International Working Group
on Data Protection
in Technology

**Working Paper on the Risks emerging from the**

**Tracking and Targeting Ecosystem in the Digital Advertising Market**

*Written procedure prior to 67th (virtual) meeting on 24* April 2021

## Introduction

1. The functioning of the modern internet makes it almost impossible to be online anonymously. Most websites and apps embed technology -sometimes without fully understanding it - that track directly or indirectly identified or singled out users across websites, apps and devices, even in their "offline-life", create profiles of them and supply information to various third parties and platforms, selling data and user-targeting services.

2. Thus, personal data is collected over widely spread data collection networks including major platform operators.[1] By selling space on their websites for advertising auctions in real time (also known as Real-Time-Bidding or RTB), integrating social-plug-ins and share-buttons, as well as using Software Development Toolkits (SDKs), analytic and measurement tools, website operators and app providers become data suppliers to the online advertising supply chains. Hence, they help to enrich the data profiles of platforms, data brokers and ad tech companies.

3. While end users can detect some of the tracking in their devices, browsers or apps, many tracking technologies operate "behind the curtains". These practices are usually revealed only after relevant investigations. The opacity that characterises this data ecosystem is exacerbated by the fact that many of the involved companies are non-consumer facing, most people have never heard of them. Even if they have, there is a dearth of information as to where the data is sourced from and whom it is shared with.[2] This has a knock-on effect on the exercise of rights and the ability to exercise any control, for example by giving informed consent or by submitting access or erasure requests.

1 ICO, Update report into adtech and real-time bidding, 20 June 2019, https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf.

2 https://privacyinternational.org/advocacy/2434/why-weve-filed-complaints-against-companies-most-people-have-never-heard-and-what.

4. The level of detail of the information processed varies: It ranges from the mere counting of individualized visits on a specific website or information about websites the user has visited before and afterwards. Beyond, it can include detailed recordings of the parts of a webpage the user looks at, content clicked on, mouse movements, reading duration, typing history and key stroke dynamics, interaction with the app etc. This data is typically associated to persistent and non-persistent unique identifiers. The information linked to the identifiers can then be crossed with demographic data and inferred data about users, based on data analysis and data collected or purchased from other sources.

**Scope**

5. The working paper on Web Tracking and Privacy published in 2013 by the IWGDPT[3] described the common methods for collecting, analyzing and processing data concerning the usage of Information Society Services with computers, tablets, smartphones and, increasingly, other 'smart' and connected devices. Some tracking is done for security and measurement purposes. However, the vast majority of these technologies aim to link user data from different websites, apps, devices and beyond to identify patterns in behavior, to allocate, derive and infer attributes to end-users and to compile this data into comprehensive digital profiles used for the personalization of ads and services, in some cases for manipulation of the user.

6. The tracking technologies and the dimensions of data gathered in big data bases have developed and increased quite significantly since 2013, especially with the ability to track users across multiple devices and considering the variety of applications and websites sharing data with third parties. What was still formulated as a vision or potential development[4] has become reality. There has also been a systemic development of the online advertising marketplace. It has established a wide range of structures of tracking and targeting users with various actors, some of them very powerful due to their market power. This paper outlines privacy and data protection concerns of this tracking, profiling and targeting ecosystem that can also be used beyond digital advertising to seek to manipulate the opinion forming process, and there are significant concerns about the consequences of this ecosystem for democracy.[5] The paper also provides recommendations to lawmakers, regulators, authorities and the companies involved.

**Tracking and Targeting Ecosystem**

7. The digital advertising market consists of a large variety of different stakeholders: The aim being that advertisers can reach the suitable customers with relevant and engaging advertising at the

3 IWGDPT, "Working Paper on Web Tracking and Privacy: Respect for context, transparency and control remains essential", 53rd meeting, 15-16 April 2013, Prague (Czech Republic).

4 IWGDPT, "Working Paper on Web Tracking and Privacy: Respect for context, transparency and control remains essential", 53rd meeting, 15-16 April 2013, Prague (Czech Republic), Para 7.

5 See https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf and https://privacyinternational.org/long-read/2850/data-exploitation-and-democratic-societies.

right time, which in turn shall help publishers monetize their creativity and content. In between those three stakeholders a lot of service providers of different kinds are involved who collect data from different sources, analyze it, link it together, build up personal profiles and/or provide it to other actors[6]. Although there have also been doubts raised on the efficacy[7], individual targeted advertisement has developed as the dominant concept to reach the desired audience.

8. The digital advertising ecosystem involves the processing of personal data of billions of individuals. User data is harvested, generated, shared and processed in a multitude of ways using a range of tacking technologies[8] such as cookies, web beacons, device fingerprinting, tags and SDKs to segment/classify customers based on pages visited, links clicked, and products purchased.

9. The various electronic tools can be used to build up user profiles. They do not just track users, but can also use any data collected for data mining to find out what may be inferred about these users' preferences and their future behavior. These profiles are used to target people in different ways, such as to tailor advertisements, content and messaging to their perceived specific interests. Social media providers and online platforms may include said electronic tools within their environments and in third parties' websites and apps interested in audience interactions and engagement.

