just to chat about the upcoming panel (Sorry to disturb (b) Robin!), but of course I'm glad to work with you. About the proposed format: Debbie suggested, and Maureen agreed, that it would maximize the use of the 30 minutes if there was no moderator. Instead, we thought that it would be fun if the two commissioners "interviewed" each other, perhaps even swapping chairs half way through the session. Maureen likes this idea, and Robin said she thought that sounded ok but I'm not sure she was able to run it past Commissioner O'Rielly. Could you see if that works for him?

Assuming so, my understanding is that we need to 1) draft a summary of the panel (my crack at it below) and 2) swap "interview" questions (i.e., I would write questions for Mike to ask Maureen, and you would write questions for Maureen to ask Mike) and then add edits or drop questions. I can get started on those questions right away.

Glad to talk about any of this!

FTC Commissioner Maureen K. Ohlhausen and FCC Commissioner Michael P. O'Rielly recently joined forces in the pages of the Wall Street Journal to explain how the FCC's Net Neutrality order may create tension between the FTC and FCC over privacy and data security issues, ultimately harming consumers. Come watch as they interview each other about privacy and data security initiatives at their respective agencies and how regulatory humility and process reform could improve consumer privacy and security outcomes in the year ahead.

From: Erin McGrath [<mailto:Erin.McGrath@fcc.gov>]
Sent: Thursday, August 27, 2015 4:44 PM
To: Scott Bergmann; Chilson, Neil
Cc: Robin Colwell; Debbie Matties
Subject: RE: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel

Thanks. Robin has been on (b) (6) so I wanted to make sure that there wasn't anything that you needed from us. I will be traveling with the Commissioner at CTIA, so please feel free to contact me if anything is needed.

Erin

From: Scott Bergmann [<mailto:SBergmann@ctia.org>]
Sent: Thursday, August 27, 2015 4:41 PM
To: Erin McGrath <Erin.McGrath@fcc.gov>; Nchilson@ftc.gov
Cc: Robin Colwell <Robin.Colwell@fcc.gov>; Debbie Matties <DMatties@ctia.org>
Subject: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel

Hi Erin and Neil,

I wanted to make a virtual introduction for you both, and to thank you once again for your commissioners' participation at Super Mobility 2015. My understanding is that Neil and Robin have been coordinating on the Commissioners' joint panel, but we wanted to loop in Erin who also staffs Commissioner O'Rielly.

I am also copying my colleague, Debbie Matties, who is our CTIA POC for this panel. Of course, please let me know if there is any assistance I can provide as you prepare for the show and panel. Best regards,

Scott

Scott K. Bergmann
Vice President, Regulatory Affairs

CTIA – The Wireless Association®

Expanding the Wireless Frontier

1400 16th Street, NW Suite 600

Washington, DC 20036

www.ctia.org

Direct: 202.736.3660 Main: 202.785.0081

Mobile: 202.997.3916 Fax: 202.736.3685

Twitter: CTIAsbergmann

From: Debbie Matties

Sent: Thursday, July 30, 2015 10:54 PM

To: Robin.Colwell@fcc.gov; Neil Chilson (Nchilson@ftc.gov)

Cc: Kathryn Dall'Asta (KDallasta@ctia.org); Heather Lee

Subject: CTIA 2015 SuperMobility - government privacy panel on Sept. 9 - new time and details

Dear Robin and Neil,

We're delighted that Commissioners Ohlhausen and O'Reilly will be participating at the CTIA show in September. This email contains some information that will be useful. Heather Lee from our convention team, copied here, will arrange for you to get additional logistical information, including registration if you haven't already registered.

As noted in the subject line, we've had one more change of time for this panel. My apologies for any inconvenience this may cause. The panel is now on **Wednesday, September 9 at 12:30 – 1:00pm**. Please confirm that this new time is acceptable for you.

Neil has agreed to take on the task of providing a title and description for your slot, and I trust he will work with Robin to ensure that both Commissioners are comfortable with it. When you have that ready to go, please send it to us. If you would prefer to provide some bullets or topics, we can draft the title and description for you. In any event, our conventions team may need to edit the title and description for clarity, length, or style.

I will be out of town on leave starting next week, returning the week of the 24th. If you should have any questions in my absence, my colleague Kathryn Dall'Asta is a good point of contact in addition to Heather in our conventions office.

We look forward to seeing you in September in Las Vegas!

Best regards,

Debbie Matties

Vice President, Privacy

CTIA-The Wireless Association®

1400 16th Street, NW Suite 600

Washington, DC 20036

www.ctia.org

Direct: 202.736.3654

Wireless: 202.758.7697

**WASHINGTON GOES MOBILE - FTC Commissioner Ohlhausen and FCC
Commissioner O’Rielly: A Conversation about Data Security and Privacy
Room: Venetian Ballroom
Wednesday, September 09, 2015: 12:30 PM - 1:00 PM**

[Enter stage; Maureen sits in Interviewer chair; Mike sits in Interviewee chair]

[MAUREEN INTERVIEWING MIKE] Commissioner O, it’s great to see you again. To the audience, welcome to the only panel at CTIA where agency Commissioners with similar initials interview each other! I’m Commissioner Maureen Ohlhausen from the FTC and this is Commissioner Mike O’Rielly from the FCC! We have a great crowd today, but only a short amount of time, so let me jump right into the questions.

- You recently co-authored a terrific op-ed in the WSJ, titled “The Consequences of a Washington Internet Power Grab.” Can you summarize for the crowd why you wrote that article and what are its key takeaways from that article?
- What is the FCC’s current role in consumer privacy and data security? What recent developments might affect that role, and how?
- The FCC’s enforcement bureau recently settled a case against TerraCom and YourTel, downward adjusting a base fine of \$9 *billion* dollars, to a “mere” \$10 million. The majority – you dissented - brought a Notice of Apparent Liability under section 222 of the Act. You worked on the Hill when this section of the Act was passed. What did Congress intend section 222 to cover, and why did you vote against the TerraCom and YourTel NAL?
- You’ve made a name for yourself calling for process reform at the FCC. In fact, you issued a series of detailed proposals on the FCC’s blog, and have repeatedly spoken about the need for such reforms. What are the biggest process problems at the FCC, and what are your top three fixes?

Commissioner O, thank you for the time. I know you are booked right after this segment, so let’s end it there.

[Swap chairs; pause in silence for a moment, get in character]

[*MIKE INTERVIEWING MAUREEN*] Commissioner O, it's great to see you again. To the audience, welcome **back** to the only panel at CTIA where agency Commissioners with similar initials interview each other! You're a great crowd, but we have even less time now, so let me jump right into the questions.

- Here at CTIA, many people are intimately familiar with the FCC. But they may be less familiar with the FTC's enforcement authority and its actions on privacy and data security specifically. Can you please snapshot the Commission's legal authority and general agency process?
- What is the FTC's role in U.S. privacy and data security policy? Can you give some recent examples of FTC enforcement actions and policy initiatives in the privacy and data security sphere?
- Under the FTC Act, the FTC is precluded from bringing enforcement actions against "common carriers." How does this exemption work? What does it cover? And how does the FCC's recent reclassification of broadband as a Title II service interact with the FTC's common carrier exemption?
- As we've discussed, FCC staff is investigating how to apply CPNI rules, designed to protect specific types of telephone data, to broadband ISPs. How important is it that these rules, if established, are compatible with the privacy approach of the FTC?
- How is the FTC's track record on protecting consumer privacy while promoting the innovation that ultimately improves consumers' lives? What agency structures have contributed to this track record? What could the FCC learn from the FTC on this?

[*Mike speaking*] Commissioner O, it's been a real pleasure speaking with you today.

[*Maureen speaking*] Commissioner O, the pleasure has been all mine.

[*Both*] Let's thank Commissioner O. [*Applause*] Thank you!

Erin McGrath

From: Debbie Matties <DMatties@ctia.org>
Sent: Wednesday, September 02, 2015 5:12 PM
To: Robin Colwell; Chilson, Neil; Erin McGrath; Scott Bergmann
Subject: RE: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel

Wonderful! We'll get this put up on the website as soon as we can. Not sure how fast, as our convention team is being stretched in all directions at the moment!

From: Robin Colwell [mailto:Robin.Colwell@fcc.gov]
Sent: Wednesday, September 02, 2015 3:48 PM
To: Debbie Matties; Chilson, Neil; Erin McGrath; Scott Bergmann
Subject: RE: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel

Hello all, sorry for the delay on our end but the description looks good to us. Looking forward to it!
-Robin

From: Debbie Matties [mailto:DMatties@ctia.org]
Sent: Wednesday, September 02, 2015 3:14 PM
To: Chilson, Neil <nchilson@fcc.gov>; Erin McGrath <Erin.McGrath@fcc.gov>; Scott Bergmann <SBergmann@ctia.org>
Cc: Robin Colwell <Robin.Colwell@fcc.gov>
Subject: RE: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel

Thanks for following up, Neil. Erin and Robin, can you please let us know by **COB tomorrow, Thursday, September 3**, whether you have any objections to the description below?

From: Chilson, Neil [mailto:nchilson@fcc.gov]
Sent: Wednesday, September 02, 2015 9:04 AM
To: 'Erin McGrath'; Scott Bergmann
Cc: Robin Colwell; Debbie Matties
Subject: RE: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel

Erin and Robin,

Hi! Hope everyone's (b) (6) was great. We're creeping up on the panel next week and CTIA needs the OK to publish the blurb below. Of course, any changes are welcome. Just let us know.

Thanks,
-Neil

From: Erin McGrath [mailto:Erin.McGrath@fcc.gov]
Sent: Thursday, August 27, 2015 5:18 PM
To: Chilson, Neil; Scott Bergmann
Cc: Robin Colwell; Debbie Matties
Subject: RE: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel

We will run this by the boss as soon as possible. The Commissioner and Robin are (b) (6) until Monday, so there may be a delay in our response.

Erin

From: Chilson, Neil [<mailto:nchilson@ftc.gov>]
Sent: Thursday, August 27, 2015 5:12 PM
To: Erin McGrath <Erin.McGrath@fcc.gov>; Scott Bergmann <SBergmann@ctia.org>
Cc: Robin Colwell <Robin.Colwell@fcc.gov>; Debbie Matties <DMatties@ctia.org>
Subject: RE: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel

Erin,

Thanks! I had pinged Robin just to chat about the upcoming panel (Sorry to disturb (b) Robin!), but of course I'm glad to work with you. About the proposed format: Debbie suggested, and Maureen agreed, that it would maximize the use of the 30 minutes if there was no moderator. Instead, we thought that it would be fun if the two commissioners "interviewed" each other, perhaps even swapping chairs half way through the session. Maureen likes this idea, and Robin said she thought that sounded ok but I'm not sure she was able to run it past Commissioner O'Rielly. Could you see if that works for him?

Assuming so, my understanding is that we need to 1) draft a summary of the panel (my crack at it below) and 2) swap "interview" questions (i.e., I would write questions for Mike to ask Maureen, and you would write questions for Maureen to ask Mike) and then add edits or drop questions. I can get started on those questions right away.

Glad to talk about any of this!

FTC Commissioner Maureen K. Ohlhausen and FCC Commissioner Michael P. O'Rielly recently joined forces in the pages of the Wall Street Journal to explain how the FCC's Net Neutrality order may create tension between the FTC and FCC over privacy and data security issues, ultimately harming consumers. Come watch as they interview each other about privacy and data security initiatives at their respective agencies and how regulatory humility and process reform could improve consumer privacy and security outcomes in the year ahead.

From: Erin McGrath [<mailto:Erin.McGrath@fcc.gov>]
Sent: Thursday, August 27, 2015 4:44 PM
To: Scott Bergmann; Chilson, Neil
Cc: Robin Colwell; Debbie Matties
Subject: RE: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel

Thanks. Robin has been (b) (6) so I wanted to make sure that there wasn't anything that you needed from us. I will be traveling with the Commissioner at CTIA, so please feel free to contact me if anything is needed.

Erin

From: Scott Bergmann [<mailto:SBergmann@ctia.org>]
Sent: Thursday, August 27, 2015 4:41 PM
To: Erin McGrath <Erin.McGrath@fcc.gov>; Nchilson@ftc.gov
Cc: Robin Colwell <Robin.Colwell@fcc.gov>; Debbie Matties <DMatties@ctia.org>
Subject: CTIA Super Mobility 2015: Commissioners O'Rielly and Ohlhausen Panel

Hi Erin and Neil,

I wanted to make a virtual introduction for you both, and to thank you once again for your commissioners' participation at Super Mobility 2015. My understanding is that Neil and Robin have been coordinating on the Commissioners' joint panel, but we wanted to loop in Erin who also staffs Commissioner O'Rielly.

I am also copying my colleague, Debbie Matties, who is our CTIA POC for this panel. Of course, please let me know if there is any assistance I can provide as you prepare for the show and panel. Best regards,

Scott

Scott K. Bergmann

Vice President, Regulatory Affairs

CTIA – The Wireless Association®

Expanding the Wireless Frontier

1400 16th Street, NW Suite 600

Washington, DC 20036

www.ctia.org

Direct: 202.736.3660 Main: 202.785.0081

Mobile: 202.997.3916 Fax: 202.736.3685

Twitter: CTIASbergmann

From: Debbie Matties

Sent: Thursday, July 30, 2015 10:54 PM

To: Robin.Colwell@fcc.gov; Neil Chilson (Nchilson@ftc.gov)

Cc: Kathryn Dall'Asta (KDallasta@ctia.org); Heather Lee

Subject: CTIA 2015 SuperMobility - government privacy panel on Sept. 9 - new time and details

Dear Robin and Neil,

We're delighted that Commissioners Ohlhausen and O'Reilly will be participating at the CTIA show in September. This email contains some information that will be useful. Heather Lee from our convention team, copied here, will arrange for you to get additional logistical information, including registration if you haven't already registered.

As noted in the subject line, we've had one more change of time for this panel. My apologies for any inconvenience this may cause. The panel is now on **Wednesday, September 9 at 12:30 – 1:00pm**. Please confirm that this new time is acceptable for you.

Neil has agreed to take on the task of providing a title and description for your slot, and I trust he will work with Robin to ensure that both Commissioners are comfortable with it. When you have that ready to go, please send it to us. If you would prefer to provide some bullets or topics, we can draft the title and description for you. In any event, our conventions team may need to edit the title and description for clarity, length, or style.

I will be out of town on leave starting next week, returning the week of the 24th. If you should have any questions in my absence, my colleague Kathryn Dall'Asta is a good point of contact in addition to Heather in our conventions office.

We look forward to seeing you in September in Las Vegas!

Best regards,

Debbie Matties

Vice President, Privacy

CTIA-The Wireless Association®
1400 16th Street, NW Suite 600
Washington, DC 20036
www.ctia.org
Direct: 202.736.3654
Wireless: 202.758.7697

Mike O'Rielly

From: Debbie Matties <DMatties@ctia.org>
Sent: Wednesday, September 09, 2015 12:52 PM
To: Ohlhausen, Maureen; 'morielly@fcc.gov'; Robin Colwell; Chilson, Neil; Erin McGrath; Mike O'Rielly
Subject: Re: FCC/FTC privacy session today at 12:30

Great. Adding Erin McGrath from Commissioner O'Rielly's office - sorry I didn't include you earlier. And I'm not sure that I had Commissioner O'Rielly's email correct; I added another version.

From: Ohlhausen, Maureen <mohlhausen@fcc.gov>
Sent: Wednesday, September 9, 2015 12:46 PM
To: Debbie Matties; 'morielly@fcc.gov'; 'robin.colwell@fcc.gov'; Chilson, Neil
Subject: Re: FCC/FTC privacy session today at 12:30

I'll be there by 12:10. Thanks Debbie.

Maureen

----- Original Message -----

From: Debbie Matties [mailto:DMatties@ctia.org]
Sent: Wednesday, September 09, 2015 12:43 PM
To: Ohlhausen, Maureen; morielly@fcc.gov <morielly@fcc.gov>; Robin Colwell <robin.colwell@fcc.gov>; Chilson, Neil
Subject: FCC/FTC privacy session today at 12:30

Hello Commissioners O'Rielly and Ohlhausen, Robin and Neil,

Checking in to make sure everyone is hear and will be ready to go at 12:30. You will be on the "Washington Goes Mobile" stage in the Venetian Ballroom. The Venetian Ballroom is on the right as you're walking into the Sands Convention Center from the Palazzo/Venetian. The entrance is before you get to the keynote ballroom.

I will plan to get there by about 12:10, and I will have paper copies of the attached session notes and questions.

In the meantime, if there's anything I can do for you, please don't hesitate to email or call - my number is 202-758-7697.

See you soon!

Debbie

Debbie Matties
Vice President, Privacy
CTIA-The Wireless Association®
1400 16th Street, NW Suite 600

Joanne Wall

From: Scott Bergmann <SBergmann@ctia.org>
Sent: Tuesday, March 01, 2016 2:15 PM
To: Nicholas Degani
Cc: Brendan Carr
Subject: Letter on Consensus Privacy Framework
Attachments: Wheeler Letter Re Privacy Principles 3 1 16.pdf

Hi Nick,

Following up on my voicemail, attached please find a letter sent today by ACA, CCA, CTIA, NCTA, and USTelecom to FCC Chairman Wheeler setting forth guidelines and principles for the FCC to consider as it moves forward with a rulemaking on broadband privacy. This consensus privacy framework will protect consumer privacy in a way that is consistent with other privacy laws that apply to other companies in the Internet ecosystem. We hope the FCC will seek comment on this consensus framework, in its entirety, in its upcoming rulemaking proceeding.

As always, please let me know if you have any questions. Best,

Scott



Scott Bergmann

Vice President, Regulatory Affairs

1400 16th Street, NW

Washington, DC 20036

202-736-3660 (office)

202-997-3916 (mobile)

sbergmann@ctia.org



March 1, 2016

The Honorable Tom Wheeler
Chairman
Federal Communications Commission
445 12th St. SW
Washington, D.C. 20554

Dear Chairman Wheeler,

Today, the American Cable Association, Competitive Carriers Association, CTIA, National Cable & Telecommunications Association, and USTelecom offer for the Commission's consideration a detailed proposal for a broadband privacy framework. After significant examination and analysis, these associations have developed the attached consensus Privacy Framework setting forth guidelines and principles to protect consumer privacy in a way that is consistent with other privacy laws that apply to companies providing services online. By adopting these principles, the Commission would establish a regime that protects consumer privacy and security while also providing flexibility for providers to implement and update their practices as consumer expectations and technologies evolve.

If the courts determine that the Commission has authority over broadband privacy, the FCC should focus on four privacy principles: (1) transparency; (2) respect for context and consumer choice; (3) data security; and (4) data breach notification. For each of these principles, the FCC should draw from and harmonize with the longstanding Federal Trade Commission unfairness and deception approach to privacy, which, before the FCC's reclassification decision, governed the privacy practices of all companies in the Internet ecosystem and will continue to apply to non-ISPs going forward.

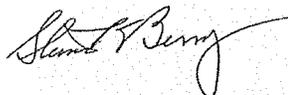
As the Commission develops its approach to broadband privacy, we respectfully request that it seek comment on the entirety of the Privacy Framework we submit today. Because regulation of broadband privacy is a new area for the Commission, it should take the necessary time to build a robust record rather than prejudge the issues by adopting tentative conclusions before there is a public discussion of the consensus Privacy Framework.

We look forward to continuing a conversation with the Commission about the best way to provide privacy and innovation benefits to consumers.

Respectfully submitted,



Matthew M. Polka
President & CEO
American Cable Association



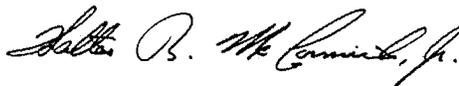
Steven K. Berry
President & CEO
Competitive Carriers Association



Meredith Attwell Baker
President & CEO
CTIA



Michael Powell
President & CEO
National Cable & Telecommunications Association



Walter B. McCormick, Jr.
President & CEO
USTelecom

cc: The Honorable Mignon Clyburn
The Honorable Jessica Rosenworcel
The Honorable Ajit Pai
The Honorable Michael O’Rielly

Privacy Framework

Discussion Paper

All entities in the Internet ecosystem should be subject to a consistent privacy framework with respect to consumer information. Consumer information should be protected based upon the sensitivity of the information to the consumer and how the information is used—not the type of business keeping it, how that business obtains it, or what regulatory agency has authority over it. Consumers should have consistent and predictable privacy protections for the information they deem private and sensitive, no matter how or with whom they share it. Consumers also will benefit from a consistent privacy framework that promotes the emergence of new business models and innovative uses of data that foster increased consumer choice and service customization.

The FCC should adopt an approach to privacy and data security for CPNI that is flexible, harmonized with the well-established and successful FTC framework, and backed up by strong but fair enforcement for unfair or deceptive acts or practices (UDAP) that materially harm consumers.¹ This well-tested consumer protection approach is consistent with the FCC's privacy recommendations in the 2010 National Broadband Plan, the FTC's and White House's 2012 Privacy Reports, and the White House's 2015 Consumer Privacy Bill of Rights, as well as with Chairman Wheeler's recent testimony before Congress acknowledging the importance of coordination with the FTC and harmonization with its privacy framework.

That approach will benefit consumers by safeguarding privacy interests as it has for years and will ensure that the same privacy and security framework applies to all entities in the Internet ecosystem. By leveraging a tested privacy model, the FCC will avoid inconsistent requirements that could otherwise hamper innovation and reduce competition. Most important, it will minimize consumer confusion as well as other harms associated with disparate privacy regulation across the ecosystem. Indeed, this approach will align with consumers' expectations that their data would be subject to consistent privacy rules regardless of whether it is used by their Internet Service Provider (ISP), application developers, operating systems, or edge providers.

When adopting a framework, the FCC should keep the following guidelines in mind:

- Consistent and Coordinated Regulatory Regimes. The FCC's rules and principles for regulating and enforcing privacy and security should be as similar as possible to the FTC approach, which will continue to govern other Internet ecosystem players' use and disclosure of the same or similar data. The consistent application of standards across sectors would fulfill the following key tenets in the White House Privacy Report: (1) avoid "inconsistent standards for related technologies" that could dampen innovation; (2)

¹ This framework is intended for discussion purposes, and we are not conceding that the FCC has authority to adopt privacy and security rules for Broadband Internet Access Services or over data related to consumers' use of Broadband Internet Access Services. To the extent it is determined that the FCC has such statutory authority, this document is intended to set forth principles for FCC consideration and possible adoption that are harmonized and consistent with the FTC and other government entities' approach to privacy and security for the same or similar data. Even if courts determine that the FCC's reclassification of Broadband Internet Access Services is a lawful exercise of authority, any rules must not exceed the text and legislative history of Section 222 of the Act.

foster a “level playing field for companies;” and, most importantly, (3) create “a consistent set of expectations for consumers.” To achieve this end, the FCC’s policies, rules, and enforcement practices should conform to the longstanding limiting principles articulated in the FTC’s Unfairness and Deception Policy Statements. In addition, the FCC and FTC can achieve their recent MOU’s stated goal of avoiding “duplicative, redundant or inconsistent oversight” by developing a new process to ensure that their substantive privacy policies and basis for enforcement are consistent going forward.

- Flexibility. The FCC’s approach should provide a flexible framework within which telecommunications service providers can implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments in this space. Specifically, this framework should identify the privacy or security *goals*, and afford providers flexibility in achieving those goals, rather than dictate the particular *methods* by which providers are expected to achieve those goals. Adopting a flexible approach also will help ensure consistent federal and state requirements governing customer information.
- Application. Consistent with the Communications Act and to eliminate unnecessary duplication of authority with other agencies, the FCC’s framework should only apply when 1) telecommunications service providers are providing telecommunications services and 2) the CPNI is made available by the customer to the telecommunications service provider solely by virtue of the carrier-customer relationship. The framework cannot lawfully apply to:
 - Providers’ non-telecommunications services and products
 - Providers’ non-telecommunications service provider affiliates
 - Information that is not made available to the carrier by the customer solely by virtue of the carrier-customer relationship
- Individually Identifiable. The FCC should carve out from the scope of its new framework any data that is de-identified, aggregated, or does not otherwise identify a known individual. The insights derived from the use of de-identified data can offer great benefits to consumers and society and such use avoids the sensitivities that may be associated with identified data.
- Unfair or Deceptive Conduct. As noted above, the FCC’s policies, rules, and enforcement practices should conform to the FTC’s longstanding limiting principles articulated in its Policy Statements on Unfairness (1980) and Deception (1983). This approach is consistent with the FCC’s commitment to conduct a cost-benefit analysis of its regulatory framework in accordance with President Obama’s Executive Orders 13563 and 13579, which require agencies to “adopt a regulation only upon a reasoned determination its benefits justify its costs” and “tailor its regulations to impose the least burden on society.”
 - Unfair Conduct. A provider acts unfairly if its act or practice (1) causes or is likely to cause substantial injury to consumers (2) which is not reasonably avoidable by consumers themselves, and (3) is not outweighed by countervailing benefits to consumers or to competition.
 - Deceptive Conduct. A provider acts deceptively if (1) it makes a statement or omission, or engages in a practice, that is likely to mislead a customer, (2) viewed from the perspective of a consumer acting reasonably under the circumstances, and (3) the deceptive statement, omission, or practice is material—meaning that

the misrepresentation or practice is likely to affect the consumer's conduct or decision with regard to a product or service.

- Additional Guidance. In coordination with other privacy regulators, the FCC could, like the FTC and various states like California, provide additional guidance on how it interprets its framework through workshops or reports. The FCC also could encourage and support the development and implementation of industry guidelines.
- Update and Harmonize Existing CPNI Rules. The existing CPNI rules should be revisited in their entirety and modernized to use the same flexible framework for all services subject to Section 222, including traditional voice services. In no event should the prescriptive outdated CPNI rules designed for legacy voice services apply to broadband services. Instead, a common set of flexible policies that allow providers to keep up with their customers' expectations and evolving technology should apply to both types of services.

With these guidelines in mind, if the courts determine that the FCC has authority to regulate broadband privacy, the FCC could adopt the following principles, which encompass and are consistent with the privacy and security framework that applies to the rest of the industry. Each of these principles and the goals noted above should provide flexibility for providers to implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments:

- Transparency. A telecommunications service provider should provide notice, which is neither deceptive nor unfair, describing the CPNI that it collects, how it will use the CPNI, and whether and for what purposes it may share CPNI with third parties.
- Respect for Context and Consumer Choice. A telecommunications service provider may use or disclose CPNI as is consistent with the context in which the customer provides, or the provider obtains, the information, provided that the provider's actions are not unfair or deceptive. For example, the use or disclosure of CPNI for the following commonly accepted data practices would not warrant a choice mechanism, either because customer consent can be inferred or because public policy considerations make choice unnecessary: product and service fulfillment, fraud prevention, compliance with law, responses to government requests, network management, first-party marketing, and affiliate sharing where the affiliate relationship is reasonably clear to consumers. Consistent with the flexible choice mechanisms available to all other entities in the Internet ecosystem, telecommunications service providers should give consumers easy-to-understand choices for non-contextual uses and disclosures of their CPNI, where the failure to provide choice would be deceptive or unfair. The provider should consider the sensitivity of the data and the context in which it was collected when determining the appropriate choice mechanism.
- Data Security. A telecommunications service provider should establish, implement, and maintain a CPNI data security program that is neither unfair nor deceptive and includes reasonable physical, technical, and administrative security safeguards to protect CPNI from unauthorized access, use, and disclosure. Providers' CPNI data security programs should provide reasonable protections in light of the nature and scope of the activities of the company, the sensitivity of the data, and the size and complexity of the relevant data operations of the company.

- Data Breach Notifications. Telecommunications service providers should notify customers whose CPNI has been breached when failure to notify would be unfair or deceptive. Given that breach investigations frequently are ongoing at the time providers offer notice to customers, a notice that turns out to be incomplete or inaccurate is not deceptive, as long as the provider corrects any material inaccuracies within a reasonable period of time of discovering them. Telecommunications providers have flexibility to determine how and when to provide such notice.

The FCC can ensure compliance with the above principles by pursuing reasonable enforcement actions against telecommunications service providers that have clearly violated these principles.

Joanne Wall

From: Scott Bergmann <SBergmann@ctia.org>
Sent: Tuesday, May 10, 2016 7:16 PM
To: Brendan Carr; Nicholas Degani
Subject: Association Privacy Letter to Judiciary Committee
Attachments: Subcommittee Privacy Letter 5.10.16.pdf

Brendan, Nick,

Just wanted to share with you this multi-association letter that was sent today to the Chair and Ranking Member of the Judiciary Committee's Subcommittee on Privacy, Technology, and the Law. The letter expresses support for a reasonable framework that adheres in all material respects to the successful FTC model that protected the privacy of broadband consumers for years, and applied uniformly to all entities in the broadband ecosystem.

Please let me know if you have any questions. Best,

Scott

Scott Bergmann
Vice President, Regulatory Affairs
1400 16th Street, NW
Washington, DC 20036
202-736-3660 (office)
202-997-3916 (mobile)
sbergmann@ctia.org



May 10, 2016

The Honorable Jeff Flake
Chairman
Subcommittee on Privacy, Technology, and the Law
Committee on the Judiciary
413 Russell Senate Office Building
Washington, D.C. 20510

The Honorable Al Franken
Ranking Member
Subcommittee on Privacy, Technology, and the Law
Committee on the Judiciary
309 Hart Senate Office Building
Washington, D.C. 20510

Dear Chairman Flake and Ranking Member Franken:

We write to commend the Subcommittee for its examination of the issues, and potential impact on consumers, competition, and innovation, arising from the Federal Communications Commission's recently proposed privacy rules for Internet Service Providers (ISPs).

The Internet has thrived under a single, unified privacy framework applicable to all entities collecting and using consumer data. Accordingly, we believe the FCC's primary objective should be to closely harmonize any ISP privacy rules it adopts with the existing FTC framework. There is nothing inherent in the FCC's decision to reclassify broadband as a Title II service that warrants departure from the FTC's successful approach to privacy based on effective notice to consumers and a meaningful choice as to how their data is used. Nothing has changed in the way ISPs collect and use data. The only thing that has changed is that the FCC's action in reclassifying broadband service has negated the FTC's power to apply its well-accepted framework to ISPs.

