Stream: Internet Architecture Board (IAB)
RFC: 9707
Category: Informational
Published: February 2025
ISSN: 2070-1721
Authors: M. Kühlewind D. Dhody M. Knodel

RFC 9707
Report from the IAB Workshop on Barriers to Internet Access of Services (BIAS)

Abstract

The "Barriers to Internet Access of Services (BIAS)" workshop was convened by the Internet Architecture Board (IAB) from January 15-17, 2024 as a three-day online meeting. Based on the submitted position papers, the workshop covered three areas of interest: the role of Community Networks in Internet access of services, reports and comments on the observed digital divide, and measurements of censorship and censorship circumvention. This report summarizes the workshop's discussions and serves as a reference for reports on the current barriers to Internet access.

Note that this document is a report on the proceedings of the workshop. The views and positions documented in this report were expressed during the workshop by participants and do not necessarily reflect the IAB's views and positions.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Architecture Board (IAB) and represents information that the IAB has deemed valuable to provide for permanent record. It represents the consensus of the Internet Architecture Board (IAB). Documents approved for publication by the IAB are not candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9707.

Copyright Notice

Table of Contents

1. Introduction

The Internet Architecture Board (IAB) holds occasional workshops designed to consider long-term issues and strategies for the Internet, and to suggest future directions for the Internet architecture. This long-term planning function of the IAB is complementary to the ongoing engineering efforts performed by working groups of the Internet Engineering Task Force (IETF).

The Internet as part of the critical infrastructure affects many aspects of our society significantly, although it impacts different parts of society differently. The Internet is an important tool for reaching the Sustainable Development Goals (SDGs) listed in [SDGs] and for globally supporting human rights. Consequently, the lack of meaningful access to digital infrastructure and services is also a form of disenfranchisement.

Solely having Internet access is not enough. At the same time as we work to connect the next billion people and reduce the digital divide, it is also important to understand persistent and novel inequalities in the digital age when accessing content and services. There are more and more barriers to meaningful access to the services and applications that run on the Internet. Even if Internet connectivity is available, information and service access may remain challenged and unequal.

This IAB workshop aimed to

- collect reports about barriers to accessing content and services on the Internet -- for example, based on filtering or on blocking, or due to general inequality of technological capabilities, e.g., device or protocol limitations.
- help the Internet community get a better understanding of how the Internet functions in different parts of the world and which technology or techniques need to be used to gain access to content.
- build an understanding of what "being connected" to the Internet means: What is the Internet to users? What is needed to be meaningfully connected? What are the minimum requirements to be able to access certain parts of the content and services provided over the Internet?

1.1. About the Content of This Workshop Report

This document is a report on the proceedings of the workshop. The views and positions documented in this report were expressed during the workshop by participants and do not necessarily reflect the IAB's views and positions.

Furthermore, the content of the report comes from presentations given by workshop participants and notes taken during the discussions, without interpretation or validation. Thus, the content of this report follows the flow and dialogue of the workshop but does not attempt to capture a consensus.

2. Workshop Scope and Discussion

The workshop was organized across three days with all-group discussion slots, one per day. The following topic areas were identified, and the program committee organized paper submissions into three main themes for each of the three discussion slots. During each discussion, those papers were presented sequentially with open discussion held at the end of each day.

2.1. Session 1: Community Networks - Their Role in Internet Access of Services

The first day of the workshop focused on the role of Community Networks [RFC7962] as a way to overcome the barriers to Internet access. Community Networks are self-organized networks wholly owned by the community and thus provide an alternative mechanism to bring connectivity and Internet services to those places that lack commercial interest.

Presentations ranged from highlighting the need for measuring Quality of Experience (QoE) for Community Networks, to the potential role the Content Delivery Network (CDN) can play in Community Networks, to the role of satellite networks, and finally, to the vital role of the spectrum in this space.

