Michael Wells
Chief Technical Officer
Regulatory Authority
1st Floor, Craig Appin House
8 Wesley Street
Hamilton, Bermuda

Center for Democracy & Technology's Response to Consultation Document:
Comments on Open Internet Framework General Determination

June 28, 2019

Dear Mr. Wells,

The Center for Democracy & Technology (CDT) respectfully submits these comments in response to the questions raised in the Regulatory Authority's consultation document regarding the open internet. CDT applauds the Regulatory Authority of Bermuda for its thorough and thoughtful consideration of the principles supporting the concept of net neutrality as well as the practical issues with implementing a regulatory scheme to preserve an open internet, and we welcome this opportunity to provide feedback on its Open Internet Consultation Document.

CDT is a nonprofit public interest group that seeks to promote free expression, privacy, individual liberty, and technological innovation on the open, decentralized internet. CDT supports laws, corporate policies, and technical tools that protect the civil liberties of internet users. CDT represents the public's interest in an open internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

We commend the Regulatory Authority for producing a promising set of proposed regulations and offer the following responses for its consideration.

Respectfully,

Stan Adams, Open Internet Counsel,
Center for Democracy & Technology

Heidi Verheggen, Stanford Law School
Juris Doctor Candidate, 2021

Comments of the Center for Democracy & Technology on the Bermuda Regulatory Authority's Open Internet Consultation Document

Overview

CDT believes that the Regulatory Authority of Bermuda has crafted a strong set of proposals that are likely to provide adequate safeguards to preserve internet openness. We generally take a positive view of all the proposals in the consultation document and offer more specific recommendations on the policies for zero-rating, traffic management, ISP obligations, and end-users' right to access and distribute content of their choice. While we do not offer more detailed comments for the Authority's proposals on ISP regulatory surveys, end-users' obligations and choice of terminal equipment, or technical and contract monitoring, CDT supports these proposals as general means of ensuring transparency, regulatory compliance, and accountability, which will help maintain the Authority's effectiveness in implementing its open internet regulations.

V.A.1 Zero-rating

1) **Please comment on the proposal of assessing zero-rating tariffs and whether the Authority should take a position as part of its open internet framework.**

CDT fully supports the Authority's proposal for assessing zero-rating tariffs. CDT was at the forefront of efforts to describe the impacts of various differential pricing programs on internet openness and cautioned against the adoption of certain forms of differential pricing programs.[1] Subsequent studies have indicated that many zero-rating practices indeed pose a significant threat to open internet principles. For instance, a recent study found that Chilean net neutrality regulations, which prohibit both negative discrimination, such as blocking, and positive discrimination, such as prioritization, effectively prevented discriminatory forms of zero-rating.[2] When the regulations were subsequently narrowed to only prohibit negative practices, however, more discriminatory forms of zero rating arose that differentiated accessibility based on content.[3]

---

[1] *See* Erik Stallman & Stan Adams, *Zero Rating: A Framework for Assessing Benefits and Harms* (Jan. 13, 2016), https://cdt.org/insight/zero-rating-a-framework-for-assessing-benefits-and-harms/

[2] Marco Correa Perez, *Zero-rating, Positive Net Neutrality, and Understanding the Chilean Regulation*, 3-4, (May 17, 2018), http://globalnetpolicy.org/research/zero-rating-net-neutrality-and-understanding-the-chilean-regulation/

[3] *Id*. at 5.

Similarly, a compilation of case studies evaluating the impact of Facebook's free social media initiatives in a variety of countries found that, for users who could not afford an alternative to the company's zero-rated service, the platform incorporated significant barriers that could discourage or prevent access to the full variety of content that the open internet would offer.[4] CDT therefore believes that a proactive policy addressing discriminatory forms of differential pricing is a critical component of any open internet framework and supports the Authority's proposed criteria for evaluating zero-rated tariffs.[5]

2) Please comment on the proposed criteria for assessing whether zero-rating tariffs should be permitted.