ISPs have strong incentives to earn and maintain their customers' loyalty by safeguarding their personal data, and considerable experience in meeting the requirements of the FTC privacy regime. As the FCC itself noted in its March 31 Notice of Proposed Rulemaking (NPRM), "[t]he importance of privacy protection is certainly not new to the nation's largest broadband providers, all of which have publicly available privacy policies, describing their use and sharing of confidential customer information."

Informed by this experience, a broad coalition urged the FCC to take the straightforward step of adopting a flexible, principles-based privacy regime that hews closely to the FTC's notice-and-choice framework applicable to the rest of the broadband ecosystem. The attached comprehensive privacy proposal includes important privacy principles such as transparency, respect for context, and choice. These concepts are at the core of the FTC framework that effectively balances the need to safeguard consumers' personal information and gives them choices over how their data is used with the benefits of enabling companies to use data in ways that foster innovation, competition, new services, and new capabilities. Adoption of this approach would be less disruptive for the broadband ecosystem, minimize consumer confusion, subject all Internet entities to comparable privacy regimes, and protect consumer privacy in a manner that provides the flexibility the marketplace needs in order to innovate and evolve.

The privacy regime proposed by the FCC in the NPRM departs from the FTC framework in significant and material respects. The FTC prudently has found that an opt-out approach should govern use of consumer data in most instances, with opt-in reserved for uses of the most sensitive consumer data. The FCC framework, however, would make opt-in the default consent mechanism for virtually all uses of customer data. This would lead to absurd results, such as restricting an ISP's ability to market accessories that work with a consumer's device. It also would make it difficult for consumers to have access to discounted offers from their providers. This broad opt-in requirement, irrespective of the sensitivity of data, would be inconsistent with common Internet practice and would harm consumer welfare. More important, it would be confusing to require consumers to opt-in to ISP data use and sharing because consumers would likely not understand how the opt-in regime would apply.

We appreciate the diligence shown by the members of the Subcommittee in examining the important issues surrounding the FCC's NPRM. We support a reasonable framework that adheres in all material respects to the successful FTC model that protected the privacy of broadband consumers for years, and applied uniformly to all entities in the broadband ecosystem. We are hopeful that your interest in, and oversight of, these issues will help to re-align the FCC's proposal more closely with the proven and effective approach administered by the FTC.

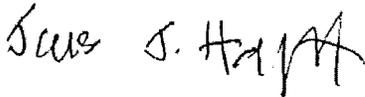
Sincerely,



Matthew M. Polka
President & CEO
American Cable Association



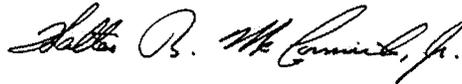
Meredith Attwell Baker
President & CEO
CTIA



Jim Halpert
President & CEO
Internet Commerce Coalition



Michael Powell
President & CEO
National Cable & Telecommunications Association



Walter B. McCormick, Jr.
President & CEO
USTelecom

cc: The Honorable Orrin G. Hatch
The Honorable David Perdue
The Honorable Mike Lee
The Honorable Thom Tillis
The Honorable Lindsey Graham
The Honorable Dianne Feinstein
The Honorable Charles E. Schumer
The Honorable Sheldon Whitehouse
The Honorable Christopher A. Coons

Privacy Framework

Discussion Paper

All entities in the Internet ecosystem should be subject to a consistent privacy framework with respect to consumer information. Consumer information should be protected based upon the sensitivity of the information to the consumer and how the information is used—not the type of business keeping it, how that business obtains it, or what regulatory agency has authority over it. Consumers should have consistent and predictable privacy protections for the information they deem private and sensitive, no matter how or with whom they share it. Consumers also will benefit from a consistent privacy framework that promotes the emergence of new business models and innovative uses of data that foster increased consumer choice and service customization.

The FCC should adopt an approach to privacy and data security for CPNI that is flexible, harmonized with the well-established and successful FTC framework, and backed up by strong but fair enforcement for unfair or deceptive acts or practices (UDAP) that materially harm consumers. This well-tested consumer protection approach is consistent with the FCC's privacy recommendations in the 2010 National Broadband Plan, the FTC's and White House's 2012 Privacy Reports, and the White House's 2015 Consumer Privacy Bill of Rights, as well as with Chairman Wheeler's recent testimony before Congress acknowledging the importance of coordination with the FTC and harmonization with its privacy framework.

That approach will benefit consumers by safeguarding privacy interests as it has for years and will ensure that the same privacy and security framework applies to all entities in the Internet ecosystem. By leveraging a tested privacy model, the FCC will avoid inconsistent requirements that could otherwise hamper innovation and reduce competition. Most important, it will minimize consumer confusion as well as other harms associated with disparate privacy regulation across the ecosystem. Indeed, this approach will align with consumers' expectations that their data would be subject to consistent privacy rules regardless of whether it is used by their Internet Service Provider (ISP), application developers, operating systems, or edge providers.

When adopting a framework, the FCC should keep the following guidelines in mind:

- Consistent and Coordinated Regulatory Regimes. The FCC's rules and principles for regulating and enforcing privacy and security should be as similar as possible to the FTC approach, which will continue to govern other Internet ecosystem players' use and disclosure of the same or similar data. The consistent application of standards across sectors would fulfill the following key tenets in the White House Privacy Report: (1) avoid "inconsistent standards for related technologies" that could dampen innovation; (2) foster a "level playing field for companies;" and, most importantly, (3) create "a consistent set of expectations for consumers." To achieve this end, the FCC's policies,

rules, and enforcement practices should conform to the longstanding limiting principles articulated in the FTC's Unfairness and Deception Policy Statements. In addition, the FCC and FTC can achieve their recent MOU's stated goal of avoiding "duplicative, redundant or inconsistent oversight" by developing a new process to ensure that their substantive privacy policies and basis for enforcement are consistent going forward.

- **Flexibility.** The FCC's approach should provide a flexible framework within which telecommunications service providers can implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments in this space. Specifically, this framework should identify the privacy or security *goals*, and afford providers flexibility in achieving those goals, rather than dictate the particular *methods* by which providers are expected to achieve those goals. Adopting a flexible approach also will help ensure consistent federal and state requirements governing customer information.
- **Application.** Consistent with the Communications Act and to eliminate unnecessary duplication of authority with other agencies, the FCC's framework should only apply when 1) telecommunications service providers are providing telecommunications services and 2) the CPNI is made available by the customer to the telecommunications service provider solely by virtue of the carrier-customer relationship. The framework cannot lawfully apply to:
 - Providers' non-telecommunications services and products
 - Providers' non-telecommunications service provider affiliates
 - Information that is not made available to the carrier by the customer solely by virtue of the carrier-customer relationship
- **Individually Identifiable.** The FCC should carve out from the scope of its new framework any data that is de-identified, aggregated, or does not otherwise identify a known individual. The insights derived from the use of de-identified data can offer great benefits to consumers and society and such use avoids the sensitivities that may be associated with identified data.
- **Unfair or Deceptive Conduct.** As noted above, the FCC's policies, rules, and enforcement practices should conform to the FTC's longstanding limiting principles articulated in its Policy Statements on Unfairness (1980) and Deception (1983). This approach is consistent with the FCC's commitment to conduct a cost-benefit analysis of its regulatory framework in accordance with President Obama's Executive Orders 13563 and 13579, which require agencies to "adopt a regulation only upon a reasoned determination its benefits justify its costs" and "tailor its regulations to impose the least burden on society."
 - **Unfair Conduct.** A provider acts unfairly if its act or practice (1) causes or is likely to cause substantial injury to consumers (2) which is not reasonably avoidable by consumers themselves, and (3) is not outweighed by countervailing benefits to consumers or to competition.
 - **Deceptive Conduct.** A provider acts deceptively if (1) it makes a statement or omission, or engages in a practice, that is likely to mislead a customer, (2) viewed from the perspective of a consumer acting reasonably under the circumstances, and (3) the deceptive statement, omission, or practice is material—meaning that the misrepresentation or practice is likely to affect the consumer's conduct or decision with regard to a product or service.

- Additional Guidance. In coordination with other privacy regulators, the FCC could, like the FTC and various states like California, provide additional guidance on how it interprets its framework through workshops or reports. The FCC also could encourage and support the development and implementation of industry guidelines.
- Update and Harmonize Existing CPNI Rules. The existing CPNI rules should be revisited in their entirety and modernized to use the same flexible framework for all services subject to Section 222, including traditional voice services. In no event should the prescriptive outdated CPNI rules designed for legacy voice services apply to broadband services. Instead, a common set of flexible policies that allow providers to keep up with their customers' expectations and evolving technology should apply to both types of services.

With these guidelines in mind, if the courts determine that the FCC has authority to regulate broadband privacy, the FCC could adopt the following principles, which encompass and are consistent with the privacy and security framework that applies to the rest of the industry. Each of these principles and the goals noted above should provide flexibility for providers to implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments:

- Transparency. A telecommunications service provider should provide notice, which is neither deceptive nor unfair, describing the CPNI that it collects, how it will use the CPNI, and whether and for what purposes it may share CPNI with third parties.
- Respect for Context and Consumer Choice. A telecommunications service provider may use or disclose CPNI as is consistent with the context in which the customer provides, or the provider obtains, the information, provided that the provider's actions are not unfair or deceptive. For example, the use or disclosure of CPNI for the following commonly accepted data practices would not warrant a choice mechanism, either because customer consent can be inferred or because public policy considerations make choice unnecessary: product and service fulfillment, fraud prevention, compliance with law, responses to government requests, network management, first-party marketing, and affiliate sharing where the affiliate relationship is reasonably clear to consumers. Consistent with the flexible choice mechanisms available to all other entities in the Internet ecosystem, telecommunications service providers should give consumers easy-to-understand choices for non-contextual uses and disclosures of their CPNI, where the failure to provide choice would be deceptive or unfair. The provider should consider the sensitivity of the data and the context in which it was collected when determining the appropriate choice mechanism.
- Data Security. A telecommunications service provider should establish, implement, and maintain a CPNI data security program that is neither unfair nor deceptive and includes reasonable physical, technical, and administrative security safeguards to protect CPNI from unauthorized access, use, and disclosure. Providers' CPNI data security programs should provide reasonable protections in light of the nature and scope of the activities of the company, the sensitivity of the data, and the size and complexity of the relevant data operations of the company.
- Data Breach Notifications. Telecommunications service providers should notify customers whose CPNI has been breached when failure to notify would be unfair or

deceptive. Given that breach investigations frequently are ongoing at the time providers offer notice to customers, a notice that turns out to be incomplete or inaccurate is not deceptive, as long as the provider corrects any material inaccuracies within a reasonable period of time of discovering them. Telecommunications providers have flexibility to determine how and when to provide such notice.

The FCC can ensure compliance with the above principles by pursuing reasonable enforcement actions against telecommunications service providers that have clearly violated these principles.

cc: The Honorable Mignon Clyburn
The Honorable Jessica Rosenworcel
The Honorable Ajit Pai
The Honorable Michael O’Rielly

Joanne Wall

From: Scott Bergmann <SBergmann@ctia.org>
Sent: Tuesday, March 01, 2016 2:15 PM
To: Nicholas Degani
Cc: Brendan Carr
Subject: Letter on Consensus Privacy Framework
Attachments: Wheeler Letter Re Privacy Principles 3 1 16.pdf

Hi Nick,

Following up on my voicemail, attached please find a letter sent today by ACA, CCA, CTIA, NCTA, and USTelecom to FCC Chairman Wheeler setting forth guidelines and principles for the FCC to consider as it moves forward with a rulemaking on broadband privacy. This consensus privacy framework will protect consumer privacy in a way that is consistent with other privacy laws that apply to other companies in the Internet ecosystem. We hope the FCC will seek comment on this consensus framework, in its entirety, in its upcoming rulemaking proceeding.

As always, please let me know if you have any questions. Best,

Scott



Scott Bergmann

Vice President, Regulatory Affairs

1400 16th Street, NW

Washington, DC 20036

202-736-3660 (office)

202-997-3916 (mobile)

sbergmann@ctia.org



March 1, 2016

The Honorable Tom Wheeler
Chairman
Federal Communications Commission
445 12th St. SW
Washington, D.C. 20554

Dear Chairman Wheeler,

Today, the American Cable Association, Competitive Carriers Association, CTIA, National Cable & Telecommunications Association, and USTelecom offer for the Commission's consideration a detailed proposal for a broadband privacy framework. After significant examination and analysis, these associations have developed the attached consensus Privacy Framework setting forth guidelines and principles to protect consumer privacy in a way that is consistent with other privacy laws that apply to companies providing services online. By adopting these principles, the Commission would establish a regime that protects consumer privacy and security while also providing flexibility for providers to implement and update their practices as consumer expectations and technologies evolve.

If the courts determine that the Commission has authority over broadband privacy, the FCC should focus on four privacy principles: (1) transparency; (2) respect for context and consumer choice; (3) data security; and (4) data breach notification. For each of these principles, the FCC should draw from and harmonize with the longstanding Federal Trade Commission unfairness and deception approach to privacy, which, before the FCC's reclassification decision, governed the privacy practices of all companies in the Internet ecosystem and will continue to apply to non-ISPs going forward.

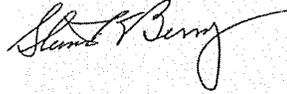
As the Commission develops its approach to broadband privacy, we respectfully request that it seek comment on the entirety of the Privacy Framework we submit today. Because regulation of broadband privacy is a new area for the Commission, it should take the necessary time to build a robust record rather than prejudge the issues by adopting tentative conclusions before there is a public discussion of the consensus Privacy Framework.

We look forward to continuing a conversation with the Commission about the best way to provide privacy and innovation benefits to consumers.

Respectfully submitted,



Matthew M. Polka
President & CEO
American Cable Association



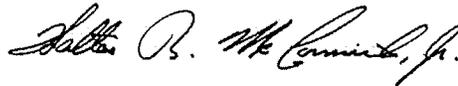
Steven K. Berry
President & CEO
Competitive Carriers Association



Meredith Attwell Baker
President & CEO
CTIA



Michael Powell
President & CEO
National Cable & Telecommunications Association



Walter B. McCormick, Jr.
President & CEO
USTelecom

cc: The Honorable Mignon Clyburn
The Honorable Jessica Rosenworcel
The Honorable Ajit Pai
The Honorable Michael O’Rielly

Privacy Framework

Discussion Paper

All entities in the Internet ecosystem should be subject to a consistent privacy framework with respect to consumer information. Consumer information should be protected based upon the sensitivity of the information to the consumer and how the information is used—not the type of business keeping it, how that business obtains it, or what regulatory agency has authority over it. Consumers should have consistent and predictable privacy protections for the information they deem private and sensitive, no matter how or with whom they share it. Consumers also will benefit from a consistent privacy framework that promotes the emergence of new business models and innovative uses of data that foster increased consumer choice and service customization.

The FCC should adopt an approach to privacy and data security for CPNI that is flexible, harmonized with the well-established and successful FTC framework, and backed up by strong but fair enforcement for unfair or deceptive acts or practices (UDAP) that materially harm consumers.¹ This well-tested consumer protection approach is consistent with the FCC’s privacy recommendations in the 2010 National Broadband Plan, the FTC’s and White House’s 2012 Privacy Reports, and the White House’s 2015 Consumer Privacy Bill of Rights, as well as with Chairman Wheeler’s recent testimony before Congress acknowledging the importance of coordination with the FTC and harmonization with its privacy framework.

That approach will benefit consumers by safeguarding privacy interests as it has for years and will ensure that the same privacy and security framework applies to all entities in the Internet ecosystem. By leveraging a tested privacy model, the FCC will avoid inconsistent requirements that could otherwise hamper innovation and reduce competition. Most important, it will minimize consumer confusion as well as other harms associated with disparate privacy regulation across the ecosystem. Indeed, this approach will align with consumers’ expectations that their data would be subject to consistent privacy rules regardless of whether it is used by their Internet Service Provider (ISP), application developers, operating systems, or edge providers.

When adopting a framework, the FCC should keep the following guidelines in mind:

- Consistent and Coordinated Regulatory Regimes. The FCC’s rules and principles for regulating and enforcing privacy and security should be as similar as possible to the FTC approach, which will continue to govern other Internet ecosystem players’ use and disclosure of the same or similar data. The consistent application of standards across sectors would fulfill the following key tenets in the White House Privacy Report: (1) avoid “inconsistent standards for related technologies” that could dampen innovation; (2)

¹ This framework is intended for discussion purposes, and we are not conceding that the FCC has authority to adopt privacy and security rules for Broadband Internet Access Services or over data related to consumers’ use of Broadband Internet Access Services. To the extent it is determined that the FCC has such statutory authority, this document is intended to set forth principles for FCC consideration and possible adoption that are harmonized and consistent with the FTC and other government entities’ approach to privacy and security for the same or similar data. Even if courts determine that the FCC’s reclassification of Broadband Internet Access Services is a lawful exercise of authority, any rules must not exceed the text and legislative history of Section 222 of the Act.

foster a “level playing field for companies;” and, most importantly, (3) create “a consistent set of expectations for consumers.” To achieve this end, the FCC’s policies, rules, and enforcement practices should conform to the longstanding limiting principles articulated in the FTC’s Unfairness and Deception Policy Statements. In addition, the FCC and FTC can achieve their recent MOU’s stated goal of avoiding “duplicative, redundant or inconsistent oversight” by developing a new process to ensure that their substantive privacy policies and basis for enforcement are consistent going forward.

- Flexibility. The FCC’s approach should provide a flexible framework within which telecommunications service providers can implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments in this space. Specifically, this framework should identify the privacy or security *goals*, and afford providers flexibility in achieving those goals, rather than dictate the particular *methods* by which providers are expected to achieve those goals. Adopting a flexible approach also will help ensure consistent federal and state requirements governing customer information.
- Application. Consistent with the Communications Act and to eliminate unnecessary duplication of authority with other agencies, the FCC’s framework should only apply when 1) telecommunications service providers are providing telecommunications services and 2) the CPNI is made available by the customer to the telecommunications service provider solely by virtue of the carrier-customer relationship. The framework cannot lawfully apply to:
 - Providers’ non-telecommunications services and products
 - Providers’ non-telecommunications service provider affiliates
 - Information that is not made available to the carrier by the customer solely by virtue of the carrier-customer relationship
- Individually Identifiable. The FCC should carve out from the scope of its new framework any data that is de-identified, aggregated, or does not otherwise identify a known individual. The insights derived from the use of de-identified data can offer great benefits to consumers and society and such use avoids the sensitivities that may be associated with identified data.
- Unfair or Deceptive Conduct. As noted above, the FCC’s policies, rules, and enforcement practices should conform to the FTC’s longstanding limiting principles articulated in its Policy Statements on Unfairness (1980) and Deception (1983). This approach is consistent with the FCC’s commitment to conduct a cost-benefit analysis of its regulatory framework in accordance with President Obama’s Executive Orders 13563 and 13579, which require agencies to “adopt a regulation only upon a reasoned determination its benefits justify its costs” and “tailor its regulations to impose the least burden on society.”
 - Unfair Conduct. A provider acts unfairly if its act or practice (1) causes or is likely to cause substantial injury to consumers (2) which is not reasonably avoidable by consumers themselves, and (3) is not outweighed by countervailing benefits to consumers or to competition.
 - Deceptive Conduct. A provider acts deceptively if (1) it makes a statement or omission, or engages in a practice, that is likely to mislead a customer, (2) viewed from the perspective of a consumer acting reasonably under the circumstances, and (3) the deceptive statement, omission, or practice is material—meaning that

the misrepresentation or practice is likely to affect the consumer's conduct or decision with regard to a product or service.

- Additional Guidance. In coordination with other privacy regulators, the FCC could, like the FTC and various states like California, provide additional guidance on how it interprets its framework through workshops or reports. The FCC also could encourage and support the development and implementation of industry guidelines.
- Update and Harmonize Existing CPNI Rules. The existing CPNI rules should be revisited in their entirety and modernized to use the same flexible framework for all services subject to Section 222, including traditional voice services. In no event should the prescriptive outdated CPNI rules designed for legacy voice services apply to broadband services. Instead, a common set of flexible policies that allow providers to keep up with their customers' expectations and evolving technology should apply to both types of services.

With these guidelines in mind, if the courts determine that the FCC has authority to regulate broadband privacy, the FCC could adopt the following principles, which encompass and are consistent with the privacy and security framework that applies to the rest of the industry. Each of these principles and the goals noted above should provide flexibility for providers to implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments:

- Transparency. A telecommunications service provider should provide notice, which is neither deceptive nor unfair, describing the CPNI that it collects, how it will use the CPNI, and whether and for what purposes it may share CPNI with third parties.
- Respect for Context and Consumer Choice. A telecommunications service provider may use or disclose CPNI as is consistent with the context in which the customer provides, or the provider obtains, the information, provided that the provider's actions are not unfair or deceptive. For example, the use or disclosure of CPNI for the following commonly accepted data practices would not warrant a choice mechanism, either because customer consent can be inferred or because public policy considerations make choice unnecessary: product and service fulfillment, fraud prevention, compliance with law, responses to government requests, network management, first-party marketing, and affiliate sharing where the affiliate relationship is reasonably clear to consumers. Consistent with the flexible choice mechanisms available to all other entities in the Internet ecosystem, telecommunications service providers should give consumers easy-to-understand choices for non-contextual uses and disclosures of their CPNI, where the failure to provide choice would be deceptive or unfair. The provider should consider the sensitivity of the data and the context in which it was collected when determining the appropriate choice mechanism.
- Data Security. A telecommunications service provider should establish, implement, and maintain a CPNI data security program that is neither unfair nor deceptive and includes reasonable physical, technical, and administrative security safeguards to protect CPNI from unauthorized access, use, and disclosure. Providers' CPNI data security programs should provide reasonable protections in light of the nature and scope of the activities of the company, the sensitivity of the data, and the size and complexity of the relevant data operations of the company.

- Data Breach Notifications. Telecommunications service providers should notify customers whose CPNI has been breached when failure to notify would be unfair or deceptive. Given that breach investigations frequently are ongoing at the time providers offer notice to customers, a notice that turns out to be incomplete or inaccurate is not deceptive, as long as the provider corrects any material inaccuracies within a reasonable period of time of discovering them. Telecommunications providers have flexibility to determine how and when to provide such notice.

The FCC can ensure compliance with the above principles by pursuing reasonable enforcement actions against telecommunications service providers that have clearly violated these principles.

Joanne Wall

From: Follansbee, Lynn <lfollansbee@ustelecom.org>
Sent: Thursday, February 11, 2016 10:09 AM
To: Nicholas Degani
Subject: Privacy Letter to Chairman Wheeler
Attachments: Privacy Letter Final 523pm.pdf

Nick:

I believe Loretta Polk from NCTA reached out to you to let you know that the joint associations were sending a letter to Chairman Wheeler on privacy. For your reference here is a copy of the letter. Please let me know if you have any questions.

Thank you,

Lynn

B. Lynn Follansbee
Vice President, Law & Policy
USTelecom
607 14th Street NW
Suite 400
Washington, DC 20005
Tel: 202-326-7256
Email: lfollansbee@ustelecom.org





February 11, 2016

The Honorable Tom Wheeler
Chairman
Federal Communications Commission
445 12th St. SW
Washington, D.C. 20554

Dear Chairman Wheeler,

As associations representing a large cross-section of the technology companies that make up today's vibrant Internet economy, our collective members are committed to providing consumers with innovative products and services and are equally committed to earning consumer trust and respecting privacy. If the courts determine that the FCC has authority to regulate broadband privacy, we encourage you to develop a framework that offers consumers robust privacy protection, while at the same time allowing broadband providers to continue to innovate and compete. We recommend that any FCC framework be consistent with the successful FTC approach, which is grounded on prohibiting unfairness and deception. The FTC's time-tested framework has accomplished two important goals—it provides consumers with meaningful privacy protection and helps to enable a dynamic marketplace that supports the emergence of innovative new business models. By developing a consistent framework, the FCC will further these important goals.

Our member companies recognize that ensuring robust privacy protection is important and have devoted substantial capital, resources and personnel to develop, maintain, and enhance meaningful data privacy and security programs. Indeed, our companies have strong incentives to earn and maintain their customers' loyalty by protecting their data. In the rapidly evolving online marketplace, our companies want to ensure that they can continue to provide such protections while meeting consumers' expectation of continued access to new innovations that enhance their experience.

All companies in the Internet ecosystem, including Internet service providers, have long operated under the FTC regulatory regime for protecting consumer privacy. The aim of this well-tested approach is to combine strong protections for consumers with flexibility that allows for rapid innovation. Under the FTC regime, all companies in the Internet ecosystem must ensure that

their privacy and data security practices are neither deceptive nor unfair. As a result, consumers are protected and all companies that collect consumer data should be able to innovate and adapt to the inevitable changes in technology and the market for online services.

We understand the FCC is considering initiating a proceeding to consider how Section 222 of the Communications Act, which governs Customer Proprietary Network Information (“CPNI”), should apply to broadband Internet access service. The applicability of Section 222 in this context is currently subject to judicial review. If the Commission nonetheless moves forward in this space, consumers would be best served by an approach to privacy and data security for CPNI that is harmonized with the FTC’s established privacy protection framework based on enforcement against unfair and deceptive acts or practices.

You have recognized that the FTC has a longstanding, thoughtful, and rational approach to privacy, and you have committed to working closely with the FTC and to developing a consistent privacy framework for Internet service providers. Ensuring consistency with this effective consumer protection approach would be in accordance with statements supporting the FTC’s privacy regime and endorsing the benefits of a consistent privacy framework for the Internet in the 2010 National Broadband Plan, the FTC’s and White House’s 2012 Privacy Reports, and the White House’s 2015 Consumer Privacy Bill of Rights.

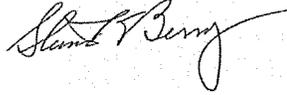
We believe it is important to maintain a consistent privacy framework for the Internet. Such an approach will protect consumers and avoid entity-based regulation that would create consumer confusion and stifle innovation. Consumers expect their data will be subject to consistent privacy standards based upon the sensitivity of the information and how it is used regardless of which entity in the Internet ecosystem uses that data. To achieve parity across the Internet ecosystem, any FCC framework for Internet service providers should be reflective of the deception and unfairness standard, consistent with the existing protections consumers receive when they engage with other companies in the Internet ecosystem.

A consistent privacy framework for the Internet also will continue to provide Internet service providers with the flexibility to update their practices in ways that meet the evolving privacy and data security needs of their customers and ensure they can provide their customers new products and customized services. Such a framework would identify privacy or security goals, and afford providers, including smaller providers with limited resources, flexibility in achieving those goals. Rules dictating specific methods quickly become out of date and out of step with constantly changing technology, and will only hamper innovation and harm consumers.

In short, if you seek to initiate a proceeding under Section 222, we respectfully urge you to ensure that the FCC acts in a manner consistent with the strong current national privacy framework applied by the FTC to other companies in the Internet ecosystem. This flexible approach would meet consumers’ privacy needs while allowing them to take advantage of innovative products and services, and would avoid inconsistent oversight. We look forward to continuing a conversation with the FCC about the best way to provide privacy and innovation benefits to consumers.



Matthew M. Polka
President & CEO
American Cable Association



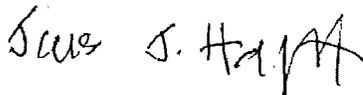
Steven K. Berry
President & CEO
Competitive Carriers Association



Gary Shapiro
President & CEO
Consumer Technology Association



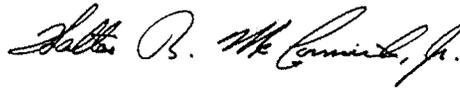
Meredith Attwell Baker
President & CEO
CTIA



Jim Halpert
President & CEO
Internet Commerce Coalition



Michael Powell
President & CEO
National Cable & Telecommunications Association



Walter B. McCormick, Jr.
President & CEO
U.S. Telecom Association

cc: The Honorable Mignon Clyburn
The Honorable Jessica Rosenworcel
The Honorable Ajit Pai
The Honorable Michael O'Rielly

Joanne Wall

From: Emma Prieskorn <EPrieskorn@ctia.org>
Sent: Friday, March 11, 2016 1:27 PM
To: Marquita Abitong
Cc: Scott Bergmann; Debbie Matties; Travis Litman; Andrew Azorsky
Subject: CTIA Meeting Request: Broadband Privacy NPRM

Hi Marquita,

I'm reaching out (again) to schedule a meeting with Travis Litman to discuss the FCC's upcoming Broadband Privacy NPRM. Attending the meeting from CTIA will be Scott Bergmann and Debbie Matties. We are hoping to schedule the meeting sometime during March 15th-18th or March 21st- 23rd.

Feel free to let me know if you have any questions.

Many thanks,
Emma



Emma (Keech) Prieskorn

Coordinator, Regulatory Affairs

1400 16th Street, NW

Washington, DC 20036

202-736-3671 (office)

Joanne Wall

From: Scott Bergmann <SBergmann@ctia.org>
Sent: Thursday, February 11, 2016 8:52 AM
To: Travis Litman
Subject: Fwd: Joint Association Letter on Privacy
Attachments: image001.png; ATT00001.htm; Privacy Letter Final 523pm.pdf; ATT00002.htm

Hi Travis, as mentioned. Feel free to give me a call with any questions. Best,

Scott

Begin forwarded message:

From: Scott Bergmann <SBergmann@ctia.org<mailto:SBergmann@ctia.org>>
Date: February 11, 2016 at 7:36:51 AM EST
To: Scott Bergmann <SBergmann@ctia.org<mailto:SBergmann@ctia.org>>
Subject: Joint Association Letter on Privacy

Attached please find a joint association letter filed today calling on the FCC, to the extent that it initiates a proceeding addressing broadband privacy, to develop a framework that offers consumers robust privacy protection, while at the same time allowing broadband providers to continue to innovate and compete. The letter - filed by ACA, CCA, CTA, CTIA, ICC, NCTA, and US Telecom - recommends that any FCC framework be consistent with the successful FTC approach, grounded on prohibiting unfairness and deception.

