PRIVACY INTERNATIONAL

Submission to the European Commission consultation on 'shaping competition policy in the era of digitisation'

October 2018

PRIVACY INTERNATIONAL

62 Britton Street
London EC1M 5UY
United Kingdom
Phone +44 (0)20 3422 4321
www.privacyinternational.org

28 September 2018

By e-mail only: COMP-DIGITAL-CONTRIBUTIONS@ec.europa.eu

Privacy International's submission to the European Commission consultation on 'shaping competition policy in the era of digitisation'

Privacy International welcomes the opportunity to contribute to the European Commission consultation on 'shaping competition policy in the era of digitisation'.

Privacy International is a non-profit, non-governmental organisation based in London, the United Kingdom, dedicated to defending the right to privacy around the world. Established in 1990, Privacy International undertakes research and investigations into government surveillance and data exploitation in the private sector with a focus on the technologies that enable these practices. To ensure universal respect for the right to privacy, Privacy International advocates for strong national, regional and international laws that protect privacy around the world. It has litigated or intervened in cases implicating the right to privacy in the courts of the United States, the UK, and Europe. It also strengthens the capacity of partner organisations in developing countries to identify and defend against threats to privacy.

Privacy International encourages the European Commission to consider the following issues (grouped under the three topics identified in the consultation.)

Competition, data, privacy and AI

Privacy International encourages the European Commission to consider ways to reform or at least re-interpret competition regulation to address the data protection implications and the broader societal challenges posed by the exploitation of data by big corporations. This includes, for example, systematic consideration of data protection issues (including though consultation with relevant data protection authorities and organisations protecting privacy and consumer rights) when assessing mergers and acquisitions and the ability for competition authorities to prohibit such mergers (and/or impose conditions) when they negatively affect the protection of personal data and the privacy of individuals.

Privacy and data protection are fundamental human rights, recognised in the European Charter on Fundamental Rights. As such, personal data "cannot be conceived as a mere economic asset".[1] Corporate activities that infringe individuals' privacy must be curtailed. And this applies also when such activities are not technically anti-competitive.

[1] EDPS Opinion on coherent enforcement of fundamental rights in the age of big data, https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf

Considering societal implications of corporate powers within the competition framework is not such a new or revolutionary proposition in the European context. It is already recognised in EU competition law that the protection of media pluralism can and should trump merely economic consideration in order to avoid excessive media concentration with negative effects on democracy as a whole. Increasingly some of the data exploitation practices by corporations have significant negative implications for the working of democratic institutions.

This is particularly so in relation to the practice of profiling done through the application of artificial intelligence. As a result, an individual or a segment of the population can receive or be excluded from receiving information or opportunities, or be targeted with advertising, which might reinforce existing social disadvantages. For example, a lawsuit is currently pending against Facebook for reportedly allowing advertisers to discriminate against legally protected groups.[2]

As noted by the European Data Protection Board (then Article 29 Working Party) "advances in technology and the capabilities of big data analytics, artificial intelligence and machine learning have made it easier to create profiles and make automated decisions with the potential to significantly impact individuals' rights and freedoms."[3]

Profiling is no longer 'just' affecting the realm of digital advertising. Increasingly corporate powers encroach on the functioning of democracy and have profound societal impacts. For example, profiling is increasingly used by political parties to identify and target potential supporters. While data-driven campaigning has been deployed for decades, the granularity of data that is available and the complexity of the data processing is something new. Recently, the practice of targeting voters by using profiling and exploiting personal data have raised concerns (and in some cases led to the opening of investigations) about political manipulation and the impact of such profiling on the democratic process in countries such as the UK[4], as well as the US[5] and Kenya.[6] Such manipulation places few corporations on the frontline of preserving democracies.

Assessing the powers of digital platforms

In the digital economy there is a trend towards corporate concentration. This is particularly true for digital platforms, such as social media platforms, search engines, digital entertainment, or online retailers. The way in which market dominance is measured traditionally does not always capture the extent of their control, particularly as their products and services are often "free".

However, their dominance is apparent in the way companies are able to impose unfair conditions on users. Because users' data is a valuable commodity (a "proxy for price", as noted by the European

[2] See Julia Angwin and Ariana Tobin, Fair Housing Groups Sue Facebook for Allowing Discrimination in Housing Ads, ProPublica, Mar. 27, 2018, https://www.propublica.org/article/facebook-fair-housing-lawsuit-ad-discrimination. The complaint is available here: https://www.documentcloud.org/documents/4424703-NFHA-v-Facebook-Complaint-W-Exhibits.html.