CDT's early work on zero-rating provides an in depth analysis of several criteria for evaluating this practice and largely affirms the Authority's proposed approach. Each individual factor of the Authority's proposed criteria is discussed in more detail below.

The degree to which the treatment of data is neutral

There is an inherent tension between a strict view of net neutrality and traffic management techniques that treat some kinds data differently than others, from a technical perspective. However, in many (if not all) forms of differential pricing, there is no technical difference in the treatment of differing data types. Rather, the only difference is whether or not the data counts against a user's data allotment. Therefore, it is important to clarify what kind of treatments are within the scope of the proposed approach. In the context of this criteria, CDT will assume that "treatment" refers to economic treatment—whether a particular datum will be counted as part of a user's allotment or not counted under a zero-rating offering.

Restrictions on the type of content or applications that may be zero-rated undermine the overall diversity of available content, thereby reducing its relevance for many users. Further, limitations as to certain types or sources of content undermine the net neutrality principles of application and content agnosticism, and pose risks of market distortion similar to the risks posed by exclusive or sponsored zero-rating arrangements. Programs limited particular providers within a class of applications or content are more problematic than those limited to a particular class of applications. Service-specific packs, such as those that bundle an application or suite of applications with voice and SMS messaging, carry a risk of market distortion that must be weighed against potential gains in broadband adoption.

When a zero-rating arrangement exempts from metered pricing all OTT providers within a particular class of applications, the potential harms of zero-rating are reduced, but not altogether eliminated. In all cases, the regulatory authority should consider the carrier's eligibility requirements for providers

[4] Global Voices, *Free Basics in Real Life* (Jul. 27, 2017), https://advox.globalvoices.org/2017/07/27/can-facebook-connect-the-next-billion/

[5] Bermuda Regulatory Authority, *Open Internet Consultation*, matter 20190520, pg. 15, ¶ 52 (May 20, 2019).

wishing to join zero rated offerings to ensure that those requirements are not themselves discriminatory toward would-be providers.

The impact on internet openness and innovation

User choice is one of the central virtues of the open internet. The power of the open internet as an engine of free expression, innovation, and economic opportunity is linked directly to the end-to-end principle that allows users to access the content and application of their choice on the platforms and devices of their choice. The more that zero-rating deviates from that principle, the greater the risk it poses to the open internet.

Unfortunately, a key feature of zero-rating arrangements makes them likely to deviate from this principle. A central paradox of zero-rated packages and platforms is that the easier it is for OTT providers to participate in zero-rating arrangements, the less likely it is that zero-rating will distort markets or foreclose competition. At the same time, the more available zero-rated content and services are to users, the less likely they are to access metered substitutes. In CDT's view, market distortion poses a greater risk and the scales should therefore tip in favor of nondiscrimination and openness.

To the degree that compromise is possible, the most 'open' zero-rating arrangements are those that give the user a certain allotment of data to use in the manner of their choice.[6] However, even these practices are not wholly unproblematic. While some would argue that they are not properly considered zero-rating because they apply to all potential sources of content and applications equally, these arrangements may still be tied to accessing content through a particular browser or on a particular device. Although constraints on devices, operating systems, or browsers may be distinct from constraints on applications and content, they undermine users' ability to access content on the device of their choice. Protection of this ability has been a core net neutrality principle to ensure the openness of the internet.

Whether the offering is exclusive to certain customers or certain content providers

Zero-rating is perhaps most problematic when it allows an OTT provider not only to receive favorable (unmetered) treatment of its own content over its competitors, but also to exclude those competitors from establishing a similar preference for their own content. Particularly where the network operator offering the zero-rating arrangement has market power, an exclusive zero-rating arrangement creates a distorted playing field that forecloses competition from existing OTT providers and new entrants.