Please let me know if you have any questions. Best,

Scott



February 11, 2016

The Honorable Tom Wheeler
Chairman
Federal Communications Commission
445 12th St. SW
Washington, D.C. 20554

Dear Chairman Wheeler,

As associations representing a large cross-section of the technology companies that make up today's vibrant Internet economy, our collective members are committed to providing consumers with innovative products and services and are equally committed to earning consumer trust and respecting privacy. If the courts determine that the FCC has authority to regulate broadband privacy, we encourage you to develop a framework that offers consumers robust privacy protection, while at the same time allowing broadband providers to continue to innovate and compete. We recommend that any FCC framework be consistent with the successful FTC approach, which is grounded on prohibiting unfairness and deception. The FTC's time-tested framework has accomplished two important goals—it provides consumers with meaningful privacy protection and helps to enable a dynamic marketplace that supports the emergence of innovative new business models. By developing a consistent framework, the FCC will further these important goals.

Our member companies recognize that ensuring robust privacy protection is important and have devoted substantial capital, resources and personnel to develop, maintain, and enhance meaningful data privacy and security programs. Indeed, our companies have strong incentives to earn and maintain their customers' loyalty by protecting their data. In the rapidly evolving online marketplace, our companies want to ensure that they can continue to provide such protections while meeting consumers' expectation of continued access to new innovations that enhance their experience.

All companies in the Internet ecosystem, including Internet service providers, have long operated under the FTC regulatory regime for protecting consumer privacy. The aim of this well-tested approach is to combine strong protections for consumers with flexibility that allows for rapid innovation. Under the FTC regime, all companies in the Internet ecosystem must ensure that

their privacy and data security practices are neither deceptive nor unfair. As a result, consumers are protected and all companies that collect consumer data should be able to innovate and adapt to the inevitable changes in technology and the market for online services.

We understand the FCC is considering initiating a proceeding to consider how Section 222 of the Communications Act, which governs Customer Proprietary Network Information (“CPNI”), should apply to broadband Internet access service. The applicability of Section 222 in this context is currently subject to judicial review. If the Commission nonetheless moves forward in this space, consumers would be best served by an approach to privacy and data security for CPNI that is harmonized with the FTC’s established privacy protection framework based on enforcement against unfair and deceptive acts or practices.

You have recognized that the FTC has a longstanding, thoughtful, and rational approach to privacy, and you have committed to working closely with the FTC and to developing a consistent privacy framework for Internet service providers. Ensuring consistency with this effective consumer protection approach would be in accordance with statements supporting the FTC’s privacy regime and endorsing the benefits of a consistent privacy framework for the Internet in the 2010 National Broadband Plan, the FTC’s and White House’s 2012 Privacy Reports, and the White House’s 2015 Consumer Privacy Bill of Rights.

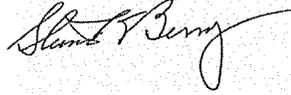
We believe it is important to maintain a consistent privacy framework for the Internet. Such an approach will protect consumers and avoid entity-based regulation that would create consumer confusion and stifle innovation. Consumers expect their data will be subject to consistent privacy standards based upon the sensitivity of the information and how it is used regardless of which entity in the Internet ecosystem uses that data. To achieve parity across the Internet ecosystem, any FCC framework for Internet service providers should be reflective of the deception and unfairness standard, consistent with the existing protections consumers receive when they engage with other companies in the Internet ecosystem.

A consistent privacy framework for the Internet also will continue to provide Internet service providers with the flexibility to update their practices in ways that meet the evolving privacy and data security needs of their customers and ensure they can provide their customers new products and customized services. Such a framework would identify privacy or security goals, and afford providers, including smaller providers with limited resources, flexibility in achieving those goals. Rules dictating specific methods quickly become out of date and out of step with constantly changing technology, and will only hamper innovation and harm consumers.

In short, if you seek to initiate a proceeding under Section 222, we respectfully urge you to ensure that the FCC acts in a manner consistent with the strong current national privacy framework applied by the FTC to other companies in the Internet ecosystem. This flexible approach would meet consumers’ privacy needs while allowing them to take advantage of innovative products and services, and would avoid inconsistent oversight. We look forward to continuing a conversation with the FCC about the best way to provide privacy and innovation benefits to consumers.



Matthew M. Polka
President & CEO
American Cable Association



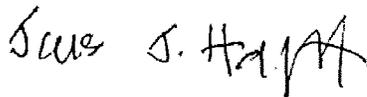
Steven K. Berry
President & CEO
Competitive Carriers Association



Gary Shapiro
President & CEO
Consumer Technology Association



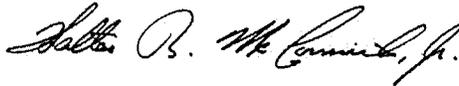
Meredith Attwell Baker
President & CEO
CTIA



Jim Halpert
President & CEO
Internet Commerce Coalition



Michael Powell
President & CEO
National Cable & Telecommunications Association



Walter B. McCormick, Jr.
President & CEO
U.S. Telecom Association

cc: The Honorable Mignon Clyburn
The Honorable Jessica Rosenworcel
The Honorable Ajit Pai
The Honorable Michael O'Rielly

Joanne Wall

From: QUINN JR., ROBERT W <rq1982@att.com>
Sent: Tuesday, March 15, 2016 3:14 PM
To: Travis Litman
Subject: the Moody's piece
Attachments: FCC's broadband privacy proposal credit negative for linear TV and wireless providers.pdf; ATT00001.txt

SECTOR COMMENT

14 March 2016

Rate this Research >>

Contacts

Neil Begley 212-553-7793
 Senior Vice President
 neil.begley@moodys.com

Mark Stodden 212-553-7718
 VP-Senior Credit
 Officer
 mark.stodden@moodys.com

John Diaz 212-553-1977
 MD-Corporate Finance
 john.diaz@moodys.com

Vincent Tingos +1 212 553 9499
 Associate Analyst
 vincent.tingos@moodys.com

FCC's broadband privacy proposal credit negative for linear TV and wireless providers

Over half a trillion of rated debt affected

On Thursday March 10th, FCC officials proposed a plan to restrict broadband providers or internet service providers (ISPs) such as [Verizon](#) (Baa1 stable), [AT&T](#) (Baa1 negative), [Comcast](#) (A3 stable), and [Charter](#) (Ba3 on review for upgrade) from collecting valuable data without affirmative consent from customers who use their networks. This is the among the first types of actions by the FCC against internet service providers (ISPs) since Title II was enacted to regulate broadband providers about a year ago. We believe this proposal will have a negative impact on both fixed and mobile broadband providers. If approved, the ability to compete with digital advertisers such as Facebook and [Google](#) (Aa2 stable), who are able to collect the same type of data from consumers who access their websites and those of others, will be severely handicapped in the future as the old guard ecosystem evolves to become more competitive. We believe this to be a long-term risk to the current TV advertising business model, as well as all broadband providers whom also have ad sales exposure to the present linear video ecosystem. It would likely lead to greater pressure for individual networks and stations to go over-the-top (OTT) and abandon the more stable Pay-TV bundle. An open question is how this proposal may impact the FCC's other recent proposal regarding unbundling the provision of the set top box from the ISP, which is also negative for broadband providers, and whether technology companies that wish to compete by selling set top boxes directly to consumers and also becoming a virtual pay-TV provider will fall under the same privacy consent constraints?

Digital advertisers like Google and Facebook are regulated under a different governmental body, the Federal Trade Commission (FTC), and thus are excluded from this proposal by the FCC. Ad sales models like theirs are putting traditional ad models under significant competitive pressure as they grow by double digit levels as compared to low single digit growth to low single digit declines in core traditional advertising. Targeted programmatic advertising, which uses consumer data, is used by these companies to efficiently place advertisements in front of the customers much more prone to consume a particular product being advertised and affected by the ad, resulting in a higher return on the advertising investment. Absent an alignment of rules between the FTC and FCC regarding these privacy laws, a distinct competitive advantage will be given to online digital advertisers as more advertising dollars will continue to move in secular fashion from traditional television providers towards digital platform providers.

The FCC's rationale for not regulating websites or apps in the same way as a broadband provider that might accumulate data, is that the consumer has the ability to move from website to website whereas the ISP will be constant throughout this movement, providing the ISP with an overall clearer picture of consumer preferences. The proposal will still allow ISP's to collect data from consumers, as long as the consumer manually chooses to opt into allowing it as compared to the structure today where the consumer has to manually opt out. As an analogy, it has long been studied the effect of opt-in/opt-out when it comes to organ donors. In a 2012 joint study conducted by Stanford and Cornell University, they concluded that organ donation rates would increase in the US (an opt-in country) if it changed its policy to an opt-out case. We believe this psychological effect to hold true if consumers have to, by default, choose to "opt-in" to allow ISP's to access their data.

The FCC's proposal also has the potential to derail efforts by wireless carriers to cultivate mobile video advertising revenues. Wireless carriers have the potential to generate significant advertising revenues due to their ability to precisely target ads to wireless subscribers. But, if the FCC restricts the carriers' ability to collect this data, the advertising revenue opportunity will be reduced. Without a robust mobile video advertising market, the product could lose relevance due to its higher cost to consumers and a potential for fewer content choices.

This publication does not announce a credit rating action. For any credit ratings referenced in this publication, please see the ratings tab on the issuer/entity page on www.moodys.com for the most updated credit rating action information and rating history.

Exhibit 1

	Rating	Outlook	Reported Debt
Wireless			
Verizon Communications Inc.	Baa1	Stable	110,194
AT&T Inc. [1]	Baa1	Negative	109,162
T-Mobile	Ba3	Stable	29,059
Sprint Corporation	B3	Negative	33,753
Total			282,168
Wireline			
Comcast Corporation	A3	Stable	52,621
Cox Communications, Inc.	Baa2	Stable	10,337
Time Warner Cable, Inc.	Baa2	RUR-DNG	22,502
CenturyLink, Inc.	Ba1	Negative	20,225
Cablevision Systems Corporation [3]	Ba2	RUR-DNG	14,515
Block Communications, Inc.	Ba3	Stable	503
Charter Communications Inc. [2]	Ba3	RUR-UPG	39,256
Cable One, Inc.	Ba3	Stable	549
Frontier Communications Corporation	Ba3	Stable	15,892
Mediacom Communications Corporation	Ba3	Stable	3,068
Acquisitions Cogeco Cable II, LP	B1	Stable	973
Midcontinent Communications	B1	Stable	883
Windstream Services, LLC	B1	Stable	10,324
Grande Communications Networks LLC	B2	Stable	316
Harron Communications LP	B2	Stable	397
RCN Telecom Services, LLC	B2	Stable	1,047
WideOpenWest Finance, LLC	B2	Negative	2,923
Cequel Communications Holdings I, LLC [3]	B3	Stable	7,276
Telecommunications Management LLC	B3	Stable	334
Wave Holdco, LLC	B3	Stable	905
Total			204,845
Networks			
Walt Disney Company (The)	A2	Stable	18,915
21st Century Fox America, Inc.	Baa1	Stable	19,737
CBS Corporation	Baa2	Stable	8,448
Time Warner Inc.	Baa2	Stable	23,792
Viacom Inc.	Baa2	Stable	12,567
Discovery Communications, LLC	Baa3	Stable	7,735
Scripps Networks Interactive, Inc.	Baa3	Stable	4,010
AMC Networks Inc.	Ba2	Stable	4,010
Total			99,215
Satellite			
DIRECTV Holdings LLC	Baa2	Stable	16,989
Dish Network Corporation	Ba3	Stable	13,756
Total			30,745
Cumulative Total Debt			616,973

[1] Excludes debt held at DirecTV

[2] Includes pro forma debt for the Time Warner Cable/BrightHouse Networks acquisitions

[3] Includes pro forma debt for the acquisition by Altice

Source: Moody's Financial Metrics

© 2016 Moody's Corporation, Moody's Investors Service, Inc., Moody's Analytics, Inc. and/or their licensors and affiliates (collectively, "MOODY'S"). All rights reserved.

CREDIT RATINGS ISSUED BY MOODY'S INVESTORS SERVICE, INC. AND ITS RATINGS AFFILIATES ("MIS") ARE MOODY'S CURRENT OPINIONS OF THE RELATIVE FUTURE CREDIT RISK OF ENTITIES, CREDIT COMMITMENTS, OR DEBT OR DEBT-LIKE SECURITIES, AND CREDIT RATINGS AND RESEARCH PUBLICATIONS PUBLISHED BY MOODY'S ("MOODY'S PUBLICATIONS") MAY INCLUDE MOODY'S CURRENT OPINIONS OF THE RELATIVE FUTURE CREDIT RISK OF ENTITIES, CREDIT COMMITMENTS, OR DEBT OR DEBT-LIKE SECURITIES. MOODY'S DEFINES CREDIT RISK AS THE RISK THAT AN ENTITY MAY NOT MEET ITS CONTRACTUAL FINANCIAL OBLIGATIONS AS THEY COME DUE AND ANY ESTIMATED FINANCIAL LOSS IN THE EVENT OF DEFAULT. CREDIT RATINGS DO NOT ADDRESS ANY OTHER RISK, INCLUDING BUT NOT LIMITED TO LIQUIDITY RISK, MARKET VALUE RISK, OR PRICE VOLATILITY. CREDIT RATINGS AND MOODY'S OPINIONS INCLUDED IN MOODY'S PUBLICATIONS ARE NOT STATEMENTS OF CURRENT OR HISTORICAL FACT. MOODY'S PUBLICATIONS MAY ALSO INCLUDE QUANTITATIVE MODEL-BASED ESTIMATES OF CREDIT RISK AND RELATED OPINIONS OR COMMENTARY PUBLISHED BY MOODY'S ANALYTICS, INC. CREDIT RATINGS AND MOODY'S PUBLICATIONS DO NOT CONSTITUTE OR PROVIDE INVESTMENT OR FINANCIAL ADVICE, AND CREDIT RATINGS AND MOODY'S PUBLICATIONS ARE NOT AND DO NOT PROVIDE RECOMMENDATIONS TO PURCHASE, SELL, OR HOLD PARTICULAR SECURITIES. NEITHER CREDIT RATINGS NOR MOODY'S PUBLICATIONS COMMENT ON THE SUITABILITY OF AN INVESTMENT FOR ANY PARTICULAR INVESTOR. MOODY'S ISSUES ITS CREDIT RATINGS AND PUBLISHES MOODY'S PUBLICATIONS WITH THE EXPECTATION AND UNDERSTANDING THAT EACH INVESTOR WILL, WITH DUE CARE, MAKE ITS OWN STUDY AND EVALUATION OF EACH SECURITY THAT IS UNDER CONSIDERATION FOR PURCHASE, HOLDING, OR SALE.

MOODY'S CREDIT RATINGS AND MOODY'S PUBLICATIONS ARE NOT INTENDED FOR USE BY RETAIL INVESTORS AND IT WOULD BE RECKLESS AND INAPPROPRIATE FOR RETAIL INVESTORS TO USE MOODY'S CREDIT RATINGS OR MOODY'S PUBLICATIONS WHEN MAKING AN INVESTMENT DECISION. IF IN DOUBT YOU SHOULD CONTACT YOUR FINANCIAL OR OTHER PROFESSIONAL ADVISER. ALL INFORMATION CONTAINED HEREIN IS PROTECTED BY LAW, INCLUDING BUT NOT LIMITED TO, COPYRIGHT LAW, AND NONE OF SUCH INFORMATION MAY BE COPIED OR OTHERWISE REPRODUCED, REPACKAGED, FURTHER TRANSMITTED, TRANSFERRED, DISSEMINATED, REDISTRIBUTED OR RESOLD, OR STORED FOR SUBSEQUENT USE FOR ANY SUCH PURPOSE, IN WHOLE OR IN PART, IN ANY FORM OR MANNER OR BY ANY MEANS WHATSOEVER, BY ANY PERSON WITHOUT MOODY'S PRIOR WRITTEN CONSENT.

All information contained herein is obtained by MOODY'S from sources believed by it to be accurate and reliable. Because of the possibility of human or mechanical error as well as other factors, however, all information contained herein is provided "AS IS" without warranty of any kind. MOODY'S adopts all necessary measures so that the information it uses in assigning a credit rating is of sufficient quality and from sources MOODY'S considers to be reliable, including, when appropriate, independent third-party sources. However, MOODY'S is not an auditor and cannot in every instance independently verify or validate information received in the rating process or in preparing the Moody's Publications.

To the extent permitted by law, MOODY'S and its directors, officers, employees, agents, representatives, licensors and suppliers disclaim liability to any person or entity for any indirect, special, consequential, or incidental losses or damages whatsoever arising from or in connection with the information contained herein or the use of or inability to use any such information, even if MOODY'S or any of its directors, officers, employees, agents, representatives, licensors or suppliers is advised in advance of the possibility of such losses or damages, including but not limited to: (a) any loss of present or prospective profits or (b) any loss or damage arising where the relevant financial instrument is not the subject of a particular credit rating assigned by MOODY'S.

To the extent permitted by law, MOODY'S and its directors, officers, employees, agents, representatives, licensors and suppliers disclaim liability for any direct or compensatory losses or damages caused to any person or entity, including but not limited to by any negligence (but excluding fraud, willful misconduct or any other type of liability that, for the avoidance of doubt, by law cannot be excluded) on the part of, or any contingency within or beyond the control of, MOODY'S or any of its directors, officers, employees, agents, representatives, licensors or suppliers, arising from or in connection with the information contained herein or the use of or inability to use any such information.

NO WARRANTY, EXPRESS OR IMPLIED, AS TO THE ACCURACY, TIMELINESS, COMPLETENESS, MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OF ANY SUCH RATING OR OTHER OPINION OR INFORMATION IS GIVEN OR MADE BY MOODY'S IN ANY FORM OR MANNER WHATSOEVER.

Moody's Investors Service, Inc., a wholly-owned credit rating agency subsidiary of Moody's Corporation ("MCO"), hereby declares that most issuers of debt securities (including corporate and municipal bonds, debentures, notes and commercial paper) and preferred stock rated by Moody's Investors Service, Inc. have, prior to assignment of any rating, agreed to pay to Moody's Investors Service, Inc. for appraisal and rating services rendered by it fees ranging from \$1,500 to approximately \$2,500,000. MCO and MIS also maintain policies and procedures to address the independence of MIS's ratings and rating processes. Information regarding certain affiliations that may exist between directors of MCO and rated entities, and between entities who hold ratings from MIS and have also publicly reported to the SEC an ownership interest in MCO of more than 5%, is posted annually at www.moody.com under the heading: Investor Relations — Corporate Governance — Director and Shareholder Affiliation Policy.

Additional terms for Australia only: Any publication into Australia of this document is pursuant to the Australian Financial Services License of MOODY'S affiliate, Moody's Investors Service Pty Limited (ABN 61 001 399 657) AFSL 396969 and/or Moody's Analytics Australia Pty Ltd (ABN 94 105 134 972) AFSL 383569 (as applicable). This document is intended to be provided only to "wholesale clients" within the meaning of section 761C of the Corporations Act 2001. By continuing to access this document from within Australia, you represent to MOODY'S that you are, or are accessing the document as a representative of, a "wholesale client" and that neither you nor the entity you represent will directly or indirectly disseminate this document or its contents to "retail clients" within the meaning of section 761C of the Corporations Act 2001. MOODY'S credit rating is an opinion as to the creditworthiness of a debt obligation of the issuer, not an equity securities of the issuer or any form of security that is available to retail investors. It would be reckless and inappropriate for retail investors to use MOODY'S credit ratings or publications when making an investment decision. If in doubt you should contact your financial or other professional adviser.

Additional terms for Japan only: Moody's Japan K.K. ("MJCK") is a wholly-owned credit rating agency subsidiary of Moody's Group Japan G.K., which is wholly-owned by Moody's Investors Service Holdings, Inc., a wholly-owned subsidiary of MCO. Moody's SF Japan K.K. ("MSJ") is a wholly-owned credit rating agency subsidiary of MJCK. MSJ is not a Nationally Recognized Statistical Rating Organization ("NRSRO"). Therefore, credit ratings assigned by MSJ are Non-NRSRO Credit Ratings. Non-NRSRO Credit Ratings are assigned by an entity that is not a NRSRO and, consequently, the rated obligation will not qualify for certain types of treatment under U.S. laws. MJCK and MSJ are credit rating agencies registered with the Japan Financial Services Agency and their registration numbers are PSA Commissioner (Rating) No. 2 and 3 respectively.

MJCK or MSJ (as applicable) hereby disclose that most issuers of debt securities (including corporate and municipal bonds, debentures, notes and commercial paper) and preferred stock rated by MJCK or MSJ (as applicable) have, prior to assignment of any rating, agreed to pay to MJCK or MSJ (as applicable) for appraisal and rating services rendered by it fees ranging from JPY200,000 to approximately JPY350,000,000.

MJCK and MSJ also maintain policies and procedures to address Japanese regulatory requirements.

REPORT NUMBER 1019671

Joanne Wall

From: Scott Bergmann <SBergmann@ctia.org>
Sent: Tuesday, March 01, 2016 2:16 PM
To: Travis Litman
Cc: Johanna Thomas
Subject: Letter on Consensus Privacy Framework
Attachments: Wheeler Letter Re Privacy Principles 3 1 16.pdf

Hi Travis,

Following up on my voicemail, attached please find a letter sent today by ACA, CCA, CTIA, NCTA, and USTelecom to FCC Chairman Wheeler setting forth guidelines and principles for the FCC to consider as it moves forward with a rulemaking on broadband privacy. This consensus privacy framework will protect consumer privacy in a way that is consistent with other privacy laws that apply to other companies in the Internet ecosystem. We hope the FCC will seek comment on this consensus framework, in its entirety, in its upcoming rulemaking proceeding.

As always, please let me know if you have any questions. Best,

Scott



Scott Bergmann

Vice President, Regulatory Affairs

1400 16th Street, NW

Washington, DC 20036

202-736-3660 (office)

202-997-3916 (mobile)

sbergmann@ctia.org



March 1, 2016

The Honorable Tom Wheeler
Chairman
Federal Communications Commission
445 12th St. SW
Washington, D.C. 20554

Dear Chairman Wheeler,

Today, the American Cable Association, Competitive Carriers Association, CTIA, National Cable & Telecommunications Association, and USTelecom offer for the Commission's consideration a detailed proposal for a broadband privacy framework. After significant examination and analysis, these associations have developed the attached consensus Privacy Framework setting forth guidelines and principles to protect consumer privacy in a way that is consistent with other privacy laws that apply to companies providing services online. By adopting these principles, the Commission would establish a regime that protects consumer privacy and security while also providing flexibility for providers to implement and update their practices as consumer expectations and technologies evolve.

If the courts determine that the Commission has authority over broadband privacy, the FCC should focus on four privacy principles: (1) transparency; (2) respect for context and consumer choice; (3) data security; and (4) data breach notification. For each of these principles, the FCC should draw from and harmonize with the longstanding Federal Trade Commission unfairness and deception approach to privacy, which, before the FCC's reclassification decision, governed the privacy practices of all companies in the Internet ecosystem and will continue to apply to non-ISPs going forward.

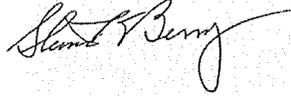
As the Commission develops its approach to broadband privacy, we respectfully request that it seek comment on the entirety of the Privacy Framework we submit today. Because regulation of broadband privacy is a new area for the Commission, it should take the necessary time to build a robust record rather than prejudge the issues by adopting tentative conclusions before there is a public discussion of the consensus Privacy Framework.

We look forward to continuing a conversation with the Commission about the best way to provide privacy and innovation benefits to consumers.

Respectfully submitted,



Matthew M. Polka
President & CEO
American Cable Association



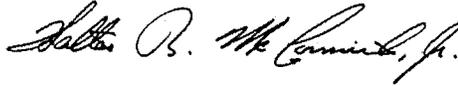
Steven K. Berry
President & CEO
Competitive Carriers Association



Meredith Attwell Baker
President & CEO
CTIA



Michael Powell
President & CEO
National Cable & Telecommunications Association



Walter B. McCormick, Jr.
President & CEO
USTelecom

cc: The Honorable Mignon Clyburn
The Honorable Jessica Rosenworcel
The Honorable Ajit Pai
The Honorable Michael O’Rielly

Privacy Framework

Discussion Paper

All entities in the Internet ecosystem should be subject to a consistent privacy framework with respect to consumer information. Consumer information should be protected based upon the sensitivity of the information to the consumer and how the information is used—not the type of business keeping it, how that business obtains it, or what regulatory agency has authority over it. Consumers should have consistent and predictable privacy protections for the information they deem private and sensitive, no matter how or with whom they share it. Consumers also will benefit from a consistent privacy framework that promotes the emergence of new business models and innovative uses of data that foster increased consumer choice and service customization.

The FCC should adopt an approach to privacy and data security for CPNI that is flexible, harmonized with the well-established and successful FTC framework, and backed up by strong but fair enforcement for unfair or deceptive acts or practices (UDAP) that materially harm consumers.¹ This well-tested consumer protection approach is consistent with the FCC’s privacy recommendations in the 2010 National Broadband Plan, the FTC’s and White House’s 2012 Privacy Reports, and the White House’s 2015 Consumer Privacy Bill of Rights, as well as with Chairman Wheeler’s recent testimony before Congress acknowledging the importance of coordination with the FTC and harmonization with its privacy framework.

That approach will benefit consumers by safeguarding privacy interests as it has for years and will ensure that the same privacy and security framework applies to all entities in the Internet ecosystem. By leveraging a tested privacy model, the FCC will avoid inconsistent requirements that could otherwise hamper innovation and reduce competition. Most important, it will minimize consumer confusion as well as other harms associated with disparate privacy regulation across the ecosystem. Indeed, this approach will align with consumers’ expectations that their data would be subject to consistent privacy rules regardless of whether it is used by their Internet Service Provider (ISP), application developers, operating systems, or edge providers.

When adopting a framework, the FCC should keep the following guidelines in mind:

- Consistent and Coordinated Regulatory Regimes. The FCC’s rules and principles for regulating and enforcing privacy and security should be as similar as possible to the FTC approach, which will continue to govern other Internet ecosystem players’ use and disclosure of the same or similar data. The consistent application of standards across sectors would fulfill the following key tenets in the White House Privacy Report: (1) avoid “inconsistent standards for related technologies” that could dampen innovation; (2)

¹ This framework is intended for discussion purposes, and we are not conceding that the FCC has authority to adopt privacy and security rules for Broadband Internet Access Services or over data related to consumers’ use of Broadband Internet Access Services. To the extent it is determined that the FCC has such statutory authority, this document is intended to set forth principles for FCC consideration and possible adoption that are harmonized and consistent with the FTC and other government entities’ approach to privacy and security for the same or similar data. Even if courts determine that the FCC’s reclassification of Broadband Internet Access Services is a lawful exercise of authority, any rules must not exceed the text and legislative history of Section 222 of the Act.

foster a “level playing field for companies;” and, most importantly, (3) create “a consistent set of expectations for consumers.” To achieve this end, the FCC’s policies, rules, and enforcement practices should conform to the longstanding limiting principles articulated in the FTC’s Unfairness and Deception Policy Statements. In addition, the FCC and FTC can achieve their recent MOU’s stated goal of avoiding “duplicative, redundant or inconsistent oversight” by developing a new process to ensure that their substantive privacy policies and basis for enforcement are consistent going forward.

- Flexibility. The FCC’s approach should provide a flexible framework within which telecommunications service providers can implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments in this space. Specifically, this framework should identify the privacy or security *goals*, and afford providers flexibility in achieving those goals, rather than dictate the particular *methods* by which providers are expected to achieve those goals. Adopting a flexible approach also will help ensure consistent federal and state requirements governing customer information.
- Application. Consistent with the Communications Act and to eliminate unnecessary duplication of authority with other agencies, the FCC’s framework should only apply when 1) telecommunications service providers are providing telecommunications services and 2) the CPNI is made available by the customer to the telecommunications service provider solely by virtue of the carrier-customer relationship. The framework cannot lawfully apply to:
 - Providers’ non-telecommunications services and products
 - Providers’ non-telecommunications service provider affiliates
 - Information that is not made available to the carrier by the customer solely by virtue of the carrier-customer relationship
- Individually Identifiable. The FCC should carve out from the scope of its new framework any data that is de-identified, aggregated, or does not otherwise identify a known individual. The insights derived from the use of de-identified data can offer great benefits to consumers and society and such use avoids the sensitivities that may be associated with identified data.
- Unfair or Deceptive Conduct. As noted above, the FCC’s policies, rules, and enforcement practices should conform to the FTC’s longstanding limiting principles articulated in its Policy Statements on Unfairness (1980) and Deception (1983). This approach is consistent with the FCC’s commitment to conduct a cost-benefit analysis of its regulatory framework in accordance with President Obama’s Executive Orders 13563 and 13579, which require agencies to “adopt a regulation only upon a reasoned determination its benefits justify its costs” and “tailor its regulations to impose the least burden on society.”
 - Unfair Conduct. A provider acts unfairly if its act or practice (1) causes or is likely to cause substantial injury to consumers (2) which is not reasonably avoidable by consumers themselves, and (3) is not outweighed by countervailing benefits to consumers or to competition.
 - Deceptive Conduct. A provider acts deceptively if (1) it makes a statement or omission, or engages in a practice, that is likely to mislead a customer, (2) viewed from the perspective of a consumer acting reasonably under the circumstances, and (3) the deceptive statement, omission, or practice is material—meaning that

the misrepresentation or practice is likely to affect the consumer's conduct or decision with regard to a product or service.