2.1.1. The Quality of Community Networks

[MARTINEZ] highlighted the need to address QoE in discussions around Community Networks. As a community-driven deployment, the knowledge and involvement of individuals can vary; therefore, there are no guarantees of connectivity or quality of service. There is a need to focus on user expectations and how they translate to measurable performance indicators. Further, it asks for better documentation of best practices in deploying Community Networks as well as careful thought regarding manageability considerations for Community Networks in protocol development. [GUIFI] as an example Community Network was discussed, and some existing resources for Community Networks [APC] [ISOC] [TBB] were shared by the participants.

The inconsistent quality and performance of satellite Internet result in a connectivity gap for Community Networks that rely on non-terrestrial networks (NTNs) for Internet access [HU].

2.1.2. Strengthening Community Networks

[BENSON] focused on the prohibitive cost of transit and Internet services for Community Networks and argued for CDNs to provide transit-like and Internet services, at no more than at-cost, in a mutually beneficial way. Community Networks still need backhaul to and from the CDN's point of presence, and models for community-backhaul and open-source CDNs were highlighted. Discussion included the status of Project PANGEA [PANGEA] as well as legal and commercial considerations related to such use of CDNs.

[HU] highlighted that satellite Internet provided by advanced low-Earth orbit (LEO) satellite constellations can play a pivotal role in closing the connectivity gap in the urban-rural digital divide via satellite-dependent Community Networks. These existing known performance and management gaps need to be focused on, to enable satellite Internet to resolve the divide. Further, research directions such as multi-layer satellite networking, autonomous maintenance, and integration between terrestrial networks and NTNs were suggested.

[RENNO] called attention to the coveted 6 GHz (part of the C-band with a desirable mix of coverage and capacity) as a prime choice for International Mobile Telecommunication (IMT) for 5G technology while it is in common unlicensed use in Community Networks (and small ISPs). Spectrum allocations directly impact industries and market access with ramifications for Community Networks. Further, there was a discussion on geopolitical tensions regarding the use of unlicensed spectrum and commercial interest in new spectrum usage.

2.1.3. Discussion

How can the technical community address the management gaps and improve best practices for Community Networks? Is the increasing complexity of the Internet making it more challenging to establish secure connections, and should this be taken into account in the design of the Internet? What steps need to be taken to make sure Community Networks are secure? Should manageability considerations be expanded to explicitly consider Community Networks? The Global Access to the Internet for All (GAIA) Research Group [GAIA] could be a venue for further discussion and research. Further discussion highlighted the need for readily available knowledge and tools for Community Networks as well as the tussle with market forces when commercial networks compete with Community Networks. Also, there is a lack of operational inputs from Community Network operators in the IETF/IRTF.

2.2. Session 2: Digital Divide - Reports and Comments

Critical Internet infrastructure affects many aspects of our society significantly, although it impacts different parts of society differently. The inequitable aspects are typically referred to as "digital inclusion"; these aspects signify that in efforts to digitalize society, there are those left out due to what is typically called the "digital divide", a related term specific to access to the Internet. These concepts together demonstrate that even if Internet connectivity is available, for some there will remain challenges towards achieving equality. This becomes especially significant as governments view the Internet as an important tool for helping them reach the SDGs listed in [SDGs] and for globally supporting human rights.

The second day of workshops was essential to understanding the nature of the digital divide. Presentations of reports interrogated at least three key aspects of the digital divide, though it is recognized that there may be more technical aspects of the digital divide that were not addressed. The three aspects presented and discussed were differences between population demographics in the provision of online resources by governments, inequality in the use of multilingualized domains and email addresses, and increased costs for end-user downloads from websites of contemporary sizes.

2.2.1. Disparities in Service Provisioning

Ralph Holz presented research that exposes the more limited DNS-mediated access to government websites by Indigenous communities in Australia as compared to less disadvantaged users in the same population in "Evidence for a digital divide? Measuring DNS dependencies in the context of the indigenous population of Australia" [HOLZ]. DNS dependency trends were analyzed between two lists of domains serving Australian government sites for Indigenous users and the general population. Researchers found "evidence that dependencies for the indigenous population are indeed differently configured," indicative of a difference in service provisioning. However, qualitative follow-up research is needed to interrogate both the potential reasons for these differences and whether the differences contribute to a digital divide that is tangible for Indigenous users.

