Stay Open.

Cologne, 30 September 2018

Open-Xchange contribution to the European Commissioner for Competition on "Shaping competition policy in the era of digitisation"

Open-Xchange would like to thank for the opportunity to express views on the most appropriate competition policies for the digitisation of the economy, and especially for the dominant over-the-top (OTT) platforms.

Our submission contains an analysis and a set of suggestions related to the three topics proposed, with current examples from the email and domain name system (DNS) industry of which we are part. For convenience, we would like to briefly summarize them here:

1. OTT companies have an inherent economic incentive to erode the privacy of their users to gain cheaper raw material for their products, so **promoting competition is vital to defend privacy as well; competition and privacy assessments and regulations for the Internet should always go together**, more than in the past. To ensure competition in data-based services, **it is also vital that the current efforts by some OTTs to establish dominance in the online identity market are restrained** to allow for portability, multiple providers, and user control on data flows. The open and fair availability of public sector information is also important.

2. Leveraging effects are visible in the consumer DNS market, with the new *"DNS-over-HTTPS"* protocol; lock-in effects are evident in messaging, particularly in instant messaging and in social networking, as a consequence of the lack of interoperability and open standards. Thus, **the right to portability recognized by article 20 of the GDPR should be completed by another norm mandating the opening of dominant digital platforms through interoperability with competitors, by the use of open and public standards**. The European public sector should also support the availability of open standards and open source software for the most common services, but should refrain from competing directly with private entities in providing consumer services.

3. Given the strong natural trend to consolidation, on the Internet dominant positions are often acquired by fast organic growth rather than by mergers – so there needs to be attention to both phenomena. In any case, dominant positions impede innovation and **the loss of innovation and competition opportunities should be a major factor in antitrust evaluations**.

We thank you for your attention, deferring you to the full text of our contribution below, and look forward to further opportunities to participate in this discussion.

About Open-Xchange

Open-Xchange (OX) is a privately held company headquartered in Cologne, Germany, with additional local presence in Finland, France, Italy, the Netherlands, Spain and the United Kingdom, and in Australia, Japan and the United States of America.

Open-Xchange is the world's leading provider of open source messaging and domain name system (DNS) software and software-as-a-service solutions for hosting, service provider and telecommunication companies. OX products and services reach more than 200 million people and include Dovecot, the world's leading mail delivery agent, used by 75% of the Internet's servers to receive, store and show email to final users, and PowerDNS, the number one DNS software for mass scale deployments in many European markets.

Full contribution by Open-Xchange to the consultation on "Shaping competition policy in the era of digitisation"

1. Competition, data, privacy, and AI

Regarding this first discussion topic, we will start by noting that, **in a world of global digital platforms, the two objectives of protecting privacy and promoting competition are strictly intertwined**.

This happens because **most of the revenues of the *"over-the-top"* (OTT) companies derive from products and services which use personal data as one of their raw materials** - often, as the only one. This is not just true of artificial intelligence or of other upcoming innovative technical devices and products; this is, in fact, already true of all the services and products that prompted the success and the dominant position of the current platforms (and created a huge transfer of wealth from Europe and elsewhere to the U.S. West Coast, up to the point of making a home in San Francisco affordable almost only to millionaires). Social networks and web tracking devices turn personal information into profiles that can be used for targeted advertising, which constitutes almost the entirety of the revenues for Google, Facebook and other smaller players. Even more traditional products like email, maps or documents are offered *"for free"* because they draw users into the platform, and the user's activity, individually or in the aggregate, can be monitored to contribute to the creation of resellable services.

Thus, **OTT platforms have a natural economic incentive to reduce the protections over personal data**, the barriers to acquiring permission for their usage, and the control that the data subjects maintain over them, because **this will make the raw material for their revenue-making products more abundantly and more cheaply available**. Increasingly, the same logic applies to other Internet companies that provide mass products (or the infrastructure over which they are built) and handle big amounts of data, such as consumer software makers[1], content delivery network (CDN) providers and so on, which find additional revenue streams in the monetization of personal information.

