How the Internet Was Won and Where It Got Us

Vittorio Bertola, *Head of Policy and Innovation, Open-Xchange*

***Abstract*— The article, building on a set of examples from email and DNS, tries to identify some factors that promoted the increasing centralization of Internet services into the hands of a few big players. The factors are very diverse and only in part technical. In the end, assuming the IAB's desire for ideas to counter such centralization, the article mentions some possible working items for the IETF and for the community as a whole.**

I. Introduction

The author is an IETF newcomer, only having attended four meetings ever, all in the last eighteen months, following a small number of working groups. The article thus represents an outsider's partial perspective; it is in no way meant to belittle the efforts and motivations of the authors of the protocols and choices that are discussed, but it tries to provoke some thoughts through a different perspective.

The author also stresses that this article is the result of a hastened one-week conceptualization phase on a subject that could rather require an entire book. It should be considered as a set of working hypotheses that could be proven or disproven through collective discussion and matching with data.

II. Clarifying the Scope of the Question

The call to which this paper is submitted[1] starts with a statement of the problem which can be summarized as follows: several protocols have presumed specific deployment models during their development phase, but actual deployments, contrarily to these expectations, have instead been highly centralized, and this is a serious issue for the Internet.

While this is not being said explicitly, the logical consequence of such a statement is that the deployment models that were expected in the development phase were always decentralized; however, it is then unclear if the problem that the IAB wants to see addressed is the repeated emergence of centralized deployments, or the fact that design expectations on deployment models were not met, independently from whether the result was more or less centralization.

The reason for raising this point is that the observation of some of the study cases – those suggested as examples in the call for papers – makes one think that the centralized deployment models are what was expected, or at least should have been expected, since the beginning; they are not *"confounded expectations"* at all.

In this case, defining the problem as *"deployment expectations were not met"* would be misleading; one would rather state the problem as *"how can the IETF stop releasing protocols that promote more centralization"* – and this is the problem that will be discussed by this paper.

If this is truly the subject, it would be useful to get a clearer statement by the IAB, and by the IETF as a whole, that centralization is a problem that has to be contrasted. A few months ago, in a discussion with a current IAB member, the author suggested that we might now also need an RFC entitled *"Centralization Is an Attack"*. It would be interesting to know whether such a stance would reach consensus in the community.

III. Old Protocols Versus New Protocols

In the author's view, a distinction can be drawn between the *"original"* mass Internet protocols – the ones released in the 80's and 90's – and the protocols released afterwards.

In the case of the original protocols, there was indeed the expectation and the design choice of a decentralized network of peers; thus, speaking of confounded expectations could make sense, though the main issue is that the surrounding conditions have evolved and changed over time.

Such evolution was however quite predictable. The pattern of a pioneering phase of great variety followed by great consolidation is true for most industries, and for all media industries in the modern age; the telephone, the radio, the television all went that way. The natural capitalist trend that rewards scale economies is compounded, in the case of media, by additional critical mass effects at the social, cultural and political level.

Some Internet pioneers, while declaring the network's *"independence from governments"*, seemed to expect that consolidation on the Internet would never have happened, because the permissionless and unregulated environment would never have blocked new entrants and hampered small services. In fact, it is exactly the opposite: in democratic countries, media sectors have always been regulated with the precise objective of preventing excessive concentration, though the entanglement of media and politics often led to regulation which was ineffective on purpose.

The lack of adequate competition regulation over the Internet is thus one of the key elements that allow, or even promote, concentration on a scale never seen before. While new technologies (new protocols) can indeed disrupt dominant positions, the size of the dominant companies is now so big that they can simply buy out any vaguely threatening innovation. It is impossible to imagine that such concentration can be disrupted just by technological evolution alone.

However, technical standardization processes should at least defend the remaining degree of diversification, not making life even more difficult for small operators, non-profit services and self-hosters. Unfortunately, this does not always happen; protocols are often being designed by the employees of big players for big players, with centralized use cases in mind; implementation problems for smaller players are not considered and called *"out of scope"*. A few examples will follow in section V.

