DNS Dependencies as an Expression of the Digital Divide: the Example of Australia

Niousha Nazemi[1][0000−0003−4085−7044], Omid Tavallaie[1][0000−0002−3367−1236], Albert Y. Zomaya[1][0000−0002−3090−1059], and Ralph Holz[1,2][0000−0001−9614−2377]

[1] School of Computer Science, The University of Sydney, Australia
[2] Department of Mathematics and Computer Science, University of Münster, Germany
{niousha.nazemi,omid.tavallaie,albert.zomaya,ralph.holz}@sydney.edu.au

Abstract. This paper investigates the relationship between the digital divide, Internet transparency, and DNS dependencies. The term "digital divide" refers to a gap between how different population groups can access and use digital technology, with disadvantaged groups generally having less access than others. Internet transparency refers to efforts that reveal and understand critical dependencies on the Internet. DNS is a vital service in the Internet infrastructure. It has become common for network and website operators to outsource the operation of their DNS services to a (limited) number of specialized DNS providers. Depending on the choice of provider, a network or site may achieve better or worse availability, especially under adversarial conditions (power outages, attacks, etc.). This work-in-progress paper analyzes DNS provisioning and dependencies for Australian government websites to identify a possible digital divide. More specifically, we investigate setups with respect to potential drawbacks in terms of availability or domestic control over the setup. We choose sites whose audience is primarily the indigenous population and sites that target the broader, general population. We can indeed identify differences between the DNS dependencies, in particular with respect to the use of hyperscalers, domestic vs. international providers, and dedicated government infrastructure. The implications for availability and control are more subtle and require further investigation. However, our results show that Internet measurement can detect signals of possible digital divides, and we believe this aspect should be added to the Internet transparency agenda.

Keywords: Internet transparency · Digital divide · DNS dependency · Indigenous people.

1 Introduction

The concept of the digital divide has been the subject of much research and discussion over the past 20 years. The term was first introduced and defined in the mid-to-late 1990s in a series of reports titled "Falling through the net" [27–29]. The definition refers to the gap between individuals or groups who have access to and effectively use digital technologies and those who do not. This includes access to technologies such as the Internet [30]. Individuals who have access to and utilize these technologies are considered advantaged, while those who lack access or proficiency are at a disadvantage [22]. A digital divide often affects already economically disadvantaged groups. The indigenous people of Australia consist of two distinct cultural groups: the Aboriginal peoples of the Australian mainland and Tasmania and the Torres Strait Islander peoples from the seas between Queensland and Papua New Guinea. It is known that indigenous communities face challenges in accessing digital information and acquiring the necessary skills for effective utilization [23].

In recent years, the term "Internet transparency" has come into use to refer to efforts to understand how the Internet works and identify critical dependencies [15]. Internet transparency has a natural connection to research on the digital divide: differences in how Internet services are set up for different groups have implications for how these groups can access the Internet. In this sense, revealing Internet dependencies can reveal implications for the digital divide. This is also evident in core Internet infrastructure, namely the Domain Name System (DNS). Here, much centralization and consolidation have occurred [9, 10]. This refers to the dominance of a limited number of large service providers who exert significant control over various aspects of the DNS. DNS employs a hierarchical configuration with multiple authoritative name servers to distribute the workload and enhance the name resolution process. However, today, much of this setup is in the hands of very few providers, and major companies such as Microsoft, Amazon, Cloudflare, and Google have significant influence over DNS provisioning. Where operators choose to outsource the operation of their DNS, the implication is that their users also rely on (a possibly limited) number of (possibly centralized) providers to access Internet services of relevance to them. It has been stated that this dependency on a few providers increases the vulnerability to potential attacks and raises concerns about the overall resilience of Internet services [4, 25].

The question we ask in this paper is whether DNS dependencies impact how vulnerable groups can access Internet-based services. We focus on analyzing the impact of the digital divide on indigenous communities in Australia regarding their DNS-mediated access to government websites. Given their geographically dispersed nature, service outages can significantly impact this vulnerable group. We examine the disparities in DNS dependencies of governmental services for the indigenous and general populations. Our findings imply differences between the setups do exist: sites for the indigenous population use different cloud providers, and when they use smaller providers, these are often domestic rather than international. While sites for the general population are sometimes run on what seems to be government-owned infrastructure, we find no such setups for sites for the indigenous population.