Fair and open competition on the market would counterbalance this naturally: if the company is mistreating user information and abusing of it, consumers will naturally move to a competing service. But when no real competition exists, as no alternative product with a different approach is available, the companies can breach the privacy of their users without fear of consequences - and will do so in several ways[2]. Even potential privacy-friendly competitors cannot enter into play, as the network effect of the existing platforms is too strong to allow new

---

[1] In fact, the ubiquitous diffusion of the *"software as a service"* paradigm means that the distinction between software makers and over-the-top service providers is now very blurred.

[2] Just as a few of several possible examples, and only from the last few weeks, see Google's recent decision to automatically identify and log in Chrome users when they use any Google property: https://blog.cryptographyengineering.com/2018/09/23/why-im-leaving-chrome/ ; the discovery that, even after turning off the collection of location information in the privacy settings of Android phones, Google's apps will still track and store your movements: https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb/AP-Exclusive:-Google-tracks-your-movements,-like-it-or-not ; Mozilla's plan to force the redirection of all the DNS queries that Firefox users perform when surfing the web to a centralized server run by their partner Cloudflare, which will be able to track them at will: https://blog.ungleich.ch/en-us/cms/blog/2018/08/04/mozillas-new-dns-resolution-is-dangerous/ .

services to flourish, and most people will grudgingly accept the loss of privacy to be able to access a service that they need and that everyone else is using.

Thus, **intervention by public authorities at the antitrust level is the only possible way** to defend not just market and growth opportunities for European companies and Europe as a whole, but also the privacy and freedom of European citizens.

Specifically, while we applaud the effort by the European Parliament in establishing the General Data Protection Regulation (GDPR), we note that **the GDPR by protecting privacy also inherently promotes competition**, yet, having been conceived only from a privacy viewpoint, **it misses a few additional elements that would also have made it fully useful for antitrust purposes**. Thus we would welcome the establishment of additional norms to fill the gaps, and for the future we think that **legislative and policy efforts regarding the digital economy should address user rights and competition at the same time in a single norm**, as the two aspects are too interconnected.

Consequently, **any assessment of the health of the competition in a given digital market**, and of how it would change in case of mergers and changes of ownership of relevant players, **should always encompass an analysis of risks to privacy, freedom and citizen rights in general**.

As another fact relevant to this issue, we will also point out that **some OTT companies are currently gaining dominance in a consumer service which is key to the entire data ecosystem: centralized online identities**. Google, Facebook and other online platforms now allow any website to authenticate users through their OTT account (the so-called *"single sign-on"* on an Internet scale), which, in turn, gives the OTT the possibility to track each and every online service where the user performs a login, and to become the global hub for the user's personal information.

These systems, though based on a public standard, are deployed in a way that is not interoperable; each website has to add support separately for each new identity provider, creating a barrier to the entry of new providers; users cannot move their accounts to a different platform – once they sign up with Facebook on a website, they will always have to use Facebook for that login or lose the account.

In this way, **the biggest OTT platforms are building a new dominant position on the management of everyone's online identity**, which will give them ample control on the online flows of personal information, and access to more and more personal data. Similarly to what we will show for other online services in the next discussion topic, **there is no technical reason why these identity systems cannot be open and interoperate with any number of other providers**, creating a competitive market that would enable users to choose who to entrust with their online identity, and would prevent further lock-in effects and privacy erosion when the data of these users will be requested for artificial intelligence systems or for any other data-based service.

This oligopoly also increases security risks, because the lack of competition disincentivizes investments in security, as in any other aspect of service quality, and because the

concentration of billions of accounts in a single platform makes any data breach immensely damaging – and this, in fact, already happened for real just a few days ago[3].

Multiple efforts by the European Internet industry to create and promote alternatives based on open standards and a competitive market are already ongoing[4], but this accomplishment also requires appropriate, proactive policy action by the European public authorities.

