Commissioner Margrethe Vestager
European Commission
Rue de la Loi / Wetstraat 200
1049 Brussels
Belgium

28 September 2018

Submission on shaping competition policy in the era of digitisation

Dear Commissioner Vestager,

I represent Brave, a rapidly growing Internet browser with offices in San Francisco and London, and employees across Europe. Brave's CEO, Brendan Eich, is the inventor of JavaScript, and co-founded Mozilla/Firefox.

The purpose of this submission to your consultation on "shaping competition policy in the era of digitisation" is to suggest an area of focus for panel 2: "Digital platforms' market power". This panel asks what can competition policy do to address leveraging and lock-in.

Where the processing of personal data confers competitive advantage, network effects in one business should not inevitably translate to network effects in another. Therefore, this submission suggests that the principle of "purpose limitation" in data protection law should be better leveraged to combat bundling, offensive leveraging, and other anti-competitive behaviour by dominant digital businesses.

Examples of how purpose limitation should curtail offensive leveraging by Google and Facebook are outlined in the middle part of this submission. The submission concludes with a proposal of two areas of work for the Commission's consideration.

**Purpose limitation**

Purpose limitation is a core principle of data protection law. It is set out in Article 5 (b) of the GDPR as follows:

> "Personal data shall be … collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes … ('purpose limitation')"

Purpose limitation is a well-established principle that dates back to the 1973 Council of Europe Resolution, the 1980 OECD "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", and the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. It was also a principle of the 1995 Data Protection Directive.

This principle could be particularly effective in preventing offensive leveraging of data custody where "special categories of personal data" are concerned. These are data that reveal any of the following about a person:

> "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".

These special categories of personal data enjoy particular protections in the GDPR, set out in Article 9. Unless the data have been made "manifestly public" by the person that they concern, the appropriate legal basis for processing those data is explicit consent.

Therefore, the purpose limitation principle protects a person's opportunity to choose to opt-in to whatever particular service they decide, and forbids a company from automatically opt-ing a person in to all of its services where this entails data processing purposes that go beyond what the person has already opted-in to.

Provided that purpose limitation is enforced, it prevents dominant digital players from automatically leveraging personal data that they have collected for one purpose in one business in another business, to the disadvantage of competitors and new entrants.

**Facebook**

Article 6 (4) of the GDPR permits an opt-out (rather than opt-in) when the additional purpose that a company wants to process data for are "compatible" with the original purpose for which personal data were shared by users. Article 6 (4) d provides that one must consider "the possible consequences of the intended further processing for data subject". This would be a serious impediment to Facebook, which is the subject of successive scandals that demonstrate harm to data subjects. Consider the following sample of Facebook crises:

- In October 2016 and December 2017, ProPublica revealed that Facebook could allow advertisers to exclude particular ethnicities[1] and age categories[2] from seeing their ads.
- In May 2017, a document leaked from Facebook in Australia that described its capacity to target teens at moments when they feel "worthless" or "insecure" for marketing purposes.[3]
- In September 2017, ProPublica revealed that it was possible to advertise to segments including "Jew haters".[4]
- In March 2018, details about Cambridge Analytica scandal emerged.[5]
- In September 2018, the Communications Workers of America and the ACLU filed charges against Facebook with the Equal Employment Opportunity Commission for allowing recruiters to discriminate against women job seekers.[6]

Therefore, Facebook would have to seek consent for the various data processing purposes appropriate to its various business interests in order to comply with the purpose limitation principle. For example:

a. Facebook Audience Network requires the processing of personal data from Facebook users to target them on other websites. It seems unlikely that its purposes will be regarded as a compatible. People should have to be asked to opt-in to this business.

b. WhatsApp advertising should require users to give their consent (an opt-in, rather than an opt-out) for their personal data on WhatsApp to be processed for purposes unrelated to WhatsApp functionality on Facebook properties other than WhatsApp. People should have to be asked to opt-in to this business.

