Panoptykon Foundation's submission to the consultation on the Digital Services Act Package

Warsaw, 8 September 2020

About Panoptykon

Panoptykon Foundation is a Warsaw-based NGO with a mission to protect fundamental rights in the context of growing surveillance and fast-changing information technologies. We believe in 'watching the watchers' and consider data a source of power. Therefore we keep an eye on entities that collect and use personal data in order to influence people (public authorities, intelligence agencies, business corporations). On the legal front we keep track of new legislation, develop alternative regulatory solutions and intervene to protect human rights. In our advocacy we address both policymakers and business lobbies. Through our research and investigations we expose risks related to commercial and public surveillance in order to raise public awareness. We visualize collected data and engage in artistic collaborations in order to reach broader audiences. Since 2010 we have been an active member of European Digital Rights (EDRi).

Contents

I. Introductory remarks

Large online platforms[1], in particular those providing social media and content-related services, have developed business models that, while generating high commercial gains, come with troubling societal and individual costs.

Constant tracking that comes in one package with these services leads to exploitation of users' personal data, including their intimate and sensitive characteristics. Large user base, which has grown as a result of network effects, generates endless streams of data, which feed platforms' analytical capacity and their ability to attract commercial clients, who are willing to pay for the promise of (micro-)targeted advertising. High profits generated by targeted advertising, maintained over time, allow large platforms to invest in even better analytical tools and secure their dominance on the advertising market.

Business models of those online platforms that offer service optimization and personalisation (such as Uber or Amazon) and make their profit from customer fees share the same flaws and generate similar risks as far as exploitation of personal data is concerned. In their overview of online platforms, DG Connect experts have noted that: “there are other important characteristics which may distinguish online platforms from other businesses: their capacity to facilitate, and extract value, from direct interactions or transactions between users by building networks where network effects are at play; the ability to collect, use and process a large amount of data in order to optimize user experience or create and shape new markets.”[2]

We argue that it is precisely this set of characteristics that makes business models of large online platforms an underlying cause for many of the problems addressed in this consultation. Therefore, in our introductory remarks, we will briefly touch on the most problematic characteristics and explain their negative effects, as seen from both individual and societal perspective.

In further parts of this submission we will suggest regulatory solutions to identified problems. We believe that the Digital Services Act package creates a unique opportunity to limit the excessive power of large online platforms and hold them accountable for negative social effects of their business operations. Please note that most of our recommendations will address problems caused by those large platforms that use data (both personal and statistical) to target, personalise or optimise content or services that are offered to individuals. Most often it will be the case of **social media and content platforms**[3] , however such activities can also be undertaken by other types of online platforms including: **e-commerce** and **collaborative economy platforms** (e.g. personalised pricing; personalised offers); **internet search services** (e.g. personalised search results); and **mobile ecosystems** (e.g. personalised features or app recommendations). Few of our recommendations will apply to *all* online platforms, regardless of their market position and their business model (e.g. transparency requirements for non-sponsored content). These cases will be clearly marked in the document.

Please also note that in this document we use the term *content* in its broadest meaning, which encompasses all types of user-facing features that are subjected to targeting or personalisation. It

[1] We decided to use this terms (instead of “dominant platforms”) following European Commission's Inception Impact Assessment.

[2] See Commission Staff Working Document on Online Platforms, p. 45.

[3] We draw from definitions and classifications of online platforms proposed in the Commission Staff Working Document on Online Platforms, *op.cit*.

includes both content uploaded by the platform's users (e.g. posts, adverts, offers from online sellers) and content generated by the platform itself (e.g. price determinations, recommendations).

Advertisers' interests shape global online platforms

Over time it has become clear that online platforms that are driven by ad revenues do not perceive their users as clients. In this business model the real service is offered to advertisers and it is their interest that shapes platforms' data collection practices. Ad-driven online platforms use so-called dark patterns[4] and default settings to secure users' "consent" for omnipresent tracking and constant collection of their personal data, which by far exceeds what would seem justified by the nature of key services offered to users.

In order to accumulate vast amounts of users' personal data, large online platforms integrate different services and connect behavioural data coming from different sources. Platforms thrive not only on the data that users share on their own initiative but – more importantly – on metadata and data inferred from their behaviour, such as observations on how they use the platform, what content they are exposed to, and how they react to it.

Collected and generated masses of personal data are then analysed with the use of advanced algorithms in the search for meaningful statistical correlations. The task of these algorithms is to establish users' hidden characteristics that they have never consciously revealed, such as their psychometric profiles, IQ level, family situation, addictions, illnesses, beliefs etc., thus creating detailed profiles, which are then offered to advertisers and used for content personalisation.