2 Related Work

The digital divide has been investigated in numerous works, including [17, 24, 31]. In [31], Wang et al. investigated the digital divide through the lens of energy poverty and found that it negatively impacts the usefulness of the Internet. The extreme remoteness and isolation of indigenous communities in Australia contribute to the existing digital divide that reduces the quality of Internet connectivity and limits access to Internet services [17, 24]. The phenomenon of Internet centralization [14] and consolidation has also been studied in previous work. For example, Zembruzki et al. [33, 34] examined the growing concentration of Internet infrastructure and the consolidation of the DNS industry. Their findings reveal the dominance of a few key DNS providers. A study by Moura et al. [19] explored the impact of centralization on DNS traffic and identified vulnerabilities, such as TsuNAME [20], which can lead to service disruptions and traffic escalation. Concerning DNS dependencies, Deccio et al. [11–13] developed graph-based models to investigate name dependencies. Xu et al. [32] proposed a general graph model that illustrates the dependency relationships between domains and servers for name resolution.

The prevalence and impact of third-party dependencies have been analyzed by Kashaf et al. [18] and Urban et al. [26], focusing on vulnerabilities and the concentration of dependencies on third-party service providers. The vulnerability of government domains has been investigated in [16]. The authors studied the availability of DNS records for government domains across more than 190 countries, including an investigation of the increasing reliance on a single third-party DNS service provider and of vulnerabilities to hijacking due to defective delegations. The authors also found that government domains are vulnerable to DNS misconfigurations, which can lead to service degradation or even service interruption.

In this paper, we explore the implications of DNS dependencies on the different population groups of one country, namely the indigenous populations in Australia and the general population of Australia. Our focus is on the effects of differing DNS setups between the services for these groups. To the best of our knowledge, this research is the first of its kind to investigate this aspect of DNS dependencies.

3 Methodology

In the following, we explain how we created lists with the domain names of the relevant services provided by the Australian government for the indigenous populations as well as the general population, and how we retrieved their DNS records. Our objective is to create two lists: one with the domain names of Australian government websites that provide services to the general population and one with domain names of Australian government websites that provide services for the indigenous populations. To the best of our knowledge, there are no existing open-access data sets for this purpose. We adopt a desk research approach to identify the domains of interest. While we go beyond second-level domains and consider subdomains (which may have their own authoritative name servers), we use the general term “domain” or “domain name” to refer to all of these jointly. We undertook the following steps in the first quarter of 2023. To achieve two distinct sets of domain names for the indigenous and the general population, we perform the steps below in two rounds. In the first round, we add the following indigenous-related terms: *indigenous*, *Aboriginal people and Torres Strait Islanders*, and *first nations* to keywords to collect domain names dedicated to services for the indigenous population. In the second round, we use keywords without these terms to capture domain names for the general public.

1. *Initialization:* By *manual* investigation, we identify 16 categories of services offered by the Australian government, including healthcare, disability support, education programs, and housing support [7]. The category names serve as the primary set of keywords to facilitate the search for relevant domains and websites.
2. *Web search:* We use Google to fetch pertinent governmental websites using our seed keywords. We restrict our search to websites with the *.gov.au* suffix to guarantee we include only official government websites.
3. *Crawling* We download the top 100 Google search results and store them.
4. *Keyword extraction:* We employ a word cloud technique to extract the top five most prevalent and contextually relevant words from each relevant web page. The relevancy check is performed manually. These extracted keywords are then compared with existing keywords in the set, and new keywords are added to the set for further web search.
5. *Domain names:* We also add the domain names of the sites to our list if we identify them (manually) as relevant.
6. *Iteration:* We iterate through steps 2-5 until we can identify no additional keywords or domain names (The final keywords set is included in Table 2 and sorted based on the 16 categories).