IV. The Early Phase

To understand how we got here, we need to identify an early phase of the concentration process; a phase in which protocols were still being designed in a federated way, but they were unable to address the issues in full, so they were deployed together with non-standard practices and functionalities on top

[1] https://mailarchive.ietf.org/arch/msg/ietf-announce/_bfpW-KxO6twNMsTk_T8PSM537g

of them, which were only accessible to players that could exploit big datasets, research resources and investment capital.

We could consider this phase to start at the end of the *"dot com bubble"* (around year 2000), and morph into the current one in the last few years, as the top Internet players progressively became the biggest private companies that mankind has ever seen. Two examples from the last fifteen years will follow.

A. Email Authentication and Delivery

SPF[2], DKIM[3] and DMARC[4] are the three protocols that the IETF released in succession to address the problem of email authentication. There is nothing centralized *per se* in these protocols; they allow any sender, big or small, to supply information that lets recipients authenticate the origin of the message. While indeed the repeated overlay of protocols on top of other protocols is not immediate to digest, the deployment of these protocols is still entirely doable for any small or individual email server administrator.

However, while these protocols solve (more or less) the problem of reliably associating a message to a sender, they never addressed the basic problem of deciding whether an unknown sender deserves the trust necessary to accept their message; thus, even full compliance with all relevant IETF standards is not enough for a sender to ensure delivery.

This other problem – associating senders with reputation and ensuring that such information is available to recipients – is not a purely technical one, but it is also not purely nontechnical. It is indeed quite hard, and so it was initially addressed with human-intensive approaches; this already had a mild centralizing effect, as costs for qualified human work are high, but there were several efforts to spread these costs through community efforts, so that they were reasonable and that acceptably good free tools were available.

The real centralization, however, started to happen when spam filtering became a sort of black magic. It was not just based on the standards above; it rather relied on arcane combinations of factors, including accumulated datasets, that could not be shared, standardized or even openly communicated, to prevent spammers from gaming them – basing the fight against spam on security by obscurity.

This created a compounded advantage for big recipients; firstly, big recipients have more resources to hire humans and, as technology became available for that, more data to train machine learning algorithms; secondly, in the absence of standardization big recipients set the standards, up to the point that today, *de facto*, spam is whatever Gmail rejects, and now it is the senders that have to work out their secret black magic just to be able to deliver an email to Google[5].

Also, big recipients do not have any incentive to care about small senders, while the cost of support for an incredible number of globally distributed small email systems, helping them to get their sending practices right, would be significant; so their support to senders that fail to deliver messages is minimal and ultimately ineffective.

Such centralization could have been prevented only if there had been a pervasive, active effort in that direction by multiple stakeholders on multiple levels:

- A regulatory environment forcing recipients to care more about the ability of legitimate senders to deliver messages, and at the same time supporting recipients better by keeping spammers at bay in the *"offline"* world, so that less importance could be placed on the effectiveness of recipient filters;
- A shared, interoperable standard to exchange reputation information and to combine several factors in a message reputation decision, not basing the decision on obscurity.

Possibly, the above recipes are just too hard to implement and could never have worked in practice. However, there never was significant push to try them out.

B. Instant Mess(aging)

Even if email is now significantly centralized, its concentration level pales when it is compared with instant messaging. There are still several millions of email servers globally, and all of them are, at least theoretically, able to interoperate; but there only are a dozen or so of instant messaging providers of significant relevance, and they, by design, do not interoperate with each other. Users must acquire multiple accounts, one per system, if they want to communicate with everyone. The lock-in effect is extreme: if users want to stop using one service and move to a different provider, they have to lose all contacts and all past conversations. Initial user adoption is king to determine which services succeed, because users cannot move easily.

Some open-standard instant messaging systems do exist, like IRC, Jabber/XMPP and Matrix, but they are relegated to technical user niches, due to their inability to compete with the commercial services in terms of investments (including those in the quality and usability of the product) and marketing.