Exclusivity can be a two-way street in the sense that OTT providers may choose to partner with only one or two carriers in a certain region. This form of

[6] *See* Denelle Dixon-Thayer, *Mozilla View on Zero Rating*, Mozilla (May 5, 2015) https://blog.mozilla.org/netpolicy/2015/05/05/mozilla-view-on-zero-rating/; Mitchell Baker, *Zero Rating and the Open Internet* (May 6, 2015), https://blog.lizardwrangler.com/2015/05/06/zero-rating-and-the-open-internet/.

exclusivity could lock in an incumbent carrier's market dominance and discourage new broadband competitors from entering the market. These concerns are amplified when both the carrier and OTT provider have market power. Non-exclusivity policies should therefore be a common feature for both network operators and OTT providers participating in zero-rating or other forms of metering exemptions.

Whether there is financial compensation is involved

Conditioning zero-rating on an exchange of payment can constructively exclude resource-constrained OTT providers from participating in zero-rating arrangements. OTT providers with greater bargaining strength will be more likely to receive favorable terms than their competitors and even when sponsored zero-rating arrangements are offered to all OTT providers on equal terms, they will tend to favor those OTT providers with greater resources. Even assuming that the cost of sponsoring data is low, sponsored data arrangements present the same 'pay-to-play' concerns as paid prioritization.[7]

Some supporters of sponsored data arrangements claim that emerging OTT providers could use zero-rating to gain a "fighting chance of competing with the entrenched giant by differentiating itself."[8] However, between an established market participant with a steady stream of income and a relative newcomer, the former seems more likely to have the ability—if not the willingness—to pay. And reliance on a commercial arrangement with a carrier rather than succeeding on the merits of their new offering is exactly the type of market distortion that open internet protections should seek to prevent.

To summarize, CDT agrees with the Authority's evaluation criteria for zero-rating practices. It is important to evaluate the impact of these practices on the open internet and broadband adoption according to both the specific zero-rating arrangement's influence on edge providers and users, as well as the attributes of the broadband market in which the arrangement is offered. With respect to OTT providers, the overriding concern is the potential for market distortion as OTT providers are either excluded from preferential arrangements or coerced to modify their content and services to benefit from them.

Thus, whether arrangements are exclusive (particularly exclusive to affiliates of the network operator), sponsored, or limited to particular sources or types of content and applications are all highly relevant considerations. For users, the ability to maintain the control of the content and services they access or create via the internet is the overriding consideration. User choice in selecting zero-rated content, the availability and cost of metered content, and the transparency of zero-rating arrangements are significant factors in determining whether zero-rating can spur broadband adoption and access to the open internet. Finally, whether zero-rating will serve as an on-ramp to "full" internet access or

---

[7] *See* David Sohn, *The Dangers of Sponsored Data*, CDT (Jan. 8, 2014) https://cdt.org/blog/the-dangers-of-"sponsored-data"/. *See also*, Stan Adams, *Paid Prioritization: We Have Solved This Problem Before*, CDT (April 23, 2018), https://cdt.org/blog/paid-prioritization-we-have-solved-this-problem-before/.

[8] Protecting and Promoting the Open Internet, *Report and Order on Remand*, 30 FCC Rcd 5601 ¶ 151, n.362, (quoting Free State Reply Comments at 14-15), (hereinafter "FCC Open Internet Order").

a roundabout of curated offerings that users exit only at great effort and expense, if at all, depends on some fundamental attributes of the broadband market: existing levels of adoption and deployment, competition, digital literacy and education. On this point, CDT notes that Bermuda enjoys relatively high rates of adoption, generally, and with respect to mobile cellular connections, specifically.[9] Arguments in favor of zero-rating as an adoption mechanism are therefore less compelling than for locations with lower rates of adoption and use.

While many of the factors for evaluating zero-rating arrangements are interdependent, CDT believes that there are several general principles the Authority should abide by in assessing these practices and their relationship to net neutrality and broadband adoption:

- Exclusive or affiliate-only arrangements should not be undertaken;
- Sponsored data arrangements should be disfavored;
- Eligibility to participate in a zero-rating arrangement should not depend on degrading security or sacrificing user privacy;
- Both the OTT provider-facing and user-facing terms of ISPs' zero-rating arrangements should be transparent;
- Zero-rating as a broadband adoption strategy should be accompanied by both technical assistance for OTT providers and digital training and education for users;
- Regulators should be clear about the terms and process by which they will assess zero-rating services.