Once the domain names are obtained, we also perform manual validation to ensure that the collected domain names align with the intended target audience. We finally obtain two lists with unique and relevant domains, each for the respective target audience (448 domains for the general population group and 54 domains for the indigenous group; the list of these domains and their DNS records are uploaded to our GitHub repository for public access [21]). We proceed to retrieve the authoritative name servers (NS) for the collected domain names by querying every authoritative NS to whom we observed a delegation. We utilize standard tools for DNS look-ups provided by the Linux operating system, as speed is no concern. To maximize coverage, we follow the delegations from the root servers, which allows us to capture the authoritative NS records. We follow the delegations until we reach the final authoritative name servers (we performed retries for several domains in Tasmania, while no such errors or timeouts were encountered in other instances). This process took place until the end of March 2023. In addition, we also utilize the WHOIS command to gather information about the associated provider for each identified name server. We create the delegation graphs to analyze the dependencies. The relationship between domains and their name servers can be categorized as either direct or indirect dependencies. A direct dependency is a domain being directly associated with its designated name servers. These associations indicate an immediate connection between a governmental website and its corresponding DNS service provider. For the analysis presented here, we focus only on these; the analysis of indirect dependencies is ongoing. We briefly revisit indirect dependencies in Section 5.

4 Results

We analyze the dependency patterns for domains for the general and indigenous populations across various DNS providers. Table 1 provides key statistics on the dependencies we find for various provider types. The table also presents the percentage of domains with a dependency on a single provider versus a dependency on multiple providers. We distinguish between the following kinds of DNS providers:

Leading providers: We use the term "leading providers" to refer to prominent DNS service providers with a significant market presence and influence. These are widely known cloud providers often referred to as hyperscalers. They are often US-headquartered and relied on by a very large number of domains. Understanding dependencies on such leading providers enables us to assess the concentration of control within the DNS infrastructure of the domain we investigate. On the one hand, if many domain names on our lists are served by the same leading provider, an outage or attack may take them all offline. Similarly, one vulnerability in a hyperscaler may impact a vast number of customers. On the other hand, such leading providers also have the resources to fend off attacks and generally have specialists to deal with security issues. Outages and vulnerabilities are hence (very) low frequency–very high impact scenarios. Hyperscalers are a common choice when services must be reachable quickly across a wide geographic area. However, the fact that they are generally headquartered in another country also implies a certain amount of loss in digital sovereignty when they are chosen over a local, domestic provider. The observed leading providers in our data set are: Amazon, Microsoft, Cloudflare, Akamai, EasyDNS, Google, Microsoft, Neustar Ultra DNS, and DNS Simple.

Non-leading providers is our term for DNS providers outside the group of the leading (hyperscaler) providers. They generally have a smaller market share and fewer cloud resources and represent a wide and diverse range of DNS service providers. Many domestic (Australian) providers fall into this category. Non-leading providers are usually unable to offer the reliability and scalability of hyperscalers. Their availability and security stance vary widely, although it is plausible that at least their availability is lower than that of a hyperscaler, and they may be less capable of fending off a sophisticated, large, or sustained attack such as one may expect from state actors.

Intra-government providers are those where the respective governmental sections are responsible for hosting and managing their DNS infrastructure, including offering DNS provisioning for other government sections. We filter the name servers with the *.gov.au suffix to find government-owned providers.

Undisclosed providers: For about two percent of general domains, we could not further identify the DNS providers from either the WHOIS or the domain names of the NS records. We label them as "undisclosed".

Table 1. Dependency on third-party DNS providers for general and indigenous domains.

Population group	General		Indigenous	
	Absolute	Relative	Absolute	Relative
Number of domains	448	100%	54	100%
Depends on…				
… leading providers	219	48.9%	29	53.7%
… non-leading providers	140	31.3%	25	46.3%
… intra-government providers	113	25.2%	0	
… single provider	412	92%	54	100%
… multiple providers	36	8%	0	0
… intra-government + 3rd party providers	19	4.2%	0	0
Undisclosed	8	1.8%	0	0

4.1 Analysis by Provider Type

Fig. 3 illustrates the relationships between domains and DNS providers that we group as “leading”, “non-leading”, and “intra-government” dependencies. While some general domains have implemented a multi-provider strategy, possibly to mitigate risks associated with a single, critical dependency, the practice is not widespread. It is particularly noteworthy that it is absent for domains for the indigenous population.

