WEDF

WEDF Student Initiative Submission

Living in the era of personalization: The illusion of valid consent.

Christina Varytimidou

According to Eli Pariser (2011) since December 2009 we live in the era of personalization, where everything we consume online has been tailored. As the vast majority of online services is free, the revenue model has evolved and is now based on targeted advertising and real-time bidding of data collected through tracking and online profiling. This aggregation of personal information including special categories of data such as health and political opinions (as defined in article 9(1) of the General Data Protection Regulation (GDPR)) has led to unprecedented commercial and political exploitation of data subjects. The scope of this essay is to explain the free online business model, its impacts on our lives and analyse why the current legal and technical measures are inadequate to deal effectively with such privacy intrusive models.

Under article 4(4) of the GDPR, online profiling is the 'automated processing of personal data… to analyse or predict aspects concerning the person's performance at work, health' etc. Basically, what companies do is to collect as much data as possible, use algorithms to look for patterns that reflect the personality of the individual (data mining) and then 'sell' these data in the ad exchanges to other companies that match the interests of each consumer. This is why usually when we buy something online, proposed products appear, relevant to our previous shopping history. Normally this could be considered just a lawful evolution of advertising. The problem however with online profiling is that it has become successful by unlawfully collecting personal data and that companies can use these predictions for decision-making purposes. If a company knows the health problems of a candidate, it might not select him. If it is aware that the individual suffers from emotional distress, it can advertise antidepressants. The Cambridge Analytica Scandal where millions of personal data on Facebook were used for Trump's political

campaign showed exactly the magnitude of the impact online profiling has in our lives and the echo chambers Facebook News feed algorithm has created are now the perfect propaganda tool (Grygiel, 2020).

In Europe, legislation has tried to mitigate the risks of the impact of online profiling mostly through data protection laws. By taking a preventive approach, these laws prohibit the processing of personal data without consent. Online profiling usually collects data by setting cookies for tracking and behavioural advertising. Under article 5(3) of the Directive 2002/58/EC (the e-Privacy Directive, 2002), only strictly necessary cookies are exempt from consent (recital 66). In its Opinion, Article 29 Working Party (2012) clearly stated it is unlikely cookies used for advertising to be included in this exemption, hence before placing cookies, website users have to be clearly and comprehensively informed. As the GDPR is a newer regulation and has changed the standards of consent, these new standards have to be met even when the e-Privacy Directive applies. In addition, any processing of personal data collected by cookies (recital 30 GDPR), and online profiling require a lawful ground, according to the key principle of lawfulness (article 5(1) (b) GDPR). Specifically, for sensitive data processing is prohibited unless explicit consent was given according to article 9(2)(a), as online profiling does not seem to fall in any other category of article 9. Although according to article 4(11) and 7 of the GDPR, multiple requirements should be met for a lawful consent, the practical issues that arise show that consent is not a panacea nor it guarantees actual personal data protection.

Firstly, consent has to be freely given (article 7(4), recital 43) specific, informed and unambiguous (recital 32). For the free online business model, these requirements are unlikely to be met. In 2018, ICO issued a warning to Washington Post because the alternative choice to turn off cookies by paying a monthly subscription implied that consent was a condition and thus not freely given. The ‘information assymetries of the data-driven market’ (Van de Waerdt, 2020) and the constant imbalance of power, makes free consent even more fanciful. According to the EDPB guidelines (2020), unambiguous consent needs a clear and affirmative act, and this is why pre-ticked boxes have already proven inadequate in ‘Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.’ (2019). As valid consent needs the user to have actually read and digested the provided information according to ‘Orange Romania SA v Autoritatea Naţională de Supraveghere a

Prelucrării Datelor cu Caracter Personal' (2020), even if the rest requirements are met, it is not realistic to demand from Internet users to cope with the information overload they will have to face before doing anything online. They will simply agree in everything. The 'clear and plain language' condition under article 7(2) poses also problems as controllers cannot really know the linguistic abilities of the data subjects nor if they are native speakers or not.

The specific and informed requirements of consent are even more difficult to be met. According to recital 42 and article 13(1), the data subject should at least be aware -among others- of the controller and the purposes of processing. But in the dynamic system of real-time bidding and data sharing without knowing in advance from whom and for which purpose these will be used, this is practically impossible to happen. This lack of information about the controllers makes all data subject's rights such as the right of access (article 15) or to withdraw consent (article 7(3)) solely theoretical constructions. The data subject will never be aware of all the controllers who use his data and thus he will never be able to exercise his rights. Furthermore, the lack of transparency does not guarantee that even known controllers will actually comply with a withdrawal request, making any further processing of these data unlawful (article 9(1)), yet with no knowledge of its continuance.

What's more, the difference between consent and explicit consent required for the processing of sensitive data is not yet clarified and the right of access under article 15(1) does not specify whether the controller should provide information about the personal data collected or also about the generated data (if personal). Another issue profiling brings is that though the input of data might not include sensitive data, the inferred data might do so, increasing the controller's chances of incompliance.

The limits of the current regime are even more apparent in automated decision-making. Article 22(1) GDPR prohibits only automated decision making which produces legal effects or these that significantly affect the data subject. This prohibition is inadequate as many automated decisions will not meet the high threshold of legal effects. Indeed, not even the Cambridge Analytica scandal can fall in this category although it led to vote manipulation. In addition, exemptions listed in article 22(2) uplift the restriction and even allow it after explicit consent, but simple consent could suffice if companies try to circumvent it by putting 'human in the loops', making it very difficult to prove if a human evaluated the results or simply ratified them.