10. Online publishers use tracking code from different companies, including not only the well-known ones such as Google and Facebook, but also a vast of largely unknown big and small companies to help target advertising. When a company's code is embedded on many different sites, it can build up detailed profiles on individuals as they move around the Web and apps by assigning them unique identifiers. Thus, users can be recognized again. Not only big companies but also company networks are capable to build up those comprehensive profiles by sharing information.

11. Even a large scale of offline activities is tracked and incorporated in the advertising ecosystem, for example, data is collected when consumers buy products in a store using a loyalty card or paying by credit or debit card. In addition, many apps permanently track the location of the device -in case of smart phones that is equivalent to the location of the user – and thereby create a detailed profile of the user's physical movement. As data is not only collected by a single company but also sold on a market, data from different sources can easily be linked to round out a profile.

12. The global digital advertising market revenue grew 15.9% to $ 124.6 billion in 2019, according to the IAB[9] Internet Advertising Revenue Report[10] conducted by PwC and published in May 2020. The IAB report identified two major factors driving growth: self-serve platforms that allow small

6 For an overview also cf. to Forbrukerrådet (Norwegian Consumer Council), Out of control, How consumers are exploited by the online advertising industry, 14 January 2020, https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of-control/, Chapter 2.2, p. 13.

7 https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf.

8 https://privacyinternational.org/explainer/2976/how-do-tracking-companies-know-what-you-did-last-summer.

9 Interactive Advertising Bureau, https://www.iab.com.

10 https://www.iab.com/wp-content/uploads/2020/05/FY19-IAB-Internet-Ad-Revenue-Report_Final.pdf.

businesses to advertise with ease on the internet, and the rise of online startups that use these self-serve platforms to sell products directly to consumers.

**Personal data in this context**

13. Data protection principles apply to any information concerning an identified or identifiable natural person. Where users visit websites or install apps which have embedded snippets of relevant third party code this code collects data from the session and associates it with a (usually unique) identifier (also possible through device-fingerprinting etc.).[11] Since the same third party code is typically embedded on multiple different websites or apps,[12] the unique identifier makes it possible to merge data across those websites, apps or devices. This results into single behavioral profiles, which include all kinds of information collected and brought together with the help of the identifier. As those profiles contain very specific information, they can even be merged between different companies or networks who use different identifiers.[13] This data has to be considered as personal data. The reference to a person may arise from the circumstances or the context in which the information is dealt with. It is not relevant, that real world names might not be connected to the data when it comes to personal references. If large parts of life take place in the online world – as with many people – it is relevant whether individuals can be identified or addressed via online identifiers. To determine whether a natural person is identifiable, it is sufficient if the individual is singled out, made distinguishable from others and clearly addressable. This is exactly the aim and purpose of the targeting eco system.

14. There might occur slight inaccuracies due to the fact that devices or browsers could be used by more than one person. Nevertheless, in times of highly individualized devices, especially smart phones, cases of shared use decrease constantly. Despite of this, if profiles are highly sophisticated it is possible to individualize the user by their actual browsing-behavior (browsing-history; user-behavior on a website, login to certain accounts etc.).

**Profiling**

15. Profiling is at the heart of the digital advertising ecosystem. Disparate and seemingly innocuous data can be combined to create a meaningful comprehensive profile of a person.[14] Advances in data analytics, as well as machine learning have made it possible to derive, infer and predict sensitive data from ever more sources of data that is not sensitive at all. For instance, content

11 Reuben Binns / Elettra Bietti, Acquisitions in the third party tracking industry: competition and data protection aspects, https://osf.io/preprints/lawarxiv/fe8u7/download , para. 1.1.

12 Reuben Binns / Elettra Bietti, Acquisitions in the third party tracking industry: competition and data protection aspects, https://osf.io/preprints/lawarxiv/fe8u7/download , para. 1.1.

13 Forbrukerrådet (Norwegian Consumer Council), Out of control, How consumers are exploited by the online advertising industry, 14 January 2020, https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of-control/, Chapter 2.5, p. 25.

14 https://privacyinternational.org/feature/1721/snapshot-corporate-profiling and https://privacyinternational.org/report/1718/data-power-profiling-and-automated-decision-making-gdpr.

shared by users on Facebook has been found to be an indicator of future occurrence of depression.[15] The very same techniques have made it easier to identify unique individuals from data about their behaviour across devices, services and even in public spaces.[16] Such profiles may allow data users to infer highly sensitive details that may or may not be accurate and that can be inaccurate in ways that systemically mischaracterise or misclassify certain groups of people. Such analysis mean that the outcome of the data analysis is greater than the sum of its parts: even seemingly innocuous data can be used together to obtain insight and inferences about sensitive details of an individual's life.

16. As profiling can be done without any further involvement of individuals, they usually do not know whether these profiles are accurate, the purposes for which they are used, as well as the consequences of such uses. In many cases, a web user does not even know or realize that the advertisement or content shown is composed based on his or her individual profile. This lack of awareness prevent individuals from being able to exercise their data protection and privacy related rights.

17. As shown above this profiling involves processing of personal data. Thus, data protection rules on profiling – where existing – must be considered.