2.2.2. Lack of Consistent Acceptance of Language Scripts

On the topic of availability of Internet services and content in multiple languages, "Universal Acceptance of Domain Names and Email Addresses: A Key to Digital Inclusion" was presented by Sarmad Hussain of ICANN [HUSSAIN]. The ICANN community has increased the options for multilingual identifiers through the expansion of the Internet's DNS for use in domains and email addresses. However, while the work of technical specifications and policy recommendations is complete, much work remains to deploy a multilingualized Internet. Today, there are around 150 internationalized domain names (IDNs), but equal rollout of these scripts at the domain level is hindered primarily by software and applications that do not yet recognize these new scripts. "Universal Acceptance" is a program of action for the Internet community at large that can ensure that IDNs are accepted and treated consistently.

2.2.3. Web Affordability and Inclusiveness

In "A Framework for Improving Web Affordability and Inclusiveness", Rumaisa Habib presented research on the connection between website size and cost to end users [HABIB]. This critical inquiry presents access in terms of affordability and through measurement demonstrates that the material costs to end users who pay for their connection based on the volume of data they download and upload have risen as the complexity of the Web grows. Their research provides a framework for optimization based on end-user affordability. This framework is anchored in reality: [HABIB] proposes a fairness metric and suggests systematic adaptations to complexity of the Web based on "geographic variations in mobile broadband prices and income levels."

2.2.4. Discussion

These three reports discuss very different aspects of current inequalities in Internet access in various parts of the world: service provisioning, availability, and economic costs. Notably, the reports discuss trends that exacerbate the digital divide beyond the question of connectivity or whether users have access to the Internet, potentially yielding concrete ways that the IETF community can address digital inclusion within its remit.

Discussants noted that while there are some interesting aspects to the problem of the digital divide, such as measurements and frameworks, most of the work involves getting this work to the appropriate people at the policy level; therefore, it is important to communicate this

technical evidence to the appropriate people. The IETF's role could be to build consensus on the proper solutions presented to decision-makers that put research and measurement not only in context but also in a consensus-driven solution space. Another method to better communicate this research is by telling stories of end users in more relatable and relevant terms; this is often a challenge at the technical level and a role for more diverse stakeholders at the more local level.

2.3. Session 3: Censorship - Reports and Circumvention

This session focused on reports of censorship as observed in recent years in different parts of the world; it also focused on the use of, and expectations for, censorship circumvention tools, mainly the use of secure VPN services.

The censorship reports highlighted legal frameworks and court actions that put legal obligations on regional network providers to block traffic. The discussion focused on Asia, specifically India, and included Russia as an example where censorship practices have recently undergone significant changes. Further, measurements to validate the blocking as well as analyses of how blocking is implemented were discussed, i.e., which protocols are used but also which kinds of devices are used to configure the blocking rules and where they are deployed.

2.3.1. Censorship Orders, Measurements, and Device Analysis

[SAMSUDIN] reported on confirmed blocking from 10 countries (Cambodia, Hong Kong (China), India, Indonesia, Malaysia, Myanmar, Philippines, Thailand, Timor-Leste, and Vietnam) in the period from 1 July 2022 to 30 June 2023. The blocking was confirmed by (1) Open Observatory of Network Interference (OONI) measurements for existing blocking fingerprints, (2) heuristics (i.e., for new blocking fingerprints as well as news reports of blocking orders), or (3) user experiences. Most of these countries block specific content such as porn, gambling, or certain news pages. Interestingly, the blocking in Hong Kong and Myanmar is focused on the military and governmental pages of foreign countries. Blocking is often realized by either DNS tampering or HTTP tampering. For DNS, either a chosen IP address, a bogon IP address (e.g., 127.0.0.1), or an empty domain (NXDOMAIN) is used. In the case of DNS tampering using a chosen IP address or HTTP tampering, some countries provide a block page that exposes the blocking; however, more transparency related to blocking is requested by civil society organizations and the Internet Monitoring Action Project (iMAP).