Single-provider setups We first investigate how many domains rely on a single DNS provider, which is a critical metric: outage of this provider will make the relying services unavailable. We find that 92% of all domains for the general population rely on a single provider. *All* of the domains for the indigenous populations do so. This implies a generally unsatisfactory state across all government domains, but it is also a first hint that there is a difference between the services for the two population groups.

Multi-provider setups Having multiple DNS providers offers benefits in terms of redundancy and resilience. In the event of a service outage or disruption from one provider, the availability of DNS services can be maintained through the alternative provider. Inequalities in the use of multi-provider strategies hence reflect differences in access to information and online services. Fig. 1 shows the distribution of domains with a multi-provider dependency for the general population (none of the indigenous websites have multiple DNS providers). We find that 20% of setups have a dependency on two distinct leading DNS providers (Amazon and Microsoft); this was observed for eight domains of the Victorian government. More than 50% of setups use a governmental provider along with a third-party DNS as an alternative server.

Use of leading providers Hyperscalers may offer higher availability and potentially better security than smaller providers. Approximately half of the domains for both the general and indigenous populations rely on a single leading DNS provider. Only around 2% of the domains for the general population employed *two leading* providers, with the remainder using either a second non-leading or intra-government provider. Fig. 2 shows a breakdown of the leading DNS providers for our domains. For the general population, 48.9% of domains

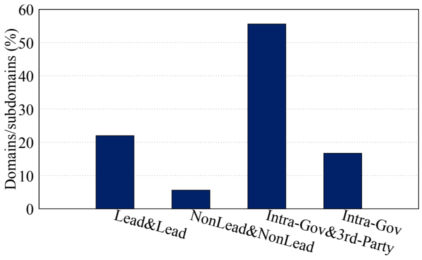

Fig. 1. Multi-DNS-provider setups. Note that no domains for the indigenous population use such a setup.

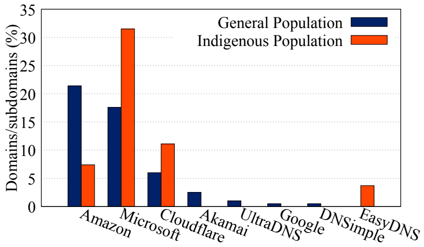

Fig. 2. Leading DNS providers.

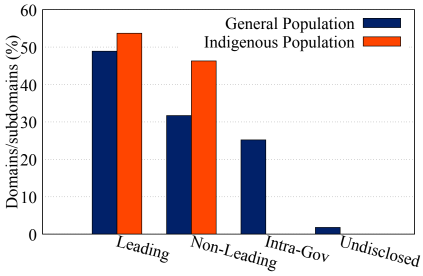

Fig. 3. DNS providers by category.

rely on leading providers, with Amazon being the most utilized provider at 21.4%. Microsoft is the second most commonly used provider at around 17%, followed by Cloudflare at 6%. Other leading providers, such as Akamai, UltraDNS, Google, DNSimple, and EasyDNS, are used in less than 5% of DNS services for the general population. Regarding domains for the indigenous population, 53.7% of them rely on leading providers. Microsoft is the most utilized provider at 31.5%, followed by Cloudflare (11.1%) and Amazon (7.4%). No other leading providers are in use for these domains. Comparing the two groups of domains, we identify a common preference for leading providers, although the preferred providers differ starkly. Cloudflare offers a free tier, which may explain this common choice in the second group of domains. There is slightly less variety in the chosen providers in the case of the domains for the indigenous population.

