To,
Shri A. Robert J. Ravi
Telecom Regulatory Authority of India,
New Delhi

New Delhi, 5 July 2016

Re: Internet Democracy Project's Comments to Pre-consultation paper on Net Neutrality

Dear Sir,

Thank you for the opportunity to comment on the pre-consultation paper on Net Neutrality.

The Internet Democracy Project is a Delhi-based civil society initiative that works for an Internet that supports freedom of expression, democracy and social justice through research, advocacy and debate in India, and beyond.

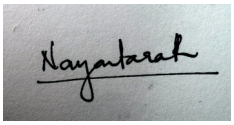
We hope that the consultation results in a clear and overarching framework that strengthens the freedom of expression that the internet has enabled, that makes strong protections for user privacy, that secures user choice by minimising Internet service provider interference and that ensures healthy competition in the telecommunications and applications market.

The framework should not constrain the evolution of the network more than is essential to guarantee the above, while at the same time providing the legal certainty that commercial and other players require to continue to develop the network and innovate.

Finally, we hope that these measures complement an increase in the provisioning of networks, and that the government supports TSPs towards this with a range of measures that do not negatively affect network neutrality.

We hope our comments will be taken into consideration.

Thanking you,
Yours Sincerely,



Nayantara Ranganathan
Programme Manager- Freedom of Expression
Internet Democracy Project

Submission by the Internet Democracy Project
(www.internetdemocracy.in)

in response to TRAI Pre-Consultation Paper on Net Neutrality
5 July 2016

The following document contains the response from the Internet Democracy Project (**www.internetdemocracy.in**) to TRAI's Pre-Consultation Paper on Net Neutrality, dated 30 May 2016.

1. What should be regarded as the core principles of net neutrality in the Indian context? What are the key issues that are required to be considered so that the principles of net neutrality are ensured?

The goal of net neutrality regulations in India should be to preserve the Internet's ability to function as a free, open and secure medium, that can facilitate political participation, enable free speech and provide a decentralised environment for social and cultural interaction.

To this end, the following principles should be adopted in India to protect net neutrality:

1. No blocking by TSPs and ISPs of specific forms of internet traffic, services and applications.
2. No slowing or "throttling" internet speeds by TSPs and ISPs of specific forms of internet traffic, services and applications.
3. No preferential treatment of services and platforms by TSPs and ISPs.

There is general agreement that blocking of applications by network providers is not acceptable.[1] Moreover, in February 2016, TRAI has already ruled that preferential treatment in the form of differential pricing is not allowed in India. But given the limitation of networks in a country where mobile internet users are expected to double between 2015 and 2017, telecommunication networks are at risk of being overburdened.[2] In light of this, it remains to be explored which forms of discrimination by network providers can be considered acceptable to reduce network congestion.

Any regulations in this regard should take into account challenges unique to India – especially tentative literacy and the likely preference for video over text that comes with that, a large number of low-income users for whom discounted and free schemes are particularly appealing, a considerably higher number of mobile data users than fixed line broadband users and the fast growth in Internet use – and ensure that the benefits of the Internet are maximised for each user within this challenging context.

While full equality on this count may be a long way away, a user should not be disadvantaged in availing of the Internet's benefits because of market practices

[1] See Department of Telecommunications Committee report page 83, para 16.4, Net Neutrality pre-consultation paper para 17.
[2] Srivastava, Moulishree (2015). Mobile Internet Users in India to Double by 2017, Says Study. *LiveMint*, 6 August, http://www.livemint.com/Industry/VThUq5I4BivpTDZdQb5sNN/Mobile-Internet-users-in-India-to-double-by-2017-says-study.html.

or of regulations that punish her for most commonly using a specific device or type of data, for her socio-economic background or location in the country.

A narrow framework that evaluates network-provider behaviour against harms related to typical vertical integration and foreclosure would not be satisfactory to achieve the goal of net neutrality regulations expanded on above. In order to preserve the Internet's ability to facilitate political participation, enable free speech and provide a decentralised environment for social and cultural interaction, a broader framework than antitrust should be evolved, against which network neutrality can be ensured. Antitrust regulation is necessary, but not sufficient.