- Additional Guidance. In coordination with other privacy regulators, the FCC could, like the FTC and various states like California, provide additional guidance on how it interprets its framework through workshops or reports. The FCC also could encourage and support the development and implementation of industry guidelines.
- Update and Harmonize Existing CPNI Rules. The existing CPNI rules should be revisited in their entirety and modernized to use the same flexible framework for all services subject to Section 222, including traditional voice services. In no event should the prescriptive outdated CPNI rules designed for legacy voice services apply to broadband services. Instead, a common set of flexible policies that allow providers to keep up with their customers' expectations and evolving technology should apply to both types of services.

With these guidelines in mind, if the courts determine that the FCC has authority to regulate broadband privacy, the FCC could adopt the following principles, which encompass and are consistent with the privacy and security framework that applies to the rest of the industry. Each of these principles and the goals noted above should provide flexibility for providers to implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments:

- Transparency. A telecommunications service provider should provide notice, which is neither deceptive nor unfair, describing the CPNI that it collects, how it will use the CPNI, and whether and for what purposes it may share CPNI with third parties.
- Respect for Context and Consumer Choice. A telecommunications service provider may use or disclose CPNI as is consistent with the context in which the customer provides, or the provider obtains, the information, provided that the provider's actions are not unfair or deceptive. For example, the use or disclosure of CPNI for the following commonly accepted data practices would not warrant a choice mechanism, either because customer consent can be inferred or because public policy considerations make choice unnecessary: product and service fulfillment, fraud prevention, compliance with law, responses to government requests, network management, first-party marketing, and affiliate sharing where the affiliate relationship is reasonably clear to consumers. Consistent with the flexible choice mechanisms available to all other entities in the Internet ecosystem, telecommunications service providers should give consumers easy-to-understand choices for non-contextual uses and disclosures of their CPNI, where the failure to provide choice would be deceptive or unfair. The provider should consider the sensitivity of the data and the context in which it was collected when determining the appropriate choice mechanism.
- Data Security. A telecommunications service provider should establish, implement, and maintain a CPNI data security program that is neither unfair nor deceptive and includes reasonable physical, technical, and administrative security safeguards to protect CPNI from unauthorized access, use, and disclosure. Providers' CPNI data security programs should provide reasonable protections in light of the nature and scope of the activities of the company, the sensitivity of the data, and the size and complexity of the relevant data operations of the company.

- Data Breach Notifications. Telecommunications service providers should notify customers whose CPNI has been breached when failure to notify would be unfair or deceptive. Given that breach investigations frequently are ongoing at the time providers offer notice to customers, a notice that turns out to be incomplete or inaccurate is not deceptive, as long as the provider corrects any material inaccuracies within a reasonable period of time of discovering them. Telecommunications providers have flexibility to determine how and when to provide such notice.

The FCC can ensure compliance with the above principles by pursuing reasonable enforcement actions against telecommunications service providers that have clearly violated these principles.

Joanne Wall

From: Marquita Abitong
Sent: Thursday, March 10, 2016 10:22 AM
To: Travis Litman
Subject: FW: VZ/Litman Mtg Request re: BB Privacy

From: Berkowitz, Ann D (Ann) [mailto:aberkowitz@verizon.com]
Sent: Wednesday, March 09, 2016 6:47 PM
To: Marquita Abitong
Subject: VZ/Litman Mtg Request re: BB Privacy

Hi Marquita –

I'd like to request a meeting for Verizon with Travis to discuss broadband privacy. The Verizon attendees will be Maggie McCreedy and Cathy Hilke. If possible, we'd like to schedule the meeting for some time next week. Thanks and please let me know if you have any questions or need additional information.

verizon[✓]

Ann D. Berkowitz
Federal Regulatory Affairs
(202) 515-2539 (O)
(202) 669-5585 (C)

Joanne Wall

From: Lisa Hone
Sent: Tuesday, March 01, 2016 2:29 PM
To: CPD Privacy Team
Cc: Daniel Kahn
Subject: FW: Industry Privacy Framework Discussion Paper
Attachments: Wheeler Letter Re Privacy Principles 3 1 16.pdf

From: Follansbee, Lynn [mailto:lfollansbee@ustelecom.org]
Sent: Tuesday, March 01, 2016 2:24 PM
To: Matthew DelNero ; Lisa Hone
Subject: Industry Privacy Framework Discussion Paper

Matt and Lisa:

Per my phone message to you, attached is a copy of the letter going to the 8th Floor today.

Please let me know if you have any questions.

Thank you,

Lynn

B. Lynn Follansbee
Vice President, Law & Policy
USTelecom
607 14th Street NW
Suite 400
Washington, DC 20005
Tel: 202-326-7256
Email: lfollansbee@ustelecom.org

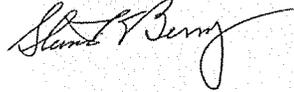


We look forward to continuing a conversation with the Commission about the best way to provide privacy and innovation benefits to consumers.

Respectfully submitted,



Matthew M. Polka
President & CEO
American Cable Association



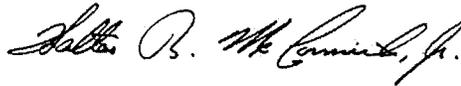
Steven K. Berry
President & CEO
Competitive Carriers Association



Meredith Attwell Baker
President & CEO
CTIA



Michael Powell
President & CEO
National Cable & Telecommunications Association



Walter B. McCormick, Jr.
President & CEO
USTelecom

cc: The Honorable Mignon Clyburn
The Honorable Jessica Rosenworcel
The Honorable Ajit Pai
The Honorable Michael O'Rielly

Privacy Framework

Discussion Paper

All entities in the Internet ecosystem should be subject to a consistent privacy framework with respect to consumer information. Consumer information should be protected based upon the sensitivity of the information to the consumer and how the information is used—not the type of business keeping it, how that business obtains it, or what regulatory agency has authority over it. Consumers should have consistent and predictable privacy protections for the information they deem private and sensitive, no matter how or with whom they share it. Consumers also will benefit from a consistent privacy framework that promotes the emergence of new business models and innovative uses of data that foster increased consumer choice and service customization.

The FCC should adopt an approach to privacy and data security for CPNI that is flexible, harmonized with the well-established and successful FTC framework, and backed up by strong but fair enforcement for unfair or deceptive acts or practices (UDAP) that materially harm consumers.¹ This well-tested consumer protection approach is consistent with the FCC's privacy recommendations in the 2010 National Broadband Plan, the FTC's and White House's 2012 Privacy Reports, and the White House's 2015 Consumer Privacy Bill of Rights, as well as with Chairman Wheeler's recent testimony before Congress acknowledging the importance of coordination with the FTC and harmonization with its privacy framework.

That approach will benefit consumers by safeguarding privacy interests as it has for years and will ensure that the same privacy and security framework applies to all entities in the Internet ecosystem. By leveraging a tested privacy model, the FCC will avoid inconsistent requirements that could otherwise hamper innovation and reduce competition. Most important, it will minimize consumer confusion as well as other harms associated with disparate privacy regulation across the ecosystem. Indeed, this approach will align with consumers' expectations that their data would be subject to consistent privacy rules regardless of whether it is used by their Internet Service Provider (ISP), application developers, operating systems, or edge providers.

When adopting a framework, the FCC should keep the following guidelines in mind:

- Consistent and Coordinated Regulatory Regimes. The FCC's rules and principles for regulating and enforcing privacy and security should be as similar as possible to the FTC approach, which will continue to govern other Internet ecosystem players' use and disclosure of the same or similar data. The consistent application of standards across sectors would fulfill the following key tenets in the White House Privacy Report: (1) avoid "inconsistent standards for related technologies" that could dampen innovation; (2)

¹ This framework is intended for discussion purposes, and we are not conceding that the FCC has authority to adopt privacy and security rules for Broadband Internet Access Services or over data related to consumers' use of Broadband Internet Access Services. To the extent it is determined that the FCC has such statutory authority, this document is intended to set forth principles for FCC consideration and possible adoption that are harmonized and consistent with the FTC and other government entities' approach to privacy and security for the same or similar data. Even if courts determine that the FCC's reclassification of Broadband Internet Access Services is a lawful exercise of authority, any rules must not exceed the text and legislative history of Section 222 of the Act.

foster a “level playing field for companies;” and, most importantly, (3) create “a consistent set of expectations for consumers.” To achieve this end, the FCC’s policies, rules, and enforcement practices should conform to the longstanding limiting principles articulated in the FTC’s Unfairness and Deception Policy Statements. In addition, the FCC and FTC can achieve their recent MOU’s stated goal of avoiding “duplicative, redundant or inconsistent oversight” by developing a new process to ensure that their substantive privacy policies and basis for enforcement are consistent going forward.

- Flexibility. The FCC’s approach should provide a flexible framework within which telecommunications service providers can implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments in this space. Specifically, this framework should identify the privacy or security *goals*, and afford providers flexibility in achieving those goals, rather than dictate the particular *methods* by which providers are expected to achieve those goals. Adopting a flexible approach also will help ensure consistent federal and state requirements governing customer information.
- Application. Consistent with the Communications Act and to eliminate unnecessary duplication of authority with other agencies, the FCC’s framework should only apply when 1) telecommunications service providers are providing telecommunications services and 2) the CPNI is made available by the customer to the telecommunications service provider solely by virtue of the carrier-customer relationship. The framework cannot lawfully apply to:
 - Providers’ non-telecommunications services and products
 - Providers’ non-telecommunications service provider affiliates
 - Information that is not made available to the carrier by the customer solely by virtue of the carrier-customer relationship
- Individually Identifiable. The FCC should carve out from the scope of its new framework any data that is de-identified, aggregated, or does not otherwise identify a known individual. The insights derived from the use of de-identified data can offer great benefits to consumers and society and such use avoids the sensitivities that may be associated with identified data.
- Unfair or Deceptive Conduct. As noted above, the FCC’s policies, rules, and enforcement practices should conform to the FTC’s longstanding limiting principles articulated in its Policy Statements on Unfairness (1980) and Deception (1983). This approach is consistent with the FCC’s commitment to conduct a cost-benefit analysis of its regulatory framework in accordance with President Obama’s Executive Orders 13563 and 13579, which require agencies to “adopt a regulation only upon a reasoned determination its benefits justify its costs” and “tailor its regulations to impose the least burden on society.”
 - Unfair Conduct. A provider acts unfairly if its act or practice (1) causes or is likely to cause substantial injury to consumers (2) which is not reasonably avoidable by consumers themselves, and (3) is not outweighed by countervailing benefits to consumers or to competition.
 - Deceptive Conduct. A provider acts deceptively if (1) it makes a statement or omission, or engages in a practice, that is likely to mislead a customer, (2) viewed from the perspective of a consumer acting reasonably under the circumstances, and (3) the deceptive statement, omission, or practice is material—meaning that

the misrepresentation or practice is likely to affect the consumer's conduct or decision with regard to a product or service.

- Additional Guidance. In coordination with other privacy regulators, the FCC could, like the FTC and various states like California, provide additional guidance on how it interprets its framework through workshops or reports. The FCC also could encourage and support the development and implementation of industry guidelines.
- Update and Harmonize Existing CPNI Rules. The existing CPNI rules should be revisited in their entirety and modernized to use the same flexible framework for all services subject to Section 222, including traditional voice services. In no event should the prescriptive outdated CPNI rules designed for legacy voice services apply to broadband services. Instead, a common set of flexible policies that allow providers to keep up with their customers' expectations and evolving technology should apply to both types of services.

With these guidelines in mind, if the courts determine that the FCC has authority to regulate broadband privacy, the FCC could adopt the following principles, which encompass and are consistent with the privacy and security framework that applies to the rest of the industry. Each of these principles and the goals noted above should provide flexibility for providers to implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments:

- Transparency. A telecommunications service provider should provide notice, which is neither deceptive nor unfair, describing the CPNI that it collects, how it will use the CPNI, and whether and for what purposes it may share CPNI with third parties.
- Respect for Context and Consumer Choice. A telecommunications service provider may use or disclose CPNI as is consistent with the context in which the customer provides, or the provider obtains, the information, provided that the provider's actions are not unfair or deceptive. For example, the use or disclosure of CPNI for the following commonly accepted data practices would not warrant a choice mechanism, either because customer consent can be inferred or because public policy considerations make choice unnecessary: product and service fulfillment, fraud prevention, compliance with law, responses to government requests, network management, first-party marketing, and affiliate sharing where the affiliate relationship is reasonably clear to consumers. Consistent with the flexible choice mechanisms available to all other entities in the Internet ecosystem, telecommunications service providers should give consumers easy-to-understand choices for non-contextual uses and disclosures of their CPNI, where the failure to provide choice would be deceptive or unfair. The provider should consider the sensitivity of the data and the context in which it was collected when determining the appropriate choice mechanism.
- Data Security. A telecommunications service provider should establish, implement, and maintain a CPNI data security program that is neither unfair nor deceptive and includes reasonable physical, technical, and administrative security safeguards to protect CPNI from unauthorized access, use, and disclosure. Providers' CPNI data security programs should provide reasonable protections in light of the nature and scope of the activities of the company, the sensitivity of the data, and the size and complexity of the relevant data operations of the company.

- Data Breach Notifications. Telecommunications service providers should notify customers whose CPNI has been breached when failure to notify would be unfair or deceptive. Given that breach investigations frequently are ongoing at the time providers offer notice to customers, a notice that turns out to be incomplete or inaccurate is not deceptive, as long as the provider corrects any material inaccuracies within a reasonable period of time of discovering them. Telecommunications providers have flexibility to determine how and when to provide such notice.

The FCC can ensure compliance with the above principles by pursuing reasonable enforcement actions against telecommunications service providers that have clearly violated these principles.

Joanne Wall

Subject: Meet with VZ re: broadband privacy
Location: 5-B142

Start: Thu 2/11/2016 4:00 PM
End: Thu 2/11/2016 4:30 PM
Show Time As: Tentative

Recurrence: (none)

Meeting Status: Not yet responded

Organizer: Lisa Hone
Required Attendees: Matthew DelNero; Daniel Kahn; Melissa Droller Kinkel; Sherwin Siy

We can add others, but I wanted to hold this for now.

Joanne Wall

From: Melissa Droller Kirkel
Sent: Friday, August 14, 2015 7:27 AM
To: Kristine Fargotstein
Cc: John Visclosky; Zachary Ross
Subject: FW: CTIA Files Petition for Partial Reconsideration of Lifeline Order on Reconsideration
Attachments: 150813 FILED CTIA Lifeline Data Security Recon Petition.pdf

Follow Up Flag: Follow up
Flag Status: Flagged

(b) (5)



From: Matthew DelNero
Sent: Thursday, August 13, 2015 6:20:43 PM
To: Scott Jordan; Jonathan Sallet; Louisa Terrell; Jennifer Tatel; Lisa Hone; Claude Aiken; Melissa Droller Kirkel; Philip Verveer; Daniel Alvarez
Subject: FW: CTIA Files Petition for Partial Reconsideration of Lifeline Order on Reconsideration

(b) (5)



Matt

From: Matthew Gerst [mailto:MGerst@ctia.org]
Sent: Thursday, August 13, 2015 5:28 PM
To: Matthew DelNero
Cc: Scott Bergmann
Subject: CTIA Files Petition for Partial Reconsideration of Lifeline Order on Reconsideration

Matt,
Attached please find a courtesy copy of CTIA's Petition for Partial Reconsideration of the FCC's Lifeline Order. We're petitioning on the narrow issue of the FCC's authority under the Communications Act to impose data security obligations, but not the Order on Reconsideration's underlying obligation that carriers must retain certain documentation that verifies the eligibility of Lifeline subscribers.
We'd be happy to discuss further if you'd like to reach out to me or Scott.

Regards,
Matt

Matthew Gerst
Director, Regulatory Affairs
CTIA-The Wireless Association®
e: MGerst@ctia.org
m: 202.288.6370
p: 202.736.3216
www.accesswireless.org

www.growingwireless.com

www.wireless911.com

www.ctia.org

It is CTIA's policy to comply fully with the antitrust laws. To ensure compliance, CTIA's employees and the representatives of CTIA member companies should follow this Checklist of antitrust "Do's" and "Don'ts" when participating in CTIA-sponsored activities: [http://files.ctia.org/pdf/Antitrust Checklist for CTIA Meetings.pdf](http://files.ctia.org/pdf/Antitrust%20Checklist%20for%20CTIA%20Meetings.pdf)

CTIA's Petition for Reconsideration Can Be Found Here:

<https://www.google.com/search?q=seeks+reconsideration+of+a+narrow%2C+discrete+aspect&ie=utf-8&oe=utf-8>

Joanne Wall

From: Lisa Hone
Sent: Monday, January 11, 2016 11:29 AM
To: Melissa Droller Kirkel
Subject: FW: Happy New Year! Following Up

(b) (5)



From: Cooney, Maureen [GA] [mailto:Maureen.Cooney@sprint.com]
Sent: Monday, January 11, 2016 10:39 AM
To: Lisa Hone
Cc: Sullivan, Matt [GA] ; Dedeaux, Sheila D [GA] ; Cooney, Maureen [GA]
Subject: RE: Happy New Year! Following Up

Happy Monday, Lisa. Thanks so much. If it is convenient for you, we will come in to sit down with you. It will be Matt Sullivan, Counsel on our team, Sheila Dedeaux, Associate Head of Privacy, and myself. Could you please let me know if anyone else from the FCC will join the meeting and, if so, their role at the FCC? We will see you on Friday unless we hear from you otherwise. Thanks, again. – Maureen

Maureen Cooney
Head of Privacy, Office of Privacy
O: 703-592-7580 / M: 202-664-7954
maureen.cooney@sprint.com

Sprint  #gettingbettereveryday

NOTICE: This communication may contain privileged or other confidential information. If you have received it in error, please advise the sender by reply email and immediately delete the message and any attachments without copying or disclosing the contents. Thank you.

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Monday, January 11, 2016 9:46 AM
To: Cooney, Maureen [GA] <Maureen.Cooney@sprint.com>
Cc: Sullivan, Matt [GA] <matthew.sullivan@sprint.com>
Subject: RE: Happy New Year! Following Up

Let's say 11 on Friday.
If that works for you.
Do you want to come in or do a conference call?

Lisa

From: Cooney, Maureen [GA] [<mailto:Maureen.Cooney@sprint.com>]
Sent: Friday, January 08, 2016 6:51 PM
To: Lisa Hone <Lisa.Hone@fcc.gov>
Cc: Sullivan, Matt [GA] <matthew.sullivan@sprint.com>
Subject: RE: Happy New Year! Following Up

Lisa – it looks like Wednesday afternoon also is workable if that is helpful. – Maureen

From: Cooney, Maureen [GA]
Sent: Friday, January 08, 2016 5:48 PM
To: Lisa Hone <Lisa.Hone@fcc.gov>
Cc: Sullivan, Matt [GA] <matthew.sullivan@sprint.com>; Cooney, Maureen [GA] <Maureen.Cooney@sprint.com>
Subject: RE: Happy New Year! Following Up

Hi, Lisa. On Friday, would 10 or 11 be workable for you? Thanks.

From: Lisa Hone [<mailto:Lisa.Hone@fcc.gov>]
Sent: Friday, January 08, 2016 5:45 PM
To: Cooney, Maureen [GA] <Maureen.Cooney@sprint.com>
Cc: Sullivan, Matt [GA] <matthew.sullivan@sprint.com>
Subject: RE: Happy New Year! Following Up

Thanks for following up.
Happy New Year.

Next Tuesday is terrible for me, and Thursday I had hoped to spend some time at the FTC PrivacyCon.
What time Friday morning would work for you?

All the best,

Lisa

From: Cooney, Maureen [GA] [<mailto:Maureen.Cooney@sprint.com>]
Sent: Friday, January 08, 2016 5:39 PM
To: Lisa Hone <Lisa.Hone@fcc.gov>
Cc: Cooney, Maureen [GA] <Maureen.Cooney@sprint.com>; Sullivan, Matt [GA] <matthew.sullivan@sprint.com>
Subject: Happy New Year! Following Up

Dear Lisa,

Happy New Year! I hope you enjoyed the holidays! Now that we are back, I would like to follow up with you on your call. I would be happy to have a phone call or to visit with you in person, along with Matt Sullivan in my office, who also attending the CPNI Principles group meeting and spoke a bit on data breach issues. We are wondering if a time next Tuesday or Thursday be convenient? Friday morning is also a possibility. I hope this is helpful. Best to you. -- Maureen

Maureen Cooney
Head of Privacy, Office of Privacy
O: 703-592-7580 / M: 202-664-7954
maureen.cooney@sprint.com

 **Sprint**  #gettingbettereveryday

NOTICE: This communication may contain privileged or other confidential information. If you have received it in error, please advise the sender by reply email and immediately delete the message and any attachments without copying or disclosing the contents. Thank you.

Learn more on how to switch to Sprint and save 50% on most Verizon, AT&T or T-Mobile rates. See sprint.com/50off for details.

This e-mail may contain Sprint proprietary information intended for the sole use of the recipient(s). Any use by others is prohibited. If you are not the intended recipient, please contact the sender and delete all copies of the message.

Learn more on how to switch to Sprint and save 50% on most Verizon, AT&T or T-Mobile rates. See sprint.com/50off for details.

This e-mail may contain Sprint proprietary information intended for the sole use of the recipient(s). Any use by others is prohibited. If you are not the intended recipient, please contact the sender and delete all copies of the message.

Learn more on how to switch to Sprint and save 50% on most Verizon, AT&T or T-Mobile rates. See sprint.com/50off for details.

This e-mail may contain Sprint proprietary information intended for the sole use of the recipient(s). Any use by others is prohibited. If you are not the intended recipient, please contact the sender and delete all copies of the message.

Joanne Wall

From: Matthew DelNero
Sent: Friday, April 01, 2016 7:06 PM
To: will.h.johnson@verizon.com
Subject: Broadband Privacy NPRM

Will, it was good to talk with you earlier. FYI, we just released the privacy NPRM (a little later in the day than hoped). https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-39A1.pdf

Look forward to hearing your thoughts after you've had a chance to review.

Thanks,

Matt

Joanne Wall

From: Debbie Matties <DMatties@ctia.org>
Sent: Wednesday, March 23, 2016 10:28 PM
To: Matthew DelNero
Cc: Scott Bergmann
Subject: EU GDPR Question

Hi Matt,

It was nice to see you today. In response to your question, the citation in the EU General Data Protection Regulation is twofold – (1) the Recital at paragraph 38 (a general provision about opt-out or, as they put it, “right to object”), and (2) Article 19 (2), which states:

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object (...) at any time to the processing of personal data concerning him or her for such marketing. At the latest at the time of the first communication with the data subject, this right shall be explicitly brought to the attention of the data subject (...) and shall be presented clearly and separately from any other information.

Hope this is helpful, and let me know if you have any further questions.

Best regards,
Debbie

ctia Everything™
Wireless

Debbie Matties

Vice President, Privacy

1400 16th Street, NW Suite 600

Washington, DC 20036

Direct: 202.736.3654

Wireless: 202.758.7697

dmatties@ctia.org

Joanne Wall

From: Matthew DelNero
Sent: Friday, May 27, 2016 3:07 PM
To: Banks, Jonathan
Subject: RE: Privacy - Wright paper

Thanks, Jon. I'll review and will share with the team. I hope you have a nice weekend.

Matt

From: Banks, Jonathan [mailto:jbanks@ustelecom.org]
Sent: Friday, May 27, 2016 11:47 AM
To: Matthew DelNero <Matthew.DelNero@fcc.gov>
Subject: Privacy - Wright paper

Matt, here is a (relatively) short and readable piece we filed on privacy today. It's worth a look. Jon

Joshua Wright's White Paper Can Be Found Elsewhere in These Responsive Documents to
FOIA 2016-686

Joanne Wall

From: QUINN JR., ROBERT W <rq1982@att.com>
Sent: Wednesday, March 25, 2015 4:53 PM
To: Matthew DelNero; BRUEGGEMAN, JEFF; POLTRONIERI, JEANINE A
Subject: RE: Pre-privacy workshop get together

Matt

I am adding Jeanine who is around next week and will likely attend for us.

Robert W. Quinn Jr.
AT&T Services, Inc
Senior Vice President - Federal Regulatory & Chief Privacy Officer
1120 20th Street NW
Suite 1000
Washington, DC 20036
(202) 457-3851 Voice
(540) 454-7033 Mobile
(832) 213-0243 Fax
rwquinn@att.com

This message and any attachments to it contain **PRIVILEGED AND CONFIDENTIAL ATTORNEY/CLIENT COMMUNICATION AND/OR WORK PRODUCT PREPARED AT THE REQUEST OF COUNSEL IN FURTHERANCE OF OR IN PREPARATION TO LITIGATION** intended exclusively for specific recipients. Please **DO NOT FORWARD OR DISTRIBUTE** to anyone else. If you have received this e-mail in error, please call Victoria Carter Hall at (202) 457-2080 to report the error and then delete this message from your system.

From: Matthew DelNero [mailto:Matthew.DelNero@fcc.gov]
Sent: Wednesday, March 25, 2015 4:43 PM
To: QUINN JR., ROBERT W; BRUEGGEMAN, JEFF
Subject: RE: Pre-privacy workshop get together

Bob, thanks. I'll keep you posted on logistics.

Matt

From: QUINN JR., ROBERT W [mailto:rq1982@att.com]
Sent: Wednesday, March 25, 2015 4:35 PM
To: BRUEGGEMAN, JEFF; Matthew DelNero
Subject: Pre-privacy workshop get together

Robert W. Quinn Jr.

AT&T Services, Inc
Senior Vice President - Federal Regulatory & Chief Privacy Officer
1120 20th Street NW
Suite 1000
Washington, DC 20036
(202) 457-3851 Voice
(540) 454-7033 Mobile
(832) 213-0243 Fax
rwquinn@att.com

This message and any attachments to it contain **PRIVILEGED AND CONFIDENTIAL ATTORNEY/CLIENT COMMUNICATION AND/OR WORK PRODUCT PREPARED AT THE REQUEST OF COUNSEL IN FURTHERANCE OF OR IN PREPARATION TO LITIGATION** intended exclusively for specific recipients. Please **DO NOT FORWARD OR DISTRIBUTE** to anyone else. If you have received this e-mail in error, please call Victoria Carter Hall at (202) 457-2080 to report the error and then delete this message from your system.

Joanne Wall

From: Matthew DelNero
Sent: Wednesday, March 25, 2015 2:45 PM
To: 'tien@eff.org'; 'MarkCooper@aol.com'; 'moy@newamerica.org';
'hfeld@publicknowledge.org'; 'mwood@freepress.net'; 'dderakhshani@consumer.org';
'edm@pirg.org'; 'jeff@democraticmedia.org'; 'sgrant@consumerfed.org';
'estallman@cdt.org'; 'csoghoian@aclu.org'; 'amb420@law.georgetown.edu';
'rotenberg@epic.org'
Cc: Parul Desai; Jennifer Tatel; Lisa Hone
Subject: RE: Privacy meeting at FCC
Attachments: FCC-15-24A1 - excerpt.pdf

Hi All:

We would be happy to setup a conference bridge and will be back in touch on that front.

To provide some further context, this will be an informal gathering to hear your views on the FCC's role concerning the privacy of subscribers of broadband Internet access service. You were included in this invitation because you or the organizations of which you are a part have been active in consumer privacy matters. We're very familiar with the diverse views of parties on consumer privacy generally, but are hoping to foster a discussion on privacy in the context of broadband Internet access service specifically. The purpose of these informal gatherings is to help inform staff as we prepare to support any future Commission activity in this area.

In terms of background reading, you may find paragraphs 462-467 from the *2015 Open Internet Order* to be helpful. I have attached that excerpt.

Best wishes,

Matt

Matthew S. DelNero
Deputy Bureau Chief
Wireline Competition Bureau, FCC

Tel: 202.418.7433
Email: matthew.delnero@fcc.gov

From: Lee Tien [<mailto:tien@eff.org>]
Sent: Wednesday, March 25, 2015 8:37 AM
To: MarkCooper@aol.com
Cc: Parul Desai; moy@newamerica.org; hfeld@publicknowledge.org; mwood@freepress.net;
dderakhshani@consumer.org; edm@pirg.org; jeff@democraticmedia.org; sgrant@consumerfed.org; estallman@cdt.org;
csoghoian@aclu.org; amb420@law.georgetown.edu; rotenberg@epic.org
Subject: Re: Privacy meeting at FCC

My team isn't in DC, so a phone line would be good.

I echo Mark's request for any working conception you might have of translating CPNI into the broadband realm.

Lee

Sent from my iPhone

On Mar 25, 2015, at 7:25 AM, MarkCooper@aol.com wrote:

I can make it. Do you have some links to current Commission policy and practice under section 222?

In a message dated 3/24/2015 7:58:17 P.M. Mid-Atlantic Standard Time, Parul.Desai@fcc.gov writes:

Hi all,

In light of the Open Internet Order and the Commission's determination that Section 222 is necessary to protect consumers, we'd like to invite you come in to discuss privacy concerns and explore the application of the statutory privacy protections to broadband Internet access service.

Also attending from the FCC will be folks from the Wireline and Enforcement Bureaus, and the General Counsel's office.

Please let me know if you can make it on March 31 at 3 PM.

Thanks!

Sincerely,
Parul

Parul P. Desai
Assistant Bureau Chief and
Director of Consumer Engagement
Consumer and Governmental Affairs Bureau
202-418-8217

1. Provisions that Protect Customer Privacy, Advance Access For Persons with Disabilities, and Foster Network Deployment

461. We generally grant extensive forbearance from the provisions and requirements that newly apply by virtue of our classification of broadband Internet access service. However, the record persuades us that we should not forbear with respect to certain key provisions that protect customer privacy, advance access for persons with disabilities, and foster network deployment.

a. Customer Privacy (Section 222)

462. As supported by a number of commenters, we decline to forbear from applying section 222 of the Act in the case of broadband Internet access service.¹³⁷⁹ We do, however, find the section 10(a) criteria met to forbear at this time from applying our implementing rules, pending the adoption of rules to govern broadband Internet access service in a separate rulemaking proceeding. Section 222 of the Act governs telecommunications carriers' protection and use of information obtained from their customers or other carriers, and calibrates the protection of such information based on its sensitivity. Congress provided protections for proprietary information, according the category of customer proprietary network information (CPNI)¹³⁸⁰ the greatest level of protection. Section 222 imposes a duty on every telecommunications carrier to protect the confidentiality of its customers' private information.¹³⁸¹ Section 222 also imposes restrictions on carriers' ability to use, disclose, or permit access to customers' CPNI without their consent.¹³⁸²

¹³⁷⁹ See, e.g., CDT Comments at 16; NMR Comments at 25; Rural Broadband Policy Group Comments at 8-9; Public Knowledge Dec. 19, 2014 *Ex Parte* Letter at 19; Free Press Nov. 21, 2014 *Ex Parte* Letter at 1; Full Service Network/TruConnect Feb. 3, 2015 *Ex Parte* Letter at 21.