Another side of this discussion relates to the general availability of the data gathered and created by the public sector – that is, the Public Sector Information (PSI). Again, **it should be ensured that all PSI is made available at equal conditions to any interested party**, be it a big Internet platform or a single citizen. In technical terms, **the best way of doing so is through the use of open data formats and licenses**.

While we recognize the long-standing effort by European institutions to make this happen, still too many public entities at the local level do not embrace these principles. Not rarely, a public administration will actually favour the access to data by the big Internet platforms, which can provide more immediate returns and better public visibility, over that by local startups and civic organizations.

Thus we support the proposed revision of the PSI Directive to promote the availability of more data in more ways, including through dynamic APIs, but we would also encourage the further strengthening of the broader principle that **any public dataset that is made available to any private party must be made available under open formats, and must be made available at the same conditions to any other party that may request it**.

We do not see reasons why exceptions to the principle, such as exclusivity rights for some datasets, should be allowed by the norm; also, from a technical standpoint, **the internal use of open formats should become a prerequisite for all public IT systems**, so that it cannot be claimed that technical conversion costs make it *"impossible"* to release of the data in an open format. In fact, in several cases all that it takes is to publish the specification of the format together with the data.

2. Digital platforms' market power

Both the anti-competitive effects mentioned in the statement of this discussion topic are real and important and deserve action by the European authorities. To justify our policy suggestion, we would like to start by mentioning briefly a few examples in our own industrial sector: Internet messaging and Domain Name System (DNS) resolution for consumers.

---

[3] More precisely, the insecure implementation of a feature in Facebook allowed attackers to gain access to (at least) 90 million accounts of Facebook users; since these accounts could also be used for *"single sign-on"* to third party websites, attackers could also access any website in which the consumer had used the Facebook account for access: https://www.theregister.co.uk/2018/09/28/facebook_accounts_hacked_bug/

[4] We would like to mention the ID4me project, in which we participate together with several other players from the DNS industry in Europe and elsewhere, working to develop an open and public standard that would make all online identity systems based on the OpenID Connect protocol, including those by the OTTs, interoperable and reciprocally portable: https://id4me.org/

Leveraging effects are currently at play in the DNS resolution[5] market. Traditionally, the DNS resolution is provided by the consumer's Internet access provider[6], as a free ancillary service to network access, and, at least in Europe, without any tracking or monetization of the user's personal information.

However, at least one browser maker has announced[7] the intention to enter the DNS resolution market and provide the service on its own, together with a technical partner, automatically making this the default for all the users of that browser, and using a new encrypted protocol called *"DNS-over-HTTPS"* to ensure that the new resolution service cannot be blocked or monitored by access providers and national governments. While they justify the move with the intention of providing a better service than average (encrypted connection for privacy, better security, faster reply…), in fact **this will allow browser makers to turn their share of the browser market into a share of the DNS resolution market, which could then be monetized through the data** that can be gathered by tracking the users.

It would be out of scope to discuss here in detail how much this would damage European consumers, circumvent the most common anti-botnet and anti-malware security barriers deployed by the ISPs, and even remove the ability by European governments to make harmful and illegal content inaccessible, but this is yet another example of how **big Internet players introduce changes that have significant competition effects, without any market and privacy impact assessment being performed in advance** by the appropriate public authorities.

Lock-in effects are clearly visible in the messaging environment, but also offer **a good way to show the difference between open and proprietary standards**.

In email – a service based on an open, public standard – there is **a lock-in effect due to the difficulty of exercising the right to data portability from one email provider to another**, as the technical infrastructure for the automated transmission described by article 20 of the GDPR does not exist yet (even the necessary standards do not fully exist); moreover, due to the way email works, the email address cannot be ported among different providers, unless the consumer is using an email address inside a domain name that he/she owns.