Use of non-leading providers and intra-government providers: As we see in Fig. 3, slightly more than half of domains for the general population rely on at least one non-leading provider or an intra-government provider, with an almost equal split between the latter two. We do not observe this for the domains of the indigenous population: here, 46.3% of the domains rely on non-leading providers, and none use intra-government providers. Government-hosted providers would be required to comply with Australian standards and government regulations, and using these providers implies a certain level of coordination and collaboration. We list the government sections we observe in the domain name of the NS records in Table 3 in the Appendix. While we observe only about 15 government agencies operating name servers, we see that they serve well over 100 different domains. It seems curious that no single service for the indigenous population is among these. Fig. 4 shows whether the non-leading providers are domestic or international.

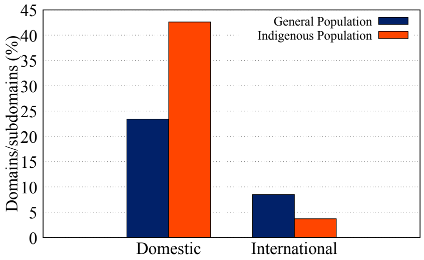

Fig. 4. Use of non-leading providers.

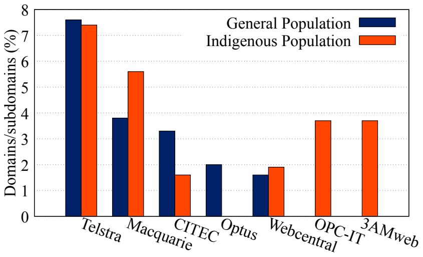

Fig. 5. Domestic providers.

The fraction of domestic providers is significantly higher for both domain groups. Concerning domains for the general population, 23.4% of domains rely on local DNS providers, indicating a preference for domestic services. The percentage of the domains for the indigenous population is considerably higher (but recall that domains of this group do not use intra-government provisioning). Fig. 5 breaks down the numbers for domestic DNS providers. Telstra, as Australia's largest telecommunications company by market share [8], is the most commonly used DNS provider. Macquarie Telecom is the second most utilized provider, followed by the Centre for Information Technology and Communication [2]) and WebCentral. While all previous, mostly common used providers are domestic, 14 domains for the general population rely on the US-based company Verizon. For the domains for the indigenous population, the order is similar, except for two providers that domains for the general population never use and that are not as well known (OPC IT and ThreeAMWeb); also, Optus is not used at all. Out of the 33 non-leading providers observed, 22 are domestic. Our primary finding here is the curious lack of intra-government provisioning for sites for the indigenous population, which comes with (or results in) the comparatively more common use of more domestic providers. On the whole, a diverse range of non-leading DNS providers is used for both the general and indigenous populations, with limited reliance on non-Australian companies.

5 Limitations

Our study has several limitations owing to the early stage of our work.

Indirect dependencies: Naturally, dependencies higher up the chain of DNS delegations have an impact on availability and security properties as well. Our analysis of indirect dependencies has only begun. So far, we have found several cases where a leading DNS provider is actually a delegation from a non-leading one. Understanding precisely in which cases this is problematic is the subject of ongoing work.

Longitudinal observations: Our current study is a snapshot in time. It would be helpful to study the DNS dependencies over a more extended period to understand the dynamics of DNS provisioning.

Small sample: There are significantly fewer domains for the indigenous population than for the general population. This is expected, but one needs to pay attention when comparing small percentages between the groups. It may also offer a partial explanation for the smaller variety of non-leading providers we find for this domain group.

Specific focus: Our findings are specific to the Australian indigenous population and the local DNS landscape. While our study is centered on analyzing DNS dependency among Australian indigenous governmental domains compared to the general population, our methodology can be adapted for broader applications. The approach we have utilized to assess DNS dependencies is transferable to other vulnerable groups within and beyond Australia. Contextual considerations should be considered when considering the applicability of results.

Other forms of outsourcing: We currently use DNS names and the WHOIS to identify the operators of authoritative name servers. However, future work will also need to investigate the ownership of the IP ranges where the authoritative nameservers reside. Although one would not expect many such configurations, it is possible to hide the identity of an actual DNS operator to varying degrees. For example, it is possible to outsource DNS provisioning to organizations that hint at their existence in neither the names of the authoritative nameservers nor the WHOIS. This would be a possibility in the case of sub-contracting. Similar forms of sub-contracting may also occur between different branches of government and be hidden in what we currently call intra-government provisioning.

