Independent Submission
Internet Draft

D. Lazanski
Last Press Label
M. McFadden
Internet policy advisors, ltd

Intended status: Informational
Expires: July 12, 2022

January 12, 2022

# Protocol and Engineering Effects of Consolidation
## draft-lazanski-consolidation-03.txt

Status of this Memo



Copyright Notice

Abstract

This document contributes to the continuing discussion on Internet consolidation. Over the last several years there have been many types of discussions around consolidation at a technical level, a economic or market level and also at an engineering level. This document aims to discuss recent areas of Internet consolidation amd provide some suggestions for advancing the discussion.

Table of Contents



## 1. Introduction

Internet consolidation has been under discussion for the last several years. The 2019 Internet Society's "Global Internet Report: Consolidation and the Internet Economy" highlighted issues of consolidation and kicked started a series of discussions and

publications around consolidation. Furthermore, a draft for the Internet Architecture Board (IAB) discussed issues of economic and technical consolidation. [1] Despite community interest, the draft expired without additional work or publication.

Further discussions on this issue have stalled in in 2020 as we have been faced with the Covid-19 pandemic and all of the challenges that this brings to working and living. Recently, however, consolidation has been under discussion again on the mailing lists of the IETF and during several of the virtual meetings. Most notably draft-nottingham-avoid-internet-centralization-01 reinvigorated discussion on consolidation from a technical point of view and provided some suggestions for mitigation. This draft aims to provide another view on the issues of Internet consolidation and bring together current discussions and trends.

## 2. Background to Consolidation Issues and the Role of Standards

Internet consolidation is "the process of increasing control over internet infrastructure and services by a small set of organizations." [2] Let us consider two general categories of concentration: "player" and "layer". By player concentration, we mean the aggregating of a market to a small number of providers for a particular service. Layer concentration means the combining of functions within a given layer. An example of "player" concentration would be a relatively small number of email service providers who offer billions of users email service. Or the number of web search providers or even web browser offerings. [3]

The Internet is being consolidated at all layers, from the application layer to the network layer. Large companies, like Facebook and Google, account for a significant amount of the content and applications that are used online today. However, several of these large companies are dominating the development of protocols which fundamentally changes the way in which the Internet works and, ultimately, drives the traffic - and data - into the hands of a few companies. For example, Google has 81% of all searches online and 94% of all mobile searches as of 2020. [4]

Market consolidation is not limited to the Internet. It happens when economies of scale provide highly aggregated firms an advantage. For the last three decades, we have witnessed concentration occurring not only in telecommunications, but in the financial sector as well, just to name one other example.[5] The acceleration of consolidation has been assisted by "cloud" technologies, such as occurred with email. In the case of email,

the service providers make use of SMTP to exchange messages, IMAP to provide those messages to a user interface, and HTTP, HTML, and JavaScript to present those messages directly to a user's browser.

In other market consolidation cases, fewer Internet standards are in play. In the case of home assistant tools such as the Amazon Echo or Google Home Assistant, communication from these devices to their respective clouds is largely proprietary in nature. In particular, the information models and schemas they use are not exposed to the outside world. This is because the bulk of the service is performed by the cloud, with relatively little processing occurring in the home. This two-sided model eliminates the lengthy standards development process, thereby permitting faster service improvements.

On the Internet over previous decades, numerous Internet Service Provider (ISP) markets were subject to deregulation, disaggregation of customers by regulatory requirement, consolidation, and to some extent, re-regulation.

Standards have been viewed as a means to prevent barriers to entry. During the 1980s, AT&T was required to abide by standards as part of the consent decree that resolved antitrust litigation, leading to the ability of anyone to connect a telephone to its network. By 1994 standards were recognized as a means to prevent technical barriers to trade (TBT) during the Uruguay Round of the World Trade Organization.