[GROVER] further focused the discussion on online censorship in India, Pakistan, and Indonesia. In India, where providers are responsible for implementing the blocking but no method is mandated, the six major ISPs (covering 98.82% of all subscribers) were tested on 4379 blocked websites (based on court orders, user reports, and publicly available or leaked government orders) by using DNS poisoning/injection or using censorship based on HTTP or the Server Name Indication (SNI). The censorship techniques used and websites blocked were different across ISPs. Multiple ISPs used two different techniques (depending on the website), and all but one provided censorship notices. Providers blocked between 1892 and 3721 (of 4379) pages with only 1115 pages (27.64%) blocked by all ISPs [Singh2020].

In contrast, in Pakistan, the government can also order the ISPs to perform blocking, and blocking has even been observed in the past at the Internet Exchange Point (IXP) level. Since 2020, there has also been a central Web Monitoring System deployed at lines of international connectivity. In Indonesia, initially, the government guided ISPs in how to perform the blocking. The regulations were updated in 2020 to allow Indonesian ISPs to block websites at their discretion. In 2022, there was a proposal by ISPs to centralize DNS. In Indonesia, a partial blocklist is publicly available, but without any indication of why something is blocked [Grover2023].

[BASSO] reported that for Russia a large increase in additions to Roskomnadzor's blocklist was observed in March 2022 as well as in December 2022, foremost covering news pages but also covering human rights organizations and social media, where more than 3500 blocking orders were added to the list by an "Unknown body". Further, blocking of domains that are not in the official Roskomnadzor blocklist has been observed as well.

An invited talk included a presentation of the work in [WANG] on locating censorship devices by using HTTP and TLS traceroutes, identifying device vendors through fingerprinting, and reverse-engineering censorship triggers by the use of fuzzing. For example, in the case of Azerbaijan and Kazakhstan, they showed that a significant portion of measurements from remote countries is blocked at the endpoint, indicating local policies, but showed that connection resets are also happening in Belarus and Russia. Further, they could identify a set of commercial network devices (with filtering techniques such as firewalls) that are used in these countries for censorship and show how fuzzing can be used to fingerprint and cluster behaviors as well as potentially circumvent the deployed methods.

All speakers called for more transparency by requiring blocking messages as well as publication and auditing of blocklists. Potentially, even standardization could help.

2.3.2. Use of VPNs for Censorship Circumventions and User Expectations

Further on in the session, the possibility and prevalence of using VPNs for circumvention were discussed, including user expectations and an analysis of security shortcomings of commercial VPN services. The analysis presented in [RAMESH-1] highlights various issues that lead to data leaks -- such as the leakage of IPv6 traffic, non-browser traffic, or failures in tunneling -- resulting in a failure to meet user expectations, particularly in scenarios involving censorship circumvention or private communication in authoritarian regimes.

The question of how common the use of VPNs for circumvention is and its legal implications, as VPNs are illegal in a few countries, was discussed. For example, VPNs are not officially banned in India, but VPN providers need to store log data and those who haven't complied stopped serving India. However, more data on VPN use and blocking might be needed.

2.3.3. Discussion

After all, there is a cat-and-mouse game between censorship and circumvention; however, continued work on protocol enhancements that protect user privacy is essential.

2.4. Key Takeaways

Some key takeaways from the workshop are as follows:

- There is a need for the technical community to address the management gaps in operating Community Networks.
- Work should be done to document best practices for operating Community Networks.
- During the development of protocols, explicit manageability considerations related to Community Networks should be carefully thought out.
- Build consensus on solutions that have the most significant impact in fostering digital inclusion. Further, promoting these solutions ensures that efforts to bridge the digital divide are effective and inclusive.
- Further work should be done to enhance protocols, ensuring that user privacy is preserved.
- Develop further protocols (or extensions to existing protocols) that enable more transparency on filtering, and promote their use and deployment.
- Develop new VPN-like services and potentially support measurements to understand their deployment and use.
- Further discussion of these topics could happen in the GAIA Research Group, the Human Rights Protocol Considerations (HRPC) Research Group, the Privacy Enhancements and Assessments Research Group (PEARG), and the Measurement and Analysis for Protocols Research Group (MAPRG), based on relevance to the research group. Management-related and operations-related discussions can be taken to the IETF Operations and Management Area Working Group (OPSAWG). The community could also explore whether a group focused on censorship (and its circumvention) could be created.