The consultation paper itself looks for further guiding principles towards network neutrality expert Prof. Dr. Barbara van Schewick's paper 'Network neutrality and Quality of Service: What a non-discrimination rule should look like', and quotes key factors that Dr. van Schewick notes should be preserved in net neutrality rules:

- user choice,
- innovation without permission, and
- low cost of application innovation.

Curiously, however, *only three of the four factors* noted by Prof. van Schewick, though they are intended to be all taken together, have been quoted in the pre-consultation paper. The requirement of '*application blindness of the network*' has been omitted. This omission is in line with TRAI's indication, that certain classes of applications might have to be treated differently. However, as we will discuss below, the omitted factor is an important one, and should be part of the characteristics that network neutrality regulations preserve.

Thus, we urge TRAI to adopt *all four factors* outlined by Prof. van Schewick as key factors of the Internet that should be retained and preserved by net neutrality regulations in India.

2. **What are the reasonable traffic management practices that may need to be followed by TSPs while providing Internet access services and in what manner could these be misused? Are there any other current or potential practices in India that may give rise to concerns about net neutrality?**

As outlined by BEUC, the European Consumer Organisation (http://www.beuc.org/publications/2012-00652-01-e.pdf), "any traffic management measure that imposes restrictions or illegitimately discriminates against specific technologies, applications, content or end-users interferes with the neutrality and openness of the Internet and should therefore not be allowed".

Other traffic management practices could, however, be considered. For example, those done to comply with legal obligations such as court orders, for security reasons or for temporary congestion management can be reasonable,

provided they adhere to a number of principles, such as transparency, proportionality, non-discrimination and respect for privacy.

As the consultation paper notes (para 24), the DoT Committee on Net Neutrality suggests suggests the following criteria against which legitimate traffic management techniques and practices may be tested:

- Adequate disclosure to users about traffic management policies and tools to allow them to make informed choices.
- Application-agnostic controls may be used but application-specific control within the “Internet traffic” class may not be permitted.
- Practices like deep packet inspection should not be used for unlawful access to the type and contents of an application in an IP packet.
- Improper (paid or otherwise) prioritisation may not be permitted.

While we are in broad agreement with these criteria, we believe they need to be qualified in a number of ways.

- Adequate disclosure should mean that the disclosure is meaningful, and systematic, as we argue in section A below.
- Applications-agnostic control should include discrimination between applications, but also between classes of applications, as we argue in section B. The choice to prioritise a particular class of application should lie with the user, and not be pre-decided by the network provider. We recognise that there is a problem of limited network resources resulting in network congestion, but the solution to this problem is really a much stronger focus on government support for greater investments in infrastructure. Allowing discrimination against video in particular would likely severely restrict the value of the Internet for India’s most disadvantaged users in particular. We agree that intrusive practices like Deep Packet Inspection could be easily misused, and there should be privacy protections against such misuse, which is discussed in comments to Question 5.
- Improper prioritisation of certain applications over others should not be permitted. Some such practices are already forbidden by the Prohibition of Discriminatory Pricing of Data Services Regulation, 2006, and we have also addressed these in our comments to the consultation on Free Data. However, *any* kind of prioritisation for a commercial purpose (e.g. throttling of an app or service that competes with an app or service owned by the TSP or ISP) would have to be improper in the network management context – this needs to be further clarified.

We also believe that it is important that proportionality is added to DoT’s criteria: where less invasive solutions than traffic management are possible, these should be given preference.

We examine the first two of DoT’s criteria in more detail below:

A. Adequate disclosure to users about traffic management policies and tools to allow them to make informed choices

For the Department of Telecommunications' disclosure requirements to be of practical use, they should be meaningful and systematic.

'Adequate' disclosure should be interpreted as meaningful disclosure

Mandatory meaningful disclosure is the first step for many network management regulations. Where TSPs use non-discriminatory traffic management techniques, it is essential that information about such techniques is published by the TSPs in question in a format that makes this information intelligible to general users.

TRAI should put in place transparency requirements in the license agreements mandating that all service providers disclose consistently traffic management tools that are available with them, the exceptional situations in which they are used, and the effect of that use, and that they do so without a prior complaint, in a systematic manner. Conversely, it should also be true that any traffic management practice that is not disclosed, even when used for legitimate exceptional cases of network congestion would be liable to penalties.

