Blurry line between private service and public infrastructure

- Area: ROADMAP FOR THE FURTHER EVOLUTION OF THE INTERNET GOVERNANCE ECOSYSTEM
- Entitled by: Micha? Andrzej Wo?niak
- Region: Poland
- Organization: Free and Open Source Software Foundation
- Sector: Civil Society
- Keywords: centralization, surveillance, open-standards, network-effect, monopolies

Abstract

ICANN and IANA decentralisation efforts mark an important milestone in the evolution of the Internet: there is finally widespread recognition of the fact that centrally controlled bodies pose a threat to the free and open nature of the Internet. ICANN and IANA are, however, but a small part of a much larger problem.More and more, communication platforms and methods are secondarily centralized; that is, in a network decentralized on lower protocol levels there are services being run that are centralized higher levels. Running on a network based on open standards are closed services, that are then used by other entities as base for their services.In other words, some private services -- offering, for example, user authentication methods -- are being used as a de facto infrastructure by large numbers of other entities.If we recognize the dangers of centrally-controlled domain name system, we should surely recognize the danger of this phenomenon also.

Document

It is of great value that the importance of decoupling IP addresses management and the domain name system management from a single state actor has been recognized and that currently there is a strong push towards multistakeholderism in this area.

There is, however, a secondary emergent centralization happening on the Internet, that potentially can pose a comparable, or even bigger, threat to the interconnected, open and independent nature of this global network.

This centralization is harder to perceive as dangerous, as it is not being actively supported by any state actor; hence, it falls under the radar for many Internet activists and technologists, that would react immediately had similar process been facilitated by a government. It does, hoever, have a potential to bring negative effects similar to a state-sponsored centralization of infrastructure.

Another reason for this process to happen unnoticed or for the possible negative effects of it to be depreciated is that it is fluid and emergent on behaviour of many actors, enforced by the network effect.

This process is most visibly exemplified in Facebook gathering over a 1bln of users, by providing a centrally-controlled walled-garden, and at the same time offering an API to developers willing to tap-into this vast resource, for example to use it as authentication service. Now, many if not most Internet services requiring log-in, as one of their options offer Facebook log-in. Some (a growing number) offer Facebook as the only option. Many offer commenting system devised by Facebook, that does not allow anonymous comments -- a user has to have a Facebook account to be able to partake in the discussion.

Similarily, Google is forcing Google+ on YouTube users; to a lesser extent, Google Search is being used by a swath of Internet services as their default internal search engine (that is, used tos earch their own website or service). GMail is also by far the most popular e-mail and XMPP service, which gives Google immense power over both.

These are two examples of services offered by private entities (in this case, Google and Facebook) that had become a *de facto* public infrastructure, meaning that an immense number other services rely and require them to work.

If we recognize the danger of a single state actor controlling ICANN or IANA, we can surely recognize the danger of a single actor (regardless of whether it is a state actor or not) controlling such an important part of Internet infrastructure.

Regardless of reasons, why this situation emerged (users' lack of tech-savvy, service operators' want of easiest and cheapest to implement and integrate solutions, etc), **it causes several problems for the free and open Internet:**

- **it hurts resillience**

If such a large part of services and actors depend on a single service (like Facebook or GMail), this in and of itself introduces a single point of failure. It is not entirely in the realm of the impossible for those companies to fail -- who will, then, provide the service? We have also seen both of them (as any other large tech company) have large-scale downtime events, taking services based on them down also.

- **it hurts independence**

In the most basic sense, any user of a service based on these *de facto* infrastructures has to comply with and agree to the underlying service (i.e. Facebook, Google) Terms of Service. If many or most of Internet services have that requirement, users and service operators alike lose independence over what they accept.

- **it hurts openness**

Operators of such *de facto* infrastructures are not obliged to provide their services in an open and standard manner -- running mostly in the application layer these services usually shut-off any attempts at interoperating with them. Examples include Twitter changing their API TOS to shut-off certain types of applications, Google announcing the

planned shut-off of XMPP server-to-server communication, Facebook using XMPP for the internal chat service with server-to-server shut-off**.**

- **it hurts accountability and transparency**

With such immense and binary (either use it, or lose it) control over users' and otehr service providers' data, *de facto* infrastructure operators do not have any incentives to share information on what is happening with the data they gather. They also have no incentives to be transparent and open about their future plans or protocols used in their services. There is no accountability other than the binary decision to "use it or lose it", which is always heavily influenced by the network effect and the huge numbers of users of these services.

- **it hurts predictability**

With no transparency, no accountability, and lack of standarization, such *de facto* infrastructure operators can act in ways that maximizes their profits, which in turn can be highly unpredictable. Twitters' changing of API TOS is a good example here.

- **it hurts interoperability**

Such *de facto* infrastructure operators are strongly incentivised to shut-off any interoperability attempts. The larger the number of users of their service, the stronger the network effect, the more other services use their service, and the bigger the influence they can have on the rest of the Internet ecosystem. Social networks are a good example here -- Twitter user cannot communicate with a Facebook user, unless they also have an account on the other network.

This is obviously not the case with e-mail (I can run my own e-mail server), at least not yet. The more people use a single provider here (i.e. GMail), the stronger GMail becomes, and the easier it would be for its operator to shut-off interoperability with other providers.

This is exactly what Google is doing with XMPP.

- **it hurts innovation**

Lack of predictability, opennes and independence obviously also hurts innovation. What used to be a free and open area of innovation is more and more becoming a set of closed-off walled-gardens controlled by a small number of powerful actors.

It is also worth noting that centralized infrastructure on any level (including the level of *de facto* infrastructure discussed herein) creates additional problems on human rights level: centralized infrastructure is easy to surveil and censor.

Hence, the first question to be asked is this: **when does a private service become *de facto* public infrastructure?**

At this point this question remains unanswered and there is not a single Internet Governance body, or indeed any actor, able to reply to it authoritatively. Nevertheless, we are all in dire need for an answer to this question, and I deem it a challenge for Internet Governance and an important topic that should be included in any Internet Governance Forums now and in the future.

The second question that ever more urgently requires an answer if we are to defent the open and not balkanized Internet is: **what should be done about private services that have become *de facto* public infrastructure?**

This question is also as of yet unanswered, but there are several possible proposals that can be made, including treating such situations as monopoly and breaking them up (so handling them outside Internet Governance), requiring public interoperable API available for other implementators, etc. This is perhaps not exactly in the purview of Internet Governance, it is however crucial for the Internet as a whole and I propose it be treated as a challenge to be art least considered at IGFs henceforth.