In fact, some big players actually started their instant messaging service using an open standard, but then removed the compatibility once the critical mass was reached[6]. This may have been justified by the desire to add new, non-standard functionalities, but also suited a commercial strategy aimed at creating lock-in. The author is not familiar enough with these events to assess which factor was more important between the technical features or the commercial strategies, but indeed the push to concentration in this field looks more commercial than technical.

V. The Mature Phase

The early phase of Internet centralization has now seamlessly morphed into a mature one, in which protocols can include centralized elements by design. Two examples follow.

A. ARC (Authenticated Received Chain)

ARC[7] is a new email authentication protocol recently approved by the IESG and about to be released as an experimental RFC. It aims to fill a gap in DMARC, since

[2] https://tools.ietf.org/html/rfc7208, https://tools.ietf.org/html/rfc4408
[3] https://tools.ietf.org/html/rfc6376, https://tools.ietf.org/html/rfc4871
[4] https://tools.ietf.org/html/rfc7489
[5] We will link here just one of many sad, funny and irate tales on how hard it is nowadays for small senders to deliver email to Gmail, and how unhelpful their support system is: https://www.tablix.org/~avian/blog/archives/2019/04/google_is_eating_our_mail/
[6] See for example http://www.h-online.com/open/news/item/Google-s-chat-client-drops-Jabber-compatibility-1866129.html
[7] https://datatracker.ietf.org/doc/draft-ietf-dmarc-arc-protocol/

legitimate email routed through intermediary systems, such as mailing list servers, often fails DMARC authentication. ARC addresses this problem by adding a mechanism through which any intermediary can verify the DMARC authentication status and relay it to the final destination together with the message.

However, since any source of abusive messages could pretend to be an intermediary server and add a successful ARC verification header, ARC does not work unless every recipient already knows each and every intermediary that it should trust.

In the absence of any established way to share and distribute trustable reputation information on email intermediaries in a free and publicly accessible way, it is immediate to expect that most ARC deployments will only trust a limited set of very well-known global intermediaries – the biggest ones that everyone knows. As an alternative, recipients that are big enough to have access to sufficient data to feed machine learning algorithms may be able to deploy predictive mechanisms to trust small unknown legitimate intermediaries (though big recipients could also consider the trouble of doing so excessive if compared with the amount of false positives).

In both cases, only big intermediaries or big recipients will be able to make use of ARC reliably, while small intermediaries and small recipients will continue to suffer from failures in email authentication and will thus be put at a disadvantage.

ARC is an experiment and it will be interesting to see if the above expectation actually stands, but one would say that ARC, as designed, inherently promotes concentration among email intermediaries, and any centralizing effects will definitely not be unexpected. Attempts to mitigate these effects, either within or outside the IETF, are not known at the moment, nor are discussed by the specification[8].

In the end, ARC seems to be the product of a mindset in which centralization is now given for granted and not seen as a particular problem, or at least as one that could and should be addressed by the IETF when devising new email protocols.

B. *DNS-over-HTTPS*

DNS-over-HTTPS[9] is presently a very well-known and hotly debated case; in the interest of space, we will not discuss here again how its adoption is promoting centralization[10]. We will however challenge the claim that such centralizing effects are unexpected, and that they could not have been foreseen and addressed prior to the approval of the standard.

As a matter of fact, the standard was approved in August 2018 and released in October, while Mozilla's centralized deployment model had been announced in late May 2018[11]. However, the expectation that DNS-over-HTTPS would be used to direct traffic to a few global public resolvers provided by very big browser makers/website operators was baked in the protocol since the beginning. In fact, in an article from December 2017[12] an IAB member was describing exactly the deployment model that is now being labelled as unexpected.

It is true that, differently from ARC, there is nothing in the concept of the DNS-over-HTTPS protocol that prevents its deployment in a decentralized way. However, in this case the centralizing effect is caused by moving DNS resolution from the network service level, which is still quite fragmented on a global scale, to the (Web) application level, which is significantly centralized on a planetary scale[13] [14].