This is fairly consistent practice in several network neutrality regulations that cover traffic management. For example, disclosure of such practices is one of the factors used to evaluate the 'reasonableness' of traffic management in the Open Internet Order passed by the Federal Communications Commission. Specifically, the Order requires a broadband provider to '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.' (https://www.law.cornell.edu/cfr/text/47/8.3)

Where TSPs draw on technical or security grounds to justify traffic management (rather than legal ones), TSPs should also be obliged to provide conclusive evidence of the need for the measures they have taken. The regulator should scrutinise this evidence for its veracity and truthfulness on a regular basis. Where false information is found to have been provided, severe penalties should apply.

Meaningful disclosure should be complemented with principle-based guidelines on network management

Para 21 of the pre-consultation paper notes that the "*adoption of clear transparency standards is one of the methods that can be used to check TSPs from imposing unreasonable restrictions on the provision of Internet access.*" However, simply requiring transparency may not be a sufficient safeguard against discriminatory practices. Even given disclosures, lack of technical knowledge and social, cultural and political implications of discrimination cannot be expected of all users. The market for telecommunications and Internet services is one of high switching costs, even in India, a country which is said to have one of the most competitive telecom markets. A bias towards

status quo could also be one of the reasons why transparency requirements on their own might not suffice.

B. Application-agnostic controls may be used but application-specific control within the "Internet traffic" class may not be permitted

The Department of Telecommunication's recommendation does not permit application-specific control. This should be qualified to mean discrimination amongst applications *as well as* discrimination amongst classes of applications, for reasons given below.

An absolute ban on discrimination or Quality of Service being available to applications would unduly restrict innovation, as many types of applications may benefit from having certainty about technical requirements like bandwidth or delay.

User-controlled prioritisation is important in the Indian context

The framework proposed by Dr. Van Schewick shares DoT's view that controls should be application-agnostic, and proposes that the choice of availing Quality of Service lie with users, so as to not disadvantage applications and users that might benefit from Quality of Service.

Video has been pegged as one of the main reasons for the need for traffic management. The pre-consultation paper quotes CISCO to say "*As per CISCO's Visual Networking Index Forecast, Internet video traffic (business and consumer, combined) is expected to constitute 74% of all Internet traffic in India by 2019, up from 46% in 2014"*. The massive use of video and the likelihood of its increase in importance is definitely a challenge. However, elsewhere CISCO notes that higher usage of videos would be one of the drivers of internet growth, in addition to surging mobile data consumption, proliferation in networked devices and faster broadband speed. (http://timesofindia.indiatimes.com/tech/tech-news/Indias-Internet-traffic-to-grow-33-annually-Cisco/articleshow/47456061.cms) This is understandable in a country where a fourth of the population is not literate, and constitutes a majority of the population that is expected to be come online in the near future. Even for the literate population, majority of the internet is not accessible as so few resources are available in regional languages and videos are an important class of application. The fallout of this conflict cannot be a TSP-led decision to discriminate against the entire class of an application for all users – esspecially not since such a decision will disproportionally affect the use that the most marginalised and disadvantaged people of the country can make of the Internet.

It has been recognised in the past that the Internet is valuable because it allows users to choose what they might do on the network. This principle should be extended to the question of prioritisation and Quality of Service as well. Users' evaluation of what applications they want higher performance for might differ from the network provider's assessment of the same. These preferences of the user also change with time. Therefore, within the limits of the data pack that the user has subscribed to, she must be able to choose which application to prioritise according to her own needs.

Real dangers of anti-competitive harms in the Indian telecom market, if telcos are allowed to prioritise one class of application over another

Network providers may treat Internet traffic differently in one of many ways. The three most obvious ways are differentiation (i) amongst applications, (ii) amongst classes of applications and (iii) amongst protocols.

The first case, of differentiating amongst applications is dangerous, and would have a business motive, as the network provider would be able to prioritise amongst applications that have similar functionalities. For example, a network provider prioritises his/her own music streaming website over a competitor's, giving better performance for the former. This is clearly violative of user choice, application blindness of the network and innovation without permission.

The second case of differentiating amongst classes of applications might not come across as discriminatory at first, but is ridden with anti-competitive dangers. The obvious problem with differentially treating classes of applications is the problem of defining classes. This neat boxing of applications on the Internet cannot be done as applications on the Internet defy clean classification as some are of different utility to every user, and also perform more than one function.