In order to secure constant flow of behavioural data about users and maximise their profits from targeted advertising, content and social media platforms need to (at least) maintain user attention and the amount of time they spend on the platform. The more time users spend on the platform, the more data they reveal; the more data they reveal, the more detailed their profiles are; the more detailed the profiles, the more revenues for platforms from selling targeted advertising[5]. In order to set this chain of events in motion, content and social media platforms use algorithms to moderate, recommend, personalise and target content.

Gatekeepers use their power to the detriment of individual users and society

Content and social media platforms have technical ability to control both the content that users won't see (result of content moderation) and the content – paid or not – that users will see (result of content targeting and personalisation). We argue that this ability to effectively control content monetisation and dissemination in global information networks is the very source of what the Commission calls the "gatekeeper power" of large platforms. The way this power is currently used by the biggest players leads to negative effects for both individual users and society as a whole.

First of all, ad-driven online platforms curate information in ways that benefit advertisers, not users. Evidence shows that the ways Facebook, Twitter, and Youtube present content are designed to maximize engagement and drive up their quarterly earnings. The commercial logic that drives

[4] For further explanation of this term and examples of such practices see: Norwegian Consumer Council, *Deceived by Design. How tech companies use dark patterns to discourage us from exercising our right to privacy*

[5] See: https://techcrunch.com/2017/06/04/when-you-look-into-the-news-feed-the-news-feed-looks-into-you

social media contributes to the spread and amplification of potentially harmful user-generated content and is detrimental to the quality of media, as it gives rise to clickbait, emotional and sensationalist messages. Citizens who are exposed to social media and low quality online content are more vulnerable to misinformation, profiling, and manipulation.

Secondly, algorithms used by large platforms to (de)rank and target content are non-transparent and non-accountable. This is particularly problematic in the case of algorithmic engines that drive content distribution across global platforms, amplifying disinformation and other forms of harmful content. These negative effects have already begun to spill over into various aspects of social life, including politics. As a matter of fact, few business entities control which voices and which views will be seen, and which will not. In addition, citizens who use large platforms in non-democratic regimes face a greater risk of government censorship and control.

Thirdly, there is a growing body of research that confirms negative impact of social media on public health, especially in the case of young people who are more likely to develop digital addictions and patterns of compulsive media consumption[6]. Recent studies[7] have linked the use of platforms like Facebook, Snapchat, and Instagram to depressive symptoms in young adults caused by negatively comparing oneself to others on social media platforms. In addition, targeted advertising has public health implications for vulnerable communities that are bombarded with advertisements for unhealthy food products.

Finally, it seems inevitable that large online platforms, which currently act as gatekeepers, will try to leverage their power in other domains, such as public health services, transport management and public security. According to Shoshana Zuboff: "Surveillance capitalism moves from a focus on individual users to a focus on populations, like cities, and eventually on society as a whole. Think of the capital that can be attracted to futures markets in which population predictions evolve to approximate certainty."[8]

GDPR offers partial remedies but won’t fix the power balance

Many of the negative examples of large platforms’ power, as described in the previous section, imply mistreatment of their users’ personal data. Therefore, in theory, mere enforcement of the GDPR should be the right tool to curb these detrimental practices. Consistent application of the GDPR[9] to large platforms’ practices should lead to the following positive effects:

- platforms should not profile users for the purposes of targeted advertising based on data that was collected as ‘necessary for the service’ (such as profile data revealed by users and device metadata) or for analytical or technical purposes (such as website analytics and

[6] See for example: Y. Hou et al., *Social media addiction: Its impact, mediation, and intervention*.

[7] See for example: J. Bettmann et al., *Young Adult Depression and Anxiety Linked to Social Media Use: Assessment and Treatment*; A. Shensa et al. *Problematic Social Media Use and Depressive Symptoms among U.S. Young Adults: A Nationally-Representative Study*.

[8] https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook

[9] This interpretation is based on the European Data Protection Board’s (and previously the Article 29 Working party) guidelines and opinions, in particular: Opinion 2/2010 on online behavioural advertising, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Guidelines 5/2020 on consent, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects.

data from social media plugins on external websites), unless users give their free and informed consent;

- users should be able to find out whether a particular piece of content has been personalised (targeted to them) and verify their personal data used for this purpose;
- users should have full and direct access to personal data that was collected about them or generated with the use of algorithms, including all inferred information;
- users should be protected by default and not subjected to dark patterns or take-it-or-leave it practices, which facilitate rampant data collection.

In reality, detrimental business practices continue to exist two years after the GDPR became fully operational. We argue that the lack of effective enforcement by data protection authorities is not the only reason that explains this paradox. There are certain aspects of platforms' power, like their algorithm-driven targeting abilities based on statistical correlations (i.e. not classified as personal data), which are not adequately addressed in the GDPR.