In this case, the *post-mortem* analysis looks different: either the IETF participants failed to understand the full implications of the likely deployment model and all the problems it would have caused, or decided to ignore them, dismissing them as not important; or, as a third case, understood exactly that the new protocol would have promoted centralization and would have disrupted a lot of things for a lot of other stakeholders, but continued because this was exactly their objective, due to their vision of the world or to their own specific interests.

In all cases, these implications were not addressed before the protocol's release because not all the right people were in the room; either some stakeholders were not there, or they were not able to get their views considered; and this is a problem of diversity among participants, and/or of fairness in defining consensus.

Getting late into that process, the author's perception was that many of the reasons given for the new protocol and for its deployment plans could only stand because they were being examined from a narrow viewpoint. For example, the different degree of concentration at the ISP level and at the Web browser level almost disappears if the view is limited to a single country; and the asserted practice of ISPs profiling users for monetization through their DNS queries seems to be highly relevant in the United States, but is almost unheard of in Europe.

This supports the conclusion that the IETF's work in this case was hampered by a lack of diversity, and by a lack of early involvement of other stakeholder groups, both technical and nontechnical, to discuss the effects of the new protocol in a number of dimensions that go well beyond technical protocol details.

VI. Considerations for the Future

If the analysis above stands, and if the IAB's desire is to discuss how to contrast further centralization of the Internet, and if we assume that this is at all possible, there are a few working items that the author would dare to suggest.

A. *The Obvious Point*

The IETF should make sure to consider any centralizing effects and any implementation and deployment issues for smaller parties before releasing any new document. This

[8] The latest draft, in two lines in section 9.3, just recognizes as a matter of fact the fundamental problem that we already identified in section IV.A: *"ARC authenticates the identity of some email handling actors. It does not make any assessment of their trustworthiness."*

[9] https://tools.ietf.org/html/rfc8484

[10] If any reader needs to understand the issue, I will shamelessly point him/her to section 4.2 of my own Internet draft:
https://datatracker.ietf.org/doc/draft-bertola-bcp-doh-clients/

[11] See https://hacks.mozilla.org/2018/05/a-cartoon-intro-to-dns-over-https/ and https://blog.nightly.mozilla.org/2018/06/01/improving-dns-privacy-in-firefox/

[12] https://blog.apnic.net/2017/12/12/internet-protocols-changing/

[13] Market share data for browsers vary across sources, but the most used browser alone (Google Chrome) is usually given at 60-65%, with three other makers (Apple, Mozilla and Microsoft) covering another 25-30%; the four biggest American makers thus hold 90%+ of the global market. See https://en.wikipedia.org/wiki/Usage_share_of_web_browsers for reference and comparison of various sources.

[14] One can argue whether this change of layer should be considered as part of the protocol's design (in this case, DNS-over-HTTPS would be a *"centralizing protocol"* in itself) or as a deployment choice (in this case, only the deployment model can be blamed). This discussion, in my opinion, is not very useful; the practical result is that DNS-over-HTTPS has immediately started to show centralizing effects even before its final release.

should by now be an immediate concern, yet the IETF still needs to work on how to make it happen.

B. A Missing Layer

The author is convinced that the original Internet architecture, and the set of *"original"* protocols, sorely miss something that should have been there since the beginning: an *"identity layer"*, dealing with authentication and with the controlled transmission of personal information[15].

It is unclear whether the lack of such a standard layer was just an oversight, failing to foresee its importance, or whether it was an actual choice, perhaps to uphold the original idea of *"on the Internet nobody knows you are a dog"* – with the unfortunate consequence that now all the advertisers, the Internet platforms and the surveillance agencies of the world know that you are a dog and also where you are and what you are doing at any time, but you still lack a simple way to prove that you are a dog when you need and want to[16].

Such a layer, for example, would make authenticating email much simpler; after all, in almost every case you do want the recipients of your message to know that you are you, and when you do not, an identity layer could just include instruments for secure pseudonymity. By making it simpler, it would also have made it easier for smaller players to implement reliable email authentication, and made shared reputation systems possible, with less need for obscurity.

C. The Camel

Many already noted that the IETF has a tendency to pile an extension upon another, rather than re-addressing a problem from scratch when decades have passed and requirements have completely changed[17].