**Privacy and Data Protection Concerns**

18. The ecosystem of tracking and targeting as it is currently working has been developed across national borders, although clear data protection legislation has been in place in some major legislations. The European Union, for example, introduced its first data protection legislation, the Data Protection Directive, in 1995[17]. It already contained the principle of Privacy by Design[18], the requirement of a specified legal basis for every processing of personal data[19] and rules on transparency of the process[20]. Thus, the main issues raised below should have been known and considered from the very beginning of these developments.

19. Regardless of the complexity of the ecosystem and possible difficulties regarding the practical feasibility, it is the responsibility of every controller and processor taking part in this ecosystem to fully comply with all regulatory rules applicable. Business models must be developed in a way respecting the legal framework they shall be implemented to.

15 https://www.pnas.org/content/115/44/11203.
16 de Montjoye, Y.-A./ Hidalgo, C.A./ Verleysen, M. & Blondel, V.D. ,Unique in the Crowd: The privacy bounds of human mobility, Nature srep. 3, 1376; DOI:10.1038/srep01376 (2013).
17 Directive 95/46/EG.
18 Rec. 46 of Directive 95/46/EG.
19 Art. 7 of Directive 95/46/EG.
20 Art. 10 – 12 of Directive 95/46/EG.

*Lack of Transparency / Comprehensibility*

20. For most users it will remain hidden that not only the website operators or app providers themselves set tracking cookies on their terminals and devices, but that technologies embedded enable third parties to set tracking cookies, collect device fingerprints, upload content via pixels etc.. Users often do not have sufficient information about the third parties involved in the processing of their data, the purposes of the data processing, the types of data collected, the categorization of their behavior and the consequences of the tracking they are subject to. This wide spread distribution of users´ data is not transparent. In many cases privacy policies and data protection declarations do not clearly state who is involved in the processing and what the data is used for.

21. Nevertheless, data controllers under many legislative frameworks are obliged to provide transparency to data subjects regarding the purpose and the extent of the data processing. In case a website operator or app provider transfers personal data to third parties or enables them to collect this data the website operator or app provider often is the only party of the ecosystem interacting with the user. Therefore, the website operator or app provider must practically be in charge of providing users with information regarding all processes their data will be subject to, even though the website operator or app provider might not conduct all the data processing itself. Nevertheless, every stakeholder that processes personal data within the ecosystem as a controller itself is responsible that sufficient transparency is provided to the user for the scope of his processing. Many controllers can only achieve this by providing clear and sufficient information to the relevant website operator or app provider.

22. Taking into account the complexity of the current ecosystem and the huge number of its participants it will hardly be possible to present the process in a way users can actually understand what is happening or might happen to their data. This applies even more since data is not only collected and used by a single actor but the collected data is often enriched by data inferred by prediction tools and linked to data sets collected and sold by other actors. These data sets are not only collected in the online-environment but also offline behavior is heavily tracked. In the end it is nearly impossible for a user to know, much less control, which data sets exist about him or her in the ecosystem and which actors do control them for which purposes. Nevertheless, transparency towards users is a legal obligation and a prerequisite for user control.

23. Conventional cookie banners are often not transparent and do not meet the requirements for data protection consent as laid down in many data protection laws. Moreover, the wording often suggests that users have a choice, which is not the case for many of those banners. On the contrary, there is often a lack of freedom of choice. Still many banners only contain an "ok"-button but no possibility to decline, or a possibility to decline that is so cumbersome that the user gives up expressing his choices. Other banners intend to create the fiction of an implied consent where the user keeps on browsing the website. Even if there is a choice, we can often see that information is not sufficient to give users any idea of the dimension of the online advertising ecosystem, into which their data is fed and what consequences arise for them.

24. While most cookies can at least be detected by users, the use of other tracking mechanisms, such as device fingerprinting, leave hardly any traces that would be comprehensible to the user. Users are left with almost no possibility to detect the data collection or to intervene. Nevertheless, many website operators or app providers are even less transparent when it comes to those alternative tracking mechanisms.

25. Many website operators claim that the data processed is pseudonymous and cannot be linked to the single person by name, pretending the users cannot be individually identified. However, even without using real names other identifiers are used to create detailed profiles linked to those identifiers and again to address them with advertisements or other messages based on the information contained in the profile. For example, hashed emails are commonly used as profile identifier as they allow to easily import external and/or offline data on the users, and they are also claimed to be pseudonymous. The prominent reference to pseudonymization is therefore rather misleading for users.

26. In the environment of apps tracking is even less transparent than on websites: If at all, there is a notification of privacy policy including the tracking tools once the app is installed. Unlike websites displaying the so called “cookie banner” every time they are opened reminding the user of the policy, apps do not show this information every time they are started. In addition, the amount of text does not suite very well a smart phone display. This must be considered when designing transparency tools of an app, e. g. by integrating different layers and highlighting the key data protection issues on the first layer.

*Lack of Control / Limited Intervention Possibilities / Linkability*

27. A big part of daily life has nowadays shifted to the internet, especially a lot of services, e. g. booking flights, reading newspapers, all kinds of shopping, interactions with banks and insurances, announcements of all kinds of events etc. Browsing the internet in a useful manner and using these services forces users to give away control over the collection and processing of personal data on their online behavior and the information/content sought.