3. IANA Considerations

This document has no IANA actions.

4. Security Considerations

This document is a workshop report and does not impact the security of the Internet.

5. Informative References

[APC] "The Association for Progressive Communications (APC)", <https://www.apc.org>.

[BASSO] Basso, S., "How Internet censorship changed in Russia during the 1st year of military conflict in Ukraine", January 2024, <https://datatracker.ietf.org/meeting/interim-2024-biasws-03/materials/slides-interim-2024-biasws-03-sessa-slide-how-internet-censorship-changed-in-russia-during-the-1st-year-of-military-conflict-in-ukraine-00.pdf>.

[BENSON] Benson, T. A. and M. Fayed, "A 'C' in CDN: Access service to and from the Internet at cost for community networks", January 2024, <https://www.ietf.org/slides/slides-biasws-a-c-in-cdn-access-service-to-and-from-the-internet-at-cost-for-community-networks-00.pdf>.

[GAIA] "Global Access to the Internet for All Research Group (GAIA)", <https://www.irtf.org/gaia.html>.

[GROVER] Grover, G., "Online censorship in India, Pakistan and Indonesia", January 2024, <https://datatracker.ietf.org/meeting/interim-2024-biasws-03/materials/slides-interim-2024-biasws-03-sessa-online-censorship-in-india-pakistan-and-indonesia-00>.

[Grover2023] Grover, G., "The infrastructure of censorship in Asia", in "Eaten by the Internet", ed. Corinne Cath, pp. 75-81, Internet Archive, Meatspace Press, October 2023, <https://archive.org/details/eaten-by-the-internet/>.

[GUIFI] "guifi.net", <https://guifi.net/en>.

[HABIB] Habib, R., Tanveer, S., Inam, A., Ahmed, H., Ali, A., Uzmi, Z. A., Qazi, Z. A., and I. A. Qazi, "A Framework for Improving Web Affordability and Inclusiveness", ACM SIGCOMM '23, pp. 592-607, DOI 10.1145/3603269.3604872, September 2023, <https://www.ietf.org/slides/slides-biasws-a-framework-for-improving-web-affordability-and-inclusiveness-00.pdf>.

[HOLZ] Holz, R., Nazemi, N., Tavallaie, O., and A. Y. Zomaya, "Evidence for a digital divide? Measuring DNS dependencies in the context of the indigenous population of Australia", 2023, <https://www.ietf.org/slides/slides-biasws-evidence-for-a-digital-divide-measuring-dns-dependencies-in-the-context-of-the-indigenous-population-of-australia-00.pdf>.

[HU] Hu, P., "Closing the Performance and Management Gaps with Satellite Internet: Challenges, Approaches, and Future Directions", January 2024, <https://www.ietf.org/slides/slides-biasws-closing-the-performance-and-management-gaps-with-satellite-internet-challenges-approaches-and-future-directions-01.pdf>.

[HUSSAIN] Hussain, S., "Universal Acceptance of Domain Names and Email Addresses: A Key to Digital Inclusion", 2023, <https://www.ietf.org/slides/slides-biasws-universal-acceptance-of-domain-names-and-email-addresses-a-key-to-digital-inclusion-01.pdf>.

[ISOC] Internet Society, "Connecting the Unconnected: Community networks help bridge the connectivity gap", <https://www.internetsociety.org/action-plan/community-networks/>.

[MARTINEZ] Martínez-Cervantes, L. M. and R. Guevara-Martínez, "Community Networks and the Quest for Quality", January 2024, <https://www.ietf.org/slides/slides-biasws-community-networks-and-the-quest-for-quality-00.pdf>.

[OHLSEN] Ohlsen, L.Y., "BIAS workshop - M-Lab Position Paper submission", December 2024, <https://www.ietf.org/slides/slides-biasws-m-lab-position-paper-01.pdf>.