[3] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Oct. 3, 2017, available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 .

[4] See Information Commissioner's Office investigation, https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf

[5] See: https://www.theverge.com/2018/5/15/17358802/facebook-cambridge-analytica-justice-department-fbi-investigation

[6] See https://www.privacyinternational.org/feature/954/texas-media-company-hired-trump-created-kenyan-presidents-viral-anonymous-attack

Data Protection Supervisor)[7], these unfair conditions tend to include excessive and exploitative collection and processing of users' personal data.[8]

When faced with a demand to consent to the terms of service and privacy policy by a company in a dominant position, users often have no genuine choice but to accept. This lack of choice is caused by a combination of factors: the significant relevance of network effects in these markets - where the utility of a service increases the more people use it, meaning that entrants require a 'critical mass' of users in order to compete, while users may only use the competing service when it has been generally adopted; lock-in of users; lack of alternatives; imposition of terms and conditions with poor privacy safeguards.[9]

Companies such as Google, Facebook, Twitter and others continue to impose terms and conditions to users which allow them to collect, analyse and share personal data in ways that people do not understand (or cannot genuinely consent to.) For example, an Associated Press investigation[10] found that many Google services on Android devices and iPhones store people's location data even if they opted out of such tracking through their phone's privacy settings. Dominant companies also continue to find ways to obtain yet more data in order to maintain and expand their control on the market. For example, Alphabet Inc.'s Google and Mastercard made a deal to give Google access to Mastercard transactions as a way to strengthen Google's dominance, thereby increasing Google's market power in digital advertising and potentially excluding potential competitors.[11]

These privacy harms are directly caused by the business models of companies in dominant positions, which increasingly rely on the availability of users' data, and can impose excessive collection of data on people who have become "captive users" to their providers, given their lack of genuine choice.

Further, the effects of this concentration of power are not limited to online and offline privacy. These companies can act as gatekeepers, for example by regulating how we can access information on the web, including in some cases (e.g. Google, Apple, Amazon) which applications can we install on our devices. And they can track and profile us across devices to predict and influence our behaviour. This is no longer 'just' affecting the realm of digital advertising. Increasingly corporate powers encroach on the functioning of democracy and have profound societal impacts.

When assessing market power, competition authorities have tended to focus on price and outputs, giving little to no consideration to other factors affecting competition, such as quality, innovation and the implications for the exercise of certain fundamental rights, such as the right to privacy. This narrow approach misses the increasingly important competition implications of the collection of personal data, particularly when done at scale. It also fails to take into consideration the multiple effects that gaining personal data has on certain types of digital services. For example, the network effects of the online market can raise the importance of gaining or losing a user because of the

[7] EDPS Opinion on coherent enforcement of fundamental rights in the age of big data, https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf

[8] See complaints filed by the organisation Noyb against Google, Facebook, WhatsApp and Instagram, https://noyb.eu

[9] For example, Whatsapp forcing its users to accept new terms and conditions that led to the sharing of personal data with Facebook (see https://www.theverge.com/2017/5/18/15657158/facebook-whatsapp-european-commission-fine-data-sharing)

[10] See: https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb

[11] See: https://www.bloomberg.com/news/articles/2018-08-30/google-and-mastercard-cut-a-secret-ad-deal-to-track-retail-sales

importance of personal data (at scale) for the functioning of certain algorithms, such as those that underpin the effectiveness of targeted advertising.[12]

In analysing this issue, Privacy International encourages the European Commission to consider how to assess the value of personal data in digital markets, beyond pure monetary terms, and in particular the data-driven network effects of the collection of personal data.

Preserving digital innovation through competition policy

Privacy International encourages the European Commission to assess the negative impact of dominant companies on innovation, particularly in the field of protection of privacy and security of data. As recent research has demonstrated, users demand both confidentiality and security of their digital communications and protection of their personal data.[13] In a competitive market, it should be expected that the level of data protection offered to individuals would be subject to genuine competition, i.e. companies would compete to offer privacy friendly services.[14]

However, in a data-intensive digital market characterised by increased corporate concentration, companies in a dominant position have no incentive to adopt businesses models and practices that enhance individuals' privacy, and they may seek to exclude any privacy enhancing players from any of the markets where they can exert market power.