28. Nearly all of these internet services are enriched with tools of the tracking ecosystem that go far beyond what is necessary for functionality and security reasons. Most users do not have effective possibilities to stop the collection of personal data based on identifiers when they want to access webpages and/or apps and have a useful experience on the internet:

29. In regards to websites, there are tools available to at least identify and block cookies. These tools enable the user to prevent some tracking activities but they cannot provide full control for the user over what personal data collected, as setting cookies is not the only tracking technology. In addition, several website owners make it mandatory to store cookies dedicated to tracking on the terminal of the user, otherwise content or services are not available.

30. In cases of apps the users even have fewer possibilities to interfere with the sharing of data with platforms or other third parties.

31. To the extent users are granted (little) control over collecting of their data by the possibility of changing privacy settings many companies seem to take big efforts to design their products in a way that users do not take these measures. This can imply tracking users being the default setting, hiding away the settings, designing the relevant buttons in a way that it is unlikely to be clicked or threatening with limited functionality. In contrast, under many laws companies are bound to the principles of privacy by design and privacy by default meaning they have an obligation to implement privacy-friendly settings by default.

*Lack of Data minimization*

32. The whole ecosystem is built on the collection of as much data, as detailed and as personalized as possible and is thereby in direct contradiction to the principle of data minimization. The success of many companies in this ecosystem directly depends on the mass of personal data they can collect. These companies claim the more data they process, the more accurate the predictions and the more tailored and targeted the advertising/content can be. Furthermore, as companies are pitted against each other through a bidding mechanism, it is crucial for them to be as targeted as possible, resulting in an incentive to always collect more data than their competitor. As it is often said nowadays: Data is the new gold or oil.

*Undermining special protection of sensitive Data*

33. It is important to note that the data exploitation practices of the ecosystem can also involve special-categories or sensitive personal data,[21] such as, for instance, health data, data concerning an individual's sex life or sexual orientation or data revealing political opinions.[22] For example, visits to health related websites or apps, especially insurance apps, if tracked, could create a picture of the state of health, diseases and therapies. While tracking on specific websites and apps can inform about religious beliefs or sexual preferences as well as the economic circumstances or political views of the user. These data categories are specially protected under many legal systems and may only be processed under special conditions of legality (e. g. expressed consent), because processing of such data create high risks of discrimination and manipulation. Such requirements of legality foresee at least knowledge of the context in which the data is used, the purposes for which it is processed and the specific types of data involved as well as the possibility to intervene. Where platforms select audiences based on the analysis of those sensitive data without making these activities transparent and giving the data subjects instruments to intervene, special

21 Cf. General Data Protection Regulation (EU) 2016/679 (GDPR), Article 9.

22 UK Information Commissioner's Office (ICO), Update report into adtech and real-time bidding, 20 June 2019, https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf.

protections foreseen by law are undermined. Vulnerabilities of individuals are easy to detect and exploit.

34. In September 2019, Privacy International published a study that reveals how popular websites about depression in France, Germany and the UK share user data with advertisers, data brokers and large tech companies, while some depression test websites leak answers and test results with third parties.[23] Another research showed that menstruation apps shared intimate details of users' sexual life and mental health with Facebook and/or third parties. This included, beyond others, information on whether users had unprotected sex, whether they are feeling anxious or depressed etc.[24] In both cases, the data collection practices of certain companies raise fundamental questions around whether such sensitive data could be potentially used to also feed into users' profiles for advertising purposes.

35. Even where the data collected in first place is not sensitive big data analysis and prediction of certain behavior can lead to very sensitive data that can be used for discriminating purposes, without any chances for the user to realize or enforce protection mechanisms.

*Automated decision-making / Profiling*

36. The ecosystem of tracking and targeting is designed as a set of fully automated processes. The decision which content or advertisement an individually targeted person will be presented is the result of user's data collected, analyzed and enriched by machines, whereas it depends on the specific case how much data is used and how specific the content is targeted at the user. The RTB-Process is a model of automated decision.

37. Although targeted advertising or content in most cases does not have immediate legal effects it has real implications. The European Data Protection Board states that the decision to present targeted advertising based on profiling may fall within the scope of Article 22 GDPR as it may significantly affect individuals.[25] If this is the case will depend on the particular characteristics of the case including:

- the intrusiveness of the profiling process, including the tracking of individuals across different websites, devices and services;
- the expectations and wishes of individuals concerned;
- the way advert is delivered and

23 https://privacyinternational.org/sites/default/files/2019-09/Your%20mental%20health%20for%20sale%20-%20Privacy%20International.pdf.

24 https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruation-apps-are-sharing-your-data.

25 Article 29 Data Protection Working Party, WP251rev.01 "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, last revised on 6 February 2018, acknowledged by the European Data Protection Board on 25 May 2018; http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053, page 22.