However, **the market for email is still quite competitive**; while Google and Microsoft, leveraging their general market power, are the biggest consumer email providers on a global scale, there are still hundreds of companies, scattered around the world, successfully providing

---

[5] "DNS resolution" is the operation that converts the name included in a Web or email address, such as europa.eu, into a network (IP) address that can then be contacted to retrieve a web page or deliver an email message. In practice, the party performing this operation can track all the destinations reached by the consumer during his/her online activities, and could even make some of these destinations inaccessible or redirect the consumer to different resources than expected.

[6] There are not many analyses regarding the consumer DNS resolution market, but an anecdotal experiment on U.S. traffic showed that, after removing the machine-generated traffic from datacenters, about three quarters of the DNS resolutions are served by each user's Internet access provider, with the remaining fourth is served by the DNS resolvers run by the OTTs and other service providers (mostly by Google): https://medium.com/@nykolas.z/dns-market-share-analysis-identifying-the-most-popular-dns-providers-80fefb2cfd05

[7] See the third link in footnote 2.

email to ample numbers of consumers; and millions of small email servers[8]. This is **due to the fact that any email user, thanks to the openness of the standard, can communicate with any other email user** in the world, regardless of the service provider they use; and since the standard is open, and open source implementations are readily available, smart users can even deploy their own server and manage their email themselves, still being able to communicate with everyone else[9].

In comparison, **the instant messaging market, mostly based on a number of competing proprietary standards and deployments used by one company each, is much less competitive and consumer-friendly**. There are only a dozen or so of instant messaging providers of significant relevance, and they do not interoperate with each other. Consumers must acquire multiple accounts, one per system, if they want to communicate with everyone; you need a Whatsapp account to contact a Whatsapp user, a Skype account for a Skype user and so on. The lock-in effect is extreme: if you wanted to stop using one service and move to a different provider, you would lose all your contacts and all your past conversations. There is not a technical or economic reason for the market to be like this; it is just a consequence of the closedness of the standards and of each provider locking in its users as far as possible[10].

This lock-in effect is similar, and even worse, when it comes to social networks. **There is no technical reason why there cannot be dozens of competitors to Facebook interoperating with it** and providing users with different, innovative interfaces and user experiences, while allowing them to receive and comment posts across the various providers; the only reason is that Facebook will not allow it, to avoid the risk of losing their current dominant position in favour of a competitor which turned out to be smarter and more friendly to the users. As the value of a social network resides in the critical mass of users, under these conditions it is not just hard to establish meaningful competition; it is plainly impossible.

While, as we pointed out, there are competition issues in the email market as well, they are orders of magnitude smaller than those in instant messaging and social networking. So this comparison shows that **the widespread concerns over the dominant position of several of the over-the-top platforms**, which are increasingly threatening Europe's economy and sometimes the rights of its citizens, **can be addressed and mitigated through competition policy aiming to establish an email-like scenario** – the one in which all players interoperate through an open standard.

---

[8] We estimate that on the Internet there are over five million different mail delivery servers hosting at least one mailbox.

[9] In fact, big email providers like Gmail (Google) and Hotmail (Microsoft) increasingly make it hard to run personal email servers, due to their *"antispam filters"* which not rarely end up rejecting non-spam traffic by a small email domain without providing any real reason or remediation mechanism. This is another way to leverage market power and disrupt competition even in an open and federated service like email, and would deserve some attention at the policy level.

[10] It must be noted that some open-standard instant messaging systems do exist, like IRC, Jabber/XMPP and Matrix, but are relegated to technical user niches due to their inability to compete with the OTT services in terms of investments and marketing. In fact, Google has a history of deploying new services that are initially compatible with open standards, helping the gathering of the initial critical mass of users, but then the compatibility is removed once the critical mass is reached and the lock-in process can begin:
http://www.h-online.com/open/news/item/Google-s-chat-client-drops-Jabber-compatibility-1866129.html

While article 20 of the GDPR is a great step forward and goes in the right direction, it only addresses a one-time move of the user's data once a competing service provider already exists; **it does not address the continuous, real-time exchange of data between multiple service providers that would make competition possible through interoperability**, especially in fields like social networking, where moving to a different provider is useless if all the other users stay with the old one.