In our attempts to confront most detrimental business practices, we have identified the following problems, which we could not tackle with mere enforcement of the GDPR:

- **Hampered access to inferred and generated data**: When confronted with data access requests, none of the large platforms has revealed the full user profile, which would include inferred and generated data[10]. Both online platforms and advertising intermediaries argue that inferred data is no longer personal (although it is contrary to the broad definition provided by the GDPR) or that inferred data constitute their trade secrets.
- **User consent fatigue**: Pervasive and interruptive requests for consent, often designed in a deceiving way (so-called dark patterns[11]), contradict the very purpose of introducing consent in the GDPR (as a safeguard for users' information autonomy). These invasive practices make users "accept" excessive data collection and processing, without making them aware of the consequences such "acceptance" may entail (i.e. rampant data collection and invasive profiling). In the context of online tracking, research confirms that most users would not have agreed to these practices, had they been offered real choice or a possibility to define their preferences (e.g. via browser settings)[12].
- **Protection of collective interests**: Data protection law focuses on protecting an individual and their personal data from abuse but does not create sufficient tools to address collective or social implications of large-scale, algorithm-driven data processing, such as unfair targeted advertising, proliferation of sensationalist content and disinformation, or the filter bubble effect.
- **Processing of statistical data that affects individuals**: Big data, understood as observations about people that result from statistical correlations, is fed into algorithmic decision making and informs outcomes that are experienced by individual users (e.g. the

[10] See for example the complaint against Uber filed by drivers who have been denied access to their inferred data that influence their score in the service: https://techcrunch.com/2020/07/20/uk-uber-drivers-are-taking-its-algorithm-to-court/

[11] See: Norwegian Consumer Council, *Deceived by Design. How tech companies use dark patterns to discourage us from exercising our right to privacy*, June 2018.

[12] See for example: https://econsultancy.com/just-23-of-web-users-would-say-yes-to-cookies/

type of content that is presented to them or determination of their marketing profile). At the same time businesses argue that their analysis of statistical data falls outside of the scope of the GDPR and, as such, triggers no legal protection against potential harms or errors. In practice it remains difficult to track how exactly big data has been used to enrich individual profiles or inform individual decisions.

- **Profiling and targeting not covered by Article 22 of the GDPR**: This provision regulates only fully automated decisions that produce legally binding or other significant effects for an individual. In consequence, it can hardly be used to ensure user's control over content targeting/personalisation. While effects of targeting and personalisation are experienced by an individual, it remains difficult to "single out" a data processing operation that relates to a given individual (for marketing purposes users are "packed" into broader groups and categories). For example, in the context of behavioural advertising it is nearly impossible for an individual to prove that she or he has been targeted based on a specific set of criteria. For the same reasons it will be difficult to demand explanation of the logic behind content recommendations or content personalisation based on Article 22 of the GDPR .

While we are aware of these challenges, we argue that the GDPR should not be reopened. Instead, a comprehensive regulation targeted at large online platforms, as contemplated by the European Commission in pending consultations, provides a much better chance to tackle them. It is in this context that we present our recommendations below.

II. Recommendations

Guiding principles for platforms regulation

Before we present detailed recommendations, which will address specific challenges related to large platforms' power to moderate, recommend, personalise and target content, we want to reinforce the following principles, which should apply to all online platforms, regardless of their size and business model:

- **Limitation of platforms' liability for user-generated content**

  Platform operators that act as intermediaries in two- and multi-sided markets should not be liable for illegal activity or content of which they do not have actual knowledge. Liability for any user-generated or user-uploaded content should primarily lie with the uploader, unless hosting intermediaries are co-creators of such content, provide content themselves or have actual knowledge of illegal content. It is important that we uphold this principle for the benefit of free expression and access to information. For the same reason, platform operators should not be obliged by the law to generally monitor content uploaded on their platforms.

- **Full legal responsibility for platforms' own actions**

  At the same time platforms should bear full legal responsibility for their own actions that affect accessibility and visibility of user-generated content (such as its moderation and algorithmic curation) and users' experience on the platform. In particular such actions should trigger legal obligations that will ensure transparency (e.g. revealing the logic behind algorithmic content curation) and accountability (e.g. due process for users affected by content moderation).

- **No binding regulation without effective enforcement**

  When designing new rules for global players, it is essential to build in strong, effective and cross-border enforcement mechanisms. Unfortunately, past experiences show that it is rather unrealistic to expect effective, cross-border cooperation from a whole array of existing enforcement bodies, which include data protection authorities (struggling even with trans-national application of the GDPR), competition authorities (looking at individual cases rather than systemic problems), and media regulators (often politicised and rarely active in online environment). Success of the DSA package will depend on the EU's ability to bridge these enforcement gaps and draw lessons from two years of cross-border application of the GDPR.