Even assuming classification is not a problem, there are anti-competitive harms in the Indian context if this is allowed. Some applications on the internet directly compete with the revenue of network operators. For example, internet telephony is widely used and preferred for long-distance calls. Indian TSPs have consistently lobbied for regulation of these applications, revenue sharing by these applications, and even banning of these applications, and are clearly unhappy with the proliferation of this particular class of service on the Internet. If the rationale for classification is the protocol behind the application, then the second category of possible differentiation and the third collapse into one hypothetical case.

The third case is of discrimination against particular types of protocols. Blocking of certain kinds of protocols could be an advantage to certain groups of people. For example, those concerned about copyright protection and piracy have an incentive to see P2P applications blocked or deprioritised, as applications like BitTorrent allow easy sharing of protected material between users. This can disadvantage an entire type of protocol.

Therefore, locating the decision to avail Quality of Service or prioritise a particular application over another should lie squarely with users. Different classes of service should be offered equally to all applications and classes of applications. Given a certain amount of data that a user has paid for, the choice of applications over which to use this data should lie with the user.

'Reasonable' network management exception

A narrow provision for network management should be available for exceptional circumstances, as provided in the framework. The TSP should be able to prove that the action was not for a commercial purpose- this is a

standard requirement in many net neutrality regimes like the United States and the European Union. However, these instances should be exceptional cases, because where isolated events of network management are concerned, it could be hard to tell what the motivations are.

3. What should be India's policy and/or regulatory approach in dealing with issues relating to net neutrality? Please comment with justifications.

In the language of the International Telecommunications Union's report, India's approach should be one of 'active reform'.[3]

As we outlined in our comments on Consultation paper no. 07/2016 on Free Data, there is a need for an overarching principle-based framework that can be used as a touchstone against which to assess network provider behaviour and existing or proposed business models.

TRAI has made a start towards this by identifying guiding principles in the Prohibition on Discriminatory Pricing of Data Services Regulation 2016. However, the details of what principles like 'non-discrimination' involve in a variety of situations have to still be fleshed out. Future consultations should aim at doing so.

India's network neutrality regulations should aim to provide clarity for industry participants up-front.

4. What precautions must be taken with respect to the activities of TSPs and content providers to ensure that national security interests are preserved? Please comment with justification.

It is unclear what TRAI means when it says 'national security' in the context of network neutrality, as the phrase is mentioned without absolutely any explanation about what the specific concerns are.

As we have pointed out in our comments to the consultation paper on OTT services of 2015:

> Internet services and apps are well-covered under the existing laws and regulations. These include the Code of Criminal Procedure, Indian Telegraph Act, Indian Telegraph Rules, and the Information Technology Act and its different rules pertaining to intermediaries and interception. These different regulations allow the Indian government and law enforcement agencies to access the data stored by internet platforms when deemed legally necessary. Any additional regulations carry grave risk of breaching user privacy – especially since the Government has still not enacted strong horizontal protections of privacy in law – and of harming users' right to freedom of expression, and would require constitutional review.

[3] International Telecommunication Union (2013). *Trends in Telecommunication Reform*. Geneva: International Telecommunication Union (chapter 2).

> The government and courts also have the power to block access to websites on the grounds of national security and public order. It has made use of these provisions and has taken such steps accordingly in the past, as has been widely reported by the media. The transparency reports periodically published by major internet companies suggests Indian government routinely requests for user data and blocking of user accounts. Between July 2014 and December 2014, Indian authorities had 5,473 requests for data, covering 7,281 user accounts from Facebook and the company had a compliance rate of 44.69%. Google had a compliance rate of 61% with respect to the requests made by different government agencies across India.
>
> As also pointed out above, where challenges relating to the implementation of Indian law where the Internet is concerned continue to exist, these are generally about jurisdictional issues. Such challenges need to be resolved through negotiations with other states, either by means of bilateral agreements or, preferably, through multilateral ones. The Government of India can also take enabling (not restrictive) measures to strengthen the start-up ecosystem within the country and to encourage peering arrangements and lower transit costs.

If TRAI believes there are any specific threats to national security as a result of the activities of TSPs and content providers that remain unaddressed in the existing legal framework, these should be spelt out in a future consultation paper, rather than be implied.