We thus suggest that **the European Union should establish a policy that any online service of broad relevance, as soon as it acquires a dominant market position, must provide an interface to exchange information with other existing or fledgling competing providers, using public open standards and protocols** that exist or that are developed for this purpose at the appropriate technical standardization bodies (the Union could also promote the bottom-up neutral development of such standards if necessary).

This will not kill innovation and investments, because the first mover will always have the advantage of the critical mass that it has built; users will not move away from it, unless the service really becomes dissatisfactory. But if it does, users will finally be able to move to a different provider, as in any properly competitive market.

If the principle of easy data portability already recognized by the GDPR is completed with a principle of fair competition among multiple interoperable providers through open standards, it can also be expected that at least some of these providers will be based on open source software, which will then become available to any interested party, allowing European citizens to gain full transparency on how these services work, to manage the service themselves keeping full control of their data, or even to start new businesses. In any case, **Europe should promote and support the availability of at least one open source implementation of any relevant open standard**.

We would however also like to stress that the proper role for competition policy is to create a level field among private parties. While it is also appropriate for the European Union to promote and support industrial action by European players, and even to build and manage public datasets, codebases and infrastructures that can then be made available to private initiatives, **it would not make sense for the Union or for member States to create public sector companies to compete directly with the OTT platforms on consumer markets**; some proposals of this kind have been seen in the past, and have always ended up in failure. The Union should create workable conditions to allow European companies to compete fairly with the big players from the United States, China and elsewhere, mandating and enforcing the technical practices that create such conditions; that would already be sufficient.

3. Preserving digital innovation through competition policy

Before getting to the point of how to preserve innovation, since the statement of the discussion topic partly focuses on digital mergers, we would like to point out that **mergers in our opinion have a more limited role in building cartels on the Internet than they have in other industries**.

In a competitive online market, thanks to the very low barriers to the movement of information and users, consolidation typically happens quickly and massively. While in more

traditional industries mergers were the main way to acquire a dominant position on the market, **in the digital world it is just as common for a single company to acquire a dominant position by being the leader in the deployment of a new product** and then *"eat up"* all the market with its organic growth. Even if this dominant position has been acquired through fair competition, often the winning company will start to deploy lock-in features and make their product incompatible with that of the competitors, to make it impossible for users to move away even if their product ceases to be the best; and, at this point in time, the dominant position ceases to be fair and legitimate.

This is also when innovation stops; even products that are clearly better have a hard time establishing themselves, if the users cannot easily move their data away and still keep the ability to interoperate with the users on the dominant platform.

So we think that, in a digital world, **antitrust intervention to force the opening of platforms to interoperation with other existing and potential competitors as soon as such platforms assume a dominant position is even more important than the control and vetting of mergers** - though, of course, assessing the impact of mergers is still important.

Generally speaking, **once a platform gains a dominant position – be it via merger or via organic growth – the potential harm to innovation is clear**. While the dominant platforms are often (though not always) deploying innovations and sometimes even releasing some of them as open standards, still, in the absence of opportunities for fair competition, all the potentially innovative ideas by any other party cannot be made real, or, as a minimum, have a much harder time finding investors and adopters. Also, given the relatively low barrier to innovation that is typical of immaterial Internet services, **it cannot be claimed that such a big concentration of market power and capital is necessary to enable the research and development of innovative products** – in fact, many of the dominant companies started out with a big innovation developed by a handful of people in the prototypical *"garage"*.

This is particularly relevant from a European point of view, since none of the currently dominant OTT platforms is European, and the inability to innovate and compete makes it very hard for any European company to become a global Internet leader in the future, creating a strategic disadvantage for Europe as a whole.

This is why we encourage **a stronger focus on the assessment of lost competition and innovation opportunities** in any antitrust assessment related to the Internet.