¹³⁸⁰ CPNI 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." 47 U.S.C. § 222(h)(1).

¹³⁸¹ 47 U.S.C. § 222(a); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6959, para. 64 (2007); Declaratory Ruling, 28 FCC Rcd 9609 (2013). We take this mandate seriously. For example, the Commission recently took enforcement action under section 222 (and section 201(b)) against two telecommunications companies that stored customers' personal information, including social security numbers, on unprotected, unencrypted Internet servers publicly accessible using a basic Internet search. This unacceptably exposed these consumers to the risk of identity theft and other harms. See *TerraCom, Inc. and YourTel America, Inc. Apparent Liability for Forfeiture*, File No.: EB-TCD-13-00009175, Notice of Apparent Liability, FCC 14-173, paras. 31-41 (rel. Oct. 24, 2014). See also, e.g., Letter from Erik Stallman, Director, Open Internet Project, CDT, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 14-28 at 3-4 (filed Feb. 4, 2015) (CDT Feb. 4, 2015 *Ex Parte* Letter).

¹³⁸² See 47 U.S.C. § 222(c)(1) (permitting a carrier, except as required by law or with the customer's consent, to use, disclose, or permit access to individually identifiable CPNI only "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."). The Commission has made clear that "to the extent a telecommunications carrier that is a provider of electronic communication services or remote computing services is compelled by 18 U.S.C. § 2258A to disclose CPNI in a report to the CyberTipline, that carrier would not be in violation of its privacy duties under section 222 of the Communications Act." *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use Of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Declaratory Ruling, 25 FCC Rcd 14335, 14336-37, para. 5 (Wireline Comp. Bur. 2010). See also *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Declaratory Ruling, 21 FCC Rcd 9990 (2006) (addressing the predecessor disclosure provision). That interpretation of section 222 remains true as to broadband Internet access service.

463. We find that forbearance from the application of section 222 with respect to broadband Internet access service is not in the public interest under section 10(a)(3), and that section 222 remains necessary for the protection of consumers under section 10(a)(2).¹³⁸³ The Commission has long supported protecting the privacy of users of advanced services, and retaining this provision thus is consistent with the general policy approach.¹³⁸⁴ The Commission has emphasized that “[c]onsumers’ privacy needs are no less important when consumers communicate over and use broadband Internet access than when they rely on [telephone] services.”¹³⁸⁵ As broadband Internet access service users access and distribute information online, the information is sent through their broadband provider. Broadband providers serve as a necessary conduit for information passing between an Internet user and Internet sites or other Internet users, and are in a position to obtain vast amounts of personal and proprietary information about their customers.¹³⁸⁶ Absent appropriate privacy protections, use or disclosure of that information could be at odds with those customers’ interests.

464. We find that if consumers have concerns about the privacy of their personal information, such concerns may restrain them from making full use of broadband Internet access services and the Internet, thereby lowering the likelihood of broadband adoption and decreasing consumer demand.¹³⁸⁷ As the Commission has found previously, the protection of customers’ personal information may spur consumer demand for those services, in turn “driving demand for broadband connections, and consequently encouraging more broadband investment and deployment” consistent with the goals of the 1996 Act.¹³⁸⁸ Notably, commenters opposing the application of section 222 to broadband Internet access service make general arguments about the associated burdens, but do not include a meaningful analysis of why the section 10(a) criteria are met (or why relief otherwise should be granted) nor why the concerns they identify—even assuming *arguendo* that they were borne out by evidence beyond that currently in the record—should outweigh the privacy concerns identified here.¹³⁸⁹ We therefore conclude that the

¹³⁸³ 47 U.S.C. § 160(a)(2), (3).

¹³⁸⁴ For example, the Commission has noted that “long before Congress enacted section 222 of the Act, the Commission had recognized the need for privacy requirements associated with the provision of enhanced services and had adopted CPNI-related requirements in conjunction with other *Computer Inquiry* obligations.” *Wireline Broadband Classification Order*, 20 FCC Rcd at 14931, para. 149 & n.447 (seeking comment on privacy protections).

¹³⁸⁵ *Id.* at 14930, para. 148 (“For example, a consumer may have questions about whether a broadband Internet access service provider will treat his or her account and usage information as confidential, or whether the provider reserves the right to use account information for marketing and other purposes.”).

¹³⁸⁶ *See, e.g.*, Access Comments at 7 (stating that broadband providers have the technological capacity to exercise monitoring and control of their customers’ use of the Internet using techniques such as deep packet inspection).

¹³⁸⁷ *See, e.g.*, 2015 *Broadband Progress Report*, paras. 104-05; National Broadband Plan at 17 (citing John Horrigan, *Broadband Adoption and Use in America* (OBI, Working Paper No. 1, 2010)). *See also, e.g.*, Pew Research Center, *Who’s not online and why*, at 6 (Sept. 2013), http://www.pewinternet.org/files/old-media/Files/Reports/2013/PIP_Offline%20adults_092513_PDF.pdf.

¹³⁸⁸ *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, CC Docket No. 96-115, WC Docket No. 04-36, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6957, para. 59 (2007); *see also* National Broadband Plan at 55 (explaining that without privacy protections, new innovation and investment in broadband applications and content may be held back, and these applications and content, in turn, are likely the most effective means to advance many of Congress’s goals for broadband).

¹³⁸⁹ *See, e.g.*, MediaFreedom Comments at 2; TIA Comments at 17; ADTRAN Reply at 17-18; Letter from Robert W. Quinn, Jr., Senior Vice President, Federal Regulatory and Chief Privacy Officer, AT&T, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 14-28 at 5 (filed May 9, 2014). Consequently, we reject those arguments.

application and enforcement of section 222 to broadband Internet access services is in the public interest, and necessary for the protection of consumers.¹³⁹⁰

465. We also reject arguments that section 706 itself provides adequate protections such that forbearance from section 222 is warranted.¹³⁹¹ While section 706 of the 1996 Act would continue to apply even if we granted forbearance here, we find that section 222 provides a more certain foundation for evaluating providers' conduct and pursuing enforcement if warranted in relevant circumstances arising in the future.¹³⁹² Among other things, while the concerns discussed in the preceding paragraph have a nexus with the standards of sections 706(a) and (b), as discussed earlier in this section, the public interest in protecting customer privacy is not limited to the universe of concerns encompassed by section 706.

466. We recognize that some commenters, while expressing concern about consumer privacy, nonetheless suggest that the Commission conceivably need not immediately apply section 222 and its implementing rules, pending further proceedings.¹³⁹³ We are persuaded by those arguments, but only as to the Commission's rules. With respect to the application of section 222 of the Act itself, as discussed above, with respect to broadband Internet access service the record here persuades us that the section 10(a) forbearance criteria are not met to justify such relief. Indeed, even as to services that historically have been subject to section 222, questions about the application of those privacy requirements can arise and must be dealt with by the Commission as technology evolves,¹³⁹⁴ and the record here does not

¹³⁹⁰ See 47 U.S.C. § 160(a)(2); see also, e.g., Free Press Comments at 83, n.180; Public Knowledge Reply at 20-22. Some commenters contend that the Commission should forbear from all of Title II based on generalized arguments about the marketplace, such as past network investment or changes in performance or price per megabit in the recent past. See, e.g., ACA Jan. 12, 2015 *Ex Parte* Letter at 10-11; Comcast Dec. 24, 2014 *Ex Parte* Letter at 4-6; NCTA Dec. 23, 2014 *Ex Parte* Letter at 19-20. We are not persuaded that those arguments justify a different outcome here, both for the reasons discussed previously, see *supra* Section V.B.1, and because commenters do not meaningfully explain how these arguments impact the section 10 analysis here, given that the need to protect consumer privacy is not self-evidently linked to such marketplace considerations. Nothing in the record suggests that concerns about consumer privacy are limited to broadband providers of a particular size, and we thus are not persuaded that a different conclusion in our forbearance analysis should be reached in the case of small broadband providers, for example. See, e.g., ACA Jan. 12, 2015 *Ex Parte* Letter at 11; AireBeam Jan. 30, 2015 *Ex Parte* Letter at 2.

¹³⁹¹ See, e.g., ACA Jan. 12, 2015 *Ex Parte* Letter at 11; NCTA Jan. 14, 2015 *Ex Parte* Letter at 3-4.

¹³⁹² See, e.g., *supra* Section III.F.4. We also note, for example, that this approach obviates the need to determine whether or to what extent section 222 is more specific than section 706 of the 1996 Act in relevant respects, and thus could be seen as exclusively governing over the provisions of section 706 of the 1996 Act as to some set of privacy issues. Cf. *Bloate v. U.S.*, 559 U.S. 196, 208 (2010) (“[g]eneral language of a statutory provision, although broad enough to include it, will not be held to apply to a matter specifically dealt with in another part of the same enactment”) (citation omitted). The approach we take avoids this potential uncertainty, and we thus need not and do not address this question.

¹³⁹³ See, e.g., CDT Comments at 16; Letter from Marvin Ammori and Julie Samuels, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 14-28, at 2 (filed Nov. 12, 2014); Letter from COMPTTEL, CCIA, Engine, and IFBA, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 14-28, at 1-2 n.1 (filed Dec. 30, 2014). While CDT references the questions regarding the application of section 222 and our implementing rules raised in the *2010 Broadband Classification NOI*, CDT Comments at 16 (citing *2010 Broadband Classification NOI*, 25 FCC Rcd at 7900-01, para. 82), that *NOI* cited reasons why the Commission might immediately apply section 222 and the Commission's implementing rules if it reclassified broadband Internet access service as well as reasons why it might defer the application of those requirements. We thus find that the *2010 NOI* does not itself counsel one way or the other, and in light of the record here, we decline to defer the application of section 222 and our implementing rules.

¹³⁹⁴ See, e.g., *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Declaratory Ruling, 28 FCC Rcd 9609 (2013) (*Wireless Device Privacy Declaratory Ruling*) (“address[ing] the real privacy and security risks that consumers face when telecommunications carriers use their control of customers' mobile devices to collect information about their customers' use of the network”). We also note in this regard that the Commission

(continued....)

demonstrate specific concerns suggesting that Commission clarification of statutory terms as needed would be inadequate in this context.¹³⁹⁵

467. We are, however, persuaded that the section 10(a) criteria are met for us to grant forbearance from applying our rules implementing section 222 insofar as they would be triggered by the classification of broadband Internet access service here. Beyond the core broadband Internet access service requirements, we apply section 222 of the Act, which itself directly provides important privacy protections.¹³⁹⁶ Further, on this record, we are not persuaded that the Commission's current rules implementing section 222 necessarily would be well suited to broadband Internet access service. The Commission fundamentally modified these rules in various ways subsequent to decisions classifying broadband Internet access service as an information service, and certain of those rules appear more focused on concerns that have been associated with voice service.¹³⁹⁷ For example, the current rules have requirements with respect to "call detail information," defined as "[a]ny information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call."¹³⁹⁸ More generally, the existing CPNI rules do not address many of the types of sensitive information to which a provider of broadband Internet access service is likely to have access, such as (to cite just one example) customers' web browsing history. Insofar as rules focused on addressing problems in the voice service context are among the central underpinnings of our CPNI rules, we find the better course to be forbearance from applying all of our CPNI rules at this time. As courts have recognized, when exercising its section 10 forbearance authority "[g]uided by section 706," the Commission permissibly may "decide[] to balance the future benefits" of encouraging broadband deployment "against [the] short term impact" from a grant of forbearance.¹³⁹⁹ In light of the record here and given that the core broadband Internet access requirements and section 222 itself will apply, and guided by section 706, we find that applying our current rules implementing sections 222—which, in critical respects, appear to be focused on addressing problems that historically arise regarding voice service—is not necessary to ensure just and reasonable rates and practice or for the protection of consumers under sections 10(a)(1) and (a)(2) and that forbearance is in the public interest under section

(Continued from previous page) _____
cannot impose a penalty in the absence of "fair notice of what is prohibited." *FCC v. Fox Television Stations*, 132 S. Ct. 2307, 2317 (2012).

¹³⁹⁵ See, e.g., CDT Comments at 17 (asserting, without explanation, that a rulemaking might be needed to "address exactly how Section 222 should apply in the Internet connectivity context, including how to define 'customer proprietary network information' (CPNI) for this purpose"); Verizon Jan. 26, 2015 *Ex Parte* Letter at 7-8 (arguing that it is unclear what certain requirements of section 222 would mean in the context of broadband Internet access service).

¹³⁹⁶ See, e.g., *TerraCom, Inc. and YourTel America, Inc. Apparent Liability for Forfeiture*, File No.: EB-TCD-13-00009175, Notice of Apparent Liability, FCC 14-173, paras. 31-41 (rel. Oct. 24, 2014); *Wireless Device Privacy Declaratory Ruling*, 28 FCC Rcd at 9619-20, paras. 29-32 (discussing statutory restrictions applicable to CPNI).

¹³⁹⁷ The Commission adopted significant reforms to its rules implementing section 222 in 2007. *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, CC Docket No. 96-115, WC Docket No. 04-36, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007). In doing so, the Commission was, in significant part, focused on dealing with problems of "pretexting," which involved "data brokers . . . obtain[ing] private and personal information, including what calls were made to and/or from a particular telephone number and the duration of such calls." *Id.* at 6928-29, para. 2; see also *id.* at 6928, para. 1 n.1 (noting Congress' criminalization of pretexting activity in 18 U.S.C. § 1039, which focuses on "phone" records).

¹³⁹⁸ 47 C.F.R. §§ 64.2003, 64.2010.

¹³⁹⁹ *EarthLink*, 462 F.3d at 9.

10(a)(3).¹⁴⁰⁰ We emphasize, however, that forbearance from our existing CPNI rules in the context of broadband Internet access services does not in any way diminish the applicability of these rules to services previously found to be within their scope.¹⁴⁰¹

b. Disability Access Provisions (Sections 225, 255, 251(a)(2))

468. We agree with commenters that we should apply section 225 and the Commission's implementing rules—rather than forbear for broadband Internet access service—because of the need to ensure meaningful access to all Americans,¹⁴⁰² except to the extent provided below with respect to contributions to the Interstate TRS Fund. Section 225 mandates the availability of interstate and intrastate TRS to the extent possible and in the most efficient manner to individuals in the United States who are deaf, hard of hearing, deaf-blind, and who have speech disabilities.¹⁴⁰³ The Act directs that TRS provide the ability for such individuals to engage in communication with other individuals, in a manner that is “functionally equivalent to the ability of a hearing individual who does not have a speech disability to communicate using voice communication services.”¹⁴⁰⁴ To achieve this, the Commission has required all interstate service providers (other than one-way paging services) to provide TRS.¹⁴⁰⁵ People who are blind, hard of hearing, deaf-blind, and who have speech disabilities increasingly rely upon Internet-based video communications, both to communicate directly (point-to-point) with other persons who are deaf or hard of hearing who use sign language and through video relay service (VRS)¹⁴⁰⁶ with individuals who do not use the same mode of communication that they do.¹⁴⁰⁷ In doing so, they rely on high definition two-

¹⁴⁰⁰ Our decision to proceed in a tailored manner is discussed in greater detail below. *See infra* paras. 495-496; Section V.C.2.a.

¹⁴⁰¹ *See, e.g., Wireless Device Privacy Declaratory Ruling*, 28 FCC Rcd 9609 (addressing how section 222 of the Act, and the Commission's implementing rules, apply to information relating to telecommunications service and interconnected VoIP service that fits the statutory definition of CPNI when such information is collected by the customer's device, provided the collection is undertaken at the mobile wireless carrier's direction and the carrier or its designee has access to or control over the information).

¹⁴⁰² *See, e.g., Public Knowledge Comments* at 95; *Rural Broadband Policy Group Comments* at 8; *Telecommunications for the Deaf and Hard of Hearing Comments* at 8-13.

¹⁴⁰³ 47 U.S.C. §§ 225(a)(3), (b)(1) .

¹⁴⁰⁴ 47 U.S.C. § 225(a)(3).

¹⁴⁰⁵ *See generally Telecommunications Relay Services, and the Americans with Disabilities Act of 1990*, CC Docket No. 90-571, Notice of Proposed Rule Making, 5 FCC Rcd 7187 (1990); Report and Order and Request for Comment, 6 FCC Rcd 4657, 4660, para. 17 (1991) (*TRS Order*); Order on Reconsideration, Second Report and Order and Further Notice of Proposed Rule Making, 8 FCC Rcd 1802 (1993) (*TRS II*); Third Report and Order, 8 FCC Rcd 5300 (1993) (*TRS III*).

¹⁴⁰⁶ VRS is a form of TRS that allows people who are blind, hard of hearing, deaf-blind, and who have speech disabilities who use sign language to communicate with voice telephone users through a CA using video transmissions over the Internet. *See* 47 C.F.R. § 64.601(a)(40).

¹⁴⁰⁷ *See generally Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities; E911 Requirements for IP-Enabled Service Providers*, CG Docket No. 03-123, WC Docket No. 05-196, Report and Order and Further Notice of Proposed Rulemaking, 23 FCC Rcd 11591 (2008) (*First Internet-Based TRS Order*); Second Report and Order on Reconsideration, 24 FCC Rcd 791 (2008) (*Second Internet-Based TRS Order*). In addition, these populations rely on other forms of Internet-based TRS (iTRS), including Internet Protocol Relay Service (IP Relay) and Internet Protocol Captioned Telephone Service (IP CTS). IP Relay is a “telecommunications relay service that permits an individual with a hearing or a speech disability to communicate in text using an Internet Protocol-enabled device via the Internet, rather than using a text telephone (TTY) and the public switched telephone network.” 47 C.F.R. § 64.601(a)(17). IP CTS is a “telecommunications relay service that permits an individual who can speak but who has difficulty hearing over the telephone to use a telephone and an Internet Protocol-enabled device via the Internet to simultaneously listen to the other party and read captions of what the other party is saying.” 47 C.F.R. § 64.601(a)(16).

Joanne Wall

From: Scott Bergmann <SBergmann@ctia.org>
Sent: Wednesday, April 01, 2015 4:55 PM
To: Matthew DelNero
Cc: Claude Aiken
Subject: RE: Thursday meeting

Thanks very much, Matt. Attending for CTIA will be Debbie Matties, VP for Privacy and me.

Do you have a sense of who else will attend the meeting from industry (groups)? Thanks!

Scott

From: Matthew DelNero [mailto:Matthew.DelNero@fcc.gov]
Sent: Tuesday, March 31, 2015 7:05 PM
To: Scott Bergmann
Cc: Claude Aiken
Subject: RE: Thursday meeting

Scott, it was good to see you last night. Just to confirm, we'll be meeting on Thursday at 3 pm for an informal conversation on privacy. The meeting will be held on the 5th floor. Please ask for Claude Aiken or me when you (or whomever is representing CTIA) arrive. Thanks.

Matt

From: Matthew DelNero
Sent: Monday, March 30, 2015 2:31 PM
To: 'Scott Bergmann'
Subject: Thursday meeting

Hi Scott,

Good to speak with you on Friday. I'm just checking in to see if you had any thoughts about who from CTIA could attend an informal meeting on privacy here at the Commission on Thursday @ 3pm. As I mentioned, VZ and AT&T will be there as well. And we'd certainly be happy to have Sprint and/or T-Mo as well if they're interested.

Thanks,
Matt

Joanne Wall

From: Matthew DelNero
Sent: Monday, October 05, 2015 10:42 AM
To: Lisa Hone
Subject: FW: Message from pending (912025152543)
Attachments: VoiceMessage.wav

FYI – VZ is updating its privacy policy, and Maggie has offered to brief us.

From: unityconnection
Sent: Monday, October 05, 2015 9:55 AM
To: Matthew DelNero
Subject: Message from pending (912025152543)

Joanne Wall

From: Daniel Kahn
Sent: Tuesday, June 14, 2016 5:53 PM
To: Lisa Hone
Subject: Accepted: Privacy meeting with AT&T

Joanne Wall

From: Debbie Matties <DMatties@ctia.org>
Sent: Friday, November 20, 2015 11:26 AM
To: Lisa Hone
Subject: Afternoon coffee monday?

assuming lunchtime is still unavailable.... I'm free after 3pm

Sent from my iPhone

Joanne Wall

From: Rosenthal, Michelle <Michelle.Rosenthal1@T-Mobile.com>
Sent: Wednesday, November 18, 2015 12:01 PM
To: Lisa Hone
Subject: Checking in

Hi Lisa – Hope all is well. Any chance you are free today for a quick call?

Michelle Rosenthal
Senior Corporate Counsel
Federal Regulatory Affairs
T-Mobile US, Inc.
Office: 202.654-5939
Mobile: 202.607.3435
Fax: 202.654.5963

Joanne Wall

From: Lisa Hone
Sent: Sunday, November 22, 2015 7:02 PM
To: Debbie Matties (DMatties@ctia.org)
Subject: Dec. 16th

Can we do our meeting Dec. 16th at 3pm?

Thanks,

Lisa

Joanne Wall

Subject: FW: BB Privacy w/ Verizon
Location: Conference Room 1
Start: Thu 3/17/2016 1:00 PM
End: Thu 3/17/2016 1:30 PM
Show Time As: Tentative
Recurrence: (none)
Meeting Status: Not yet responded
Organizer: Sherry Wood

Matt, Lisa, and Jennifer – attendance optional.

-----Original Appointment-----

From: Sherry Wood
Sent: Sunday, March 13, 2016 9:40 PM
To: Sherry Wood; Gigi Sohn; Stephanie Weiner; Louisa Terrell
Subject: BB Privacy w/ Verizon
When: Thursday, March 17, 2016 1:00 PM-1:30 PM (UTC-05:00) Eastern Time (US & Canada).
Where: Conference Room 1

Broadband Privacy

Attendees:

Maggie McCready
Cathy Hilke

Joanne Wall

From: Lisa Hone
Sent: Thursday, March 10, 2016 4:36 PM
To: Jennifer Tatel
Subject: Re: Call

Ok

From: Jennifer Tatel
Sent: Thursday, March 10, 2016 4:06 PM
To: Lisa Hone
Subject: FW: Call

She and I have been playing phone tag, so in my latest message to her, I said that she could call you if she couldn't reach me. I have a Hill call at 4:15.

From: Debbie Matties [mailto:DMatties@ctia.org]
Sent: Thursday, March 10, 2016 3:11 PM
To: Jennifer Tatel
Subject: Call

Hi Jennifer,

Thanks so much for the call. Would you be available to talk later, after 4pm? Or tomorrow before 10 or after about 2:30?

Best,
Debbie

ctia Everything™
***** Wireless

Debbie Matties

Vice President, Privacy
1400 16th Street, NW Suite 600
Washington, DC 20036
Direct: 202.736.3654
Wireless: 202.758.7697
dmatties@ctia.org

Joanne Wall

From: Lisa Hone
Sent: Sunday, December 13, 2015 10:34 PM
To: Matthew DelNero; Jennifer Tatel; Melissa Droller Kinkel
Subject: FW: Dec. 16 meeting

Wow.

I have asked Debbie to add company/organization identifiers.

Off the top of my head, I am only absolutely sure about 8 of them- though, I might succeed with educated guesses re: another bunch.

Lisa

From: Debbie Matties [mailto:DMatties@ctia.org]
Sent: Sunday, December 13, 2015 10:20 AM
To: Lisa Hone
Cc: Latoya Toles
Subject: RE: Dec. 16 meeting

Hi Lisa and LaToya,

Here's our list. I think probably 10 of the people below have pre-issued visitor badges. And yes, we're a smidge over 16. Sorry.

1. Debbie Matties
2. Scott Bergmann
3. Loretta Polk
4. Jennifer McKee
5. Lynn Follansbee
6. Courtney Neville
7. Maureen Cooney
8. Matthew Sullivan
9. Maggie McCready
10. Cathy Hilke
11. Jonathan Zimmerman
12. Jeff Brueggeman
13. Jackie Fleming
14. Michelle Rosenthal
15. Rudy Brioche
16. Mary McManus
17. Frank Buono
18. Ross Lieberman (maybe)

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Saturday, December 5, 2015 9:23 AM
To: Debbie Matties <DMatties@ctia.org>
Cc: Latoya Toles <Latoya.Toles@fcc.gov>
Subject: Re: Dec. 16 meeting

Debbie - bringing in 16 people should be fine.

I am copying LaToya Toles, Matt DelNero's assistant, so she can coordinate with Security about getting so many people in the building for one meeting.

It might be helpful for her to know how many people in your group have pre-issued visitors badges.

From the FCC, I expect:

Matt DelNero, WCB Bureau Chief

Lisa Hone, WCB Associate Chief

Melissa Kirkel, Assistant Division Chief, Competition Policy Division, WCB

Jennifer Tatel, Associate General Counsel

Scott Jordan, FCC Chief Technologist

And one or two attorneys from CPD

From: Debbie Matties

Sent: Friday, December 4, 2015 11:34 AM

To: Lisa Hone

Subject: Dec. 16 meeting

Hi Lisa – great panel this morning! Sorry I didn't say goodbye, but you were wrapped up in conversation with someone I didn't know and I didn't want to interrupt.

We're putting together our group to meet with you on the 16th and it's getting quite large. Will you be able to reserve a really big room? I think we could have as many as 16 people.

And do you know who from the FCC will be attending? Many folks are curious.

Thanks!

Debbie

Joanne Wall

From: Matthew DelNero
Sent: Wednesday, April 01, 2015 7:24 PM
To: Jennifer Tatel; Lisa Hone; Parul Desai
Subject: FW: Thursday meeting

fyi

From: Scott Bergmann [mailto:SBergmann@ctia.org]
Sent: Wednesday, April 01, 2015 4:55 PM
To: Matthew DelNero
Cc: Claude Aiken
Subject: RE: Thursday meeting

Thanks very much, Matt. Attending for CTIA will be Debbie Matties, VP for Privacy and me.

Do you have a sense of who else will attend the meeting from industry (groups)? Thanks!

Scott

From: Matthew DelNero [mailto:Matthew.DelNero@fcc.gov]
Sent: Tuesday, March 31, 2015 7:05 PM
To: Scott Bergmann
Cc: Claude Aiken
Subject: RE: Thursday meeting

Scott, it was good to see you last night. Just to confirm, we'll be meeting on Thursday at 3 pm for an informal conversation on privacy. The meeting will be held on the 5th floor. Please ask for Claude Aiken or me when you (or whomever is representing CTIA) arrive. Thanks.

Matt

From: Matthew DelNero
Sent: Monday, March 30, 2015 2:31 PM
To: 'Scott Bergmann'
Subject: Thursday meeting

Hi Scott,

Good to speak with you on Friday. I'm just checking in to see if you had any thoughts about who from CTIA could attend an informal meeting on privacy here at the Commission on Thursday @ 3pm. As I mentioned, VZ and AT&T will be there as well. And we'd certainly be happy to have Sprint and/or T-Mo as well if they're interested.

Thanks,
Matt

Joanne Wall

From: Lisa Hone
Sent: Thursday, February 11, 2016 8:38 AM
To: CPD Privacy Team
Cc: Daniel Kahn; Michael Jacobs
Subject: Fw: Trade association letter on broadband privacy
Attachments: Privacy Letter Final 523pm.pdf

Fyi.

From: Debbie Matties
Sent: Thursday, February 11, 2016 8:14 AM
To: Matthew DelNero; Lisa Hone; Jennifer Tatel
Subject: Trade association letter on broadband privacy

Dear Matt, Lisa and Jennifer,

I hope you're all well this morning. As I spoke to Jennifer and Lisa about yesterday, this morning CTIA and other tech trade associations sent the attached letter to FCC Chairman Wheeler concerning the upcoming broadband privacy proceeding at the FCC.

Best,

Debbie

ctia Everything™
***** Wireless

Debbie Matties

Vice President, Privacy
1400 16th Street, NW Suite 600
Washington, DC 20036
Direct: 202.736.3654
Wireless: 202.758.7697
dmatties@ctia.org



February 11, 2016

The Honorable Tom Wheeler
Chairman
Federal Communications Commission
445 12th St. SW
Washington, D.C. 20554

Dear Chairman Wheeler,

As associations representing a large cross-section of the technology companies that make up today's vibrant Internet economy, our collective members are committed to providing consumers with innovative products and services and are equally committed to earning consumer trust and respecting privacy. If the courts determine that the FCC has authority to regulate broadband privacy, we encourage you to develop a framework that offers consumers robust privacy protection, while at the same time allowing broadband providers to continue to innovate and compete. We recommend that any FCC framework be consistent with the successful FTC approach, which is grounded on prohibiting unfairness and deception. The FTC's time-tested framework has accomplished two important goals—it provides consumers with meaningful privacy protection and helps to enable a dynamic marketplace that supports the emergence of innovative new business models. By developing a consistent framework, the FCC will further these important goals.

Our member companies recognize that ensuring robust privacy protection is important and have devoted substantial capital, resources and personnel to develop, maintain, and enhance meaningful data privacy and security programs. Indeed, our companies have strong incentives to earn and maintain their customers' loyalty by protecting their data. In the rapidly evolving online marketplace, our companies want to ensure that they can continue to provide such protections while meeting consumers' expectation of continued access to new innovations that enhance their experience.