6 Discussion and Conclusion

We summarize our findings, discuss possible implications, and give future research directions:

Summary: In line with previous findings, we find a significant concentration of DNS services among a few providers for both domain groups: about half of the domains in each group use leading providers. Only some domains for the general population use a multi-provider setup; otherwise, this approach to increase availability and resilience is never used. The leading providers differ between the domain groups, with Amazon being more commonly used in the group of domains for the general population and Microsoft in the one for the indigenous population. Cloudflare is also much more common for the latter group. The company's free tier may be a reason, although this needs to be investigated in more detail. Domains for the indigenous population also use a smaller number of leading providers overall; but here, we need to caution that the number of domains in this group is much smaller. The possibly most interesting difference between the two domain groups can be found in the use of intra-government provisioning. The latter does not occur for domains for the indigenous population but is common for domains for the general population.

Implications: We set out to identify possible disparities in the DNS dependencies for sites for different population groups. We find evidence that dependencies for the indigenous population are indeed differently configured, and we view our evidence as indicative of different provisioning concepts being employed. However, the exact implications of this are much less clear. In particular, does this result in a tangible digital divide? It seems clear to us that follow-up measurements will be needed to decide this question. In the following, we offer some more detailed thoughts. The lack of intra-government provisioning for indigenous population domains is noteworthy, but there may be practical or legal reasons why we do not find such setups. A qualitative study could shed light on this. As single-provider setups are so common, it is too early to speak of a digital divide in terms of availability. In particular, it is unclear whether intra-government provisioning or the use of smaller domestic providers will improve availability, which can be decided with Internet measurements. We observed some lack of provider diversity among both domain groups, particularly in the case of leading providers used by domains for the indigenous population. Here, Cloudflare was also more common (possibly because of their free tier). Together with the fact that over 40% of indigenous domains use domestic DNS providers, this may indicate a desire to improve DNS resolution but an inability or unwillingness to move to the cloud. Again, a qualitative study could help illuminate this. Finally, we observe that nearly half of the domains use domestic DNS providers (non-leading or intra-governmental), across both domain groups, which means less reliance on international corporations. In this respect, the nature of the divide is different (non-leading vs. intra-governmental provisioning), but not the quantity.

Perhaps most importantly, our findings support the case for Internet transparency. More precisely, we argue that it is a worthwhile undertaking to add measurements of digital divides to the agenda, using both quantitative and qualitative methods. In addition to investigating DNS dependencies, we recognize the significance of considering other measurements that might contribute to a comprehensive assessment of the digital divide. These include availability measurements by using datasets such as Common Crawl [3] or OONI (Open Observatory of Network Interference) [5], routing measurements, and measuring the use of web content management systems. Data from active DNS measurement (OpenINTEL [6]), passive DNS observation, or data from CT (Certificate Transparency) [1] may also be helpful data sets. In the future, we need to qualitatively assess the criticality of services for different population groups and explore the correlation between popularity and criticality. However, it is important to note that the statistical significance of popularity in the case of less popular domains remains unclear. Based on our preliminary results, we have started investigating more in-depth, beginning with indirect dependencies. We plan to continue with more detailed investigations of the various setups to understand possible reasons and weaknesses. This will include long-time monitoring of availability and changes in providers. We will also analyze which services tend to be supported by intra-government provisioning. Finally, we plan to extend our analysis to other countries around the globe.

Appendix

Table 2. Keywords set.