c. Facebook's Newsfeed advertising should require consent, where the personal data concerned are "special category" data, unless these have been "manifestly made public by the data subject" – such as being marked "public" or visible to

[1] Julia Angwin and Terry Parris Jr., "Facebook lets advertisers exclude users by race", *ProPublica*, 28 October 2016 (URL: https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race)
[2] Julia Angwin, "Facebook jobs ads raise concerns about age discrimination", The New York Times, 20 December 2017 (URL: https://www.nytimes.com/2017/12/20/business/facebook-job-ads.html)
[3] "Facebook targets insecure young people to sell ads", *The Australian*, 1 May 2017 (URL: http://www.theaustralian.com.au/business/media/digital/facebook-targets-insecure-young-people-to-sell-ads/news-story/a89949ad016eee7d7a61c3c30c909fa6); see Facebook's reply of 30 April 2017 (URL: https://newsroom.fb.com/news/h/comments-on-research-and-ad-targeting/).
[4] Julia Angwin et. al, "Facebook enabled advertisers to reach 'Jew haters'", *ProPublica*, 14 September 2017 (URL: https://www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters).
[5] Carole Cadwalladr and emma Gragam-Harrison, "Revealed: 50 million Facebook profiles garvested for Cambridge Analytica in major data breach", The Guardian, 17 March 2018 (URL: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election).
[6] Noam Scheiber, "Facebook accused of allowing bias against women in job ads", *The New York Times*, 18 September 2018 (URL: https://www.nytimes.com/2018/09/18/business/economy/facebook-job-ads.html).

"friends of friends".[7] This includes all photos, videos, texts, etc. that reveal features such as ethnicity. People should have to be asked to opt-in to this business.

d. Facebook processes phone numbers submitted solely for a security purpose (two factor authentication) for other purposes related to its advertising business.[8]

**Google**

Google would have to seek consent for the various data processing purposes appropriate to its various business interests if it were to comply with the purpose limitation principle. For example, consider Google's various advertising businesses:

a. All personalised advertising[9] on Google properties including Search, Youtube, Maps, and the websites where Google provides advertising should require that users opt-in.

   The services that should be affected include targeting features of AdWords such as "remarketing",[10] "affinity audiences",[11] "custom affinity audiences",[12] "in-market audiences",[13] "similar audiences",[14] "demographic targeting",[15] "Floodlight" cross-device tracking,[16] "Customer Match", which targets users and similar users based on personal data contributed by an advertisers,[17] (A prospect would have had to give their consent to the advertiser for this to

[7] An average user has 40,000 friends of friends, though the 99th percentile has 800,000. See Lars Backstrom, "People you may know", 12 July 2010 (URL: www.graphanalysis.org/SIAM-AN10/01_Backstrom.pdf).
[8] Giridhari Venkatadri, Elena Lucherini, Piotr Sapiezynski, and Alan Mislove, "Investigating sources of PII used in Facebook's targeted advertising", *Proceedings on Privacy Enhancing Technologies*, 1, 18, 2018, p. 13 (URL: https://mislove.org/publications/PII-PETS.pdf)
[9] "Personalized advertising", Google Advertising Policies Help, (URL: https://support.google.com/adwordspolicy/answer/143465?hl=en). Note that even users who are not signed out receive personalised search results, as described in Brian Horling and Matthew Kulick, "Personalized Search for everyone", 4 December 2009, Google Blog (URL: https://googleblog.blogspot.ie/2009/12/personalized-search-for-everyone.html).
[10] "About remarketing lists for search ads", Google AdWords Help, (URL: https://support.google.com/adwords/answer/2701222?hl=en).
[11] According to Google, this is "based on their specific interests as they browse pages, apps, channels, videos, and content across YouTube and the Google Display Network as well as on YouTube search results". See "About targeting your ads by audience interests", Google AdWords Help, (URL:https://support.google.com/adwords/answer/2497941?hl=en).
[12] "About targeting your ads by audience interests", Google AdWords Help (URL: https://support.google.com/adwords/answer/2497941?hl=en)
[13] "In-Market Audiences", Think with Google (URL: https://www.thinkwithgoogle.com/products/in-market-audiences/).
[14] "AdWords looks at browsing activity on Display Network sites over the last 30 days, and uses this, along with its contextual engine, to understand the shared interests and characteristics of the people in your remarketing list." "About similar audiences on the Display Network", Google AdWords Help (URL: https://support.google.com/adwords/answer/2676774?hl=en).
[15] "When people are signed in from their Google Account, we may use demographics derived from their settings or activity on Google properties, depending on their account status", "About demographic targeting", AdWords Help (URL: https://support.google.com/adwords/answer/2580383?co=ADWORDS.IsAWNCustomer%3Dfalse&hl=en).
[16] "About Floodlight", DoubleClick Digital Marketing Partners Help https://support.google.com/dcm/partner/answer/4304205?hl=en&ref_topic=4241549.
[17] "About Customer Match", Google AdWords Help (URL: https://support.google.com/adwords/answer/6379332?hl=en).