All companies in the Internet ecosystem, including Internet service providers, have long operated under the FTC regulatory regime for protecting consumer privacy. The aim of this well-tested approach is to combine strong protections for consumers with flexibility that allows for rapid innovation. Under the FTC regime, all companies in the Internet ecosystem must ensure that

their privacy and data security practices are neither deceptive nor unfair. As a result, consumers are protected and all companies that collect consumer data should be able to innovate and adapt to the inevitable changes in technology and the market for online services.

We understand the FCC is considering initiating a proceeding to consider how Section 222 of the Communications Act, which governs Customer Proprietary Network Information (“CPNI”), should apply to broadband Internet access service. The applicability of Section 222 in this context is currently subject to judicial review. If the Commission nonetheless moves forward in this space, consumers would be best served by an approach to privacy and data security for CPNI that is harmonized with the FTC’s established privacy protection framework based on enforcement against unfair and deceptive acts or practices.

You have recognized that the FTC has a longstanding, thoughtful, and rational approach to privacy, and you have committed to working closely with the FTC and to developing a consistent privacy framework for Internet service providers. Ensuring consistency with this effective consumer protection approach would be in accordance with statements supporting the FTC’s privacy regime and endorsing the benefits of a consistent privacy framework for the Internet in the 2010 National Broadband Plan, the FTC’s and White House’s 2012 Privacy Reports, and the White House’s 2015 Consumer Privacy Bill of Rights.

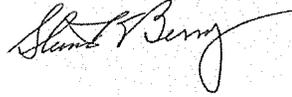
We believe it is important to maintain a consistent privacy framework for the Internet. Such an approach will protect consumers and avoid entity-based regulation that would create consumer confusion and stifle innovation. Consumers expect their data will be subject to consistent privacy standards based upon the sensitivity of the information and how it is used regardless of which entity in the Internet ecosystem uses that data. To achieve parity across the Internet ecosystem, any FCC framework for Internet service providers should be reflective of the deception and unfairness standard, consistent with the existing protections consumers receive when they engage with other companies in the Internet ecosystem.

A consistent privacy framework for the Internet also will continue to provide Internet service providers with the flexibility to update their practices in ways that meet the evolving privacy and data security needs of their customers and ensure they can provide their customers new products and customized services. Such a framework would identify privacy or security goals, and afford providers, including smaller providers with limited resources, flexibility in achieving those goals. Rules dictating specific methods quickly become out of date and out of step with constantly changing technology, and will only hamper innovation and harm consumers.

In short, if you seek to initiate a proceeding under Section 222, we respectfully urge you to ensure that the FCC acts in a manner consistent with the strong current national privacy framework applied by the FTC to other companies in the Internet ecosystem. This flexible approach would meet consumers’ privacy needs while allowing them to take advantage of innovative products and services, and would avoid inconsistent oversight. We look forward to continuing a conversation with the FCC about the best way to provide privacy and innovation benefits to consumers.



Matthew M. Polka
President & CEO
American Cable Association



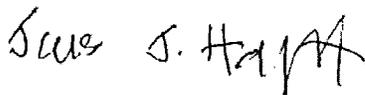
Steven K. Berry
President & CEO
Competitive Carriers Association



Gary Shapiro
President & CEO
Consumer Technology Association



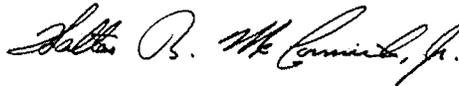
Meredith Attwell Baker
President & CEO
CTIA



Jim Halpert
President & CEO
Internet Commerce Coalition



Michael Powell
President & CEO
National Cable & Telecommunications Association



Walter B. McCormick, Jr.
President & CEO
U.S. Telecom Association

cc: The Honorable Mignon Clyburn
The Honorable Jessica Rosenworcel
The Honorable Ajit Pai
The Honorable Michael O'Rielly

Joanne Wall

From: Lisa Hone
Sent: Thursday, February 25, 2016 2:21 PM
To: CPD Privacy Team; Daniel Kahn
Subject: Fw: Updated Privacy Framework from the telecom trades
Attachments: BB Privacy Framework 2.19.16.pdf

Fyi

From: Debbie Matties
Sent: Thursday, February 25, 2016 2:09 PM
To: Lisa Hone
Subject: Updated Privacy Framework from the telecom trades

Hi Lisa,

Maggie mentioned to you that we had made a few revisions to the Privacy Framework that we had given you back in December. I've attached the new version here, dated February 19.

We made two substantive changes on the last page. First, at the top, we added "The provider should consider the sensitivity of the data and the context in which it was collected when determining the appropriate choice mechanism." Second we reworked the data breach bullet. We also made a few stylistic edits on the earlier pages in anticipation of releasing it publicly.

Please let me know if you have any questions.

Best,

Debbie

ctia Everything™
***** Wireless

Debbie Matties

Vice President, Privacy
1400 16th Street, NW Suite 600
Washington, DC 20036
Direct: 202.736.3654
Wireless: 202.758.7697
dmatties@ctia.org

Privacy Framework

Draft Discussion Paper

All entities in the Internet ecosystem should be subject to a consistent privacy framework with respect to consumer information. Consumer information should be protected based upon the sensitivity of the information to the consumer and how the information is used—not the type of business keeping it, how that business obtains it, or what regulatory agency has authority over it. Consumers should have consistent and predictable privacy protections for the information they deem private and sensitive, no matter how or with whom they share it. Consumers also will benefit from a consistent privacy framework that promotes the emergence of new business models and innovative uses of data that foster increased consumer choice and service customization.

The FCC should adopt an approach to privacy and data security for CPNI that is flexible, harmonized with the well-established and successful FTC framework, and backed up by strong but fair enforcement for unfair or deceptive acts or practices (UDAP) that materially harm consumers.¹ This well-tested consumer protection approach is consistent with the FCC's privacy recommendations in the 2010 National Broadband Plan, the FTC's and White House's 2012 Privacy Reports, and the White House's 2015 Consumer Privacy Bill of Rights, as well as with Chairman Wheeler's recent testimony before Congress acknowledging the importance of coordination with the FTC and harmonization with its privacy framework.

That approach will benefit consumers by safeguarding privacy interests as it has for years and will ensure that the same privacy and security framework applies to all entities in the Internet ecosystem. By leveraging a tested privacy model, the FCC will avoid arbitrarily inconsistent requirements that could otherwise hamper innovation and reduce competition. Most important, it will minimize consumer confusion as well as other harms associated with disparate privacy regulation across the ecosystem. Indeed, this approach will align with consumers' expectations that their data would be subject to consistent privacy rules regardless of whether it is used by their Internet Service Provider (ISP), application developers, operating systems, or edge providers.

When adopting a framework, the FCC should keep the following guidelines in mind:

- **Consistent and Coordinated Regulatory Regimes.** The FCC's rules and principles for regulating and enforcing privacy and security should be as similar as possible to the FTC approach, which will continue to govern other Internet ecosystem players' use and disclosure of the same or similar data. The consistent application of standards across

¹ This framework is intended for discussion purposes, and we are not conceding that the FCC has authority to adopt privacy and security rules for Broadband Internet Access Services or over data related to consumers' use of Broadband Internet Access Services. To the extent it is determined that the FCC has such statutory authority, this document is intended to set forth principles for FCC consideration and possible adoption that are harmonized and consistent with the FTC and other government entities' approach to privacy and security for the same or similar data. Even if courts determine that the FCC's reclassification of Broadband Internet Access Services is a lawful exercise of authority, any rules must not exceed the text and legislative history of Section 222 of the Act.

sectors would fulfill the following key tenets in the White House Privacy Report: (1) avoid “inconsistent standards for related technologies” that could dampen innovation; (2) foster a “level playing field for companies;” and, most importantly, (3) create “a consistent set of expectations for consumers.” To achieve this end, the FCC’s policies, rules, and enforcement practices should conform to the longstanding limiting principles articulated in the FTC’s Unfairness and Deception Policy Statements. In addition, the FCC and FTC can achieve their recent MOU’s stated goal of avoiding “duplicative, redundant or inconsistent oversight” by developing a new process to ensure that their substantive privacy policies and basis for enforcement are consistent going forward.

- Flexibility. The FCC’s approach should provide a flexible framework within which telecommunications service providers can implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments in this space. Specifically, this framework should identify the privacy or security *goals*, and afford providers flexibility in achieving those goals, rather than dictate the particular *methods* by which providers are expected to achieve those goals. Adopting a flexible approach also will help ensure consistent federal and state requirements governing customer information.
- Application. Consistent with the Communications Act and to eliminate unnecessary duplication of authority with other agencies, the FCC’s framework should only apply when 1) telecommunications service providers are providing telecommunications services and 2) the CPNI is made available by the customer to the telecommunications service provider solely by virtue of the carrier-customer relationship. The framework cannot lawfully apply to:
 - Providers’ non-telecommunications services and products
 - Providers’ non-telecommunications service provider affiliates
 - Information that is not made available to the carrier by the customer solely by virtue of the carrier-customer relationship
- Individually Identifiable. The FCC should carve out from the scope of its new framework any data that is de-identified, aggregated, or does not otherwise identify a known individual. The insights derived from the use of de-identified data can offer great benefits to consumers and society and such use avoids the sensitivities that may be associated with identified data.
- Unfair or Deceptive Conduct. As noted above, the FCC’s policies, rules, and enforcement practices should conform to the FTC’s longstanding limiting principles articulated in its Policy Statements on Unfairness (1980) and Deception (1983). This approach is consistent with the FCC’s commitment to conduct a cost-benefit analysis of its regulatory framework in accordance with President Obama’s Executive Orders 13563 and 13579, which require agencies to “adopt a regulation only upon a reasoned determination its benefits justify its costs” and “tailor its regulations to impose the least burden on society.”

- Unfair Conduct. A provider acts unfairly if its act or practice (1) causes or is likely to cause substantial injury to consumers (2) which is not reasonably avoidable by consumers themselves, and (3) is not outweighed by countervailing benefits to consumers or to competition.
- Deceptive Conduct. A provider acts deceptively if (1) it makes a statement or omission, or engages in a practice, that is likely to mislead a customer, (2) viewed from the perspective of a consumer acting reasonably under the circumstances, and (3) the deceptive statement, omission, or practice is material—meaning that the misrepresentation or practice is likely to affect the consumer’s conduct or decision with regard to a product or service.
- Additional Guidance. In coordination with other privacy regulators, the FCC could, like the FTC and various states like California, provide additional guidance on how it interprets its framework through workshops or reports. The FCC also could encourage and support the development and implementation of industry guidelines.
- Update and Harmonize Existing CPNI Rules. The existing CPNI rules should be revisited in their entirety and modernized to use the same flexible framework for all services subject to Section 222, including traditional voice services. In no event should the prescriptive outdated rules designed for legacy voice services apply to broadband services. Instead, a common set of flexible policies that allow providers to keep up with their customers’ expectations and evolving technology should apply to both types of services.

With these guidelines in mind, and only to the extent the FCC has the requisite jurisdiction, the FCC could adopt the following principles, which encompass and are consistent with the privacy and security framework that applies to the rest of the industry. Each of these principles and the goals noted above should provide flexibility for providers to implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments:

- Transparency. A telecommunications service provider should provide notice, which is neither deceptive nor unfair, describing the CPNI that it collects, how it will use the CPNI, and whether and for what purposes it may share CPNI with third parties.
- Respect for Context and Consumer Choice. A telecommunications service provider may use or disclose CPNI as is consistent with the context in which the customer provides, or the provider obtains, the information, provided that the provider’s actions are not unfair or deceptive. For example, the use or disclosure of CPNI for the following commonly accepted data practices would not warrant a choice mechanism, either because customer consent can be inferred or because public policy considerations make choice unnecessary: product and service fulfillment, fraud prevention, compliance with law, responses to government requests, network management, first-party marketing, and affiliate sharing where the affiliate relationship is reasonably clear to consumers. Consistent with the flexible choice mechanisms available to all other entities in the Internet ecosystem, telecommunications service providers should give consumers easy-

to-understand choices for non-contextual uses and disclosures of their CPNI, where the failure to provide choice would be deceptive or unfair. The provider should consider the sensitivity of the data and the context in which it was collected when determining the appropriate choice mechanism.

- Data Security. A telecommunications service provider should establish, implement, and maintain a CPNI data security program that is neither unfair nor deceptive and includes reasonable physical, technical, and administrative security safeguards to protect CPNI from unauthorized access, use, and disclosure. Providers' CPNI data security programs should provide reasonable protections in light of the nature and scope of the activities of the company, the sensitivity of the data, and the size and complexity of the relevant data operations of the company.
- Data Breach Notifications. Telecommunications service providers should notify customers whose CPNI has been breached when failure to notify would be unfair or deceptive. Given that breach investigations frequently are ongoing at the time providers offer notice to customers, a notice that turns out to be incomplete or inaccurate is not deceptive, as long as the provider corrects any material inaccuracies within a reasonable period of time of discovering them. Telecommunications providers have flexibility to determine how and when to provide such notice.

The FCC can ensure compliance with the above principles by pursuing reasonable enforcement actions against telecommunications service providers that have clearly violated these principles.

American Cable Association
Competitive Carriers Association
CTIA
National Cable & Telecommunications Association
U.S. Telecom Association

Dated: February 19, 2016

Joanne Wall

From: Lisa Hone
Sent: Thursday, February 25, 2016 2:24 PM
To: Ruth Milkman; Louisa Terrell; Gigi Sohn; Stephanie Weiner; Matthew DelNero; Jonathan Sallet; Jennifer Tatel; Philip Verveer; Shannon Gilson; Eric Feigenbaum
Subject: Fw: Updated Privacy Framework from the telecom trades
Attachments: BB Privacy Framework 2.19.16.pdf

The telecom companies and associations have tweaked their framework a bit.

See Debbie Matties' email below and attachment.

Lisa

From: Debbie Matties
Sent: Thursday, February 25, 2016 2:09 PM
To: Lisa Hone
Subject: Updated Privacy Framework from the telecom trades

Hi Lisa,

Maggie mentioned to you that we had made a few revisions to the Privacy Framework that we had given you back in December. I've attached the new version here, dated February 19.

We made two substantive changes on the last page. First, at the top, we added "The provider should consider the sensitivity of the data and the context in which it was collected when determining the appropriate choice mechanism." Second we reworked the data breach bullet. We also made a few stylistic edits on the earlier pages in anticipation of releasing it publicly.

Please let me know if you have any questions.

Best,

Debbie

 Everything™
Wireless

Debbie Matties

Vice President, Privacy
1400 16th Street, NW Suite 600
Washington, DC 20036
Direct: 202.736.3654
Wireless: 202.758.7697
dmatties@ctia.org

Joanne Wall

From: FLEMMING, JACQUELYNE <jw1196@att.com>
Sent: Friday, March 11, 2016 10:28 AM
To: Lisa Hone
Subject: got your message. Thanks for the callback.

Jackie Flemming

AVP-External Affairs/Regulatory
AT&T Services
1120 20th St. NW, Suite 1000
Washington, DC 20036
O: (202) 457-3032
C: (202) 531-9801
email:jackie.flemming@att.com

This e-mail and any files transmitted with it are confidential, and are intended solely for the use of the individual or entity to whom this e-mail is addressed. If you are not one of the named recipient(s) or otherwise have reason to believe that you have received this message in error, please notify the sender at [202 457-3032] and delete this message immediately from your computer. Any other use, retention, dissemination, forwarding, printing, or copying of this e-mail is strictly prohibited.

Joanne Wall

From: Debbie Matties <DMatties@ctia.org>
Sent: Wednesday, April 01, 2015 2:24 PM
To: Lisa Hone
Subject: Hi!

Hi Lisa – How are you? I hear you're going to be at a meeting I'm attending tomorrow at the FCC. Is that true? If so, do you have time for a quick chat?

And this just reminds me how overdue we are for lunch. I fear I dropped a ball somewhere on that.

Debbie Matties
Vice President, Privacy
CTIA-The Wireless Association®
1400 16th Street, NW Suite 600
Washington, DC 20036
www.ctia.org
Direct: 202.736.3654
Wireless: 202.758.7697

Joanne Wall

From: Debbie Matties <DMatties@ctia.org>
Sent: Friday, May 22, 2015 10:54 AM
To: Lisa Hone
Subject: Lunch or coffee?

Hi Lisa – sorry you guys can't make my BBQ this weekend – are you going somewhere fun?

Would you like to get lunch or coffee next week? Would love to catch up, and maybe we can chat about stuff like ISPs a little. ☺

Debbie Matties
Vice President, Privacy
CTIA-The Wireless Association®
1400 16th Street, NW Suite 600
Washington, DC 20036
www.ctia.org
Direct: 202.736.3654
Wireless: 202.758.7697

Joanne Wall

From: Rosenthal, Michelle <Michelle.Rosenthal1@T-Mobile.com>
Sent: Thursday, May 28, 2015 9:54 AM
To: Lisa Hone
Subject: Lunch

Hi Lisa,

Does lunch still work for you today at 12:30? My meeting got cancelled, so I am a little more flexible if an earlier or later time works better for you. I'll plan to come your way, but I don't know what is around there for lunch. Any suggestions? I'm happy with casual or sit-down – whatever you prefer. Look forward to catching up!

Michelle

Michelle Rosenthal
Corporate Counsel
Federal Regulatory Affairs
T-Mobile US, Inc.
Office: 202.654-5939
Mobile: 202.607.3435
Fax: 202.654.5963

Joanne Wall

Subject: Meeting with Verizon (RM) MDN,JT,LH
Location: conf. room #1

Start: Thu 5/5/2016 10:00 AM
End: Thu 5/5/2016 10:30 AM
Show Time As: Tentative

Recurrence: (none)

Meeting Status: Not yet responded

Organizer: Kim Mattos
Required Attendees: Ruth Milkman (Ruth.Milkman@fcc.gov); Matthew DelNero; Jennifer Tatel; Lisa Hone
Optional Attendees: Natividad Persaud

5/4-

Updated to add three others, who will also be joining Will. Thank you. -k
Karen Zacharia, Mike Berg, and Maggie McCready

==

4/26-

Dear all:

Per Ruth's request. Thank you. -k
Meeting attendees: tbd

From: Johnson, William H [<mailto:will.h.johnson@verizon.com>]
Sent: Friday, April 22, 2016 6:11 PM
To: Matthew DelNero <Matthew.DelNero@fcc.gov>
Subject: Scheduling

Following up on days that would work for the first meeting we discussed (deeper dive on our programs and practices). The days that work best for us are May 4-6, 11 or 12. Any of those work for you guys?

Will

<image001.png>

William H. Johnson
Senior Vice President, Federal Regulatory & Legal Affairs
Verizon
1300 I St. NW, Suite 400 West
Washington, DC 20005
will.h.johnson@verizon.com
t: (202) 515-2492
c: (202) 805-4321

Joanne Wall

Subject: Meeting with Verizon re: new privacy policy
Location: 5-B112

Start: Thu 11/19/2015 2:00 PM
End: Thu 11/19/2015 2:30 PM
Show Time As: Tentative

Recurrence: (none)

Meeting Status: Not yet responded

Organizer: Lisa Hone
Required Attendees: Matthew DelNero; Melissa Droller Kirkel; John Visclosky; Kristine Fargotstein; Zachary Ross; David Brody; Jennifer Tatel; Douglas Klein

Adding room number.

Verizon is going to come in to talk about its new privacy policy.
Maggie Macready is going to come with Karen Zachariah and perhaps others.
They are not prepared to talk about the 222 proceeding.

Joanne Wall

From: Lisa Hone
Sent: Thursday, May 07, 2015 11:31 AM
To: 'maggie.m.mccready@verizon.com'
Subject: privacy discussion

Maggie – Here are some times that we could be available for a discussion with Verizon about broadband privacy:

5/15: 1:00; 1:30, 2:00, 2:30; 4:00

5/18: 4:00

5/19: 11am; 4:30pm

Please let me know if any of those work for you.

Thanks,

Lisa Hone

Joanne Wall

Subject: Privacy meeting with AT&T
Location: 5-B112 Dividable North Conf Rm 1 (Room)

Start: Fri 6/24/2016 1:00 PM
End: Fri 6/24/2016 1:30 PM
Show Time As: Tentative

Recurrence: (none)

Meeting Status: Not yet responded

Organizer: Lisa Hone
Required Attendees: Matthew DelNero; Melissa Droller Kinkel; Daniel Kahn; Sherwin Siy
Resources: 5-B112 Dividable North Conf Rm 1 (Room)

I will find out what specific issues they want to talk about and that may help us decide who else should attend this meeting.

Lisa

Joanne Wall

From: Debbie Matties <DMatties@ctia.org>
Sent: Monday, December 21, 2015 5:38 PM
To: Lisa Hone
Subject: Privacy

Hi Lisa,

I hope you're well, and maybe off work this week? Thank you for meeting with us last week, and for the time all the others took as well. We'll be interested to hear what you think about our proposal after you've had time to digest it.

Best,
Debbie

ctia Everything™
***** Wireless

Debbie Matties

Vice President, Privacy
1400 16th Street, NW Suite 600
Washington, DC 20036
Direct: 202.736.3654
Wireless: 202.758.7697
dmatties@ctia.org

Joanne Wall

From: McCreedy, Margaret (Maggie McCreedy) <maggie.m.mccreedy@verizon.com>
Sent: Friday, January 29, 2016 1:26 PM
To: Lisa Hone
Subject: Proposed meeting dates

Lisa,
Here are some dates and times that work for Vz to meet with you to discuss the industry proposal. Do any of these work on your end?

Feb 10th 4 PM
Feb 11th 4 PM
Feb 12th 10 or 11 AM

Maggie McCreedy
202-515-2543 (office)
202-281-9272 (cell)

Joanne Wall

From: Rosenthal, Michelle <Michelle.Rosenthal1@T-Mobile.com>
Sent: Friday, March 18, 2016 3:28 PM
To: Lisa Hone
Subject: Quick call

Hey – good to see you earlier. I realize I have your cell phone, but not your work number. Can you send? I have a very quick question that will take a minute or two tops.

Michelle Rosenthal
Senior Corporate Counsel
Federal Regulatory Affairs
T-Mobile US, Inc.
Office: 202.654-5939
Mobile: 202.607.3435
Fax: 202.654.5963

Joanne Wall

From: Rosenthal, Michelle <Michelle.Rosenthal1@T-Mobile.com>
Sent: Tuesday, September 01, 2015 10:51 AM
To: Lisa Hone
Subject: Quick question for you

Do you have a minute to chat this morning? I wanted to run something by you.

Michelle Rosenthal
Corporate Counsel
Federal Regulatory Affairs
T-Mobile US, Inc.
Office: 202.654-5939
Mobile: 202.607.3435
Fax: 202.654.5963

Joanne Wall

From: Lisa Hone
Sent: Thursday, February 04, 2016 11:29 PM
To: McCready, Margaret (Maggie Mccready)
Subject: Re:

Still works for me.
Does it work for you?

Lisa

From: McCready, Margaret (Maggie Mccready)
Sent: Thursday, February 4, 2016 7:48 AM
To: Lisa Hone
Subject:

Hi Lisa,
Just checking in to see if coffee tomorrow afternoon at 2 still works for you. If so, I will see you then.
Maggie McCready
202-515-2543 (office)
202-281-9272 (cell)

Joanne Wall

From: Lisa Hone
Sent: Friday, November 20, 2015 2:48 PM
To: Debbie Matties
Subject: Re: Afternoon coffee monday?

Ok

Original Message
From: Debbie Matties
Sent: Friday, November 20, 2015 2:46 PM
To: Lisa Hone
Subject: RE: Afternoon coffee monday?

That's good. Want to call me at 202-736-3654?

-----Original Message-----
From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Friday, November 20, 2015 2:39 PM
To: Debbie Matties
Subject: Re: Afternoon coffee monday?

Sure. How about 3:30?

Original Message
From: Debbie Matties
Sent: Friday, November 20, 2015 2:10 PM
To: Lisa Hone
Subject: RE: Afternoon coffee monday?

Yes, that's great. Also, can we jump on the phone for 15 minutes this afternoon? I'm free other than 2:30-3.

-----Original Message-----
From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Friday, November 20, 2015 11:38 AM
To: Debbie Matties
Subject: Re: Afternoon coffee monday?

Great - does 4pm work for you?

Original Message
From: Debbie Matties
Sent: Friday, November 20, 2015 11:26 AM
To: Lisa Hone
Subject: Afternoon coffee monday?

assuming lunchtime is still unavailable.... I'm free after 3pm

Sent from my iPhone

Joanne Wall

From: Debbie Matties <DMatties@ctia.org>
Sent: Monday, December 07, 2015 3:55 PM
To: Lisa Hone
Cc: Latoya Toles
Subject: RE: Dec. 16 meeting

Thanks Lisa. I hope to have a list for LaToya by the end of the week.

ctia Everything™
***** Wireless

Debbie Matties

Vice President, Privacy
1400 16th Street, NW Suite 600
Washington, DC 20036
Direct: 202.736.3654
Wireless: 202.758.7697
dmatties@ctia.org

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Saturday, December 05, 2015 9:23 AM
To: Debbie Matties
Cc: Latoya Toles
Subject: Re: Dec. 16 meeting

Debbie - bringing in 16 people should be fine.

I am copying LaToya Toles, Matt DelNero's assistant, so she can coordinate with Security about getting so many people in the building for one meeting.

It might be helpful for her to know how many people in your group have pre-issued visitors badges.

From the FCC, I expect:

Matt DelNero, WCB Bureau Chief
Lisa Hone, WCB Associate Chief
Melissa Kirkel, Assistant Division Chief, Competition Policy Division, WCB
Jennifer Tatel, Associate General Counsel
Scott Jordan, FCC Chief Technologist
And one or two attorneys from CPD

From: Debbie Matties
Sent: Friday, December 4, 2015 11:34 AM
To: Lisa Hone
Subject: Dec. 16 meeting

Hi Lisa – great panel this morning! Sorry I didn't say goodbye, but you were wrapped up in conversation with someone I didn't know and I didn't want to interrupt.

We're putting together our group to meet with you on the 16th and it's getting quite large. Will you be able to reserve a really big room? I think we could have as many as 16 people.

And do you know who from the FCC will be attending? Many folks are curious.

Thanks!
Debbie

Joanne Wall

From: Debbie Matties <DMatties@ctia.org>
Sent: Tuesday, December 15, 2015 3:50 PM
To: Lisa Hone
Cc: Latoya Toles
Subject: RE: Dec. 16 meeting

Thank you. This information means nothing to me. ☺

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Tuesday, December 15, 2015 3:32 PM
To: Debbie Matties
Cc: Latoya Toles
Subject: RE: Dec. 16 meeting

Jeez – talk about inside baseball.

2-South

From: Debbie Matties [mailto:DMatties@ctia.org]
Sent: Tuesday, December 15, 2015 3:27 PM
To: Lisa Hone <Lisa.Hone@fcc.gov>
Cc: Latoya Toles <Latoya.Toles@fcc.gov>
Subject: RE: Dec. 16 meeting

Thanks for the update. I've been asked if I know what room we're in...

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Tuesday, December 15, 2015 3:24 PM
To: Debbie Matties
Cc: Latoya Toles
Subject: RE: Dec. 16 meeting

From the FCC I have added:

Charles Mathias, Associate Bureau Chief, Wireless Telecommunications Bureau
Doug Klein, Office of General Counsel

This is going to be one crowded meeting.

From: Debbie Matties [mailto:DMatties@ctia.org]
Sent: Monday, December 07, 2015 3:55 PM
To: Lisa Hone <Lisa.Hone@fcc.gov>
Cc: Latoya Toles <Latoya.Toles@fcc.gov>
Subject: RE: Dec. 16 meeting

Thanks Lisa. I hope to have a list for LaToya by the end of the week.

ctia Everything™
***** Wireless
Debbie Matties

Vice President, Privacy
1400 16th Street, NW Suite 600
Washington, DC 20036
Direct: 202.736.3654
Wireless: 202.758.7697
dmatties@ctia.org

From: Lisa Hone [<mailto:Lisa.Hone@fcc.gov>]
Sent: Saturday, December 05, 2015 9:23 AM
To: Debbie Matties
Cc: LaToya Toles
Subject: Re: Dec. 16 meeting

Debbie - bringing in 16 people should be fine.

I am copying LaToya Toles, Matt DelNero's assistant, so she can coordinate with Security about getting so many people in the building for one meeting.

It might be helpful for her to know how many people in your group have pre-issued visitors badges.

From the FCC, I expect:

Matt DelNero, WCB Bureau Chief
Lisa Hone, WCB Associate Chief
Melissa Kirkel, Assistant Division Chief, Competition Policy Division, WCB
Jennifer Tatel, Associate General Counsel
Scott Jordan, FCC Chief Technologist
And one or two attorneys from CPD

From: Debbie Matties
Sent: Friday, December 4, 2015 11:34 AM
To: Lisa Hone
Subject: Dec. 16 meeting

Hi Lisa – great panel this morning! Sorry I didn't say goodbye, but you were wrapped up in conversation with someone I didn't know and I didn't want to interrupt.

We're putting together our group to meet with you on the 16th and it's getting quite large. Will you be able to reserve a really big room? I think we could have as many as 16 people.

And do you know who from the FCC will be attending? Many folks are curious.

Thanks!
Debbie

Joanne Wall

From: Latoya Toles
Sent: Tuesday, December 15, 2015 3:32 PM
To: Debbie Matties; Lisa Hone
Subject: RE: Dec. 16 meeting

2-b516. But I/someone will escort you to the room. Thanks!

From: Debbie Matties [mailto:DMatties@ctia.org]
Sent: Tuesday, December 15, 2015 3:27 PM
To: Lisa Hone
Cc: Latoya Toles
Subject: RE: Dec. 16 meeting

Thanks for the update. I've been asked if I know what room we're in...

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Tuesday, December 15, 2015 3:24 PM
To: Debbie Matties
Cc: Latoya Toles
Subject: RE: Dec. 16 meeting

From the FCC I have added:

Charles Mathias, Associate Bureau Chief, Wireless Telecommunications Bureau
Doug Klein, Office of General Counsel

This is going to be one crowded meeting.