[OTT] Ott, J., Bartolomeo, G., Bese, M.M., Bose, R., Bosk, M., Guzman, D., Kärkkäinen, L., Kosek, M., Mohan, N., Trossen, D., Welzl, M., and L. Vogel, "The Internet: Only for the Fast?", January 2024, <https://www.ietf.org/slides/slides-biasws-the-internet-only-for-the-fast-00.pdf>.

[PANGEA] Cloudflare, "Project Pangea: Helping underserved communities expand access to the Internet for free", <https://www.cloudflare.com/en-gb/pangea/>.

[RAMESH-1] Ramesh, R., "Investigating the VPN Ecosystem through the lens of Security, Privacy, and Usability", January 2024, <https://datatracker.ietf.org/meeting/interim-2024-biasws-03/materials/slides-interim-2024-biasws-03-sessa-investigating-the-vpn-ecosystem-through-the-lens-of-security-privacy-and-usability-00>.

[RAMESH-2] Ramesh, R., Vyas, A., and R. Ensafi, ""All of them claim to be the best": Multi-perspective study of VPN users and VPN providers", 32nd USENIX Security Symposium (USENIX Security '23, August 2023, <https://www.usenix.org/conference/usenixsecurity23/presentation/ramesh-vpn>.

[RENNO] Rennó, R., "Maximising Connectivity: The Spectrum's Vital Role in Technology Access", January 2024, <https://www.ietf.org/slides/slides-biasws-position-paper-by-raquel-renno-01.pdf>.

[RFC7962] Saldana, J., Ed., Arcia-Moret, A., Braem, B., Pietrosemoli, E., Sathiaseelan, A., and M. Zennaro, "Alternative Network Deployments: Taxonomy, Characterization, Technologies, and Architectures", RFC 7962, DOI 10.17487/RFC7962, August 2016, <https://www.rfc-editor.org/info/rfc7962>.

[SAMSUDIN] Samsudin, S., "iMAP (Internet Monitoring Action Project) 2023 Internet Censorship Report", January 2024, <https://www.ietf.org/slides/slides-biasws-imap-internet-monitoring-action-project-internet-censorship-report-02.pdf>.

[SDGs] United Nations Department of Economic and Social Affairs - Sustainable Development, "The 17 Goals", <https://sdgs.un.org/goals>.

[Singh2020] Singh, K., Grover, G., and V. Bansal, "How India Censors the Web", WebSci '20: Proceedings of the 12th ACM Conference on Web Science, pp. 21-28, DOI 10.1145/3394231.3397891, July 2020, <https://arxiv.org/pdf/1912.08590>.

[TBB] "Tribal Broadband Bootcamp", <https://tribalbroadbandbootcamp.org/>.

[WANG] Raman, R. S., Wang, M., Dalek, J., Mayer, J., and R. Ensafi, "Network Measurement Methods for Locating and Examining Censorship Devices", November 2023, <https://datatracker.ietf.org/meeting/interim-2024-biasws-03/materials/slides-interim-2024-biasws-03-sessa-network-measurement-methods-for-locating-and-examining-censorship-devices-00.pdf>.

Appendix A. Position Papers

Nineteen position papers were submitted to the workshop call for papers. Twelve were selected for publication. Papers that were not published either (1) only provided a very prelimited analysis of an idea that was felt to be incomprehensive for discussion at the workshop or (2) addressed problems that were considered beyond the scope as dedicated for the workshop discussion, e.g., discussing cybersecurity threats as a barrier to participation or implication of technology in a regulation that imposes blocking. Both of these topics pose a potentially severe risk for the open Internet; however, they might pose a high risk for all Internet users but do not necessarily imply an unbalance.

All accepted papers are available at <https://datatracker.ietf.org/group/biasws/materials/>.