It deserves to be pointed out here that increasing communications surveillance by the State has not proven to reduce threats to national security. At the same time, in the absence of strong privacy protections, these initiatives are a big blow to the civil liberties of citizens. Drag-net surveillance initiatives cost enormous amounts of money, and end up obfuscating threats by bringing into the fold all communications, and not just ones worth pursuing.

5. What precautions must be taken with respect to the activities of TSPs and content providers to maintain customer privacy? Please comment with justification.

Para 23 of the Pre-Consultation Paper on Net Neutrality notes that

> OTT communications and OTT media can also pose a threat to the privacy of individual users. While the open architecture of the Internet is responsible for the phenomenal growth of OTT services, it also causes the transfer of personal information on the Internet to be fraught with potential risks and scope for misuse. This calls for a need to examine the legal and regulatory framework required for governing the privacy of users of OTT services.

Undeniably, the digital age sees a strong need for strong horizontal user privacy protections in the law. While a number of the protections required are beyond TRAI's ambit and cannot be fleshed out through its regulations, there are a number of actions that TRAI can take.

Thus, there should be protection against collection and use of personal information derived from the flow of network traffic. Such privacy protections are part of network neutrality regimes that recognise that network

management tools are liable to misuse. For example, the Canadian Radio-television and Telecommunications Commission

> directs all primary ISPs, as a condition of providing retail Internet services, not to use for other purposes personal information collected for the purposes of traffic management and not to disclose such information.
>
> […] In order to ensure that customers of secondary ISPs are afforded the same degree of privacy protection as those of primary ISPs, the Commission **directs** all primary ISPs, as a condition of providing wholesale services to secondary ISPs, to include, in their service contracts or other arrangements with secondary ISPs, the requirement that the latter not use for other purposes personal information collected for the purposes of traffic management and not disclose such information.
>
> […] The Commission notes that ISPs use aggregated information collected for the purposes of network planning and engineering, and expects that they will continue to rely on aggregated information for such purposes.[4]

Network neutrality regulations should clearly forbid technical practices like Deep Packet Inspection (DPI) for uses other than where they are strictly required to ensure network security or where lawfully demanded by the government for security purposes, as DPI can be misused by network operators to determine the content of data packets and the misuse often cannot even be detected by the end user. Explicit privacy protections against possible misuses of intrusive tools like Deep Packet Inspection also need to be included in net neutrality regulations. Where misuse of such tools by network operators is discovered, it should be met with appropriate, stringent punishments.

Further, end-to-end encryption should be strongly encouraged or incentivised for all Internet traffic. A Public Interest Litigation seeking to direct the government to require private keys of encrypted messaging services like Whatsapp was recently dismissed by the Supreme Court. The petitioner was asked to approach TRAI for concerns in this regard.[5] We welcome this move by the Supreme Court. TRAI should encourage adoption of strong encryption as a means to protect privacy. [WHY?]

6. What further issues should be considered for a comprehensive policy framework for defining the relationship between TSPs and OTT content providers?

We have answered related questions posed by TRAI in its Consultation Paper no. 2/2015 on Regulatory Framework for Over-the-Top Services in detail earlier, in our submission to TRAI dated 24 April 2015. Our comments made then continue to hold relevance today, and we refer the reader to that submission for full details.

---

[4] Canadian Radio-Television and Telecommunications Commission (2006). Telecom Decision CRTC 2006-15. Ottawa, Canadian Radio-Television and Telecommunications Commission, http://www.crtc.gc.ca/eng/archive/2006/dt2006-15.htm.

[5] Express News Service (2016). Supreme Court Refused to Hear PIL on WhatsApp Encryption. *Indian Express*, 30 June. http://indianexpress.com/article/technology/tech-news-technology/supreme-court-refuses-to-hear-pil-on-whatsapp-encryption-2884631/

There are two points we would like to highlight in particular again here.