CDT supports the Authority's proposed evaluation criteria because they appear capable of satisfying these principles.

3) Please comment on the preliminary position described by the Authority relating to zero-rating.

Based on concerns raised by its own analysis and by subsequent studies of other advocacy organizations, CDT fully supports the Authority's preliminary position not to allow zero-rated tariffs due to their anti-competitive nature.

4) Please comment on how the Authority can oversee tariffs offered by ICOLs, specifically if the tariffs may raise concerns relating to an open internet framework.

One way for the Authority to conduct oversight of zero-rating tariffs would be to incorporate reporting requirements on differential pricing practices into its existing transparency obligations for ISPs. For instance, providers should disclose to regulators information about how their differential pricing schemes work, including technical and substantive requirements for participating in their schemes, how they measure usage and track various data streams. ISPs should also provide information to consumers about how their differential pricing schemes are implemented and the alternative options available. CDT believes that with careful monitoring and proper reporting incentives, concerns surrounding such practices can be effectively managed.

---

[9] The World Bank, *Individuals using the internet (% of population),* https://data.worldbank.org/indicator/IT.NET.USER.ZS?name_desc=false.

V.A.2 Traffic management

5) Please comment on the Authority's proposed position regarding traffic management.

CDT generally agrees that reasonable traffic management practices can and should be allowed under specific circumstances, including those identified by the Authority, i.e., during periods of high levels of congestion or in response to threats to the security of the network. It is critical, however, that providers disclose the management practices they use, including information about how, when, and for how long those practices are employed.

6) Please comment on the specific idea of banning blocking, throttling or prioritization of internet access traffic.

Since blocking, throttling and paid prioritization all pose significant threats to the openness and accessibility of the internet for all, CDT fully supports a policy that would prohibit these practices to preserve net neutrality. However, CDT advises the Authority to consider carefully the way it defines the concept of prioritization; ideally, ISPs should be allowed to perform some prioritization of traffic to improve the quality of experience for their subscribers, so long as that prioritization is not motivated by anti-competitive incentives, such as favoring affiliates or coercing OTT providers to pay for priority treatment.

7) Please comment on how and when traffic management should be allowed and how the behavior of ICOLs can be assessed as part of an open internet framework.

In CDT's view, traffic management practices should be allowed when they are intended to improve or protect network functionality, but not when they serve other "business" or "commercial" purposes that may relate to an ISP's motives to influence competition among OTT providers or that create discriminatory effects among providers.[10] This allows network operators to treat different kinds of traffic differently while maintaining the kind of neutrality the regulations intend to protect. Generally, the goal of open internet regulations should be to prevent access providers from leveraging their positions in the network to effect change or exert influence in other areas of the network or outside of it. Any exception for reasonable network management practices should preserve that goal.

For the determination of which practices satisfy this requirement, CDT endorses a broad regulatory approach, in which the regulator permits differential treatment of internet traffic through the use of management practices defined as reasonable. CDT prefers this approach because it offers more durability, flexibility, and certainty. A regulation framed in terms of what network operators may do, rather than identifying certain practices they may not engage in, confines the set of acceptable traffic

[10] FCC Open Internet Order at 11, ¶ 32; TSM Regulation, Art. 3(3).

management practices (TMPs) to those which are in keeping with the purpose of the regulation, thereby ensuring that even as new TMPs develop and evolve, they can be analyzed in light of their reasonableness. Thus, this approach is more durable than the narrow, exclusive list approach because such a list would need to be constantly updated as practices change and evolve.