Recommendations for the DSA package

In response to the problems summarised in our introductory remarks, as well as building on the guiding principles that we explained above, we came up with the following (groups of) recommendations for the DSA package:

1. **Enhanced transparency**: new regulation should impose high standards of transparency for all online platforms that engage in content moderation, curation (personalisation), and targeting. At the same time there should be different transparency mechanisms for the general public (incl. researchers and watchdogs) and for individual users.
2. **Effective tools to control the use of data and algorithms**: building on individual data protection rights, as defined by the GDPR, new regulation should equip users of the large platforms with more effective tools to control both the use of their personal data and the use of big data and algorithms that affect their online experience. These tools should include both default protections and granular data management settings (including but not restricted to personal data).
3. **Minimum standard of interoperability**: we recommend introducing data and protocol interoperability in the DSA package, as a precondition that will enable the development and provision of effective (i.e. independent from platforms' own business interests and their proprietary interfaces) tools for users to manage their data and shape their online experience (e.g. set own parameters for content personalisation).

In the following points we will present detailed recommendations in each of these categories.

1. Enhanced transparency of the targeting process

Algorithm-driven content targeting and personalisation, despite being the very source of the platforms' power, remains highly opaque. It has been confirmed by multiple studies[13] that voluntary measures adopted by platforms (including those inspired by the Commission in the Code of conduct on disinformation) to increase the transparency of this process are still insufficient. Major online platforms have, indeed, increased transparency in selected aspects of

[13] See for example: ERGA report on the implementation of the EU Code of practice on disinformation, P. Leersen et al. *Platform Ad Archives: Promises and Pitfalls*, A. Andreou et al. Investigating Ad Transparency Mechanisms in Social Media: A Case Study of Facebook's Explanations, Panoptykon Foundation *Who (Really) Targets You*, European Partnership for Democracy, Virtual Insanity. Transparency in digital political advertising.

their operations, such as content served and reach of adverts (relevant data has been revealed in ad libraries) and content moderation (by creating specialised bodies such as Facebook's Oversight Board). However, at the same time they continue to refuse any meaningful explanation of or insights into their targeting and personalisation machineries, both for the public (incl. researchers and watchdogs) and for affected users.

At present, except for the GDPR that applies to the processing of personal data in individual cases[14], there are no binding laws that would determine the scope and form of disclosures expected from platforms that engage in content targeting and personalisation. As a result users and the general public cannot hold platforms to account, while it is against platforms' economic interests to reveal the inner workings of their targeting engines. Voluntary, self-regulatory measures won't solve this problem (such measures depend on platforms' goodwill, can be revoked at any time and create an uneven standard across the market).

While transparency on its own is not sufficient to limit large platforms' gatekeeping power, we see it as a basic prerequisite for legal accountability. **Enhanced transparency** of the targeting process, by the mere fact of casting light on practices that were previously outside of the public eye, has the potential of eradicating misuse of personal data or other unlawful practices. It will also allow users, researchers, nonprofits and regulators to identify potential abuses (e.g. verify whether users' vulnerabilities are exploited in the targeting process) and obtain evidence for law enforcement or for more informed policy debate (incl. on the need to further regulate or deregulate online environment).

A meaningful transparency framework should cover the targeting of both sponsored and non-sponsored content[15]. These two situations differ mainly in terms of involved parties. While content personalisation is fully controlled by the platform, ad targeting normally involves third parties (advertisers) who initiate the targeting process, create their own messages, and choose the profile of their target audience. Despite this difference, both types of targeting present similar risks in terms of manipulation and exploitation of users' vulnerabilities. Notably they rely on similar mechanisms (i.e. the use of big data and algorithms) and benefit from rampant data collection and unique analytical capacities of large platforms.

In relation to sponsored content, platforms are not merely passive intermediaries between advertisers and users but play a key role that shapes the end result of targeting[16]. They do so by:

- shepherding the choices that advertisers can select from in the first place,
- using algorithms to interpret criteria selected by advertisers and to determine which users fulfil them (based on personal data collected by the platform itself and statistical analysis),
- optimising the delivery of ads to fulfil the advertiser's objectives (i.e. showing the ad to individual users who are - on the basis of data controlled by the platform - more likely to

[14] Please refer to introductory remarks on the deficiencies of the data protection framework in the context of algorithmically-driven content dissemination and targeting.

[15] In the broad sense, as explained in introductory remarks: recommendations, news feed, personalised search engine results, personalised offers etc.

[16] See in the example of Facebook: Panoptykon Foundation, *Ad targeting explained*, in: *Who (really) targets you. Facebook in Polish election campaigns*.

respond in a way that the advertiser desires, even if the result of this process is discriminatory[17]).

As far as new transparency measures are concerned, we find it useful to distinguish between:

(a) public-facing, general transparency measures that reveal non-personal information to anyone interested (incl. researchers and regulators) and have the potential to expose platforms' and advertisers' practices for public scrutiny, and

(b) individual transparency, which aims at explaining the targeting process in particular cases and helping users understand why they are confronted with particular content.