Healthcare Preventive care Chronic conditions Specialist care Telehealth services Vaccination Medical services	**Disability support** Rehabilitation services Assistive technology Improve accessibility Promote social inclusion Community program promote independence	**Family support** Child support Childhood Development Childcare Youth support Adolescent support Violence prevention Foster care Residential care
Education training programs School programs Vocational training Adult education	**Housing** homelessness support Affordable housing Appropriate housing Home-ownership	**Community development** Individuals support Cultural maintenance Social connection
Disaster relief Emergency services Rebuilding homes Infrastructure improvement Temporary accommodation Distribution of food	**Economic development** Employment services Job training Job seeking Financial assistance Financial stability	**Women support** Women health Accommodation service Support groups Employment opportunities Domestic violence
Retirement Support Age pension Superannuation savings	**Cultural preservation** Language program Traditional arts and crafts	**Mental health** Well-being Counselling services
Legal services Legal aid Resolving disputes Justice Family law Criminal law	**Environmental programs** Land management Protect sacred sites Traditional lands Natural resources Preserve cultural heritage	**Business support** Business training Business mentoring Entrepreneurship Procurement policies Provide funding Business networking
Addiction support Substance abuse Treatment service		

Table 3. List of Australian government services providing DNS services.

Government of Australian Capital Territory (Department of Education and Training)
Australian Antarctic Division
APRA (Australian Prudential Regulation Authority)
Department of Defence
Department of Education, Skills, and Employment
Department of Social Services, Government of New South Wales (Department of Customer Service)
Government of Queensland (Department of Housing and Public Works)
Government of South Australia (Department of Premier and Cabinet)
Tasmania Department of Premier and Cabinet
Government of Victoria (Department of Premier and Cabinet)
Government of Western Australia (Department of Premier and Cabinet)
National Library of Australia
New South Wales Department of Education and Communities
Queensland Department of Education and Training
Services Australia

References

1. Certificate Transparency. https://certificate.transparency.dev/ (2023), accessed on August 17, 2023
2. Citec. https://services.citec.com.au/about/ (2023), accessed on March 26, 2023
3. Common Crawl. https://commoncrawl.org/ (2023), accessed on August 17, 2023
4. Global internet report 2019: Consolidation in the internet economy. https://www.internetsociety.org/resources/doc/2019/global-internet-report-2019 (2023), accessed on Jun 13, 2023
5. OONI Data. https://ooni.org/data/ (2023), accessed on August 17, 2023
6. Openintel. https://openintel.nl (2023), accessed on May 29, 2023
7. Services australia. https://www.servicesaustralia.gov.au (2023), accessed on Jun 1, 2023
8. Telstra group limited. https://en.wikipedia.org/wiki/Telstra (2023), accessed on March 26, 2023
9. Arkko, J.: Centralised architectures in internet infrastructure. Internet-Draft draft-arkko-arch-infrastructure-centralisation-00, Internet Engineering Task Force (nov 2019), https://datatracker.ietf.org/doc/draft-arkko-arch-infrastructure-centralisation/00/
10. Arkko, J., Trammell, B., Nottingham, M., Huitema, C., Thomson, M., Tantsura, J., ten Oever, N.: Considerations on internet consolidation and the internet architecture. Internet draft, IETF (2019), https://tools.ietf.org/html/draft-arkko-iab-internet-consolidation-02
11. Deccio, C., Chen, C.C., Mohapatra, P., Sedayao, J., Kant, K.: Quality of name resolution in the domain name system. In: 2009 17th IEEE International Conference on Network Protocols. pp. 113–122. IEEE (2009)
12. Deccio, C., Sedayao, J., Kant, K., Mohapatra, P.: Measuring availability in the domain name system. In: 2010 Proceedings IEEE INFOCOM. pp. 1–5. IEEE (2010)
13. Deccio, C., Sedayao, J., Kant, K., Mohapatra, P.: Quantifying dns namespace influence. Computer Networks **56**(2), 780–794 (2012)
14. Fiebig, T., Gürses, S., Gañán, C.H., Kotkamp, E., Kuipers, F., Lindorfer, M., Prisse, M., Sari, T.: Heads in the clouds? measuring universities' migration to public clouds: Implications for privacy & academic freedom. In: Proceedings on Privacy Enhancing Technologies Symposium. vol. 2023 (2022)
15. Hesselman, C., Grosso, P., Holz, R., Kuipers, F., Xue, J.H., Jonker, M., de Ruiter, J., Sperotto, A., van Rijswijk-Deij, R., Moura, G.C.M., Pras, A., de Laat, C.: A responsible internet to increase trust in the digital world. J. Network and Systems Management **28**(4) (oct 2020)
16. Houser, R., Hao, S., Cotton, C., Wang, H.: A comprehensive, longitudinal study of government dns deployment at global scale. In: 2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). pp. 193–204. IEEE (2022)
17. Intahchomphoo, C.: Indigenous peoples, social media, and the digital divide: A systematic literature review. American Indian Culture and Research Journal **42**(4), 85–111 (2018)
18. Kashaf, A., Dou, J., Belova, M., Apostolaki, M., Agarwal, Y., Sekar, V.: A first look at third-party service dependencies of web services in africa. In: Passive and Active Measurement: 24th International Conference, PAM 2023, Virtual Event, March 21–23, 2023, Proceedings. pp. 595–622. Springer (2023)