As mentioned, both the Internet Society and participants of the IETF have recently published on the subject of consolidation. At the IAB's Design Expectations vs. Deployment Reality in Protocol Development Workshop 2019 a handful of the participants discussed concentration and consolidation. [4] Andrew Sullivan looked at three types of concentration in open protocols; web services, network services and standardisation. Both Christian Huitema and Julien Maisonneuve noted concentration, which leads to consolidation, as an effect of economies of scale and network effects in business models in the implementation of business practices. Jari Arkko discussed the impacts of consolidation on the Internet infrastructure in a document for the IETF[6], with the document identifying issues including loss of resilience and increased risk of surveillance. It goes on to note that "it seems prudent to recommend that whenever it comes to Internet infrastructure services, centralised designs should be avoided where possible".[7] From networks to applications, the overarching theme was that consolidation is taking place from one end of the Internet to the other. Additionally, the Journal of Cyber Policy published a special edition on Consolidation of the

Internet. Topics in this special issue included market concentration and security, DNS consolidation, supply chains, interoperability and Internet architecture. However, much is still yet to be discussed on consolidation at most layers of the Internet stack. [8]

Recently, the US has scrutinized Internet platform services. The release of report Investigation of Competition in Digital Markets in October 2020 [9] showed that both concentration and consolidation in the online marketplace has left consumers with little choice, again at the application layer. Additionally, the US Justice Department announced it is suing Google for Antitrust violations on 20 October 2020.[10] Both the report and the lawsuit show that concentration of power of Internet platform services has alarmed the House of Representatives and the Department of Justice to the point of investigation and possible criminal charges. None of this would have happed without consolidation of the application layer. The EU has been investigating the 'gatekeeper' status of big tech. [11] Recent reports reveal that the EU is considering ex ante solutions to the issue of the dominance of certain, large platforms. Such remedies, being discussed in the European Commission to date, include mandatory data sharing and/or mandatory interoperability requirements.[12] Such remedies seek to address the dominant market share of application layer services by American tech companies in Europe.

The rhetoric and discussion of consolidation primarily focuses on Internet services and data. However, it is important to draw attention to the issues and risks of consolidation at other layers of the Internet beyond just the application layer. The application layer is directly user facing and, as a result, is what users experience. But the underlying infrastructure and protocols are also going through consolidation as they develop. The complete end to end encryption model forces data into endpoints which consolidates data into and handful of companies. Furthermore, protocol standards are facilitating this consolidation.

The QUIC protocol is an example of the consolidation between layers of the Internet - and not at the application layer. Designed and deployed as a transport layer protocol, it effectively replaces TCP at the network layer while also adding improved security. The result is the merging or consolidation of three layers. QUIC should improve efficiency and delivery of applications, but also forces all data to be managed at the endpoint, which in this case is a browser, making it more difficult to manage traffic at the network layer.

## 3. Overarching Issues Related to Consolidation

### 3.1. Technical

Consolidation has led to the development of a few, large Internet companies which consumers are using by way of platform consolidation, as mentioned above. But consolidation also has led to the development of a protocols which are developed and used by these few, large Internet companies to control traffic flow and data capture as well.

Overarching technical issues related to consolidation include an over-reliance on one or two entities and a handful of protocols. Large stakeholders who have developed and implemented these protocols control the rollout of upgraded versions without competition of even knowledge of it due to the lack of diversity in the market.

For example, over 80% of the web browser market is held by two browsers: Chrome and Safari. Chrome alone accounts for 65% of the market overall [13] The makers of Chrome and Safari, Google and Mozilla, have dominated the development of protocols recently and the development QUIC, DoH and TLS.

"Did the IETF create a better internet when it approved DoH? There's a lot of disagreement about that, but what has upset many is that DoH was a surprise - the IETF standardised it without consulting some who it was likely to affect," it says in RFC 8890 [14] However, there was little multistakeholder consultation and discussion prior to the adoption of DoH. This was more of a rapid development and deployment process, without the market driving the use cases and uptake. But what did drive the rapid development was the need for Google, with 65% of the browser market, to ensure that the data coming into and onto their services remained there. By forcing the concentration of the data at the endpoint, the data is consolidated into the service provider at that endpoint. Does this make a better internet?