Based on these observations, we propose the following transparency framework to be mandated in the Digital Services Act:

1.1. Public-facing transparency of advertising (sponsored content)

In our view the introduction of ad libraries by major online platforms has been a good step towards enhancing transparency of ads. However, the fact that platforms have full discretion in terms of whether to maintain ad libraries at all and what information should be made available, seriously undermines the reliability and the usefulness of this tool, as platforms can withdraw from this commitment at any time and tend to avoid exposing their own role in the ad targeting process. Therefore we recommend that the new regulation include an obligation for advertising-driven social media platforms to maintain ad libraries, and specify a minimum standard for disclosures made by the platforms.

In terms of scope, ad libraries should include all ads, not only political or issue ads. First of all, the concept of a "political" ad is highly ambiguous and difficult to enforce in practice (of which there is plenty of evidence[18]). It is also the only way to make sure that researchers and institutions scrutinising political adverts are not missing anything, and that platforms' rules are being enforced properly. Second of all, commercial targeted advertising also creates many risks that may require intervention - especially on behalf of children and other vulnerable groups. Comprehensive transparency rules enable research into harmful commercial advertising (e.g. the sale of illegal or restricted products, the use of manipulative tactics, or discriminatory ad targeting), and are important from the perspective of consumer protection and data protection authorities.

In terms of disclosed information, ad libraries should contain *at least*:

(1) the content of the advert itself;

(2) *all* targeting criteria and options selected by advertisers for a particular ad or campaign, including optimisation goal and - if applicable - specification of the so-called seed audience for lookalike targeting and indication of the category of the source of data uploaded by the

[17] Empirical academic research into Facebook's advertising engine confirms that ad optimisation algorithms used by this platform can lead to discrimination of certain groups even when the advertiser did not intend to do that, as well as contribute to political polarisation and creating filter bubbles by showing users only these political adverts that correspond with their views. See: M. Ali et al., *Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes* and *Ad Delivery Algorithms: The Hidden Arbiters of Political Messaging*.

[18] See for example: M. Silva et al., *Facebook Ads Monitor: An Independent Auditing System for Political Ads on Facebook*, A. Hounsel et al., *Estimating Publication Rates of Non-Election Ads by Facebook and Google*, Sky News, *Researchers fear 'catastrophe' as political ads 'disappear' from Facebook library*.

advertiser to a custom audience tool (such as newsletter list, website/app pixel, customers database), and information on A/B testing;

(3) aggregated information on the impact of an ad (the number of impressions that an ad received within specific geographic and demographic criteria (e.g. within a political district, in a certain age range), broken down by paid vs. organic reach).

In addition, the following information related to financing and engagement should be revealed for at least **political or elections-related ads**:

(1) the exact amount spent on the advertising campaign;

(2) information on who paid for the advert;

(3) engagements and interactions with the advert beyond viewing, such as numbers of "click-throughs" and "shares" of the advert.

We are conscious of the difficulties related to defining what constitutes a political or elections-related ad. At the same time we acknowledge that disclaimers that we propose above may be considered excessive by commercial actors, whose advertising budgets and tactics are not restricted by law. This extra level of scrutiny is justified in the case of political or election-related ads due to their sensitivity and potential impact. While we are not ready to offer a bullet-proof definition of political or election-related ads, we trust that it is possible to develop such definition in a multi-stakeholder process, led by European institutions.

Access to ad libraries should be possible for anyone interested via a **standardised and programmable API** (application programming interface), to enable continuous and automated collection of data from both public and personal ad libraries (described in point 1.2 (b) below). APIs that are currently offered by platforms have limited functionalities and have proved to be unreliable[19]. We argue that transparency in the world of data is mediated through and conditioned by interfaces. Therefore it should not be left to online platforms alone to design such interfaces. While binding legislation might not be the best tool to shape the design of interfaces offered by online platforms, it can at least formulate minimum requirements for their APIs[20].

1.2. User-facing transparency of targeting and personalisation

We propose a framework for user-facing, individual transparency that consists of the following two elements:

(a) explanation of the logic behind targeting and personalisation (for both sponsored and non-sponsored content)

Individuals who are targeted with a particular ad or shown a personalised piece of content (e.g. a recommendation) should be able to understand why they are seeing it (i.e. what specific data and criteria were taken into account in the targeting process in their particular case). On the one hand our proposal aims at facilitating access to data and information required by the GDPR (such as the purpose of processing). On the other hand it aims at filling the regulatory gap left by Article 22 of the GDPR when it comes to the use of big data in algorithmic decision making.