- using knowledge of the vulnerabilities of the data subjects targeted. [26]

The affection of users becomes more significant when it is not only advertisement that is personally targeted, but also content of websites and apps. It can be highly intrusive and discriminating when individuals on the basis of their profile are not shown certain job offers and it has a severe impact on a user if the content shown is curated upon his or her profile, e. g. on his or her political views without him or her realizing it. This might prevent the user from a balanced information regarding political or other societally discourses. Sometimes this system can create a "content bubble" that threaten our common understanding of events, which is the basis for a functioning democracy.

38. Regardless of the specific legal framework for automated decisions these operations represent processing of personal data and as such are subject to general transparency obligations of the respective controller. Furthermore, users should have the possibility to decide if the profiling should take place or not.

*Lack of Legality*

39. A key requirement of most data protection frameworks is that the processing of personal data must have a legal basis or justification, additional justification is often required for the processing of sensitive or special categories of personal data. This applies to each and every actor in the ecosystem processing personal data as a controller.

40. The various actors in the digital advertising ecosystem appear to rely on a range of legal bases for the processing of their personal data. However, it is often not clear which legal basis is relied on for which processing operation and then if so, whether the legal standard is met.

41. Legitimate interest can be a basis for processing personal data in a number of legal frameworks. Nevertheless, this also includes a balance of interests between the legitimate interests of the controller and the data subject's privacy interests. Questions arise in the context of digital advertising regarding people's reasonable expectation, especially for profiling related processing of personal data. Research shows that people do not want to be tracked and monitored.[27] For instance, a 2018 study by the think-tank Doteveryone found that 91% of respondents considered important to choose how much data they share with companies,[28] while a 2019 special

26 Article 29 Data Protection Working Party, WP251rev.01 "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", last revised on 6 February 2018, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053, page 22.

27 See also: UK Competition and Markets Authority, Online platforms and digital advertising Market study interim report, Appendix G: Summary of research on consumers' attitudes and behaviour (2019), https://assets.publishing.service.gov.uk/media/5df9ed39e5274a08dbcdfe0f/Appendix_G_digital_markets_study.pdf.

28 https://www.doteveryone.org.uk/wp-content/uploads/2018/06/People-Power-and-Technology-Doteveryone-Digital-Attitudes-Report-2018.compressed.pdf.

Eurobarometer by the European Commission found that consumers who did not have control over their data were generally concerned about not having full control.[29]

Inferences drawn from the data that is collected can be highly intrusive both due to the sensitivity and due to the scale. The majority of players in the digital advertising ecosystem do not have direct relationship with individuals. Taking into account the severe interference with fundamental privacy rights, it is doubtful whether the legitimate economic interests of the players of the advertising ecosystem can prevail.

42. Contract might be another basis for processing in some data protection frameworks, where an individual enters into a contract, for example via terms of services with a platform. However, in most cases tracking users is not necessary to deliver the service subject to the contract. Questions arise as to whether it is ever fair for a service to be conditional on the use of consumer's data for profiling and targeted advertising.

43. User-consent might be another possible legal basis for processing data in the ecosystem. Nevertheless, consent should be freely given, specific, informed and unambiguous. By the means of consent, data subjects shall be given control over the dimension in which their personal data is processed.
However, consent for the use of personal data for digital advertising and profiling, if asked for at all, is often made conditional for the access to a website or service or the use of an app. In contrast freely given consent would require that there is a real choice to use the service with or without the relevant data processing. There is also the question of nudging and the design of consent mechanisms.[30] Consent requires an unambiguous deliberate action by the individual data subject. As such, a user continuing to browse a website shall never amount to that user's consent. The same applies to the pure omission of settings, where sharing the data is set by default. Additionally, the terms and conditions shall not be used as a method for obtaining consent.

Another potential risk in this ecosystem is that of settings whereby users are invited to provide their consent for a broad range of actions (global consent). Individuals are asked to consent to the processing of its personal data by multiple parties for multiple purposes bundled together, as opposed to specific consent. It is questionable if such consent can meet the purpose of granting the data subject control over its personal data. Consent should be granular, including giving users separate options for separate purposes to allow the users control. The control in addition is undermined by the fact that withdrawing a given consent is made extremely challenging.

Referring to the issues with transparency highlighted above, providing sufficient information to enable users to take their decision for consent in an informed basis knowing what exactly he or

29 European Commission, Special Eurobarometer 487a: the General Data Protection Regulation, 2019.

30 Links to questions raised by the Forbrukerrådet (Norwegian Consumer Council), Deceived by design, How tech companies use dark patterns to discourage us from exercising our rights to privacy, 27 June 2018, https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/.

she is allowing the different controllers in the ecosystem, is another challenge that is hard to meet by the relevant stakeholders. Indeed, for consent to be informed, the user shall be able to identify all parties processing and the type of processing each one conducts.

44. Regardless of the legal basis, all controllers and processors under many legislations are bound to the principles of privacy by design and/or privacy by default meaning that data protection friendly technical design and settings are to be implemented from the very beginning. Looking at the advertising ecosystem, we cannot see many serious efforts to develop technologies addressing these obligations.