### 3.2. Economic

According to the Internet Society's 2019 report Consolidation In the Internet Economy the Internet economy is broadly defined as, "àeconomic activities that either support the Internet or are fundamentally dependent on the Internet's existence."[15] Internet applications, service infrastructure and access provision are the primary three areas of economic activities on the Internet.

One focus of consolidation is around the concentration of power - consumer, technical and financial - into a handful of large Internet companies. The first point of engagement with any of these companies, including Facebook and Google, is through consumer applications. The ability to easily understand consolidation at an application layer, because of the widespread and common use of Facebook and Google, has caused the focus of consolidation and anti-competitive issues from policy makers and politicians to be at the application layer.

However, consolidation doesn't always have its downsides. Consolidation allows for economies of scale, investment in infrastructure and the ability for small and medium enterprises to buy and use services, like cloud storage, content distribution networks and security technology, without having to build them from the ground up every time. However, the lack of market diversity means a lack of competition which, in turn means a lack of innovation and a lack of consumer choice.

Amazon offers affordable cloud services and Cloudflare is one of only a handful of companies that are content delivery networks at a large scale. So large, in fact, that a substantial amount of Internet traffic transits through Cloudflare's servers, though there are many thousands of small CDNs. Rather than each and every Internet application company create their own storage and content delivery network, it is easier and more affordable to outsource both to other companies. Because of the cost of CDNs at scale, few companies offer these services.

The market should be a regulating factor in consolidation. New entrants and competition in a market creates options for consumers that potentially pulls them away from popular websites and applications. When a market is not competitive or viable, regulation and anti-trust measures can intervene to remedy a consolidated market which is tending towards or has achieved monopoly status. Legal and regulatory intervention, however, tends to create its own set of issues as seen through several decades of EU intervention in big tech starting with Microsoft in 2004.  Unintended consequences with regulatory or legal intervention may skew the market even further.

### 3.3. Security

Consolidation of protocol development which has facilitated the secure, end to end encryption of information going over networks in recent years. New technologies such as DNS-over-HTTPS (DoH) and DNS-

over-TLS (DoT) standardised through the IETF process allow for confidential look up of DNS queries. However, it has forced updates onto many DNS servers and operating systems. This change in the look up process is forcing the technology to develop in a way which has narrowed the ability for companies and small industries to do DNS look ups without updating out of date hardware and software, thereby disenfranchising developing countries and smaller companies without big budgets. This is a form of market consolidation based on development choices by several large companies. These development choices are often technically opaque without transparency of what happens when updates take place, resulting in more difficulty when trying to troubleshoot security issues.

The development of these protocols, while providing increased privacy and addressing issues concerning government surveillance, have forced other unintended consequences which is promoting consolidation.

Consequences of the security of the global Internet are evident. On June 8, 2021, a global outage of Fastly, a content delivery network (CDN), was caused by a software update which included an undiscovered bug. [16] While this was resolved within a working day, one of the main causes of the outage was a dependency on the limited number of CDNs running services in the cloud. Other CDNs, which resolved traffic via Fastly for redundancy, were also taken down as a result of the Fastly outage. This dependency is caused by consolidation and a concentration of infrastructure. A highly consolidated CDN network facilitates a less secure environment because of the weakening of resilience [17]

## 4. Implications of Consolidation on Internet Architecture

### 4.1. The Changing Architecture of the Internet

The phenomenon of consolidation may be in the eyes of the beholder. A government may see market failure or a need for regulation. [18] A civil society advocate may see it from the point of view of privacy or free speech. For the purposes of this draft we view it from the perspective of the underlying architecture of the public Internet.