As the law is only one of the forces that regulate our actions according to Lessig's pathetic dot theory (1999), the GDPR correctly acknowledges the power of architecture and specifically establishes in article 25 the legal obligation for controllers to implement privacy-friendly technology. Each controller after conducting a DPIA (article 35(2) (a) and (b)) which will allow him to realise the high risks online profiling involves, will have to design the technology with embedded data protection principles from the beginning. For instance, to comply with the privacy by design obligation under article 25(1) controllers have to take appropriate technical organisation measures such as pseudonymization, while privacy by default compliance can only be achieved when a do-not-track by default mechanism is implemented, that requires an active opt-in for each different purpose of processing. The new proposed E-Privacy Regulation (2017) in article 10 emphasizes these requirements as the user will have to consent prior to the installment of software or placement of cookies creating a more robust data protection by default, but the opacity of the whole online profiling and advertising system makes all these requirements enforceable only to the controllers that actually appear to consumers.

It seems that the very nature of the free business model makes it GDPR incompliant overall, since it basically infringes every key principle of article 5 including transparency, storage limitation, and data minimization. Companies collect and retain as much data as possible because this will help patterns and inferences become more accurate and thus maximise their revenue. The GDPR has simply not been designed to cope with this model.

Part of this inadequacy is due to the one-sided approach it follows. Some of the most imminent risks resulting from the vast aggregation of data for predicting consumer behaviour are consumer manipulation, discrimination and undue influence. The GDPR does not have consumers in mind. Only data subjects. This detachment from the consequences of the problem is the reason why it cannot fully protect us. The reliance on s.7 of the Consumer Protection from Unfair Trading Regulations 2008 and the prohibition of unfair commercial practices such as undue influence under article 8 of the Directive 2005/29/EC as proposed by Hörnle (2019) can address better the risks of data processing but has to overcome two major issues: the borderless nature of Internet which makes any non-global consumer protection regulation difficult to enforce and that in this business model individuals are no longer consumers but 'the product being sold', as Andrew

Lewis stated. Our transformation from consumers into products is the reason why consumer law seems not applicable in this case and the respect to human dignity is at stake.

As the 'genie' of our times is technology (Hörnle,2019) perhaps it is better to save the third wish and ask for a technology that actually solves the root of the problem. Blockchain and self-sovereign identity providers along with embedded ethics in algorithms and AI tools used for online profiling might be the future solution that will give people actual direct control and lawfully consent on what personal information he is sharing and with whom. But this technology will only be applied if the people change their willingness to give their data for free. If the market is short in 'data-supplies', then eventually the business model will have to adapt to this demand. The only real question therefore is if people are willing to take back control of their autonomy with the risk of having to change the norm of 'free Internet'.

References

1. ARTICLE 29 DATA PROTECTION WORKING PARTY, (2012), 'Opinion 04/2012 on Cookie Consent Exemption' 7June 2012[online]. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf (Accessed: 6 February 2021).

2. 'Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)' (2002) OJ L 201, 31.7.2002, p. 37–47 (e-Privacy Directive).

3. EDPB, (2020) 'Guidelines 05/2020 on consent under Regulation 2016/679' version 1.1, 4 May 2020. Available at: https://edpb.europa.eu/our-work-tools/our-documents/topic/consent_en (Accessed: 6 February 2021).

4. Grygiel, J., (2020). Algorithmic Propaganda: how Facebook meddles with democracy, Communications Law 2020. **25**(1), pp. 23-30. Available at: https://uk.westlaw.com/Document/I16032B7059C411EAA5A3930791C9FB81/View/FullText.html (Accessed: 6 February 2021).

5. Hill, R. (2018) Washington Post offers invalid cookie consent under EU rules – ICO, The Register, 19 November [online]. Available at: https://www.theregister.com/2018/11/19/ico_washington_post/ (Accessed: 6 February 2021).

6. Hornle, J. et al. (2019) 'Regulating online advertising for gambling - once the genie is out of the bottle.', Information & Communications Technology Law, 28(3), pp. 311–334. Available at: http://search.ebscohost.com.ezproxy.library.qmul.ac.uk/login.aspx?direct=true&db=edswst&AN=edswst.2494651&site=eds-live (Accessed: 6 February 2021).

7. Lessig., L. (1999) Code: and other laws of cyberspace. New York: Basic Books.

8. Orange România SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (2020) Case no. C-61/19, para 46. Available at: http://curia.europa.eu/juris/document/document.jsf;jsessionid=417A61A85012E09CA5DF6C811D74D26F?text=&docid=233544&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=3371805 (Accessed: 6 February 2021).

9. Pariser, E. (2011) The Filter Bubble: What the Internet is hiding from you. London: Penguin Books.

10. Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. (2019) Case no. C-673/17, para 63. European Electronic Reports of Cases. Available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=3372166 (Accessed: 6 February 2021).
11. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), (2017), 2017/0003(COD)(E-Privacy Regulation).

12. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016) OJ L 119/1 (GDPR)

13. Van de Waerdt, P. J. (2020). Information asymmetries: recognizing the limits of the GDPR on the data-driven market. Computer Law & Security Review: The International Journal of Technology Law and Practice, **38**. Available from: doi: 10.1016/j.clsr.2020.105436.