While this approach has several advantages, in some cases it may lead to such a complexity that it becomes very hard for new entrants and smaller players to get everything right, turning a technology into the playfield of a small set of gurus and established companies. Still, the result may be so constrained by backward compatibility that it is not good enough to solve the new needs, leading to those proprietary additions, non-interoperable practices and black magic recipes that pave the way to centralization – or leading to the emergence of a completely new alternative led by the biggest players, likely to promote centralization as well.

In fact, DNS could be a good example for this; the now proverbial *"DNS camel"* introduced by Bert Hubert at IETF 101[18], with its complexity and major shortcomings, is being overturned by the disruptive deployment of DNS-over-HTTPS – unfortunately, bringing forth more centralization.

On the other hand, a new, simpler protocol that drops obsolete requirements and fulfills very well the newer ones, if designed and deployed in a federated way, could make implementation easier for smaller players and independent developers, preventing centralization rather than promoting it.

D. Diversity Is Not Just About Gender

A newcomer to the IETF, especially if used at other Internet governance venues such as ICANN and the United Nations' IGF, immediately notices a lack of diversity across many dimensions: gender, language, nationality, ethnicity, employer type, stakeholder group, background, culture, values. Moreover, the commendable efforts by the IETF leadership to address this problem seem to focus only on a few of these dimensions – basically, almost only on gender.

A look at the IETF leadership roles and at active participation in meetings is also troubling; the set of the most active and influential participants seems to be even less diverse than the set of participants overall.

The author fully acknowledges that competence and experience are the dominating factors in the selection of leaders in any community, especially a technical one, but holds the view that such a limited diversity hampers the IETF's ability to fully understand the nontechnical consequences of its releases, to address the needs of all Internet stakeholders fairly, and ultimately to carry on its mission with full success.

Specifically, the apparent disproportionate participation by employees of U.S. West Coast companies, and the relative lack of advocates for other views and interests, could be a factor incentivizing centralization in Internet protocols.

When *"code is law"*, code needs to be written considering more than the technical issues. The IETF could achieve this by involving more diverse participants, or by cooperating proactively with the venues where these participants are, before releasing work with strong nontechnical implications.

E. Who Will Think of the Future?

More generally, if preventing the centralization of the Internet is a strategic objective, then strategic thought and collective action is necessary.

However, the IETF, as a set of bottom-up processes, is not well poised to lead the strategic development of the Internet. Consensus-based processes do what is possible, not what is necessary; they can be blocked by any determined significant minority, and the leadership is there as a steward to its community, not as a strategic drive for the Internet. Moreover, the IETF only deals with protocols, while, as noted throughout the paper, many of the issues happen elsewhere and cannot be addressed through protocol standardization.

The private companies that benefit from Internet centralization legitimately plan their moves, and work strategically to pursue more centralization. To oppose this trend as a community, strategy and organization is also necessary, coordinating action among a number of like-minded stakeholders on several planes. It is clear that this goes well beyond the IETF's role, especially if we consider that the entities that benefit from centralization are legitimate members of its community. Where and how a coalition of pro-open-Internet forces could form is thus an open question.

However, the author is also sure that many in the IETF community, independently from their affiliation, still cherish the view that the original, decentralized, federated model of the Internet is good for the planet. This is why the author believes that the IETF can, and will, do its part.

[15] For a slightly more defined idea of the author's thoughts on how such a layer could look like, see this expired Internet draft: https://www.ietf.org/archive/id/draft-bertola-dns-openid-pidi-architecture-01.txt

[16] In fact, this need is so strong that a couple of non-federated, Internet-wide single-sign-on services have been wildly successful in the last few years; unfortunately, they are provided by Google and Facebook and thus are yet another brick in the wall of the garden.

[17] This is even codified in section 2.1.2 ("Incremental Deployability") of RFC 5218. https://tools.ietf.org/html/rfc5218

[18] https://datatracker.ietf.org/meeting/101/materials/slides-101-dnsop-sessa-the-dns-camel-01