    The digital advertising ecosystem must comply with data protection obligations relating to the integrity and confidentiality of the data. Concerns have been raised that the Real Time Bidding system in digital advertising involves the unauthorized, and potential unlimited, disclosure and processing of personal data.[31]

    *Erosion of Purpose limitation*

45. Personal data should be collected for a specified, explicit and legitimate purpose and not be further processed in a manner incompatible with this purpose. The compatibility assessment of the purpose of processing requires consideration of the context in which the data has been collected and the reasonable expectations of the data subject regarding further use as well as the nature of the data and the impact on the data subject. It should also, where relevant, involve consideration of the nature of the relationship between the data controller and the data subject.

46. The EDPS in its opinion on Online Manipulation[32] has re-stated the importance of the purpose limitation in the context of profiling, noting that: "*The concern of using data from profiles for different purposes through algorithms is that the data loses its original context. Repurposing of data is likely to affect a person's informational self-determination, further reduce the control of data subjects' over their data, thus affecting trust in digital environments and services. Hence the crucial importance of purpose limitation as a principle of data protection law.*" [33]It goes on: "*Data analytics involve methods and usage patterns which neither the entity collecting the data, nor the data subject considered or could have even imagined at the time of collection. Algorithmic processing of personal data creates possibilities to generate new data. When a data subject shares a few discrete pieces of data, it is often possible for those data to be merged, generating second*

31 See complaints to Irish, French and UK data protection authorities https://fixad.tech/september2018/ . The issue of security was also raised at a recent fact finding forum by the UK ICO https://ico.org.uk/about-the-ico/research-and-reports/adtech-fact-finding-forum.

32 European Data Protection Supervisor (EDPS), Opinion on online manipulation and personal data, Opinion 3/2018, https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.

33 European Data Protection Supervisor (EDPS), Opinion on online manipulation and personal data, Opinion 3/2018, https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.

*and even third generations of data about the person*."[34] The same conclusion is drawn by Wolfie Christl stating: "*At the same time, information about people's behaviors, social relationships, and most private moments is increasingly applied in contexts or for purposes completely different from those for which it was recorded*."[35]

47. In the web-tracking ecosystem, data collected is not only used for the purpose of targeting advertisements and messages, but also to perform editorial personalization of the content provided to the data subjects without participants' knowledge. Publishers show different content, may it be different advertisements, different headlines for an article, or a different design etc., and carefully track the users' online behavior to find out which one has a better reception on the audience.[36] This shows that data once collected or acquired can be used in the system for all kinds of purposes without sticking to the rule of purpose limitation.

*Implications for exercising rights*

48. Due to the complexity and opacity of the current system, it is nearly impossible for users to exercise their privacy rights in regards of their personal data stored and processed in the advertising ecosystem. In many cases the user does not even realize that his or her personal data is collected and by whom and he or she definitely does not have enough information to whom this information is transferred. This makes it already impossible to identify the companies he or she would have to ask for access to his or her data or other rights. Should the user be able to do so, the question of the technical means through which the user is able to claim his identity and exercise his rights is still open, especially with controllers that use "pseudonymous" identifier not trivially linked to the user.

**Other Fundamental Freedoms and Rights at Risk**

49. Data protection law and privacy requirements are fundamental rights; they are also enabling rights that act as a prerequisite for the exercise of other fundamental rights. If the rights to privacy and data protection are not respected, there are implications for a range of civil and political as well as social, economic and cultural rights.

50. The United Nations High Commissioner for Human Rights has affirmed that states are obligated to exercise regulatory jurisdiction over private companies to ensure that human rights protections extend to people whose privacy is impacted by the companies generating, collecting, and using

34 European Data Protection Supervisor (EDPS), Opinion on online manipulation and personal data, Opinion 3/2018, https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.

35 Wolfie Christl, Corporate Surveillance in Everyday Life, Cracked Labs, June 2017, http://crackedlabs.org/en/corporate-surveillance.

36 Wolfie Christl, Corporate Surveillance in Everyday Life, Cracked Labs, June 2017, http://crackedlabs.org/en/corporate-surveillance, para 7.7 p. 78.

their personal data.[37] States are further obligated to "*mitigate the impact on human rights from [...] power and information asymmetries*" that exist between people and private companies in the use of peoples' personal data. He highlighted that "[*b]usiness enterprises and States continuously exchange and fuse personal data from various sources and databases, with data brokers assuming a key position. As a consequence, individuals find themselves in a position of powerlessness, as it seems almost impossible to keep track of who holds what kind of information about them, let alone to control the many ways in which that information can be used.*"[38]

51. When people worry about how their data is used and might be abused by private companies or public authorities in an ecosystem based on tracking and profiling, they may self-censor their words, thoughts, and actions. This limits their ability to seek out new information, formulate ideas, express dissent and organise to effect social change. That in turn can have a great impact on individuals' rights to freedom of expression (Article 19 of the Universal Declaration of Human Rights (UDHR)), freedom of association (Article 19 UDHR) and the right to political participation (Article 21 UDHR) as well as the right not to be discriminated against (Article 7 UDHR).

52. The right to freedom of expression and information includes the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. Such freedom is limited where information is filtered based on highly granular profiles, based on factors such as the previous behavior (e.g. browsing history, pages liked, articles read), inferred assumptions and other data from a vast array of sources. People face the disadvantage of being targeted with information and messaging according to the categorization of their data.