Consolidation in the Internet's architecture is not a new development. The approach of providing intermediaries to deliver service or content rather than the more traditional end-to-end approach has been in place for more than a decade. However, it is possible to argue that the architecture of the Internet has changed dramatically in the last decade.

The architecture of the Internet is always changing. New services, applications and content mean that the market creates new ways to deliver them. Consolidation clearly has economic, social and policy issues, but it is important to understand how consolidation affects the underlying architecture of the Internet. The impact of intermediaries on architecture is often not obvious.

The use of intermediaries in the Internet's architecture may include the use of third parties to provide services, applications or content. In the early days of the Web, this was evident when rendering a web page that included content from multiple sources. In today's Internet the intermediaries are not so obvious. Authentication servers, content distribution networks, certificate authorities, malicious content protection and DNS resolution services are all examples of tools provided to the Internet by intermediaries - often without the knowledge or approval of both endpoints.

Having intermediaries embedded in the architecture is a different effect from having them embedded in the service structure. The domination by a few companies of the content and application layer is largely an economic effect of scale. On the other hand, there is a prevalent belief that the Internet puts intelligence at the edge. While that may have been true in the past, it is hard to argue that this is a feature of the contemporary Internet.

There is a suggestion that the network simply provides for the transport of data. There are almost no network connections like that in today's Internet.  A consumer's view of the Internet is limited by unseen intermediaries of many types - some delivering positive services, others not. In either case, a consumer on the Internet seldom makes choices about those intermediaries: they are simply part of the fabric that makes up the Internet.

It is into just consolidation from the perspective of a consumer. Almost all important parts of the architecture have been affected by consolidation: DNS resolution, access service, transit provision, content distribution and authorization. Consolidation in these areas has a direct effect on engineering and protocol design.

### 4.2. The End-to-End Principle Redux

The end-to-end principle is the idea that reliability and trustworthiness reside at the end nodes of networks rather than in the network itself. In other words, the idea was that the network itself was dumb and intelligence was at the edge or end. However,

Internet architecture is evolving in such a way that this principle is changing.

Networks and the devices on the networks are acting as access consolidators. While, in the past, the network was a simple transporter of bits, today's networks see intermediaries consolidating both access and the delivery of information (e.g. streaming media). For example, 5G will allow for different services, systems and use cases at a very specific level. Network slicing in 5G will concentrate services like video on demand into concentrated - and consolidation - areas on a network. [19] In other words, as specific types of services are relegated to a segregated part of a network, the availability and access of that service is limited to accessing a specific network. Depending on the type of device or maturity of the network infrastructure available at the point of the attempted access, options for access might be limited. If a network slice on 5G is where a specific service is located, for example, but it is only possible to use a 3G mobile network, then the service is unavailable. Thus, the service is only available on a consolidated part of the mobile network.

Another change is how the layers of the Internet, as discussed in the QUIC example, are consolidating. Differentiation among layers is fading fast with the development of applications which require network access and control.

Rapidly, the end-to-end principle is becoming the edge-to-edge principle. The layers of the internet are morphing into several consolidated layers and it is becoming difficult to differentiate between the end or edge, and also nearly impossible to ensure the reliability of the internet because of it. But the important part of this is the network is not dumb. Data processing, storage and highly evolved services (including custom data and metadata processing at the edge) means that the 'dumb' network is no longer dumb.

If the number of organizations that provide those "network services" that we rely upon is small, our dependence is higher. In extreme cases of engineering, we put ourselves at risk of engineering a single point of failure. But also if organisations can't and won't enter the market, the market is left with very few options and choices. If the number of organizations that provide those "network services" that we rely upon is small, our dependence is higher. In extreme cases of engineering, we put ourselves at risk of engineering a single point of failure.

The trend toward highly specific and concentrated processing, as well as the drive for highly customised applications and services will drive the Internet away from an end-to-end principle. This will create not a network of networks, but a mesh. If the mesh is dependent on a small number of very large providers through consolidation, we will have engineered a single source of failure into the Internet.