The first is that any such framework should be built on assumptions that are correct. The sometimes heard claim that so-called communications OTT content providers are cannibalising voice revenues of telecom operators is a claim that has proven to be incorrect, and should therefore be discarded in total. As we noted in our submission of 24 April 2015:

> There is absolutely no evidence to suggest that VoIP services like Hike or Skype are cannibalising voice revenues of telecom operators. In fact, heads of more than one Indian telecom operator have clearly stated the same over the past few months. For example, Airtel India CEO Gopal Vittal had said during the company's earnings conference call, earlier this year, that there's no evidence of VoIP cannibalisation of voice services. Last year, Idea Cellular MD Himanshu Kapania had also said that OTT apps like Viber have had some impact on their International calling business, but on regular voice calls, there was no impact.
>
> Indeed, it is important to remember that Internet-based services have often led to *new practices and habits* among consumers, rather than merely a shift of old practices and habits to new platforms. The argument that the growth of the Internet/OTT is impacting the traditional revenue stream of telecom operators presumes that all communication-related activities that now take place using the Internet would have taken place using more traditional means of communication instead if the Internet did not exist. There is no evidence to support this contention. On the contrary, it is clear, for example, that if far larger number of private persons now communicate on a regular basis with people who live abroad, they do so because Internet-based communication has made this far more affordable than it was before. If prices go up again significantly, it is likely that many of those calls simply will never be made, severely and negatively impacting on Indians' ability to keep in touch with loved ones and communicate with people around the world.
>
> We also need to remember that data revenues also fall under the traditional revenue streams category as per the Unified Access License Agreement (http://www.dot.gov.in/access-services/introduction-unified-access-servicescellular-mobile-services). So, it is factually incorrect to say that increase in data revenues will affect traditional revenue streams.
>
> A Morgan Stanley report on the Indian telecom industry from last year mentions that data revenues is likely to contribute about 23% of telecom operators' overall revenues over the next two years. A study jointly done by AT Kearney and Google estimated that telecom companies will earn an additional $8 billion in revenues by 2017 due to the proliferation of data and data-based services.

A year later, there is no evidence that anything has changed.

The second point that we would restate explicitly is that the distinction made earlier by TRAI between communications and non-communications OTT content providers is an inappropriate one. As we pointed out in our comments dated 24 April 2015:

> As they both sit on top of the network provided by the telecom operators, Internet-based communication services and non-communication services are fundamentally the same. From a technical perspective, drawing a distinction between them is, thus, false.
>
> Moreover, again pointing to the fundamental similarity between communication services and non-communication services on the Internet, many non-communication services on the Internet also offer real-time chat or video interaction features for the benefit of customers. Such features will be affected by bringing such services under a licensing regime, which will in turn negatively impact consumers' interests.
>
> At the same time, the spectrum that telecom operators utilise to offer this network on pipe is already licensed.
>
> For all these reasons, there is no need for additional licensing of Internet based communication service providers. To suggest such a move merely creates the impression that the TRAI consultation is tilted in favour of telecom operators' commercial interests.
>
> The extent of innovation we have witnessed over the years has been greatly aided by the low cost of entry. Any form of regulation or licensing will increase the entry cost, thereby hindering innovation and equal opportunity to start-ups to establish themselves in the market. Behind every Zoho, WhatsApp and Skype there are numerous failures. Licensing will essentially increase the cost and likelihood of failure - and greatly discourage innovation.

We also noted then:

> Requiring licensing of online services and mobile apps under the current telecom framework in India would have enormous negative consequences. The tremendous burdens imposed by such licensing would results in many such globally developed services and apps not being launched in India, while our own start-up efforts to develop local versions of such apps would be killed in their early stages. Licensing for OTT communication services would likely pose an even bigger barrier for social entrepreneurs and not-for-profit organisations who seek to incorporate aspects of communication services in their social development services.
>
> The net results would be decreased user benefit; a massive slowdown in innovation; reduced "Make in India" efforts due to the regulatory cost of doing business becoming very high; and an overall slowing down of economic and social development spurred by the Internet.

We hope that any net neutrality regulations framed by TRAI will take these realities into account.

While this may not fall within the ambit of TRAI's mandate, it also deserves pointing out here that for India's telecom operators to be able to make the investments in infrastructure necessary to welcome the entire country fully into the Internet age, changes to *other* parts of the digital ecosystem do need to be made. The most prominent among these are the spectrum auctions and the conditions imposed by the telecom licenses. That our telecom operators at times have too little leeway is correct. To impose a comparative regulatory burden on other actors is, however, not a solution to that ill, but will only lead to an increase in the number of undesirable outcomes.