[19] See for example: Algorithm Watch, *For researchers, accessing data is one thing. Assessing its quality another.*

[20] See for example: J. Ausloos et al., Operationalizing Research Access in Platform Governance. What to Learn from Other Industries? and Mozilla, Facebook and Google: This is What an Effective Ad Archive API Looks Like.

The following information about the logic behind targeting or personalisation should be offered to individuals in real-time, for each piece of content:

Type of information	Detailed specification for sponsored content (ads)	Detailed specification for non-sponsored content
individual explanation of targeting	parameters selected by the advertiser in the targeting process that apply to the user in question	reasons explaining why the user is presented with a specific piece of content or recommendation, including (but not limited to) personal data taken into account
	reasons why the platform has decided that the user meets the advertiser's criteria, including (but not limited to) personal data that were relevant in this process	
sources of personal data	source of user's personal data uploaded to the platform (e.g. website tracking, mobile app, newsletter, loyalty card) and the legal basis for uploading data [only if a custom audience tool was used]	n/a
	sources of user's personal data used in the targeting process by the platform (e.g. users' activity on the platform, its subsidiary, external website, data broker) [always]	
GDPR obligations	legal basis and the purpose for processing personal data, specified for particular data sets	
explanation of the optimisation logic	optimisation goal selected by the advertiser (e.g. conversion) and parameters taken into account by the platform when deciding that this specific goal can be achieved by targeting the user in question (e.g. user's past behaviour or a specific feature attributed to them by the platform)	optimisation goal pursued by the platform operator (e.g. engagement)

(b) personal ad library

Individual users should be given access to a database containing all ads that have been targeted at them and all advertisers who targeted them within a specified time (we propose 5 years). This database would work as a personal ad library, which does not repeat information that is available in the public ad library but contains relevant links (to general information about targeting, impact, and budget of the ad etc.). Items stored in the personal ad library should also link to individual explanations of the targeting process (as described in point a above).

Because such personal ad libraries would only show ads that are relevant to particular users, this interface would not be as overwhelming for them as the public ad library, which presents vast amounts of ads and requires advanced research skills. In addition, users could grant access to their respective personal ad libraries to researchers via an API[21], thereby making it easier for e.g. election monitoring groups to monitor how election-related ads are deployed.

1.3. Accountability of algorithms and AI systems used by platforms for targeting purposes

Targeting and personalisation systems rely on machine-learning algorithms that are optimised to increase platforms' revenues, rather than users' well-being. Researchers, investigative journalists and civil society organisations have exposed multiple examples of harmful or discriminatory effects of such algorithms[22]. In this context we argue that, apart from the transparency measures proposed above, the EU should introduce accountability procedures and effective regulatory oversight for AI systems that affect humans. Such procedures should include mandatory human rights impact assessments and independent audits.

These obligations, however, are not specific to online platforms and should apply to all companies and public institutions that use AI systems affecting humans. As such they should be introduced in a horizontal regulation on AI rather than in the DSA package. We have explained our proposition for a comprehensive transparency and accountability framework for AI systems in our response to public consultations of the White Paper on Artificial Intelligence. Please refer to this document for more information.

2. Tools for people to control the use of (their) data and algorithms

2.1. Tools to control data more effectively

While the GDPR has created a sound legal framework for users to control their data, we see the DSA package as an opportunity to address asymmetries and imbalances of power in users' relationship with large platforms and to solve problems that systematically occur on all platforms that exploit personal data. We argue that further regulatory measures are needed to foster the development of (commercial and non-commercial) tools for users to manage their personal data and use their rights without barriers (such as complex "privacy" settings and interfaces designed to discourage users' choice and limit their access to personal data).

This goal can be achieved by the following set of measures:

[21] Provided minimum API and/or interoperability requirements are in place.

[22] See for example: Facebook allowing advertisers to target teens based on psychological vulnerabilities, examples of bias against women and people of colour in job adverts.

(a) specific rules that clarify the GDPR standard for online platforms

In order not to overburden users with pop-ups and nudging requests to consent to online tracking, the new regulation should introduce default protections, which do not repeat GDPR rules but make them more explicit and unequivocal when applied to online platforms.

We propose the following rules for **all online platforms** (regardless of their size and business model):

- By default users' behavioural data should not be used for targeted advertising and, in particular, for political advertising. Platforms should be required to obtain *explicit* consent for ad targeting (separately for political advertising and for other adverts). To mitigate consent fatigue and the burden of managing their data, default settings should be set to "no targeting" and the law should explicitly prohibit nudging users with requests for consent.
- Change of *default settings* should require action taken at the user's own initiative. The law should also prohibit online platforms from using contractual clauses that link privacy-protective settings with any negative consequences for users, in particular financial burdens.
- Online platforms should be required by the law to offer users an *opt out* from content personalisation without the need for any justification.
- Online platforms should be required by the law to facilitate and encourage their users' access to *all* data that was collected or generated on them. The same interface should allow users to verify the source of data and the purpose of processing (e.g. provision of service, statistical purposes, authentication, content personalisation, ad targeting).