## 5. Implications of Consolidation on Protocol Design

### 5.1. Does Protocol Design Really Affect Consolidation?

There is an idealized view of collaborative, multistakeholder approaches to Internet protocol development that it is democratic with all parties thinking about the greater good, like in the IETF. In reality, protocol development and standards are subject to vested interests, personal approaches and commercial realities.[20] Developing protocols, and standards more generally, takes time, much discussion and a bottom up approach. However, commercial organisations have different goals in the process of trying to standardize protocols. Larger organisations have more resources dedicated to protocol and standards development. Larger organisations with staff specifically dedicated to standards tend to have the ability to push for their proposals and their protocols. There is no coincidence that these companies are the ones that have facilitated consolidation on a commercial level and are facilitating consolidation on a protocol level.

### 5.2. Case Studies in Consolidation and Protocol Design

#### 5.2.1. DNS over HTTPS (DOH)

The development of encrypted DNS, specifically DNS-over-HTTPS (DoH), has been driven by a desire to show full end-to-end encryption of network connections. The protocol was completed and the DoH working groupwound up in March 2020 despite the absence of both resolver discovery and selection mechanisms. This may be addressed in the future.[21]
Client software is developing with interim discovery solutions which almost always favour the large, cloud-based resolver operators. This is leading to a situation where users are being presented with a very small number of pre-configured resolver options irrespective of their location - in some client software as few as three or four options may be presented. [22] Currently, there are many thousands of servers operating without DoH.

It is likely that most of the DNS traffic will be consolidated onto a handful of global operators, if multiple options for discovery mechanisms are not developed. The impact that such a loss of diversity of providers may have on the long-term resilience of DNS should not be underestimated. [23] Nor should the attractiveness of these potential network chokepoints to attack be overlooked either to access consolidated data or launch an attack from.
One danger is that if DNS traffic is concentrated onto a small handful of global operators and turned 'automatically-on' the result would be default adoption by the vast majority of the Internet's clients. The suggestion that there were mechanisms for users to opt-out would not matter in the face of statistics that regularly show that users almost never change default settings. Currently, the deployment approach for DoH is opt-in. For CDNs, DoH default-on would disrupt and render CDN geolocation designed to manage traffic flows more efficient closer to the desired delivery location. Thus, protocol design decisions that are enshrined in default settings will become the norm. In this case, default on, which facilitates consolidation, will become standard.

By routing the DNS over HTTPS, it becomes much easier to track user activity through the use of cookies. Therefore a protocol that was developed to enhance user privacy and security could actually undermine both: privacy through the use of cookies and security by consolidating DNS traffic onto far fewer resolver operators that are far more attractive targets for malicious actors of various types.

### 5.2.2. Encrypted Server Name Indication (eSNI)

Options to encrypt the Server Name Indication (SNI) have been explored in the TLS working group but to date it has not been possible to develop a solution without shortcomings. This flaw in the encrypted SNI (eSNI) options under evaluation required a rethink in the approach being taken.
The solution now proposed, Encrypted Client Hello (ECH, previously called ECHO) assumes that private origins will co-locate with or hide behind a provider (CDN, application server etc.) which can protect SNIs for all of the domains that it hosts.[24] Whilst there is logic in this approach, the consequence is that the would-be standard encourages further consolidation of data to aid privacy. What it does not appear to consider is the attractiveness of this larger data pool to an attacker, compared with more dispersed solutions.

### 5.2.3. Privacy Pass

The Privacy Pass protocol provides a set of cross-domain authorization tokens that protect the client's anonymity in message exchanges with a server. This allows clients to communicate an attestation of a previously authenticated server action, without having to reauthenticate manually. The tokens retain anonymity in the sense that the act of revealing them cannot be linked back to the session where they were initially issued.