occur), and "Remarketing lists for search ads (RLSA)".[18]

Some of these products may share common purposes, but people should have to be asked to opt-in to many separate processing purposes before Google can necessarily rely on all of these products.

b. "Location targeting",[19] and "location extensions", technologies in Google Maps enable advertising to target users based on geographical proximity. This may not be accepted as a compatible purpose with the original purpose for which location data were shared by users. If so, people should have to be asked to opt-in to this business.

c. Google Marketing Platform (previously "DoubleClick"), is Google's "programmatic" advertising business, which targets specific ads to specific individuals on websites. It should require multiple opt-ins, because it involves a large number of separate processing purposes. For example, this is a not-exhaustive list of purposes that are currently pursued by the industry (note that many are probably unlawful, and few are openly acknowledged).

- To inform the agents of prospective advertisers that you are on visiting the web site, so that the website can solicit bids for the opportunity to show an ad to you.
- To combine your browsing habits with data they already have collected about you (and infer further insights about you) so that they can select relevant ads for you. These ads may be for products you have shown interest in previously. This profile may include your income bracket, age and gender, habits, social media influence, ethnicity, sexual orientation, religion, political leaning, etc.
- To use your browsing habits to build or improve a profile about you, in order to sell these data to partners for online marketing, credit scoring, insurance companies, background checking services, and law enforcement.©This profile may include your income bracket, age and gender, habits, social media influence, ethnicity, sexual orientation, religion, political leaning, etc.
- To identify whether you are the kind of person that its advertising clients want to show ads to.
- To combine your browsing habits with data they already have collected about you (and infer further insights about you), to personalize the service or product that it offers you. This may include determining whether to offer you discounts. This profile may include your income bracket, age and gender, habits, social media influence, ethnicity, sexual orientation, religion, political leaning, etc.

[18] "About remarketing lists for search ads", Google AdWords Help (URL: https://support.google.com/adwords/answer/2701222?hl=en).
[19] "Target customers near an address with location extensions", Google AdWords Help (URL:https://support.google.com/adwords/answer/2914785?hl=en&ref_topic=3119074).

- To monitor your behaviour on websites in order to determine if you have viewed or interacted with an ad.
- To determine whether you have purchased one of its products or services following your viewing of or interaction with an ad that it has paid for.
- To combine your browsing habits with data they already have collected about you (and infer further insights about you), to verify that you are human rather than a "bot" attempting to defraud advertisers. This profile may include your income bracket, age and gender, habits, social media influence, ethnicity, sexual orientation, religion, political leaning, etc.
- To record the number of times you have viewed each ad, to prevent a single ad being shown to you too frequently.
- To combine your browsing habits with data they already have collected about you (and infer further insights about you), to understand how you and people similar to you browse the web.◎◎This profile may include your income bracket, age and gender, habits, social media influence, ethnicity, sexual orientation, religion, political leaning, etc.

People should have to be asked to opt-in to each of these purposes, and may have to do so in multiple contexts, before Google can process personal data for this business.