Likewise, under a reasonableness approach, consideration of any specific TMP is contextual, which would allow practices to be classified as either reasonable or unreasonable, depending on the circumstances. This approach offers the flexibility to use practices (that might otherwise be excluded) when they are necessary or more efficient, so long as they are implemented in a reasonable manner. For example, practices like temporarily limiting the bandwidth available to individual subscriber accounts if they exceed certain usage parameters during times of congestion may be a reasonable way of managing network congestion, but capping bandwidth based on commercial incentives or in the absence of congestion would not be reasonable. This flexibility also allows technical choices to be made by those in the "best position to understand the technical consequences and tradeoffs associated with different choices,"[11] and avoids the potential for a more rigid approach to stifle network operators' ability to innovate and efficiently respond to network management issues.

Finally, the broad approach provides more certainty for both regulators and service providers because it allows all reasonable TMPs and excludes those that are unreasonable. Thus, regulators can be certain that undesirable practices are already prohibited, even though they may not have been explicitly described or even anticipated. Similarly, service providers are free to innovate or differently implement management practices (as long as they conform to the reasonableness standards) with more certainty than trying a new practice under the narrow approach with the risk that the practice might later be added to the list of prohibited practices.

The classification of network management practices that are considered reasonable should take into account the enforcement context in which they will be applied. For example, the U.S. FCC previously implemented a relatively broad definition of traffic management practices that would be exempt from its network neutrality regulations, allowing those that were "primarily used for … a legitimate management" purpose.[12] This approach leaves more interpretative discretion for the enforcing agency by allowing it to define "legitimate" and to evaluate a practice's primary use and purpose.

The FCC's approach depends on case-by-case determinations, which require a relatively high level of involvement for the regulator, but also allows for more individualized and nuanced contextual determinations depending on the "particular network architecture and technology" of the access service.[13] The flexibility of this approach may be preferable when there is a unified enforcement agency with sufficient resources and expertise to sustain a high level of involvement. By contrast, the guidelines implemented by BEREC are more detailed, requiring assessment of whether a particular practice is "transparent, non-discriminatory, and proportionate" and whether it is justified by "objectively different technical QoS requirements" as measured by latency, jitter,

[11] FCC Open Internet Order at 101, ¶ 218, and n. 563, quoting CDT's comments at 9.

[12] *Id*. at 11, ¶ 21

[13] *Id*.

packet loss and bandwidth.[14] On top of this, BEREC adds that management practices shall not be based on commercial considerations, shall not monitor specific content, and shall not be maintained longer than necessary.[15] In the EU context, this added level of detail may provide more consistency in the implementation of the regulation by various National Regulatory Authorities.

While it is unclear whether, in the Bermudan context, a more detailed approach like the EU's would ultimately result in a more effective preservation of net neutrality, it seems unlikely to detract from the regulation's potential efficacy so long as the enforcing agency is not constrained to a fixed set of factors in determining whether a management practice is reasonable. So long as the enforcing agency retains sufficient flexibility to address undesirable management practices, a list of factors that will be considered when assessing a practice's reasonability may provide greater certainty for regulated entities and promote accountability and consistency on the part of the regulator.

The risks of attempting to define or classify traffic for the purpose of the differential treatment by network operators may outweigh the potential benefits. While an objective classification system may offer some additional certainty for network operators, a system that is overly tailored to existing technologies may lose relevance as new technologies emerge and application usage trends develop. With or without objectively defined classes of traffic, traffic management practices should be application-agnostic. That is not to say that latency-sensitive traffic may not be prioritized over other kinds of traffic, but rather that specific applications should not be prioritized over other similar applications.[16]

Differential treatment of traffic on an application-specific basis inherently creates the kind of discriminatory effects net neutrality regulation strives to prevent. By contrast, user-defined traffic management policies, although perhaps difficult to implement, do not conflict with the concept of net neutrality so long as users are not subject to coercive pressures or other inappropriate influences from network operators. In general an exception for reasonable traffic management should view favorably those practices that improve the average quality of experience without significantly impacting any individual's quality of experience.