19. Moura, G.C.M., Castro, S., Hardaker, W., Wullink, M., Hesselman, C.: Clouding up the internet: how centralized is dns traffic becoming? In: Proceedings of the ACM Internet Measurement Conference (IMC '20). pp. 42–49. Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3419394.3423625
20. Moura, G.C., Castro, S., Heidemann, J., Hardaker, W.: tsuname: exploiting misconfiguration and vulnerability to ddos dns. In: Proceedings of the 21st ACM Internet Measurement Conference. pp. 398–418 (2021)
21. Nazemi, N., Tavallaie, O., Zomaya, Y.A., Holz, R.: AUSGovDomains GitHub Repository, https://github.sydney.edu.au/nnaz6977/AUSGovDomains
22. Rogers, E.M.: The digital divide. Convergence **7**(4), 96–111 (2001)
23. Samaras, K.: Indigenous australians and the 'digital divide'. International Journal of Libraries and Information Studies **55**(2-3), 84–95 (2005)
24. Singleton, G., Rola-Rubzen, M.F., Muir, K., Muir, D., McGregor, M.: Youth empowerment and information and communication technologies: A case study of a remote australian aboriginal community. GeoJournal **74**, 403–413 (2009)
25. The Register: AWS DNS DDoS attack overwhelmed its servers for hours. https://www.theregister.com/2019/10/22/aws_dns_ddos (October 2019), accessed on April 7, 2023
26. Urban, T., Degeling, M., Holz, T., Pohlmann, N.: Beyond the front page: Measuring third party dynamics in the field. In: Proceedings of The Web Conference 2020. pp. 1275–1286 (2020)
27. U.S. Department of Commerce: Falling through the net: A survey of the" have nots" in rural and urban america (July 1995), https://ntia.gov/page/falling-through-net-survey-have-nots-rural-and-urban-america
28. U.S. Department of Commerce: Falling through the net ii: New data on the digital divide (July 1998), https://ntia.gov/page/falling-through-net-ii-new-data-digital-divide
29. U.S. Department of Commerce: Falling through the net: Defining the digital divide (July 1999), https://ntia.gov/report/1999/falling-through-net-defining-digital-divide
30. Van Dijk, J.: The digital divide. John Wiley & Sons (2020)
31. Wang, S., Cao, A., Wang, G., Xiao, Y.: The impact of energy poverty on the digital divide: The mediating effect of depression and internet perception. Technology in Society **68**, 101884 (2022)
32. Xu, H., Zhang, Z., Yan, J., Chai, T.: Name dependency and domain name resolution risk assessment. IEEE Transactions on Network and Service Management **19**(3), 3413–3424 (2022)
33. Zembruzki, L., Jacobs, A.S., Granville, L.Z.: On the consolidation of the internet domain name system. In: GLOBECOM 2022-2022 IEEE Global Communications Conference. pp. 2122–2127. IEEE (2022)
34. Zembruzki, L., Sommese, R., Granville, L.Z., Jacobs, A.S., Jonker, M., Moura, G.C.: Hosting industry centralization and consolidation. In: NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium. pp. 1–9. IEEE (2022)