This is the list of all published papers:

Community Networks:

- Martínez-Cervantes, L. M. and R. Guevara-Martínez: Community Networks and the Quest for Quality [MARTINEZ]
- Benson, T. A. and M. Fayed: A 'C' in CDN: Access service to and from the Internet at cost for community networks [BENSON]
- Hu, P.: Closing the Performance and Management Gaps with Satellite Internet: Challenges, Approaches, and Future Directions [HU]
- Rennó, R.: Maximising Connectivity: The Spectrum's Vital Role in Technology Access [RENNO]

Digital Divide:

- Holz, R., Nazemi, N., Tavallaie, O., and A. Y. Zomaya: Evidence for a digital divide? Measuring DNS dependencies in the context of the indigenous population of Australia [HOLZ]
- Hussain, S.: Universal Acceptance of Domain Names and Email Addresses: A Key to Digital Inclusion [HUSSAIN]
- Habib, R., Tanveer, S., Inam, A., Ahmed, H., Ali, A., Uzmi, Z. A., Qazi, Z. A., and I. A. Qazi: A Framework for Improving Web Affordability and Inclusiveness [HABIB]
- Ott, J., Bartolomeo, G., Bese, M.M., Bose, R., Bosk, M., Guzman, D., Kärkkäinen, L., Kosek, M., Mohan, N., Trossen, D., Welzl, M., and L. Vogel: The Internet: Only for the Fast? [OTT]
- Ohlsen, L.Y.: BIAS workshop - M-Lab Position Paper submission [OHLSEN]

Censorship:

- Samsudin, S.: iMAP (Internet Monitoring Action Project) 2023 Internet Censorship Report [SAMSUDIN]
- Grover, G.: The infrastructure of censorship in Asia [Grover2023]
- Basso, S.: How Internet censorship changed in Russia during the 1st year of military conflict in Ukraine [BASSO]

In addition to the submitted papers, two invited talks were included, based on published papers:

- Raman, R. S., Wang, M., Dalek, J., Mayer, J., and R. Ensafi: Network Measurement Methods for Locating and Examining Censorship Devices [WANG]
- Ramesh, R., Vyas, A., and R. Ensafi: "All of them claim to be the best": Multi-perspective study of VPN users and VPN providers [RAMESH-2]

Appendix B. Workshop Participants

The workshop participants were Arnaud Taddei, Carlos Pignataro, Carsten Bormann, Cindy Morgan, Colin Perkins, Cory Myers, Dan Sexton, David Guzman, David Millman, David Schinazi, Dhruv Dhody, Gurshabad Grover, Hanna Kreitem, Jane Coffin, Jiankang Yao, Jörg Ott, Juan Peirano, Lai Yi Ohlsen, Luis Martinez, Mallory Knodel, Marwan Fayed, Matthew Bocci, Michael Welzl, Michuki Mwangi, Mirja Kühlewind, Mona Wang, Peng Hu, Ralph Holz, Raquel Rennó, Reethika Ramesh, Rumaisa Habib, Sarmad Hussain, Simone Basso, Siti Nurliza Samsudin, Suresh Krishnan, Theophilus Benson, Tirumaleswar Reddy.K, Tommy Pauly, Vesna Manojlovic, and Wes Hardaker.

Appendix C. Workshop Program Committee

The workshop program committee members were Christopher Wood (IAB, Cloudflare), Dhruv Dhody (IAB, Huawei), Mallory Knodel (IAB, Center for Democracy and Technology), Mirja Kühlewind (IAB, Ericsson), and Tommy Pauly (IAB, Apple).

IAB Members at the Time of Approval

Internet Architecture Board members at the time this document was approved for publication were:

Matthew Bocci

Alissa Cooper

Roman Danyliw

Dhruv Dhody

Wes Hardaker

Cullen Jennings

Suresh Krishnan

Mirja Kühlewind

Tommy Pauly

Alvaro Retana

David Schinazi

Christopher Wood

Qin Wu

Acknowledgments

Thanks to Arnaud Taddei for helpful suggestions to improve this report.

Authors' Addresses

Mirja Kühlewind
Email: ietf@kuehlewind.net

Dhruv Dhody
Email: dd@dhruvdhody.com

Mallory Knodel
Email: Mallory.knodel@nyu.edu