If, however, users have manually chosen to "sign in" to Google Search or Chrome, Google may argue that the purpose of these technologies is "compatible" with purposes users agreed to, and hope to use an opt-out rather than an opt-in.

Google did not give users choice in this matter. It recently introduced a policy wherein users of Google Chrome are automatically signed in to all Google businesses.

Following a loud user outcry, Google announced a partial reversal the auto opt-in-to-everything policy on 26 September, announcing that the next Chrome update will give users an opt-out.[20] However, for the reasons outlined above, this opt-out is hardly an adequate or lawful solution. Purpose limitation in this context should mean that Google can not leverage its dominant position in one business (such as Chrome) to leverage a person's data in another business (such as Shopping).

**Suggested areas of work**

Purpose limitation has the potential to be a useful and proportionate tool to enhance data protection, and prevent undue cross-market dominance. There are two areas that merit attention if this potential is to be realised.

[20] Zach Koch, "Product updates based on your feedback", The Keyword, Google, 26 September 2018 (URL:https://www.blog.google/products/chrome/product-updates-based-your-feedback/)

**First**, the individual purpose must be tightly defined, so that anti-competitive conflation of multiple purposes can be clearly identified and addressed.

What a "purpose" is has not yet been strictly defined. The definition is absent from the GDPR, and from the previous Data Protection Directive. In its 2013 opinion on "purpose limitation", the Article 29 Working Party of Member State data protection authorities went some way toward a definition: a purpose must be "sufficiently defined to enable the implementation of any necessary data protection safeguards," and must be "sufficiently unambiguous and clearly expressed".[21] The test for judging what a single purpose is appears to be (quoting the 2013 opinion):

> "If a purpose is sufficiently specific and clear, individuals will know what to expect: the way data are processed will be predictable."[22]

One reading of this is that a purpose must be describable to the extent that the processing undertaken for it would not surprise the person who gave consent for it.

The concern is that this may not be specific enough to clearly define where a single purpose begins and ends, or to protect against the conflation of separate purposes as one "catch-all" purpose.

Also worrying is that the 2013 opinion on purpose limitation observed that "It is generally possible to break a 'purpose' down into a number of sub-purposes" in example 11, on page 53 of that opinion. Without further guidance, this could provide a pretext for the hiding of various purposes under an umbrella when they should actually be presented clearly and in a granular way. This would risk unanticipated use of personal data by the controller or by third parties and in loss of data subject control.[23]

**Second**, the competition and data protection authorities should together consider whether there is adequate enforcement of the purpose limitation principle. Google and Facebook are prime candidates for enforcement, and should be unable to use the personal data they process for the purpose of providing their service for other purposes without user permission. But in reality, they do currently use a "service-wide" opt-in for almost everything. The implications of this extend to both

[21] "Opinion 03/2013 on purpose limitation", Article 29 Working Party, 2 April 2013, p. 12.
[22] "Opinion 03/2013 on purpose limitation", Article 29 Working Party, 2 April 2013, p. 13.
[23] "Opinion 03/2013 on purpose limitation", Article 29 Working Party, 2 April 2013, p. 12.

data protection and competition, and are matters for cooperation between competent authorities.

**Request**
As Joseph Stiglitz observed during the Federal Trade Commission's hearings on competition and consumer protection last week:

> "there have been innovations in anti-competitive practices. It may not be showing up in GDP. But it's showing up in market power".

For example, Google and Facebook today enjoy concentrated data power, and exploit their position to engage in offensive leveraging. It is likely that their so far uninterrupted success doing so will become a model to be emulated.

There are tools in data protection law that can be refined and applied to correct this. Therefore, the Commission is invited to consider these two areas of work, and the merit of using purpose limitation as a means to curb platform leveraging concerns.

We would be delighted to contribute to the conference on these matters, and to provide our insight into the online media and advertising sector.

Sincerely,

Dr Johnny Ryan FRHistS
Chief Policy & Industry Relations Officer
Brave