53. The data and the ecosystem can be tapped into by anyone with sufficient resources and can be used by all kinds of players regardless of what they want to sell.[39] Each participation in the system carries the inherent risks, such as the ability to target individuals when they are vulnerable to strategic influence,[40] or in a way that discriminates against specific groups. The latter might be attempt to bypass anti-discrimination laws[41] and special protections afforded under data

37 UN High Commissioner of Human Rights, Right to Privacy in the Digital Age, August 3, 2018 A/HRC/39/29, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement (accessed March 27, 2019).

38 UN High Commissioner of Human Rights, Right to Privacy in the Digital Age, August 3, 2018 A/HRC/39/29, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement (accessed March 27, 2019).

39 Function creep of the digital advertisement ecosystem: In Ghosh, Dipayan / Scott, Ben, "Digital Deceit – The Technologies behind Precision Propaganda on the Internet, 2018, https://www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit/, it is argued that there is a "fundamental flaw" in the digital ecosystem that makes advertising-supported platforms vulnerable to being manipulated by bad actors of all sorts).

40 Example in Nadler, Anthony/Crain, Matthew/Donovan, Joan, "Weaponizing the Digital Influence Machine: The Political Perils of Online Ad Tech", Data & Society (2018), https://datasociety.net/wp-content/uploads/2018/10/DS_Digital_Influence_Machine.pdf; *S. 15.*

41 *See, e.g., Online personalisation enables invisible - and illegal - discrimination,* (https://privacyinternational.org/examples/868/online-personalisation-enables-invisible-and-illegal-discrimination .

protection legislation by using micro-targeting as proxies to circumnavigate being explicit about race, political opinions, disability, religion, or other categories in ways that are prohibited.

54. Concern about this industry has also been raised by the European Data Protection Supervisor (EDPS) specifically with regards to the myriad of ways in which data analytics methods can be used to merge data or derive, infer or predict other data about a data subject: "*Companies in the business of selling digital ad space profit from the placing of targeted content irrespective of any ethical considerations: there is no distinction made between a good or bad click from a target demographic. These micro-targeting activities may have little effect on some individuals, but the complexity of the technology, low levels of trust and the avowed intentions of several important tech players point towards a culture of manipulation in the online environment. This manipulation may occur as a result of the business strategies chosen by market players themselves, or because of the actions of individuals and states seeking to use platforms intermediaries to disrupt or subvert markets and public discourse.*[42]"

55. Many of these concerns extend to the context of political campaigning and the entailed risks for democracy:

    If political campaigns and media content are highly individualized and tailored to the single recipient they are withdrawn from the public discourse by media and other actors, one of the guarantees of democracy (the so called 4th power), as campaigns and messages are not accessible to all public anymore.

    If political messages are precisely targeted the risk for the publisher that these messages are challenged or even questioned can be minimized. Negative reaction can be reduced even more by live monitoring the reaction of the audience and adjusting the targeting accordingly. This mechanism enables players to spread very extreme messages without being threatened by broad backlash effects[43].

    When political campaigns and media content are highly targeted, individuals are presented with news and arguments that are very similar or sometimes, very opposite (to leverage on confrontation for increased engagement). This deprives individuals from the possibility to hear other voices and opinions and thus can damage democratic processes.

56. The tracking ecosystem includes a high potential of manipulation of the behavior of individuals. The deepened knowledge about individual users, especially about the emotional constitution, can be used to identify personal biases and weaknesses and allow publishers of any kind to exploit this

42 European Data Protection Supervisor (EDPS), Opinion on online manipulation and personal data, Opinion 3/2018, https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.

43 Nadler, Anthony/Crain, Matthew/Donovan, Joan, "Weaponizing the Digital Influence Machine: The Political Perils of Online Ad Tech", Data & Society (2018), https://datasociety.net/wp-content/uploads/2018/10/DS_Digital_Influence_Machine.pdf; , chapter 3, p. 31/32.

to influence or even control individual behavior. According to Zuboff there is already a market of behavioral control composed of those who sell opportunities to influence behavior and those who purchase these opportunities[44]. The concentration process of the advertisement market[45] provided this potential for manipulation to a handful of big technology companies whose user base extends all over the world.

57. For example, Facebook in 2012 manipulated the newsfeed of 1.9 million of its users in the US in order to cause them to go to vote. Facebook claims that it could increase the share of voters within this group by 3 percentage points[46]. If Facebook or other social networks, hypothetically, applied such manipulation only to users of a certain political spectrum that could have crucial influence on the result of elections. Similar mechanisms could also be employed to make people not to vote or vote in a certain way. This is only one example to show the tremendous potentials of influence on democracy and society hold by private stakeholders. In fact it is unknown if and to what extent this influence is already enforced in election processes.

**Recommendations**

*Lawmakers*

58. The whole tracking and targeting ecosystem has obviously developed despite clear rules in some laws across national borders. This means that some common business practices of the ecosystem might reveal themselves as illegal, as the state of the ecosystem cannot be the basis for the regulation. To tackle the problem lawmakers should acknowledge that strengthening data protection regulation and privacy rights safeguards other fundamental rights and secures the functioning of democracy. Where it is not clear enough it is necessary to implement more specific, clear and concrete data protection regulation that leaves no doubt as to what is permissible and what is not.