For Privacy Pass to succeed clients must be able to acquire tokens that they can later redeem with greater privacy and anonymity. This document does not discuss the goals of privacy or anonymity. Instead, it identifies a problem related to the upper bound in number of servers that affects the Privacy Pass ecosystem.

"Server centralization" is the strict limit or upper bound in the number of servers available from which a client can acquire a token for later redemption.

The architecture draft for Privacy Pass specifies an upper limit of four for this upper bound. Four is a small number through which to run authorizations. There is little room for mistakes or redundancy.

An upper bound to available Privacy Pass servers creates architectural, engineering and practical problems for the deployment of the protocol. Any successful deployment of Privacy Pass must find mitigations for these problems.

## 6 Potential Technical Risks

There are a number of potential risks to the security, stability and performance of the Internet and many of them are well articulated in draft-livingood-doh-implementation-risks-issues-04, but some notable ones are:

1. Significant operational shift of the global Internet from a highly distributed to a centralised system. This would impact both security and resilience.
2. Decreased stability due to the fact that a centralised system will have higher fragility, fewer points of failure and greater impact on the system when it does fail.
3. Increased security issues caused by the reduction of number of recursive DNS operators. [see https://hbswk.hbs.edu/item/evidence-of-decreasing-internet-

entropy-the-lack-of-redundancy-in-dns-resolution-by-major-websites-and-services] Lack of distributed and recursive DNS creates a lack of redundancy for when security attacks hit parts of the Internet.

4. Loss of security threat visibility due to degraded ability to use DNS blocklists and overall network management for malware, phishing, spam, DDoS and etc if DNS management is consolidated into a few operators.
5. Reduced diversity in the Internet ecosystem. Diversity creates greater redundancy, resilience and agility to respond to attacks, outages and network issues.

## 6. Actions for the IETF, IRTF and IAB

This document proposes a set of concrete actions:

1] using MAPRG in the IRTF to attempt to establish metrics for consolidation. The goal would be to attempt to gain consensus on measurements for consolidation and a mechanism for gathering those metrics over time to answer the question of how much and how quickly the Internet is consolidating.

2] encouraging the consideration of consolidation in protocol design either through the requirement of a new section in RFCs that addresses consolidation or thorough guidance to area director reviews of documents in IETF Last Call.

3] a new IAB workshop on the Implications of Consolidation on Protocol Design with the goal of encouraging position papers from a variety of stakeholders in the protocol design and implementation process.

4] potentially expanding the human rights review process for protocols to include examination of individual protocol design on markets, enterprises and society.

5]attract and retain the participation of operators and implementors who may be impacted.

6]ensure detailed community assessment of risks and issues. In particular, assess the following issues:

- What is the threat model that makes this technical change justifiable?
- What are the security and privacy implications?
- What are the implications for stability, operations, network and systems administration, software development, diversity and etc?
- Do the benefits outweigh any drawbacks?
- What alternatives to the changes could be made?

## 7. Security Considerations

While this document does not describe a specific protocol, it does discuss the evolving architecture of the Internet. Changes to the Internet's architecture have direct and indirect implications for the Internet's threat model. In another draft [25], we discuss how the evolution of the Internet has changed the threat model. Specifically, the changes to the end-to-end model (see section 4.2 above) have inserted new interfaces which must be reflected in security considerations for new protocols.

## 8. IANA Considerations

This memo contains no instructions or requests for IANA. The authors continue to appreciate the efforts of IANA staff in support of the IETF.

## 9. Conclusions

This document seeks to rekindle and restart the discussion on consolidation. As argued above, Internet consolidation is happening at different places and different layers of the Internet. Though there has been interest in the Internet consolidation in the past, now is the time to start the discussions again.

## 10. References

### 10.1. Informative References

[1] Considerations on Internet Consolidation and the Internet Architecture [draft-arkko-iab-internet-consolidation-02].

[2] IBID

[3] Google has over at least 80% worldwide market share. https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/

[4] Investigation of Competition in Digital Markets, Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, United States House of Representatives, 6 October 2020.