We expect that these specific rules, built on top of the GDPR, will not only help users control their data more effectively but also limit large platforms' power to act as gatekeepers by pulling the plug on practices that fuel such powers (e.g. excessive data collection; take-it-or-leave it provisions in terms and conditions; hiding real purposes of data processing in unclear "privacy" policies).

(b) positive obligations for large online platforms to foster interoperability

For a meaningful control over their own data, users of online platforms need:

- easy, real time access to their *full* profile (including all inferred or generated data),
- easy way to correct or delete particular data points,
- access to one-click, real-time data portability,
- easy way to verify legal basis and purposes for processing specific categories of data.

As we explained in our introductory remarks, users of large platforms face serious barriers in exercising their data rights, even though such barriers may contradict the GDPR. As demonstrated by multiple studies[23], existing user interfaces often discourage or complicate their interaction with the platform operator (e.g. by forcing users to use pre-defined contact forms or referring them to

[23] See for example: A. Andreou et. al, *op.cit.*, Privacy International, *No, Facebook is not telling you everything*, R. Mahieu et al., *Collectively exercising the right of access: individual effort, societal effect*, J. Ausloos et al., *Getting Data Subjects Rights Right*, The Verge, *GDPR makes it easier to get your data, but that doesn't mean you'll understand it*.

Q&As) and prioritise platforms' commercial interests (e.g. by enabling users to verify and control only selected, uncontroversial data points and hiding full marketing profiles).

In order to solve these problems, the new regulation for **large platforms** should define effective procedures for users to exercise their data rights, which will work independently from platforms' own interfaces.

In practical terms, users should be able to:

- communicate their GDPR requests via **standard protocols** (such as "Do Not Track" signal or a more granular feature) and have them recognised by the platform;
- use **tools independent from platforms' interfaces** (i.e. offered by other companies or non-profits, on the basis of minimum interoperability standards) to directly manage their personal data.

In point 3 below we continue this reasoning by proposing minimum interoperability obligations for large platforms.

2.2. Tools to shape users' own online experience (control over algorithms)

In addition to new tools that help users access, verify and control their own data (or statistical data that shapes their profile) in a more effective way, the new regulation should provide for tools that enable users to shape their online experience. In practice it translates to at least some degree of control over algorithms that are used to curate content for individual users. We argue that individual users, acting alone or via their trusted intermediaries, should be able to set their own parameters, expectations and limitations for what is currently called "personalisation".

As we argued in introductory remarks, "personalisation", in the form implemented by global social media platforms, serves advertisers' (not users') interests, as it has one overarching objective: maintaining user engagement and maximising their exposure to sponsored content. In order to reduce (or at least prevent further escalation of) negative individual and societal effects caused by this business model, the European Commission should propose legal and technical solutions that will shift power over "personalisation" (content curation and content targeting) from platforms and their commercial clients to individual users.

In practical terms, users of **large online platforms** should be able to:

- express their preferences with regard to content targeting and personalisation (both sponsored and organic) using more *granular* settings than a simple opt-in/out-out feature (e.g. set their own parameters for content presented to them during certain times of the day, at work, during weekends or holidays; set limitations protecting their vulnerabilities, such as "no health-related sponsored content" or "no sponsored content aimed at children");
- filter and prioritise content based on their *own feedback and preferences* (for example calibrate their own filters for hate speech and misinformation);
- communicate their choices with the platform using a *standard protocol*, e.g. by sending a signal (much more granular but otherwise similar to "Do Not Track") to express their tracking and personalisation (targeting) preferences via their browser or another independent intermediary;

- choose their *own client* (developed and operated by an independent company or a non-profit) to manage personalisation (targeting) preferences and content filters (in addition to managing their personal data, as described in point 2.1 (b) above).

3. Minimum standard for interoperability

3.1. The need to shift the power balance in online environment

Large platforms (incl. Facebook and Twitter) already offer APIs (application programming interfaces) that allow more advanced users and independent software providers to send data from other sources and connect new applications with the platforms (e.g. gaming applications or simple plug-ins). However, such APIs do not allow users to independently manage their data or content settings. Large platforms reserve their right to restrict or revoke access to API for any reason.

Moreover, existing APIs can only be accessed on behalf of large platforms' users, not on behalf of users of another service. It seems that large platforms, when acting at their own initiative, are only willing to offer "interoperability" in one direction, i.e. to enable the flow of data and independent services from outside, so that it benefits their own business model.

It is against this background that we argue that the new regulation for large platforms, as contemplated by the European Commission, should include minimum interoperability obligations at least for those large platforms that act as gatekeepers. There should be explicit obligations on gatekeepers to support interoperability, and duties to avoid measures that impede it. Just as in the European Electronic Communications Code, the European Commission should be given powers to designate technical standards (such as the World Wide Web Consortium's ActivityPub) that must be supported by specific gatekeepers.