From: Debbie Matties [mailto:DMatties@ctia.org]
Sent: Monday, December 07, 2015 3:55 PM
To: Lisa Hone <Lisa.Hone@fcc.gov>
Cc: Latoya Toles <Latoya.Toles@fcc.gov>
Subject: RE: Dec. 16 meeting

Thanks Lisa. I hope to have a list for LaToya by the end of the week.

ctia Everything™
***** Wireless
Debbie Matties
Vice President, Privacy
1400 16th Street, NW Suite 600
Washington, DC 20036
Direct: 202.736.3654
Wireless: 202.758.7697
dmatties@ctia.org

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Saturday, December 05, 2015 9:23 AM
To: Debbie Matties
Cc: Latoya Toles
Subject: Re: Dec. 16 meeting

Debbie - bringing in 16 people should be fine.

I am copying LaToya Toles, Matt DelNero's assistant, so she can coordinate with Security about getting so many people in the building for one meeting.

It might be helpful for her to know how many people in your group have pre-issued visitors badges.

From the FCC, I expect:

Matt DelNero, WCB Bureau Chief
Lisa Hone, WCB Associate Chief
Melissa Kinkel, Assistant Division Chief, Competition Policy Division, WCB
Jennifer Tatel, Associate General Counsel
Scott Jordan, FCC Chief Technologist
And one or two attorneys from CPD

From: Debbie Matties
Sent: Friday, December 4, 2015 11:34 AM
To: Lisa Hone
Subject: Dec. 16 meeting

Hi Lisa – great panel this morning! Sorry I didn't say goodbye, but you were wrapped up in conversation with someone I didn't know and I didn't want to interrupt.

We're putting together our group to meet with you on the 16th and it's getting quite large. Will you be able to reserve a really big room? I think we could have as many as 16 people.

And do you know who from the FCC will be attending? Many folks are curious.

Thanks!
Debbie

Joanne Wall

From: Lisa Hone
Sent: Tuesday, December 15, 2015 4:28 PM
To: Debbie Matties
Subject: RE: Dec. 16 meeting

Indeed.

From: Debbie Matties [mailto:DMatties@ctia.org]
Sent: Tuesday, December 15, 2015 4:26 PM
To: Lisa Hone
Subject: RE: Dec. 16 meeting

We should insert jokes throughout about how many people are there.

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Tuesday, December 15, 2015 3:24 PM
To: Debbie Matties
Cc: Latoya Toles
Subject: RE: Dec. 16 meeting

From the FCC I have added:

Charles Mathias, Associate Bureau Chief, Wireless Telecommunications Bureau
Doug Klein, Office of General Counsel

This is going to be one crowded meeting.

From: Debbie Matties [mailto:DMatties@ctia.org]
Sent: Monday, December 07, 2015 3:55 PM
To: Lisa Hone <Lisa.Hone@fcc.gov>
Cc: Latoya Toles <Latoya.Toles@fcc.gov>
Subject: RE: Dec. 16 meeting

Thanks Lisa. I hope to have a list for LaToya by the end of the week.

ctia Everything™
***** Wireless
Debbie Matties
Vice President, Privacy
1400 16th Street, NW Suite 600
Washington, DC 20036
Direct: 202.736.3654
Wireless: 202.758.7697
dmatties@ctia.org

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Saturday, December 05, 2015 9:23 AM
To: Debbie Matties
Cc: Latoya Toles
Subject: Re: Dec. 16 meeting

Debbie - bringing in 16 people should be fine.

I am copying LaToya Toles, Matt DelNero's assistant, so she can coordinate with Security about getting so many people in the building for one meeting.

It might be helpful for her to know how many people in your group have pre-issued visitors badges.

From the FCC, I expect:

Matt DelNero, WCB Bureau Chief
Lisa Hone, WCB Associate Chief
Melissa Kirkel, Assistant Division Chief, Competition Policy Division, WCB
Jennifer Tatel, Associate General Counsel
Scott Jordan, FCC Chief Technologist
And one or two attorneys from CPD

From: Debbie Matties
Sent: Friday, December 4, 2015 11:34 AM
To: Lisa Hone
Subject: Dec. 16 meeting

Hi Lisa – great panel this morning! Sorry I didn't say goodbye, but you were wrapped up in conversation with someone I didn't know and I didn't want to interrupt.

We're putting together our group to meet with you on the 16th and it's getting quite large. Will you be able to reserve a really big room? I think we could have as many as 16 people.

And do you know who from the FCC will be attending? Many folks are curious.

Thanks!
Debbie

Joanne Wall

From: Lisa Hone
Sent: Monday, December 14, 2015 11:47 AM
To: Debbie Matties
Subject: RE: Dec. 16 meeting

Thx,

Lisa

From: Debbie Matties [mailto:DMatties@ctia.org]
Sent: Monday, December 14, 2015 9:49 AM
To: Lisa Hone
Cc: Latoya Toles
Subject: RE: Dec. 16 meeting

Sure thing – see below.

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Sunday, December 13, 2015 9:27 PM
To: Debbie Matties <DMatties@ctia.org>
Cc: Latoya Toles <Latoya.Toles@fcc.gov>
Subject: RE: Dec. 16 meeting

Thanks – would you please add company and or association identifiers?

Appreciate it,

Lisa

From: Debbie Matties [mailto:DMatties@ctia.org]
Sent: Sunday, December 13, 2015 10:20 AM
To: Lisa Hone <Lisa.Hone@fcc.gov>
Cc: Latoya Toles <Latoya.Toles@fcc.gov>
Subject: RE: Dec. 16 meeting

Hi Lisa and LaToya,

Here's our list. I think probably 10 of the people below have pre-issued visitor badges. And yes, we're a smidge over 16. Sorry.

1. Debbie Matties - CTIA
2. Scott Bergmann - CTIA
3. Loretta Polk - NCTA
4. Jennifer McKee - NCTA
5. Lynn Follansbee - USTA
6. Courtney Neville – CCA
7. Maureen Cooney - Sprint

8. Matthew Sullivan - Sprint
9. Maggie McCready - Verizon
10. Cathy Hilke - Verizon
11. Jonathan Zimmerman – AT&T
12. Jeff Brueggeman – AT&T
13. Jackie Fleming – AT&T
14. Michelle Rosenthal - TMobile
15. Rudy Brioche - Comcast
16. Mary McManus - Comcast
17. Frank Buono – Comcast outside counsel
18. Ross Lieberman (maybe) - ACA

From: Lisa Hone [<mailto:Lisa.Hone@fcc.gov>]
Sent: Saturday, December 5, 2015 9:23 AM
To: Debbie Matties <DMatties@ctia.org>
Cc: LaToya Toles <LaToya.Toles@fcc.gov>
Subject: Re: Dec. 16 meeting

Debbie - bringing in 16 people should be fine.

I am copying LaToya Toles, Matt DelNero's assistant, so she can coordinate with Security about getting so many people in the building for one meeting.

It might be helpful for her to know how many people in your group have pre-issued visitors badges.

From the FCC, I expect:

Matt DelNero, WCB Bureau Chief
Lisa Hone, WCB Associate Chief
Melissa Kirkel, Assistant Division Chief, Competition Policy Division, WCB
Jennifer Tatel, Associate General Counsel
Scott Jordan, FCC Chief Technologist
And one or two attorneys from CPD

From: Debbie Matties
Sent: Friday, December 4, 2015 11:34 AM
To: Lisa Hone
Subject: Dec. 16 meeting

Hi Lisa – great panel this morning! Sorry I didn't say goodbye, but you were wrapped up in conversation with someone I didn't know and I didn't want to interrupt.

We're putting together our group to meet with you on the 16th and it's getting quite large. Will you be able to reserve a really big room? I think we could have as many as 16 people.

And do you know who from the FCC will be attending? Many folks are curious.

Thanks!
Debbie

Joanne Wall

From: Melissa Droller Kinkel
Sent: Monday, December 14, 2015 8:35 AM
To: Lisa Hone
Subject: RE: Dec. 16 meeting

(b) (5)

Melissa Droller Kinkel
Acting Assistant Division Chief
Competition Policy Division
Wireline Competition Bureau
Federal Communications Commission
Phone: (202) 418-7958

*** Non-Public: For Internal Use Only ***

From: Lisa Hone
Sent: Sunday, December 13, 2015 10:34 PM
To: Matthew DelNero ; Jennifer Tatel ; Melissa Droller Kinkel
Subject: FW: Dec. 16 meeting

Wow.

I have asked Debbie to add company/organization identifiers.

Off the top of my head, I am only absolutely sure about 8 of them- though, I might succeed with educated guesses re: another bunch.

Lisa

From: Debbie Matties [<mailto:DMatties@ctia.org>]
Sent: Sunday, December 13, 2015 10:20 AM
To: Lisa Hone <Lisa.Hone@fcc.gov>
Cc: Latoya Toles <Latoya.Toles@fcc.gov>
Subject: RE: Dec. 16 meeting

Hi Lisa and LaToya,

Here's our list. I think probably 10 of the people below have pre-issued visitor badges. And yes, we're a smidge over 16. Sorry.

1. Debbie Matties
2. Scott Bergmann
3. Loretta Polk
4. Jennifer McKee
5. Lynn Follansbee
6. Courtney Neville
7. Maureen Cooney
8. Matthew Sullivan
9. Maggie McCready

10. Cathy Hilke
11. Jonathan Zimmerman
12. Jeff Brueggeman
13. Jackie Fleming
14. Michelle Rosenthal
15. Rudy Brioche
16. Mary McManus
17. Frank Buono
18. Ross Lieberman (maybe)

From: Lisa Hone [<mailto:Lisa.Hone@fcc.gov>]
Sent: Saturday, December 5, 2015 9:23 AM
To: Debbie Matties <DMatties@ctia.org>
Cc: Latoya Toles <Latoya.Toles@fcc.gov>
Subject: Re: Dec. 16 meeting

Debbie - bringing in 16 people should be fine.

I am copying LaToya Toles, Matt DelNero's assistant, so she can coordinate with Security about getting so many people in the building for one meeting.

It might be helpful for her to know how many people in your group have pre-issued visitors badges.

From the FCC, I expect:

Matt DelNero, WCB Bureau Chief
Lisa Hone, WCB Associate Chief
Melissa Kirkel, Assistant Division Chief, Competition Policy Division, WCB
Jennifer Tatel, Associate General Counsel
Scott Jordan, FCC Chief Technologist
And one or two attorneys from CPD

From: Debbie Matties
Sent: Friday, December 4, 2015 11:34 AM
To: Lisa Hone
Subject: Dec. 16 meeting

Hi Lisa – great panel this morning! Sorry I didn't say goodbye, but you were wrapped up in conversation with someone I didn't know and I didn't want to interrupt.

We're putting together our group to meet with you on the 16th and it's getting quite large. Will you be able to reserve a really big room? I think we could have as many as 16 people.

And do you know who from the FCC will be attending? Many folks are curious.

Thanks!
Debbie

Joanne Wall

From: Lisa Hone
Sent: Monday, November 23, 2015 12:13 PM
To: Debbie Matties
Subject: Re: Dec. 16th

Ok - tea and small bites at 4pm. See you then.

From: Debbie Matties
Sent: Monday, November 23, 2015 12:05 PM
To: Lisa Hone
Subject: RE: Dec. 16th

Hi Lisa – yes, the 16th at 3pm works – let’s book it.

The Mandarin Oriental only does formal tea service Friday, Saturday and Sunday, but the Empress Lounge is open at 4 for us to order off the menu, including tea and small bites. Choices might be limited but that’s not a concern for me if it’s ok with you. See you there at 4?

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Sunday, November 22, 2015 7:02 PM
To: Debbie Matties
Subject: Dec. 16th

Can we do our meeting Dec. 16th at 3pm?

Thanks,
Lisa

Joanne Wall

From: McCready, Margaret (Maggie Mccready) <maggie.m.mccready@verizon.com>
Sent: Friday, February 05, 2016 6:57 AM
To: Lisa Hone
Subject: Re: [E] Re:

Yes. See you this afternoon.

Sent from Divide managed by MobileIron

On Feb 4, 2016 11:28:37 PM, Lisa Hone wrote:
Still works for me.
Does it work for you?

Lisa

From: McCready, Margaret (Maggie Mccready)
Sent: Thursday, February 4, 2016 7:48 AM
To: Lisa Hone
Subject:

Hi Lisa,
Just checking in to see if coffee tomorrow afternoon at 2 still works for you. If so, I will see you then.
Maggie McCready
202-515-2543 (office)
202-281-9272 (cell)

Joanne Wall

From: Lisa Hone
Sent: Thursday, November 19, 2015 2:08 PM
To: McCready, Margaret (Maggie Mccready)
Subject: RE: [E] RE: Stuck in traffic

Our meeting is at 2pm – but where are you?

From: McCready, Margaret (Maggie Mccready) [mailto:maggie.m.mccready@verizon.com]
Sent: Thursday, November 19, 2015 2:06 PM
To: Lisa Hone
Subject: RE: [E] RE: Stuck in traffic

We are here but it looks like the meeting is 2:30 not 2. We are waiting in the try floor lobby.

-----Original Message-----

From: Lisa Hone [Lisa.Hone@fcc.gov]
Sent: Thursday, November 19, 2015 01:57 PM Eastern Standard Time
To: McCready, Margaret (Maggie Mccready)
Subject: [E] RE: Stuck in traffic

Do me a favor and let me know when you arrive.

Thx,

-----Original Message-----

From: McCready, Margaret (Maggie Mccready) [mailto:maggie.m.mccready@verizon.com]
Sent: Thursday, November 19, 2015 1:50 PM
To: Lisa Hone <Lisa.Hone@fcc.gov>
Subject: Stuck in traffic

But we will be there as soon as possible.

Joanne Wall

From: McCready, Margaret (Maggie Mccready) <maggie.m.mccready@verizon.com>
Sent: Tuesday, November 10, 2015 7:11 PM
To: Lisa Hone
Subject: RE: [E] RE: Vz Privacy Policy meeting

Thanks.

-----Original Message-----

From: Lisa Hone [Lisa.Hone@fcc.gov]
Sent: Tuesday, November 10, 2015 05:55 PM Eastern Standard Time
To: McCready, Margaret (Maggie Mccready)
Cc: Latoya Toles
Subject: [E] RE: Vz Privacy Policy meeting

Great – I have scheduled a room. You can have the security desk contact Latoya Toles, copied here, when you arrive.

I expect the following people to attend:

Matt DelNero, WCB Bureau Chief
Melissa Kirkel, TAPD Assistant Director
John Visclosky, TAPD
Kristine Fargotstein, TAPD
Zac Ross, TAPD
David Brody, TAPD
Jennifer Tatel, Associate General Counsel
Doug Klein, OGC
Lisa
Lisa Hone
Associate Chief
Wireline Competition Bureau
Federal Communications Commission
202.418.0869
Lisa.Hone@fcc.gov

From: McCready, Margaret (Maggie Mccready) [<mailto:maggie.m.mccready@verizon.com>]
Sent: Tuesday, November 10, 2015 9:20 AM
To: Lisa Hone
Subject: Vz Privacy Policy meeting

Lisa,
Thursday Nov 19th at 2 PM works for Vz to meet with you to discuss our new privacy policy. Hopefully that still works on your end. Please let me know, and if it works, whom should we have the desk contact for access? A few of the Vz attendees do not have visitor badges. Thanks.

Maggie McCready
202-515-2543 (office)
202-281-9272 (cell)

Joanne Wall

From: Rosenthal, Michelle <Michelle.Rosenthal1@T-Mobile.com>
Sent: Friday, May 15, 2015 10:25 AM
To: Lisa Hone
Subject: RE: Hello!

You're right. I do now remember seeing you right after I left, but I also can't remember where that was. May 28 works for me! I'll send you a scheduler and will plan to come to your area. Is there any place you prefer around there? Look forward to catching up.

Michelle

-----Original Message-----

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Thursday, May 14, 2015 8:51 PM
To: Rosenthal, Michelle
Subject: Re: Hello!

Michelle - I am curious to hear why you decided to leave the FTC and how you like T-Mo. I did know you went there, I feel like we were both at an event shortly after you made the switch, but I don't know what event.

Lunch would be great. Would May 28 work for you? If not, sometime the week of June 15? (Crazy I know, but I am travelling most of the week of June 1 and the end of the school year is always a big challenge).

All the best,

Lisa

From: Rosenthal, Michelle
Sent: Thursday, May 14, 2015 6:27 PM
To: Lisa Hone
Subject: Hello!

Hey Lisa,

It was great to see you at the FCC workshop a few weeks ago (great job!) and it was a good reminder that I have some old FTC friends at the FCC. I'm not sure if I even spoke to you prior to my move last year, but I left the FTC and started at T-Mobile in January of last year doing privacy and data security regulatory work. (So here I am in the world of telecom. It's a crazy place.) Anyway, it occurred to me after I saw you that I may not have even told you I had left the agency. I was thinking it would be great to grab lunch at some point over the next couple weeks and catch up, assuming you have the time. Let me know!

Hope all is well.

Michelle

Michelle Rosenthal
Corporate Counsel
Federal Regulatory Affairs
T-Mobile US, Inc.

Office: 202.654-5939
Mobile: 202.607.3435
Fax: 202.654.5963

Joanne Wall

From: Lisa Hone
Sent: Wednesday, April 01, 2015 9:23 PM
To: Debbie Matties
Subject: Re: Hi!

You too.

Original Message
From: Debbie Matties
Sent: Wednesday, April 1, 2015 9:20 PM
To: Lisa Hone
Subject: RE: Hi!

Thanks. Have a good night!

-----Original Message-----
From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Wednesday, April 1, 2015 9:10 PM
To: Debbie Matties
Subject: Re: Hi!

Sure.
202-418-0869.

From: Debbie Matties
Sent: Wednesday, April 1, 2015 9:07 PM
To: Lisa Hone
Subject: RE: Hi!

Sure - that's good. (b) (6) so is it ok if I call you within 5-10 minutes of 9am when he's settled? If so, what's a good number?

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Wednesday, April 1, 2015 8:07 PM
To: Debbie Matties
Subject: RE: Hi!

Hey - that's great.
Sorry, a bit of a crazy day.
Are you free to chat tomorrow at 9am?

From: Debbie Matties [mailto:DMatties@ctia.org]
Sent: Wednesday, April 01, 2015 2:24 PM
To: Lisa Hone
Subject: Hi!

Hi Lisa - How are you? I hear you're going to be at a meeting I'm attending tomorrow at the FCC. Is that true? If so, do you have time for a quick chat?

And this just reminds me how overdue we are for lunch. I fear I dropped a ball somewhere on that.

Debbie Matties
Vice President, Privacy
CTIA-The Wireless Association(r)
1400 16th Street, NW Suite 600
Washington, DC 20036
www.ctia.org<<http://www.ctia.org>>
Direct: 202.736.3654
Wireless: 202.758.7697

Joanne Wall

From: Rosenthal, Michelle <Michelle.Rosenthal1@T-Mobile.com>
Sent: Thursday, May 28, 2015 10:39 AM
To: Lisa Hone
Subject: RE: Lunch

Awesome! See you soon.

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Thursday, May 28, 2015 10:25 AM
To: Rosenthal, Michelle
Subject: RE: Lunch

Great – I will make reservations.

From: Rosenthal, Michelle [mailto:Michelle.Rosenthal1@T-Mobile.com]
Sent: Thursday, May 28, 2015 10:25 AM
To: Lisa Hone
Subject: RE: Lunch

Sure! That's perfect. 12:30?

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Thursday, May 28, 2015 10:09 AM
To: Rosenthal, Michelle
Subject: RE: Lunch

Sadly there is nothing this way.
How would you feel about meeting at Partisan? 709 D St. NW

From: Rosenthal, Michelle [mailto:Michelle.Rosenthal1@T-Mobile.com]
Sent: Thursday, May 28, 2015 9:54 AM
To: Lisa Hone
Subject: Lunch

Hi Lisa,

Does lunch still work for you today at 12:30? My meeting got cancelled, so I am a little more flexible if an earlier or later time works better for you. I'll plan to come your way, but I don't know what is around there for lunch. Any suggestions? I'm happy with casual or sit-down – whatever you prefer. Look forward to catching up!

Michelle

Michelle Rosenthal
Corporate Counsel
Federal Regulatory Affairs
T-Mobile US, Inc.

Office: 202.654-5939
Mobile: 202.607.3435
Fax: 202.654.5963

Joanne Wall

From: Lisa Hone
Sent: Monday, December 21, 2015 5:58 PM
To: Rosenthal, Michelle
Subject: Re: Maureen Cooney's phone number

Thx!

From: Rosenthal, Michelle
Sent: Monday, December 21, 2015 3:42 PM
To: Lisa Hone
Subject: RE: Maureen Cooney's phone number

Sure. Her work line is 703.592.7580, and her cell is 2(b) (6).

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Monday, December 21, 2015 3:35 PM
To: Rosenthal, Michelle
Subject: Maureen Cooney's phone number
Do you have Maureen Cooney's phone number?
Thanks,
Lisa

Joanne Wall

From: FLEMMING, JACQUELYNE <jw1196@att.com>
Sent: Tuesday, June 14, 2016 6:01 PM
To: Lisa Hone
Subject: RE: Meeting dates

I'll get you our list of issues before the end of this week---hopefully tomorrow or Thursday.

Although we will want to talk about some operational issues, we mainly want to discuss the merits of the proposal. After all the comments are in and you have had the opportunity to consider the merits of the various proposals, we are certainly open to a subsequent meeting to talk more about our practices and operationalizing options. Does that work for you?

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Tuesday, June 14, 2016 5:23 PM
To: FLEMMING, JACQUELYNE
Subject: RE: Meeting dates

Ok.

Are there specific issues you know you want to focus on?
That will help us decide who on the team to have join us.

Thanks,

Lisa

From: FLEMMING, JACQUELYNE [mailto:jw1196@att.com]
Sent: Tuesday, June 14, 2016 2:48 PM
To: Lisa Hone <Lisa.Hone@fcc.gov>
Subject: RE: Meeting dates

Your voice mail indicated Friday afternoon as an option. Is Friday, 6/24 at 1pm still an option? I hate Friday afternoon meetings, but this looks like our best option.

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Monday, June 13, 2016 5:55 PM
To: FLEMMING, JACQUELYNE
Subject: RE: Meeting dates

Too bad-- we would love to hear from AT&T's expert about its privacy practices and operationalizing the various options raised by the broadband privacy NPRM and in the comments.

Thanks,

Lisa

From: FLEMMING, JACQUELYNE [mailto:jw1196@att.com]
Sent: Monday, June 13, 2016 5:53 PM
To: Lisa Hone <Lisa.Hone@fcc.gov>
Subject: RE: Meeting dates

You are correct, we want to come in on Privacy. Our Chief Privacy Officer, Lori Fink, will not be joining us.

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Monday, June 13, 2016 5:49 PM
To: FLEMMING, JACQUELYNE
Subject: RE: Meeting dates

You are right, I got ahead of myself by a week.
Just to be clear – I assume you want to come in on privacy, but I don't think your voicemail actually said that.
Is that right?
Will your Chief Privacy Officer be joining you?

Here are possible times.

This week.

Wed. 2:30 or 3:00
Friday. 10, 10:30, 3, 3:30 or 4

Next week.

Tuesday: 11 or 4
Wed: 2:30 or 3:0
Thur: 4

From: FLEMMING, JACQUELYNE [mailto:jw1196@att.com]
Sent: Monday, June 13, 2016 2:52 PM
To: Lisa Hone <Lisa.Hone@fcc.gov>
Subject: Meeting dates

Hi Lisa! Hope all is well on this gorgeous Monday afternoon. I just wanted to confirm that the possible meeting dates that you left on my voice mail are as follows: Tuesday, June 21st after 4pm; Wednesday, June 22nd anytime in the afternoon; Friday, June 24th anytime in the afternoon.

I just wanted to make sure that your references to the available days were for the week beginning June 20th and this week. If you have some available time this week, please let me know that as well.

Thanks,

Jackie Flemming
AVP-External Affairs/Regulatory
AT&T Services
1120 20th St. NW, Suite 1000

Washington, DC 20036

O: (202) 457-3032

C: (202) 531-9801

email:jackie.flemming@att.com

This e-mail and any files transmitted with it are confidential, and are intended solely for the use of the individual or entity to whom this e-mail is addressed. If you are not one of the named recipient(s) or otherwise have reason to believe that you have received this message in error, please notify the sender at [202 457-3032] and delete this message immediately from your computer. Any other use, retention, dissemination, forwarding, printing, or copying of this e-mail is strictly prohibited.

Joanne Wall

From: Lisa Hone
Sent: Monday, May 11, 2015 10:30 AM
To: 'McCready, Margaret (Maggie Mccready)'
Subject: RE: privacy discussion

Please have them call me, and if I am missing in action, have them call the WCB front office line at 418-1500.

From: McCready, Margaret (Maggie Mccready) [mailto:maggie.m.mccready@verizon.com]
Sent: Monday, May 11, 2015 10:26 AM
To: Lisa Hone
Subject: RE: privacy discussion

Thanks. I will take it. Whom should I have the front desk call when we arrive?

Maggie McCready
202-515-2543 (office)
202-281-9272 (cell)

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Monday, May 11, 2015 10:23 AM
To: McCready, Margaret (Maggie Mccready)
Subject: RE: privacy discussion

I am happily surprised to say that it is available – though we will be limited to 30 minutes.

Lisa

From: McCready, Margaret (Maggie Mccready) [mailto:maggie.m.mccready@verizon.com]
Sent: Monday, May 11, 2015 10:20 AM
To: Lisa Hone
Subject: RE: privacy discussion

Sorry for the delay in getting back to you. Is 5/19 at 11 still an option? If so, I would like to confirm it.

Maggie McCready
202-515-2543 (office)
202-281-9272 (cell)

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Thursday, May 07, 2015 11:31 AM
To: McCready, Margaret (Maggie Mccready)
Subject: privacy discussion

Maggie – Here are some times that we could be available for a discussion with Verizon about broadband privacy:

5/15: 1:00; 1:30, 2:00, 2:30; 4:00

5/18: 4:00

5/19: 11am; 4:30pm

Please let me know if any of those work for you.

Thanks,

Lisa Hone

Joanne Wall

From: Lisa Hone
Sent: Friday, January 29, 2016 2:22 PM
To: McCready, Margaret (Maggie Mccready)
Subject: Re: Proposed meeting dates

We are so efficient (today).

From: McCready, Margaret (Maggie Mccready)
Sent: Friday, January 29, 2016 1:43 PM
To: Lisa Hone
Subject: RE: Proposed meeting dates

Sold.
Maggie McCready
202-515-2543 (office)
202-281-9272 (cell)

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Friday, January 29, 2016 1:29 PM
To: McCready, Margaret (Maggie Mccready)
Subject: [E] RE: Proposed meeting dates
Let's do 2/11 at 4pm!
Thanks,
Lisa

From: McCready, Margaret (Maggie Mccready) [mailto:maggie.m.mccready@verizon.com]
Sent: Friday, January 29, 2016 1:26 PM
To: Lisa Hone <Lisa.Hone@fcc.gov>
Subject: Proposed meeting dates
Lisa,

Here are some dates and times that work for Vz to meet with you to discuss the industry proposal. Do any of these work on your end?

Feb 10th 4 PM
Feb 11th 4 PM
Feb 12th 10 or 11 AM
Maggie McCready
202-515-2543 (office)
202-281-9272 (cell)

Joanne Wall

From: Rosenthal, Michelle <Michelle.Rosenthal1@T-Mobile.com>
Sent: Thursday, November 19, 2015 1:19 PM
To: Lisa Hone
Subject: RE: Re: Checking in

Yes. Perfect. I'll call you then.

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Thursday, November 19, 2015 1:11 PM
To: Rosenthal, Michelle
Subject: RE: Re: Checking in

I am now jammed up until 3pm.
Can we try to touch base at 3:05?

From: Rosenthal, Michelle [mailto:Michelle.Rosenthal1@T-Mobile.com]
Sent: Thursday, November 19, 2015 11:23 AM
To: Lisa Hone <Lisa.Hone@fcc.gov>
Subject: RE: Re: Checking in

Just call me whenever you're free, and I'll pop out of my meeting. Cell phone is 202-607-3435 and that will be the best way to reach me.

From: Rosenthal, Michelle
Sent: Thursday, November 19, 2015 8:36 AM
To: Lisa Hone <lisa.hone@fcc.gov>
Subject: RE: Re: Checking in

No worries! I have a call from 1 to 3. Are you free between 12 and 1? Or I could probably go late to the 1 pm call. This should be quick -- 5 mins.

Michelle

-----Original Message-----

From: Lisa Hone [Lisa.Hone@fcc.gov]
Received: Nov 19, 8:14 AM
To: Rosenthal, Michelle [Michelle.Rosenthal1@T-Mobile.com]
Subject: Re: Checking in

Sorry!!!

Crazy day.
And today doesn't look much better.
Are you free early this afternoon?

From: Rosenthal, Michelle
Sent: Wednesday, November 18, 2015 12:01 PM
To: Lisa Hone
Subject: Checking in

Hi Lisa – Hope all is well. Any chance you are free today for a quick call?

Michelle Rosenthal
Senior Corporate Counsel
Federal Regulatory Affairs
T-Mobile US, Inc.
Office: 202.654-5939
Mobile: 202.607.3435
Fax: 202.654.5963

Joanne Wall

From: Lisa Hone
Sent: Thursday, November 19, 2015 1:57 PM
To: McCready, Margaret (Maggie Mccready)
Subject: RE: Stuck in traffic

Do me a favor and let me know when you arrive.

Thx,

-----Original Message-----

From: McCready, Margaret (Maggie Mccready) [mailto:maggie.m.mccready@verizon.com]
Sent: Thursday, November 19, 2015 1:50 PM
To: Lisa Hone <Lisa.Hone@fcc.gov>
Subject: Stuck in traffic

But we will be there as soon as possible.