[5] Following An Unexpected Rebound In M&A, Businesses Are Banking On A New Kind Of Dealmaking For Growth In A Post-Covid World https://www.prnewswire.com/news-releases/following-an-unexpected-rebound-in-ma-businesses-are-banking-on-a-new-kind-of-dealmaking-for-growth-in-a-post-covid-world-301228786.html

[6] Design Expectations vs. Deployment Reality in Protocol Development Workshop 2019, Intern Architecture Board https://www.iab.org/activities/workshops/dedr-workshop/position-papers/

[7] Centralised Architecture in Internet Infrastructure [draft-arkko-arch-infrastructure-centralisation-00].

[8] IBID page 5.

[9] Journal of Cyber Policy, Volume 5, Issue 1 (2020) Special Issue: Consolidation of the Internet (https://www.tandfonline.com/toc/rcyb20/5/1)

[10] Investigation of Competition in Digital Markets, Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, United States House of Representatives, 6 October 2020.

[11] Statement of the Attorney General on the Announcement Of Civil Antitrust Lawsuit Filed Against Google, United States Department of Justice, 20 October 2020. https://www.justice.gov/opa/pr/statement-attorney-general-announcement-civil-antitrust-lawsuit-filed-against-google

[12] Digital Services Act package, European Commission, ongoing https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12418-Digital-Services-Act-package-ex-ante-regulatory-instrument-of-very-large-online-platforms-acting-as-gatekeepers

[13] Browser & Platform Market Share January 2021 https://www.w3counter.com/globalstats.php

[14] RFC 8890, The Internet is for End Users. Nottingham, Mark. August 2020. https://www.rfc-editor.org/info/rfc8890

[15] Consolidation In the Internet Economy, Internet Society, 2019. https://future.internetsociety.org/2019/consolidation-in-the-internet-economy

[16] Fastly Blog, June 8, 2021. https://www.fastly.com/blog/summary-of-june-8-outage

[17] The Deeper Root Cause of the Fastly and Akamai Outages, CircleID, June 28, 2021 https://www.circleid.com/posts/20210628-the-deeper-root-cause-of-the-fastly-and-akamai-outages/

[18] See Google, antitrust and how to best regulate big tech, The Economist, 7 October 2020 https://www.economist.com/business/2020/10/07/google-antitrust-and-how-best-to-regulate-big-tech

[19] What is Network Slicing? https://5g.co.uk/guides/what-is-network-slicing/

[20] Dominique Lazanski, Governance in international technical standards-making: a tripartite model, Journal of Cyber Policy, 4:3, 362-379, 2019. https://www.tandfonline.com/doi/full/10.1080/23738871.2019.1696851

[21] DNS over HTTPS (doh) https://datatracker.ietf.org/group/doh/about/

[22] At the time of writing, the Firefox browser presents a list of three pre-configured resolver options to North American users: Cloudflare, NextDNS and Comcast.

[23] Cloudflare DNS goes down taking a large piece of the Internet with it, 17 July 2020. https://techcrunch.com/2020/07/17/cloudflare-dns-goes-down-taking-a-large-piece-of-the-internet-with-it/

[24] TLS Encrypted Client Hello draft-ietf-tls-esni-07 https://tools.ietf.org/html/draft-ietf-tls-esni-07

[25] An Internet for Users Again draft-lazanski-smart-users-internet-00 https://tools.ietf.org/html/draft-lazanski-smart-users-internet-00

## 11. Acknowledgments

Many thanks to all who discussed this with us, especially Jason Livingood.

This document was prepared using 2-Word-v2.0.template.dot.

Authors' Addresses

Dominique Lazanski
Last Press Label
London, UK

Email: dml@lastpresslabel.com

Mark McFadden
Internet policy advisors ltd
Chepstow, Wales, UK

Email: mark@internetpolicyadvisors.com