Consolidation, Privacy, Jurisdiction, and the Health of the Internet

John Mattsson, Ericsson Research

Abstract: This paper discusses how the Internet and the Web are no longer the open, distributed, and decentralized platforms they were designed to be. The Internet application domain is dominated by a few global players and there are worrying signs that the consolidation will continue to increase. New privacy regulation and privacy mechanisms are well needed, but may create annoyance and open up new privacy problems if not deployed with care. Location privacy leaks from the IP protocol are a major enabler for limiting end user choice.

1. Introduction

The Internet and the Web were both designed to be open, distributed, and decentralized platforms. Current deployments are not living up to the expectations. Several countries are heavily censoring and filtering Internet traffic [1], in practice creating their own separated Internets. In some markets, there is very little competition as a few large players have created oligopolies or near-monopolies. It is difficult to create a new global business, and sometimes existing players have also been able to buy their newer competitors. The situation is worst in the Internet application domain [2]. In the West, Google is dominating Internet search, Facebook is by far the largest player in social networking and messaging, and together they have an oligopoly on digital advertisement, etc. As stated in the call for papers, such consolidation present a risk to user choice, privacy, and future protocol evolution.

Consolidation as such occurs naturally and can create benefits to society like improved efficiency and companies with the ability to take on large long-term R&D projects. It is a problem when it goes too far, and this is what has happened with the modern web. Too much consolidation stymies competition, concentrates power, and creates arrogant companies that believe they can get away with almost everything. The creator of the Web, Tim Berners Lee, stated that the Web in the wrong hand could become a “destroyer of worlds” [3].

Concentration of end user data is especially dangerous, not only from a privacy perspective, but also from a national security perspective. In the wrong hands, access to end user data and platforms to efficiently spread disinformation can easily be turned into cyber-weapons. The worst breach yet is arguable the Facebook–Cambridge Analytica data scandal [4]. Facebook knowingly allowed third-party apps to access vast amounts of end user data, ignoring the security and privacy risks. Cambridge Analytica used information from such an application for psychological targeting of ads during several elections and referendums.

2. Risk for Increasing Consolidation

There are worrying signs that the consolidation will continue to increase. Google's Accelerated Mobile Pages (AMP), Facebook's Instant Articles, and Apple News promise faster page loads with less noise, but they also risk creating a far less open Web. Such a Web would be consolidated not only when it comes to content, but also when it comes to creating the technical specifications.

New privacy regulation such as the EU General Data Protection Regulation (GDPR) is significantly improving privacy. It forces companies to protect personal data and to motivate collection and storage of such data. But, like most kind of regulation it has several drawbacks [5]. GDPR and other EU regulations such as "the right to be forgotten" have to some degree created separated versions of the Internet, where a search inside the European Union gives different results from a search outside of EU. Instead of complying with GDPR, several major US websites are simply blocking EU users. Both of these examples also highlight how the IP protocol itself is a major privacy leak, revealing the location of people without their consent. The location privacy leaks from the IP protocol are a major enabler for a separated and discriminating Internet.

The GDPR requirement to inform and ask for consent has transformed the web experience in the EU with so called GDPR popups. While the intention is good, having a popup for every site is likely more annoying than helpful for most users. Earlier research [6] shows that people ignore 45% of security warnings shown on first page load. The amount of ignorance is likely much higher for GDPR popups given that they are not even warnings, and they are shown very often, leading to so called "warning fatigue". Not only are GDPR popups annoying, there also risk driving people to closed ecosystems like Facebook and Google AMP where there are fewer annoying popups.

Current deployments for DNS resolution have a range of problems (eavesdropping, manipulation, censorship) that should be fixed sooner rather than later. DNS-over-HTTPS (DoH) [7] seems to be the most promising solution. While HTTPS (and ESNI) increases the consolidation of end user information, they do so by hiding information from other parties than the end-points. The effects of DoH are very different. In many cases DoH does not only conceal information from certain parties, it also gives the information to new parties that did not have access to the information before. While the access network is often in the country and jurisdiction as the end user, the DoH server may be in a completely different jurisdiction unknown to the end user. This creates significant privacy problems. Even if the company operating the DoH server gives guarantees on how the data will be used, the data will be accessible to one or more governments that could not access the information before, and that the end user may not trust. While all governments can access information stored within their country, several countries have laws giving authorities access to data, regardless of where in the world the data is stored. One example is the US CLOUD Act that give US authorities access to all data handled by US cloud service providers [8].

When deploying new technologies like DoH that transfers access to end user data from one party to another, potentially to another country and jurisdiction, it is important that the end user have a choice and is made aware of the changed jurisdiction and what implications this may have.

3. Conclusion

Consolidation is hard to battle from a technical standpoint. It is mainly a question for regulators. There are however are areas where we believe the Internet Community can do more.

We recommend that the Internet Community should:

- Actively work to hinder monopolies and oligopolies on the web and also work on mitigating the negative consequences when such monopolies and oligopolies form.
- Drive standardization to accelerate the mobile web. Proprietary technologies controlled by a single company are not good enough even if are "open-source".
- Be a driving force for how to handle information, consent, end user choice, usability and privacy. E.g. when it comes to GDPR pop-ups and DoH.
- Long-term come up with a plan to stop the major location privacy leaks from use of the IP protocol.

References

[1] Wikipedia, "Internet censorship and surveillance by country",
https://en.wikipedia.org/wiki/Internet_censorship_and_surveillance_by_country

[2] Internet Society, "Consolidation in the Internet Economy", 2019
https://future.internetsociety.org/2019/wp-content/uploads/sites/2/2019/04/InternetSociety-GlobalInternetReport-ConsolidationintheInternetEconomy.pdf

[3] Vanity Fair, ""I Was Devastated": Tim Berners-Lee, the Man Who Created the World Wide Web, Has Some Regrets", 2018
https://www.vanityfair.com/news/2018/07/the-man-who-created-the-world-wide-web-has-some-regrets

[4] Wikipedia, "Facebook–Cambridge Analytica data scandal"
https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal

[5] WIRED, "The tyranny of GDPR popups and the websites failing to adapt"
https://www.wired.co.uk/article/gdpr-cookies-eprivacy-regulation-popups

[6] Jenkins et. al., "More Harm Than Good? How Messages That Interrupt Can Make Us Vulnerable", 2016
https://pubsonline.informs.org/doi/pdf/10.1287/isre.2016.0644

[7] IETF RFC 8484, "DNS Queries over HTTPS (DoH)", 2018
https://tools.ietf.org/html/rfc8484

[8] Hamilton, "The US CLOUD Act – impact and implications", 2019
https://www.hamilton.se/en/2019/01/the-us-cloud-act-impact-and-implications-2/