Joanne Wall

From: Lisa Hone
Sent: Thursday, November 19, 2015 1:52 PM
To: McCready, Margaret (Maggie Mccready)
Subject: RE: Stuck in traffic

Thanks for the heads up

-----Original Message-----

From: McCready, Margaret (Maggie Mccready) [mailto:maggie.m.mccready@verizon.com]

Sent: Thursday, November 19, 2015 1:50 PM

To: Lisa Hone <Lisa.Hone@fcc.gov>

Subject: Stuck in traffic

But we will be there as soon as possible.

Joanne Wall

From: Debbie Matties <DMatties@ctia.org>
Sent: Wednesday, April 22, 2015 10:06 AM
To: Lisa Hone
Subject: RE: thanks for the good suggestion yesterday

Ok!

-----Original Message-----

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Wednesday, April 22, 2015 9:21 AM
To: Debbie Matties
Subject: Re: thanks for the good suggestion yesterday

The agenda will get posted before noon today.

From: Debbie Matties
Sent: Wednesday, April 22, 2015 9:19 AM
To: Lisa Hone
Subject: RE: thanks for the good suggestion yesterday

I'm glad it worked out. :)

Do you happen to know who is moderating the second panel?

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Wednesday, April 22, 2015 8:43 AM
To: Debbie Matties
Subject: thanks for the good suggestion yesterday

Nancy Libin has agreed to be on the panel - appreciate your continued consideration of the issue.

Joanne Wall

From: McCready, Margaret (Maggie Mccready) <maggie.m.mccready@verizon.com>
Sent: Monday, October 19, 2015 12:04 PM
To: Lisa Hone
Subject: RE: thanks

Our privacy policy expert can't make these dates. Do you have options for the following week - Nov 9th?

Maggie McCready
202-515-2543 (office)
202-281-9272 (cell)

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Friday, October 16, 2015 6:00 PM
To: McCready, Margaret (Maggie Mccready)
Subject: [E] RE: thanks

Here are some proposed dates/times to hear about Verizon's new privacy policy.

10/28 at 3:30
10/29 at 3:30
11/4 at 3:30
11/6 at 4pm (just to do something a little different).

Thanks,

Lisa

From: Lisa Hone
Sent: Friday, October 09, 2015 5:28 PM
To: maggie.m.mccready@verizon.com
Subject: thanks

Maggie – I got your message and will try to find some times and get back to you.

Have a good weekend.

Thanks,

Lisa

Lisa Hone
Associate Chief
Wireline Competition Bureau
Federal Communications Commission
202.418.0869
Lisa.Hone@fcc.gov

Joanne Wall

From: McCready, Margaret (Maggie Mccready) <maggie.m.mccready@verizon.com>
Sent: Monday, October 19, 2015 8:00 AM
To: Lisa Hone
Subject: RE: thanks

I can already tell you that the 28th is NOT an option so you can remove that hold. I will be back in touch with what does work. Thanks.

Maggie McCready
202-515-2543 (office)
202-281-9272 (cell)

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Friday, October 16, 2015 6:00 PM
To: McCready, Margaret (Maggie Mccready)
Subject: [E] RE: thanks

Here are some proposed dates/times to hear about Verizon's new privacy policy.

10/28 at 3:30
10/29 at 3:30
11/4 at 3:30
11/6 at 4pm (just to do something a little different).

Thanks,

Lisa

From: Lisa Hone
Sent: Friday, October 09, 2015 5:28 PM
To: maggie.m.mccready@verizon.com
Subject: thanks

Maggie – I got your message and will try to find some times and get back to you.

Have a good weekend.

Thanks,

Lisa

Lisa Hone
Associate Chief
Wireline Competition Bureau
Federal Communications Commission
202.418.0869

Lisa.Hone@fcc.gov

Joanne Wall

From: Matthew DelNero
Sent: Wednesday, April 01, 2015 8:13 PM
To: Lisa Hone
Subject: RE: Thursday meeting

Thanks.

From: Lisa Hone
Sent: Wednesday, April 01, 2015 8:08 PM
To: Matthew DelNero; Jennifer Tatel; Parul Desai
Subject: RE: Thursday meeting

I got an email from Debbie, who I used to work with at the FTC, asking if I am free to chat before the meeting. I will let you know if I learn anything.

Lisa

From: Matthew DelNero
Sent: Wednesday, April 01, 2015 7:24 PM
To: Jennifer Tatel; Lisa Hone; Parul Desai
Subject: FW: Thursday meeting

fyi

From: Scott Bergmann [<mailto:SBergmann@ctia.org>]
Sent: Wednesday, April 01, 2015 4:55 PM
To: Matthew DelNero
Cc: Claude Aiken
Subject: RE: Thursday meeting

Thanks very much, Matt. Attending for CTIA will be Debbie Matties, VP for Privacy and me.

Do you have a sense of who else will attend the meeting from industry (groups)? Thanks!

Scott

From: Matthew DelNero [<mailto:Matthew.DelNero@fcc.gov>]
Sent: Tuesday, March 31, 2015 7:05 PM
To: Scott Bergmann
Cc: Claude Aiken
Subject: RE: Thursday meeting

Scott, it was good to see you last night. Just to confirm, we'll be meeting on Thursday at 3 pm for an informal conversation on privacy. The meeting will be held on the 5th floor. Please ask for Claude Aiken or me when you (or whomever is representing CTIA) arrive. Thanks.

Matt

From: Matthew DelNero
Sent: Monday, March 30, 2015 2:31 PM
To: 'Scott Bergmann'
Subject: Thursday meeting

Hi Scott,

Good to speak with you on Friday. I'm just checking in to see if you had any thoughts about who from CTIA could attend an informal meeting on privacy here at the Commission on Thursday @ 3pm. As I mentioned, VZ and AT&T will be there as well. And we'd certainly be happy to have Sprint and/or T-Mo as well if they're interested.

Thanks,
Matt

Joanne Wall

From: Lisa Hone
Sent: Thursday, February 11, 2016 11:43 AM
To: Debbie Matties; Matthew DelNero; Jennifer Tatel
Subject: RE: Trade association letter on broadband privacy

Thank you.

Lisa

From: Debbie Matties [mailto:DMatties@ctia.org]
Sent: Thursday, February 11, 2016 8:12 AM
To: Matthew DelNero ; Lisa Hone ; Jennifer Tatel
Subject: Trade association letter on broadband privacy

Dear Matt, Lisa and Jennifer,

I hope you're all well this morning. As I spoke to Jennifer and Lisa about yesterday, this morning CTIA and other tech trade associations sent the attached letter to FCC Chairman Wheeler concerning the upcoming broadband privacy proceeding at the FCC.

Best,
Debbie

ctia Everything™
***** Wireless
Debbie Matties
Vice President, Privacy
1400 16th Street, NW Suite 600
Washington, DC 20036
Direct: 202.736.3654
Wireless: 202.758.7697
dmatties@ctia.org

Joanne Wall

From: Lisa Hone
Sent: Thursday, February 25, 2016 5:13 PM
To: Ruth Milkman
Cc: Louisa Terrell
Subject: RE: Updated Privacy Framework from the telecom trades

(b) (5)



From: Ruth Milkman
Sent: Thursday, February 25, 2016 2:41 PM
To: Lisa Hone
Subject: RE: Updated Privacy Framework from the telecom trades

(b) (5)



From: Lisa Hone
Sent: Thursday, February 25, 2016 2:24 PM
To: Ruth Milkman <Ruth.Milkman@fcc.gov>; Louisa Terrell <Louisa.Terrell@fcc.gov>; Gigi Sohn <Gigi.Sohn@fcc.gov>; Stephanie Weiner <Stephanie.Weiner@fcc.gov>; Matthew DelNero <Matthew.DelNero@fcc.gov>; Jonathan Sallet <Jonathan.Sallet@fcc.gov>; Jennifer Tatel <Jennifer.Tatel@fcc.gov>; Philip Verveer <Philip.Verveer@fcc.gov>; Shannon Gilson <Shannon.Gilson@fcc.gov>; Eric Feigenbaum <Eric.Feigenbaum@fcc.gov>
Subject: Fw: Updated Privacy Framework from the telecom trades

The telecom companies and associations have tweaked their framework a bit.

See Debbie Matties' email below and attachment.

Lisa

From: Debbie Matties <DMatties@ctia.org>
Sent: Thursday, February 25, 2016 2:09 PM
To: Lisa Hone
Subject: Updated Privacy Framework from the telecom trades

Hi Lisa,

Maggie mentioned to you that we had made a few revisions to the Privacy Framework that we had given you back in December. I've attached the new version here, dated February 19.

We made two substantive changes on the last page. First, at the top, we added "The provider should consider the sensitivity of the data and the context in which it was collected when determining the appropriate choice mechanism." Second we reworked the data breach bullet. We also made a few stylistic edits on the earlier pages in anticipation of releasing it publicly.

Please let me know if you have any questions.

Best,
Debbie

ctia Everything™
***** Wireless
Debbie Matties
Vice President, Privacy
1400 16th Street, NW Suite 600
Washington, DC 20036
Direct: 202.736.3654
Wireless: 202.758.7697
dmatties@ctia.org

Joanne Wall

From: Lisa Hone
Sent: Tuesday, November 10, 2015 5:55 PM
To: McCready, Margaret (Maggie Mccready)
Cc: Latoya Toles
Subject: RE: Vz Privacy Policy meeting

Great – I have scheduled a room. You can have the security desk contact Latoya Toles, copied here, when you arrive.

I expect the following people to attend:

Matt DelNero, WCB Bureau Chief
Melissa Kirkel, TAPD Assistant Director
John Visclosky, TAPD
Kristine Fargotstein, TAPD
Zac Ross, TAPD
David Brody, TAPD
Jennifer Tatel, Associate General Counsel
Doug Klein, OGC

Lisa

Lisa Hone
Associate Chief
Wireline Competition Bureau
Federal Communications Commission
202.418.0869
Lisa.Hone@fcc.gov

From: McCready, Margaret (Maggie Mccready) [mailto:maggie.m.mccready@verizon.com]
Sent: Tuesday, November 10, 2015 9:20 AM
To: Lisa Hone
Subject: Vz Privacy Policy meeting

Lisa,
Thursday Nov 19th at 2 PM works for Vz to meet with you to discuss our new privacy policy. Hopefully that still works on your end. Please let me know, and if it works, whom should we have the desk contact for access? A few of the Vz attendees do not have visitor badges. Thanks.

Maggie McCready
202-515-2543 (office)
202-281-9272 (cell)

Joanne Wall

From: Lisa Hone
Sent: Thursday, February 11, 2016 4:00 PM
To: McCready, Margaret (Maggie Mccready)
Subject: Re: We are here

Are they sending you up to 5?

Original Message

From: McCready, Margaret (Maggie Mccready)
Sent: Thursday, February 11, 2016 3:49 PM
To: Lisa Hone
Subject: We are here

But the guard can't reach anyone to let us up.
Sent from Divide managed by MobileIron

Joanne Wall

From: Debbie Matties <DMatties@ctia.org>
Sent: Friday, May 29, 2015 10:42 AM
To: Lisa Hone
Subject: RE: Wed?

Sounds great! I've never been to your house, and of course I love brownies. See you then!

-----Original Message-----

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Friday, May 29, 2015 10:28 AM
To: Debbie Matties
Subject: RE: Wed?

Great.

Do you want to come over to my house at about 4pm?

(b) (6)

Spring Mill just opened in my neighborhood, so I will get some of their crazy good brownies to munch on.

Lisa

-----Original Message-----

From: Debbie Matties [mailto:DMatties@ctia.org]
Sent: Thursday, May 28, 2015 11:04 PM
To: Lisa Hone
Subject: RE: Wed?

You're very brave.

Look forward to seeing you tomorrow afternoon. Let me know where you'd like to meet and we can firm up the time as you better know your schedule. And no worries - this gives me an excuse to leave work early! :)

-----Original Message-----

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Thursday, May 28, 2015 11:19 AM
To: Debbie Matties
Subject: RE: Wed?

(b) (6)

(b) (6)

I have to leave here at 4:30, so let's work on the (b) (6) option.

I should be back (b) (6) no later than 3pm (and hopefully much sooner).

Sorry it's so complicated,

Lisa

-----Original Message-----

From: Debbie Matties [mailto:DMatties@ctia.org]
Sent: Thursday, May 28, 2015 10:46 AM
To: Lisa Hone
Subject: RE: Wed?

If 4:30 today doesn't interfere (b) (6) then I'm pretty sure I could meet you in (b) (6) tomorrow afternoon.

-----Original Message-----

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Thursday, May 28, 2015 10:38 AM
To: Debbie Matties
Subject: RE: Wed?

What are you doing late tomorrow afternoon?

You want to swing my (b) (6)?

-----Original Message-----

From: Debbie Matties [mailto:DMatties@ctia.org]
Sent: Thursday, May 28, 2015 10:34 AM
To: Lisa Hone
Subject: RE: Wed?

Any chance 5:30 today would work?

-----Original Message-----

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Thursday, May 28, 2015 10:19 AM
To: Debbie Matties
Subject: RE: Wed?

I am travelling Monday - Thursday and pretty booked on Friday.

-----Original Message-----

From: Debbie Matties [mailto:DMatties@ctia.org]
Sent: Thursday, May 28, 2015 10:14 AM
To: Lisa Hone
Subject: RE: Wed?

(b) (6) s. I think today isn't going to happen, sadly. How about next week? Monday after 3:30, Tuesday anytime except lunchtime, or Wednesday around 1:30 or after? As of now, I have my (b) (6) meeting from 12-1:15 at the Constitution Center, so will be right in your hood. (But sometimes it might get moved to the following week, in which case I'd be free for lunch Wednesday!)

-----Original Message-----

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Thursday, May 28, 2015 9:57 AM
To: Debbie Matties
Subject: RE: Wed?

Thanks for the heads up.
Doesn't sound promising.

I am working from home tomorrow (b) (6), and I have conference calls all morning.

-----Original Message-----

From: Debbie Matties [mailto:DMatties@ctia.org]
Sent: Thursday, May 28, 2015 9:54 AM
To: Lisa Hone
Subject: RE: Wed?

(b) (6) Still hopeful that I can get out of here by 10:30 to meet you at 11, but not certain anymore. Any chance you have some time tomorrow in case I can't get out of here? And I have a departure lunch at noon (b) (6) who is moving to NY - can't miss it.

-----Original Message-----

From: Debbie Matties
Sent: Wednesday, May 27, 2015 9:44 AM
To: Lisa Hone
Subject: RE: Wed?

Yes, that's fine. If I free up earlier do you have flexibility? And where do you propose? I'll be coming by cab so it doesn't need to be near a metro.

-----Original Message-----

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Wednesday, May 27, 2015 9:41 AM
To: Debbie Matties
Subject: RE: Wed?

Sure, if you don't mind coming down here.

Lisa

-----Original Message-----

From: Debbie Matties [mailto:DMatties@ctia.org]
Sent: Wednesday, May 27, 2015 9:35 AM
To: Lisa Hone
Subject: RE: Wed?

No worries. Tomorrow I could meet around 11 - does that work? (b) (6)

(b) (6)

(b) (6)

-----Original Message-----

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]
Sent: Wednesday, May 27, 2015 9:27 AM
To: Debbie Matties
Subject: RE: Wed?

Sorry, I dropped the ball because this week is ugly and next week I am travelling Monday - Thursday.

Any chance you are free to grab coffee Thursday morning.

(b) (6)

Lisa

-----Original Message-----

From: Debbie Matties [mailto:DMatties@ctia.org]

Sent: Saturday, May 23, 2015 8:40 AM

To: Lisa Hone

Subject: RE: Wed?

(b) (6)

Wednesday I am free until about 1:30 - have two back-to-back doctor appointments in the afternoon from 2- 5.

-----Original Message-----

From: Lisa Hone [mailto:Lisa.Hone@fcc.gov]

Sent: Friday, May 22, 2015 6:54 PM

To: Debbie Matties

Subject: Wed?

(b) (6)

Do you want to grab coffee on Wednesday afternoon?

Lisa

Joanne Wall

From: Lisa Hone
Sent: Wednesday, October 07, 2015 5:57 PM
To: Matthew DelNero; Melissa Droller Kinkel; Jennifer Tatel
Subject: RE: What Verizon's privacy updates really mean

Maggie called me back to give me the heads up about this earlier today - (b) (6).

Lisa

Lisa Hone
Associate Chief
Wireline Competition Bureau
Federal Communications Commission
202.418.0869
Lisa.Hone@fcc.gov

From: Matthew DelNero
Sent: Wednesday, October 07, 2015 4:08 PM
To: Lisa Hone ; Melissa Droller Kinkel ; Jennifer Tatel
Subject: FW: What Verizon's privacy updates really mean

fyi

From: Verizon Public Policy [<mailto:public.policy=verizon.com@mail254.suw14.mcdlv.net>] **On Behalf Of** Verizon Public Policy
Sent: Wednesday, October 07, 2015 3:19 PM
To: Matthew DelNero <Matthew.DelNero@fcc.gov>
Subject: What Verizon's privacy updates really mean

Our privacy policy is based on three simple but powerful principles: Transparency, Choice, and Control.

[View this email in your browser](#)



What Verizon's privacy updates really mean

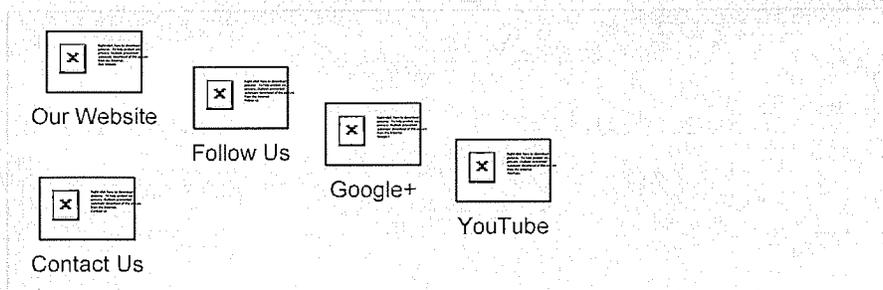
By Karen Zacharia, Chief Privacy Officer

Earlier this week, we started proactively telling our wireless customers how Verizon and AOL will work together, including how the combination will help deliver services that are more personalized and useful to them, and the choices they can make to control the use of their information.

The Verizon family of companies offers a wide and growing variety of free services that are made possible by advertising. The best type of advertising provides content that customers may actually want, and this is what we want to give to our customers. To that end, starting in November we are combining Verizon's existing Wireless advertising programs – Relevant Mobile Advertising and Verizon Selects – with the AOL Advertising Network. The combination will help make the ads our customers see more relevant to them, and therefore more useful, across the different devices and services they see.

We are making some changes to how the Verizon programs will operate. In particular, we are changing who will receive the Verizon advertising identifier, known as a Unique Identifier Header (UIDH)... (MORE)

Continue reading this post on the Verizon Policy Blog.



[About](#) [Verizon](#) [News](#) [Center](#) [Careers](#) [Responsibility](#)

Copyright © 2015 Verizon, All rights reserved.
[unsubscribe from this list](#) [update subscription preferences](#)

Joanne Wall

From: Debbie Matties <DMatties@ctia.org>
Sent: Monday, December 07, 2015 9:43 PM
To: Lisa Hone
Subject: Re: Where r u?

Sorry just saw this. I really should be better about checking my wireless device. ?

Sent from my iPhone

On Dec 7, 2015, at 8:35 PM, Lisa Hone <Lisa.Hone@fcc.gov<mailto:Lisa.Hone@fcc.gov>> wrote:

Joanne Wall

From: Lisa Hone
Sent: Wednesday, April 22, 2015 8:43 AM
To: Debbie Matties (DMatties@ctia.org)
Subject: thanks for the good suggestion yesterday

Nancy Libin has agreed to be on the panel – appreciate your continued consideration of the issue.

Joanne Wall

From: Lisa Hone
Sent: Friday, October 09, 2015 5:28 PM
To: maggie.m.mccready@verizon.com
Subject: thanks

Maggie – I got your message and will try to find some times and get back to you.

Have a good weekend.

Thanks,

Lisa

Lisa Hone
Associate Chief
Wireline Competition Bureau
Federal Communications Commission
202.418.0869
Lisa.Hone@fcc.gov

Joanne Wall

From: McCreedy, Margaret (Maggie McCreedy) <maggie.m.mccreedy@verizon.com>
Sent: Thursday, February 04, 2016 7:48 AM
To: Lisa Hone

Hi Lisa,
Just checking in to see if coffee tomorrow afternoon at 2 still works for you. If so, I will see you then.

Maggie McCreedy
202-515-2543 (office)
202-281-9272 (cell)

Joanne Wall

From: McCready, Margaret (Maggie Mccready) <maggie.m.mccready@verizon.com>
Sent: Friday, February 05, 2016 2:02 PM
To: Lisa Hone

I am at Starbucks now.

Sent from Divide managed by MobileIron

Joanne Wall

From: Rosenthal, Michelle <Michelle.Rosenthal1@T-Mobile.com>
Sent: Friday, September 18, 2015 10:58 AM
To: Lisa Hone
Subject: Update and question for you

Hey Lisa,

I wanted to check in on our previous conversation and also ask you a quick question. Do you have 5 minutes to chat this morning or afternoon? I have a lunch at 12 and a couple afternoon meetings, but if you're free, let me know your availability, and I'll give you a quick call.

Happy Friday!

Michelle

Michelle Rosenthal
Corporate Counsel
Federal Regulatory Affairs
T-Mobile US, Inc.
Office: 202.654-5939
Mobile: 202.607.3435
Fax: 202.654.5963

Joanne Wall

From: McCreedy, Margaret (Maggie Mccreedy) <maggie.m.mccreedy@verizon.com>
Sent: Tuesday, November 10, 2015 9:20 AM
To: Lisa Hone
Subject: Vz Privacy Policy meeting

Lisa,
Thursday Nov 19th at 2 PM works for Vz to meet with you to discuss our new privacy policy. Hopefully that still works on your end. Please let me know, and if it works, whom should we have the desk contact for access? A few of the Vz attendees do not have visitor badges. Thanks.

Maggie McCreedy
202-515-2543 (office)
202-281-9272 (cell)

Privacy Framework

Draft Discussion Paper

All entities in the Internet ecosystem should be subject to a consistent privacy framework with respect to consumer information. Consumer information should be protected based upon the sensitivity of the information to the consumer and how the information is used—not the type of business keeping it, how that business obtains it, or what regulatory agency has authority over it. Consumers should have consistent and predictable privacy protections for the information they deem private and sensitive, no matter how or with whom they share it. Government regulation should not give some players in the Internet ecosystem a competitive advantage over others because it would stifle the emergence of new business models and thwart new uses of data that foster increased consumer choice and service customization.

The FCC should adopt an approach to privacy and data security for CPNI that is flexible, harmonized with the well-established and successful FTC framework, and backed up by strong but fair enforcement for unfair or deceptive acts or practices (UDAP) that materially harm consumers.¹ This well-tested consumer protection approach is consistent with the FCC's privacy recommendations in the 2010 National Broadband Plan, the FTC's and White House's 2012 Privacy Reports, and the White House's 2015 Consumer Privacy Bill of Rights, as well as with Chairman Wheeler's recent testimony before Congress acknowledging the importance of coordination with the FTC and harmonization with its privacy framework.

That approach will benefit consumers by safeguarding privacy interests as it has for years and will ensure that the same privacy and security framework applies to all entities in the Internet ecosystem. By relying upon a tested privacy model, the FCC will avoid arbitrarily inconsistent requirements that could otherwise hamper innovation and reduce competition. Most important, it will minimize consumer confusion as well as other harms associated with disparate privacy regulation across the ecosystem. Indeed, this approach will align with consumers' expectations that their data would be subject to the same privacy rules regardless of whether it is used by their Internet Service Provider (ISP), application developers, operating systems, or edge providers.

¹ This framework is intended for discussion purposes, and we are not conceding that the FCC has authority to adopt privacy and security rules for Broadband Internet Access Services or over data related to consumers' use of Broadband Internet Access Services. To the extent it is determined that the FCC has such statutory authority, this document is intended to set forth principles for FCC consideration and possible adoption that are harmonized and consistent with the FTC and other government entities' approach to privacy and security for the same or similar data. Even if courts determine that the FCC's reclassification of Broadband Internet Access Services is a lawful exercise of authority, any rules must not exceed the text and legislative history of Section 222 of the Act.

When adopting a framework, the FCC should keep the following guidelines in mind:

- Consistent and Coordinated Regulatory Regimes. The FCC's rules and principles for regulating and enforcing privacy and security should be as similar as possible to the FTC approach, which will continue to govern other Internet ecosystem players' use and disclosure of the same or similar data. The consistent application of standards across sectors would fulfill the following key tenets in the White House Privacy Report: (1) avoid "inconsistent standards for related technologies" that could dampen innovation; (2) foster a "level playing field for companies;" and, most importantly, (3) create "a consistent set of expectations for consumers." To achieve this end, the FCC's policies, rules, and enforcement practices should conform to the longstanding limiting principles articulated in the FTC's Unfairness and Deception Policy Statements. In addition, the FCC and FTC can achieve their recent MOU's stated goal of avoiding "duplicative, redundant or inconsistent oversight" by developing a new process to ensure that their substantive privacy policies and basis for enforcement are consistent going forward.
- Flexibility. The FCC's approach should provide a flexible framework within which telecommunications service providers can implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments in this space. Specifically, this framework should identify the privacy or security *goals*, and afford providers flexibility in achieving those goals, rather than dictate the particular *methods* by which providers are expected to achieve those goals. Adopting a flexible approach also will help ensure consistent federal and state requirements governing customer information.
- Application. Consistent with the Communications Act and to eliminate unnecessary duplication of authority with other agencies, the FCC's framework should only apply when 1) telecommunications service providers are providing telecommunications services and 2) the CPNI is made available by the customer to the telecommunications service provider solely by virtue of the carrier-customer relationship. The framework cannot lawfully apply to:
 - Providers' non-telecommunications services and products
 - Providers' non-telecommunications service provider affiliates
 - Information that is not made available to the carrier by the customer solely by virtue of the carrier-customer relationship
- Individually Identifiable. The FCC should carve out from the scope of its new framework any data that is de-identified, aggregated, or does not otherwise identify a known individual. The insights derived from the use of de-identified data can offer great benefits to consumers and society and such use avoids the sensitivities that may be associated with identified data.

- Unfair or Deceptive Conduct. As noted above, the FCC’s policies, rules, and enforcement practices should conform to the FTC’s longstanding limiting principles articulated in its Policy Statements on Unfairness (1980) and Deception (1983). This approach is consistent with the FCC’s commitment to conduct a cost-benefit analysis of its regulatory framework in accordance with President Obama’s Executive Orders 13563 and 13579, which require agencies to “adopt a regulation only upon a reasoned determination its benefits justify its costs” and “tailor its regulations to impose the least burden on society.”
 - Unfair Conduct. A provider acts unfairly if its act or practice (1) causes or is likely to cause substantial injury to consumers (2) which is not reasonably avoidable by consumers themselves, and (3) is not outweighed by countervailing benefits to consumers or to competition.
 - Deceptive Conduct. A provider acts deceptively if (1) it makes a statement or omission, or engages in a practice, that is likely to mislead a consumer, (2) viewed from the perspective of a consumer acting reasonably under the circumstances, and (3) the deceptive statement, omission, or practice is material—meaning that the misrepresentation or practice is likely to affect the consumer’s conduct or decision with regard to a product or service.
- Additional Guidance. In coordination with other privacy regulators, the FCC could, like the FTC and various states like California, provide additional guidance on how it interprets its framework through workshops or reports. The FCC also could encourage and support the development and implementation of industry guidelines.
- Update and Harmonize Existing CPNI Rules. The existing CPNI rules should be revisited in their entirety and modernized to use the same flexible framework for all services subject to Section 222, including traditional voice services. In no event should the prescriptive outdated rules designed for legacy voice services apply to broadband services. Instead, a common set of flexible policies that allow providers to keep up with their customers’ expectations and evolving technology should apply to both types of services.

With these guidelines in mind, and only to the extent the FCC has the requisite jurisdiction, the FCC could adopt the following principles, which encompass and are consistent with the privacy and security framework that applies to the rest of the industry. Each of these principles and the goals noted above should provide flexibility for providers to implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments:

- Transparency. A telecommunications service provider should provide notice, which is neither deceptive nor unfair, describing the CPNI that it collects, how it will use the CPNI, and whether and for what purposes it may share CPNI with third parties.

- Respect for Context and Consumer Choice. A telecommunications service provider may use or disclose CPNI as is consistent with the context in which the customer provides, or the provider obtains, the information, provided that the provider's actions are not unfair or deceptive. For example, the use or disclosure of CPNI for the following commonly accepted data practices would not warrant a choice mechanism, either because customer consent can be inferred or because public policy considerations make choice unnecessary: product and service fulfillment, fraud prevention, compliance with law, responses to government requests, network management, first-party marketing, and affiliate sharing where the affiliate relationship is reasonably clear to consumers. Consistent with the flexible choice mechanisms available to all other entities in the Internet ecosystem, telecommunications service providers should give consumers easy-to-understand choices for non-contextual uses and disclosures of their CPNI, where the failure to provide choice would be deceptive or unfair.
- Data Security. A telecommunications service provider should establish, implement, and maintain a CPNI data security program that is neither unfair nor deceptive and includes reasonable physical, technical, and administrative security safeguards to protect CPNI from unauthorized access, use, and disclosure. Providers' CPNI data security programs should provide reasonable protections in light of the nature and scope of the activities of the company, the sensitivity of the data, and the size and complexity of the relevant data operations of the company.
- Data Breach Notifications. Telecommunications service providers should notify customers whose CPNI has been breached when such breach is likely to cause substantial harm to customers and failure to notify would be unfair or deceptive. Telecommunications providers have flexibility to determine how and when to provide such notice.

The FCC can ensure compliance with the above principles by pursuing reasonable enforcement actions against telecommunications service providers that have clearly violated these principles.

American Cable Association
Competitive Carriers Association
CTIA
National Cable & Telecommunications Association
US Telecom – The Broadband Association

Dated: December 16, 2015