8) Please comment on the need to recognize specific services that may be subject to traffic management that could be otherwise be considered a breach of an open internet framework.

---

[14] Body of European Regulators for Electronic Communication, *BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules* ("BEREC Guidelines") at 16-17; The FCC addresses transparency separately. "A person engaged in the provision of broadband Internet access service shall publicly disclose accurate information regarding the network management practices, performance, and commercial terms of its broadband Internet access services sufficient for consumers to make informed choices regarding use of such services and for content, application, service, and device providers to develop, market, and maintain Internet offerings." 47 C.F.R. § 8.3.

[15] BEREC Guidelines at 17.

[16] The term "application" may, itself, be confusing. For instance, Voice over Internet Protocol (VoIP) may be referred to as an example of a latency-sensitive application, but at the same time, a company's individual VoIP offering (such as Whatsapp, Viber, Skype, etc.) is also an application. Prioritizing VoIP traffic over less latency-sensitive traffic may be reasonable, but prioritizing the VoIP traffic an individual company over other VoIP traffic is not.

CDT believes it is acceptable to allow specific services to be subject to traffic management only if certain safeguards are maintained. In particular, carefully worded definition of these services, as well as vigilant monitoring to guard against the risk of such services overtaking standard internet access are critical to reconciling this allowance with open internet principles.

Regarding the definition of exempt services, the approach previously taken by the FCC offers a good example. With the Open Internet Order, the FCC adopted a simple, binary classification of services that would be covered by its net neutrality regulations. Either a service met the definition of Broadband Internet Access Service (BIAS) and would be subject to regulation or it did not and was considered non-BIAS.[17] The definition of BIAS effectively captured those services at which the regulations were aimed, including services which might not be marketed as internet access services but which amounted to the "functional equivalent." At the same time, it excluded existing and emerging services which used the same transmission infrastructure but did not provide access to "all or virtually all endpoints" of the internet.[18]

If the Authority were to implement a similar approach for classifying services covered by its open internet regulations, important safeguards would involve monitoring compliance with a variety of standards. For instance, non-BIAS or "specialized services" should not be allowed to use network capacity in a way that diminishes from the network's speed, efficiency, or ability to provide general internet access services.[19] Ideally, capacity building incentives will at least match demand for bandwidth by both internet access and other services. Regulators should also be wary of the potential for various services currently available through standard internet access to be isolated and re-marketed as stand-alone "specialized" services, thereby detracting from a full and open internet, cannibalizing network capacity, and escaping regulatory control. To that end, a provision excluding specialized services from the open internet regulations unless they are used to circumvent the regulations, could limit the incentives and ability to take such actions.[20] Any exception for specialized services should be considered carefully in light of emerging network functions associated with 5G networks, namely "network slicing," which could enable even more granular tailoring of network capabilities like speed, latency, and reliability. Network slicing is a notable step away from the 'best efforts' standard for transmitting network traffic and appears poised to reshape the way network operators allocate network resources among competing application providers and end users.

---

[17] FCC Open Internet Order at ¶ 167.

[18] "A mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up Internet access service. This term also encompasses any service that the Commission finds to be providing a functional equivalent of the service described in the previous sentence, or that is used to evade the protections set forth in this Part." FCC Open Internet Order at 9-10, para. 25.

[19] BEREC Guidelines at 25, ¶ 102 "...specialised services are not to the detriment of the availability or general quality of the IAS for end users."; FCC Open Internet Order at 97, ¶ 210 "The Commission will take "appropriate enforcement action...if...these types of services are undermining...end user benefits."

[20] BEREC Guidelines at 7, ¶ 18.

9) **Please identify the specific services and how they need to be managed. How can it be ensured that these services do not impinge on general internet access?**

As emphasized in the above response to questions 7 and 8, it would be more efficient for the Authority to adopt a classification of specific services based on their functionality rather than maintaining a list of specific services that should be allowed. This would provide more flexibility in enforcement as regulators would not need to constantly update a list of permissible services in order to keep pace with development of new services, but could rather rely on a set of principles based on functionality that could apply to both current and future services that might become available. This is the approach recommended by CDT.