Access to interoperability interfaces should not discriminate between different competitors and should not come with strenuous obligations. Interoperability interfaces, such as APIs, should be easy to find, well-documented, and transparent (The Fair, Reasonable and Non-Discriminatory or FRAND principles from telecommunications regulation could be adapted here.)

3.2. Specific obligations and prohibitions for large platforms

On a general level, new regulation for large platforms should mandate for[24]:

(a) protocol interoperability, which would allow users to communicate with the platform in alternative ways (for example by sending a standard, DNT-like signal through their browser in order to express their tracking preferences or by choosing another client to manage their privacy settings);

(b) data interoperability, which (on a basic level) can empower users to use their data rights (in particular the right to access, correct and move their own data, as discussed in point 2.1 (b) above) in a more effective way, without being limited by platforms' own interfaces.

More specifically, in order to achieve minimum interoperability, large platforms should be obliged to:

- adopt a standard protocol or publish their own protocol/API specification through which third parties can interface with it;

[24] Both concepts - protocol and data interoperability - are discussed in Margrethe Vestager's 2019 special advisers' report on digital competition.

- ensure non-discriminatory access to this interface and allow all competitors to build independent services (i.e. applications and plug-ins) that complement, modify or replace some of the platform's functionalities; in the case of social media platforms this obligation should lead to unbundling hosting and content curation activities, so that third parties can offer content curation to the platforms' users;
- inform users about alternative applications and plug-ins whenever the platform prompts a user to install its own application (try new services);
- maintain API for users (and their trusted agents) according to the standard defined by the regulator (or specified in the regulation itself), which gives users real-time access to their own data (processed by the platform operator) and facilitates the exercise of their data rights, as defined by the GDPR;
- respect standard protocols (recognised by the European law or international standard-setting bodies) in communication with their own users (e.g. to manage privacy settings; set targeting and tracking preferences; access and transfer data) and in communication with competing services (e.g. to federate newsfeeds or send/receive direct messages).

The DSA package should also prohibit practices and behaviours of large online platforms that impede access to the market for competitors, in particular:

- self-preferencing (i.e. nudging users to install applications owned by the platform operator when alternatives exist);
- limiting access to the platform ecosystem (e.g. app store) for independent software providers, as long as these providers respect data protection and data security standards defined by the European law;
- offering privileged access to own API to selected software developers or a more limited API (than available internally) to all potential competitors;
- reserving their right to restrict or revoke access to API for any reason;
- ignoring signals communicated by their users (e.g. via their trusted agents) with the use of other protocols, as long as these protocols have been recognised by the European law or international standard setting bodies.

In addition to introducing legal obligations and prohibitions for all large platforms, the European Commission should consider remedies tailored for individual platforms (*ex ante* rules).

This regulatory toolbox should include:

- data sharing obligations, such as an obligation to allow competitors to access behavioural data collected by the platform and/or statistical models developed on the basis of such data (if access to raw data would compromise users' privacy) to the extent it is necessary for the development and provision of the competing service;
- prohibitions and limitations when it comes to the use of personal and/or aggregated users' data, such as prohibition of integrating 1st and 3rd party data for targeted advertising purposes.

3.3. Expected impact on the digital market

Full protocol interoperability, when combined with data interoperability, should not only enable users to delegate a third-party software to interact with a platform on their behalf (e.g. send messages, like and comment on posts, read content) but also to federate selected features with competing platforms. Mandating for **vertical and horizontal interoperability** in the new regulation for large platforms will open the way for deep changes in the whole online ecosystem and certainly undermine large platforms' power to act as gatekeepers.

We expect that it would foster the development of competing services that not only have the ability to connect users on different platforms (e.g. with messaging services) but also function on top of the large platform's ecosystem - complementing, modifying or replacing some of the platform's functionalities. In this scenario users of large platforms would not only be able to connect with peers on a different platform but also to curate their own newsfeed or recommendations and define their own content filters using independent software. Mere existence of such competing services, capable of modifying large platform's key functionalities, would radically change the power balance in the online environment. European Digital Rights argues[25] that interoperability would drastically reduce the imbalance of power between platforms on the one side and individuals on the other.

Summing up, we expect that mandatory interoperability, once imposed on large platforms, would serve as a positive disruption in the existing online ecosystem, paving the way for:

- true federation in the social media space, which means that users can freely choose their main platform operator and, regardless of this choice, still communicate with other social networks and access information shared on other platforms;
- new markets of online services that are built on top of large platforms, such as third-party clients for data management or content moderation plug-ins.

[25] See: European Digital Rights, *Platform Regulation Done Right*.