This is demonstrated by the way companies exploiting personal data often view privacy and data protection legislation: as a threat to their business models. In its 2016 Annual report, Facebook noted how its business may be negatively affected by privacy, data protection, consumer and competition laws.[15] Alphabet Inc.'s 2017 Annual Report to the US Securities and Exchange

---

[12] Academics have described ten implications of data-driven network effects, which are relevant to this analysis. See Maurice Stucke and Allen Grunes, Big data and competition policy, Oxford University Press, 2016, pages 200-205.

[13] For evidence of concerns on the current lack of strong privacy and data protection laws, see in the United States, National Telecommunications and Information Administration, "Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities, May 13, 2016, https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may- deter-economic-and-other-online-activities, and in the European Union, European Commission, Eurobarometer on ePrivacy, Dec. 19, 2016, available at https://ec.europa.eu/digital-single-market/en/news/eurobarometer-eprivacy .

[14] In its 2014 assessment of the proposed merger of Facebook and WhatsApp (Case No. COMP/M.7217), the European Commission acknowledged that "competition on privacy" exists. It stated that "apps compete for customers by attempting to offer the best communication experience," including with respect to "privacy and security, the importance of which varies from user to user but which are becoming increasingly valued, as shown by the introduction of consumer communications apps specifically addressing privacy and security issues." For additional authorities on this point, see Francisco Costa-Cabral & Orla Lynskey, Family ties: the intersection between data protection and competition in EU law, Common Market Law Review, 54: 11-50, 2017, available at http://eprints.lse.ac.uk/68470/7/Lynskey_Family%20ties%20the%20intersection%20between_Author_2016_LSERO.pdf .

[15] Facebook, Annual Report 2016, available at http://www.annualreports.com/HostedData/AnnualReportArchive/f/NASDAQ_FB_2016.pdf ("Our business is subject to complex and evolving U.S. and foreign laws and regulations regarding privacy, data protection, competition, consumer protection, and other matters. Many of these laws and regulations are subject to change and uncertain interpretation, and could result in claims, changes to our business practices, monetary penalties, increased cost of operations, or declines in user growth or engagement, or otherwise harm our business."

Commission notes similar concerns and specifically states in relation to data protection regulation that "these legislative and regulatory proposals, if adopted . . . could, in addition to the possibility of fines, result in an order requiring that we change our data practices, which could have an adverse effect on our business and results of operations. Complying with these various laws could cause us to incur substantial costs or require us to change our business practices in a manner adverse to our business."[16]

Dominant market players often criticise data protection legislation on the grounds that it would harm smaller companies with smaller compliance teams. A more accurate description, however, would be that it threatens their own, current business model.

As two leading academics in the UK state on this point, companies "may already be exercising their market power to foment consumers' supposed lack of interest for data protection: competition on this parameter may be suppressed, as a result of which the current data protection conditions offered do not reflect the competitive level. An analogy could be made to situations where an undertaking has already exercised its power to impose high prices, and thus the current price does not reflect a competitive price… [I]t may be market power that is preventing such competition from emerging."[17]

Failing to innovate on data protection has negative effects on innovating to protect security of data. A business model that relies on excessive generation and processing of data increases the chances of data breaches. For example, the lack of market incentives to provide privacy by design leads to the marketing of devices and services that generate excessive amounts of data about people and their behaviours yet with weak levels of security -- this is done due to poor adherence to standards (accompanied by companies' attempt to avoid the imposition of standards through regulation)[18], the use of cheap components, and the need to generate sufficient data to be of interest to acquisition by the dominant corporations.

Privacy International believes that privacy standards, including the protection of personal data and data security, should be part of any assessment of the quality of a digital service for the purpose of determining competitiveness of a market.

[16] See Alphabet Inc., Form 10-K, available at https://abc.xyz/investor/pdf/20171231_alphabet_10K.pdf.
[17] Costa-Cabral & Lynskey, Family ties: the intersection between data protection and competition in EU law, *supra*.
[18] See industry stance on the current negotiations of the draft e-privacy regulation, https://privacyinternational.org/blog/2061/between-scylla-and-charybdis-fate-e-privacy-regulation