10) **Please comment on the proposal that OTT services should not perform worse as described in the proposed approach.**

CDT generally agrees that OTT services should be actively encouraged, and accordingly, the Authority's suggested approach to prevent them from being superseded in terms of performance by specialized services is important to maintain fair competition between these types of services. It is our position that, while specialized services may provide benefits in certain applications, ISPs should be encouraged to continue to improve network capacity and performance for internet access services, which should continue to grow alongside network improvements for specialized services. CDT addresses this question more fully in response to Question 8.

V.A.3 End-users' right to access and distribute content of their choice

11) **Please comment on the Authority's proposed position – that end-users have the explicit right to access and distribute legal content, as well as use legal applications and services of their choice on the internet.**

Individual users' ability to access and distribute lawful information and content online, without being subjected to differential treatment, is central to the principle of internet openness. As such, CDT fully supports the Authority's proposed position that end-users possess this explicit right.

V.B ISP obligations

15) **Please comment on the proposals of the Authority regarding obligations on ICOLs regarding:**

a. Transparency regarding traffic management practices;
b. Clarity on performance limitations;
c. Giving realistic expectations on speed performance;
d. Providing end-users with a clear route of complaint and remedy in the case of continuing failure in performance;
e. Ensuring the privacy of end-users and the protection of their personal data; and
f. Updating end-users and the Authority if practices or performance changes.

16) Please comment on the options identified in the proposed approach.

The informational criteria specified by the Authority in its ISP reporting obligations is relevant to end-users and consumers making their internet access purchasing decisions. Requiring ISPs to provide this information would therefore be helpful in fostering informed choices among internet service providers and allowing end-users, in addition to regulators, to hold ISPs accountable for deviations from regulatory policies or ISPs' own disclosures. CDT therefore supports the Authority's enforcement of these obligations. We also concur with the inclusion of a privacy protection obligation on ISPs. There are important and innovative ways in which ISPs may make use of the customer information to which they have access because of the service they provide, but customers should be empowered with both knowledge and choice as to how their carriers use that information.

CDT suggests that the Authority also consider the scope and sensitivity of the personal information that service providers can access. It is particularly important for the Authority to be aware that, although the use of encryption technologies has become more common, these technologies may still leave some personal or private information exposed.[21] This is due, in part, to the structure of individual Internet Protocol (IP) packets, which contain several layers of unencrypted metadata outside the actual content of the packet, which may or may not be encrypted.[22] This packet metadata, especially when associated with other customer-specific information an ISP may have, like names and addresses, can be used to build comprehensive customer profiles and make detailed inferences about the online and offline behavior of individuals.[23]

Perhaps even more concerning is that ISPs can access more detailed and sensitive information using technologies that enable them to look beyond packet metadata. The Authority should be aware of this practice, sometimes called deep packet inspection (DPI), in developing safeguards for user privacy. This practice is sometimes used by network operators to enhance their traffic management practices, but is not necessary for network functionality. Given the privacy implications of DPI, CDT therefore recommends that such practices be discouraged, or in the alternative, only implemented at the request of the customers.

June 28, 2019

[21] I*n the matter of Protecting the Privacy of Customers of Broadband and other Telecommunications Services,* Comments of the Center for Democracy & Technology, at 16-17 ("CDT Broadband Privacy Comments") (May 27, 2016) available at: https://cdt.org/files/2016/05/Broadband-Privacy-Comment-FINAL-word.pdf.

[22] See Center for Democracy & Technology, *Applying Communications Act Consumer Privacy Protections to Broadband Providers* (Jan. 20, 2016), https://cdt.org/insight/applying-communications-act-consumer-privacyprotections-to-broadband-providers/.

[23] CDT Broadband Privacy Comments at 16.