44 Zuboff, Shoshana, Big Other: surveillance capitalism and the prospects of an information civilization, 4 April 2015, Journal of Information Technology (2015) 30, 70-89; https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754&download=yes, p. 85.

45 A study conducted by Princeton researchers in 2016 found that Google Analytics, a product used to log visitors to websites that integrates with the company's ad-targeting systems, was found on almost 70 percent of sites. DoubleClick, a dedicated ad-serving system from Google, was found on close to 50 percent of sites. The top five most common tracking tools were all Google-owned. To sum up, Google offers more than 228 products and services from Gmail and Google Alerts to Google AdWords Editor and YouTube (https://www.webrankinfo.com/google) and bought nearly 200 startups, online companies, and robotic systems etc. .. In a report dated December 2018, Privacy International revealed how Facebook routinely tracks users, non-users and logged-out users outside its platform through Facebook Business Tools, specifically the Facebook SDK. Similarly, a report by Digital Content Next found that "a major part of Google's data collection occurs while a user is not directly engaged with any of its products". These are just a few examples of the wide range of tracking methods used by companies. Through all the entities they own and control, the GAFAM know our way of life by tracking and crosschecking our personal information and it has now become almost impossible to remain anonymous online.

46 Sifry, Micah L., Facebook Wants You to Vote on Tuesday. Here's How It Messed With Your Feed in 2012, MotherJones, Politics, 31 October 2014, https://www.motherjones.com/politics/2014/10/can-voting-facebook-button-improve-voter-turnout/.

59. Data protection laws should take greater account of the fact that often there is not a single data controller, but that data processing is increasingly carried out in chains of controllers or in systems that are controlled by many organizations. It becomes more and more important that regulation provides mechanisms to clearly allocate responsibility. In this regard, greater attention should be paid to scenarios where controllers enable other controllers to access the data of end-users by embedding technology in their websites for instance. Particularly in cases of joint controllership, controllers should be obliged to make sure by binding agreements and effective controls that other controllers they cooperate with are accountable and reliable and the further processing of the data is lawfully.

60. Lawmakers should take into account that the whole ecosystem of tracking and targeting is a highly specialized industry with the main goal to collect, link and evaluate as many personal data as possible and use them to individually influence people's behavior. This constitutes a risk for fundamental rights and freedoms. Thus effective data protection legislation is essential to guarantee those for the future.

61. Lawmakers should impose specific transparency obligations on the companies tracking individuals, even if they do not have direct contact with the user, by means of providing such information to the entities (e.g. web operator) who are in contact with the respective individuals.

62. Given the strong dependence and relation between the data protection and privacy in this context, the lawmakers should make sure that the enforcement of legislation on tracking is assigned to the data protection authorities and not to other regulators. Having two separate authorities enforcing privacy and data protection rules is clearly less efficient than having one.

*Regulators / Data Protection Authorities*

63. Where lawmakers do not specify the regulation on data processing in the ecosystem of tracking and targeting it is the task of Data Protection Authorities must interprete the abstract regulations and strongly enforce them. This includes a clear guidance to controllers on what is allowed and what not and enforcement where there is a lack of compliance.

64. Given that the system consists of a complex network of controllers all over the world, international collaboration of authorities is crucial to form a significant counterweight to the tracking industry.

65. As displayed above the tracking ecosystem does not only affect privacy issues of single data subjects but has rather broad effects on fundamental rights and public interest. Thus other monitoring bodies such as national electoral commissions and electoral monitoring bodies, consumer associations, commissioners for equality and anti-discrimination, should be involved in their special fields of supervising.

66. Authorities must – within the scope of their legal means - enforce data protection on the structures as a whole, including systemic complaints and collective redress, and not limit their actions to the assessment of individual complaints.

*Companies*

67. Companies first of all have the obligation to comply with the relevant legal framework. It is in their responsibility to develop business models that are in full compliance with data protection legislation and respect privacy rights of data subjects and all aspects raised above. It would be highly efficient if standard frameworks would be created by groups or associations of controllers and processors, e.g. as a binding code of conduct.

68. Wherever associations or subjects develop such standards they should seek consultation by the relevant data protection authorities or other experts to make sure beforehand that they comply with legal obligation.

69. Private companies or public authorities should not engage with service providers, which do not offer clear information on the tracking of users and on the processing of user personal data.

70. When companies develop new business models and the respective technical tools they should from the very beginning consider all applicable data protection legislation, especially the principle of privacy by default and by design.

71. As users' first interface to the web, browsers can play an important actor in the implementation of data protection and privacy measures. As such, browser operators are bound to the principle of data protection by default and should implement means for users to express their choices regarding the acceptance of cookies or further processing of their data as well as means for companies to contact users to ask for their acceptance in a standardized way.

72. When user consent is the legal basis for processing data, companies shall make sure that said consent if freely, given, specific, informed and unambiguous by making sure the user has a real choice to say 'yes' or 'no'.

73. The access to the contents of websites should not be conditional to the acceptance of user tracking.