

## i-call working paper

No. 2023/01

# Google's Privacy Sandbox Initiative: Old wine in new skins

Michael Fässler\*

FEBRUARY 2023

### ABSTRACT

This paper discusses the Google «Privacy Sandbox Initiative» (PSI), which aims to change existing tracking technology to better protect user privacy. The proposal is examined in its technical dimensions, while additional context concerning its development is provided by discussing outside pressures coming from other actors. If the PSI is to be implemented, the process of tracking will change, but the digital advertising business will not. The paper aims to assess these unaddressed problems by taking political ads as example of the effects such advertising has on democracies. Towards the end of the paper, further thoughts on how to approach the regulation of intermediaries like Google are sketched out.

### KEY WORDS

Google, The Privacy Sandbox Initiative, intermediaries, targeting, artificial intelligence, polarization, regulation, public utilities

\*Michael Fässler, MLaw, is an academic assistant and PhD student at the chair of Prof. Dr. iur. Christoph Beat Graber at the University of Zurich. Comments are appreciated and welcome at [michael.faessler@rwi.uzh.ch](mailto:michael.faessler@rwi.uzh.ch).

---

I-CALL WORKING PAPERS are the result of research that takes place at the Chair for Legal Sociology and Media Law (Professor C.B. Graber) at the University of Zurich. The papers have been peer-reviewed.

SUGGESTED CITATION: Fässler, Michael, 'Google's Privacy Sandbox Initiative: Old wine in new skins, *i-call Working Paper No. 01 2023*, Zurich, Switzerland: University of Zurich.

Published by:  
i-call, Information • Communication • Art • Law Lab at the University of Zurich  
Professor Christoph B. Graber, PhD  
Chair for Legal Sociology and Media Law  
University of Zurich, Faculty of Law  
Treichlerstrasse 10  
8032 Zurich  
Switzerland

ISSN 1664-0144  
© Information • Communication • Art • Law Lab, Switzerland

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, mechanical, photocopying, recording or otherwise, without prior written permission of the publisher.

Permission to use this content must be obtained from the copyright owner.

# Google's Privacy Sandbox Initiative: Old wine in new skins

<b>1</b>	<b>INTRODUCTION.....</b>	<b>4</b>
<b>2</b>	<b>GOOGLE'S BUSINESS MODEL .....</b>	<b>5</b>
	2.1 ADVERTISEMENTS ON GOOGLE.....	5
	2.2 USER TRACKING.....	6
	2.2.1 Cookies and fingerprinting.....	6
	2.2.2 The privacy-debate.....	8
<b>3</b>	<b>THE «PRIVACY SANDBOX INITIATIVE» .....</b>	<b>9</b>
	3.1 CONCEPT AND PROGRESS.....	9
	3.2 RECENT DEVELOPMENTS AROUND TRACKING TECHNOLOGY .....	11
	3.2.1 Tearing down «cookie-walls» .....	11
	3.2.2 Pressure from non-state actors .....	12
<b>4</b>	<b>THE EFFECTS OF TARGETED ADS ON DEMOCRACY.....</b>	<b>13</b>
	4.1 MEASURING THE IMPACT OF POLITICAL ADVERTISING.....	13
	4.2 CASE STUDY: THE 2016 U.S.-PRESIDENTIAL ELECTION.....	14
	4.2.1 Timeline and Outcome.....	14
	4.2.2 Political advertising and democracy.....	16
	4.2.3 State of the political landscape in the U.S.....	18
<b>5</b>	<b>REGULATING TARGETED POLITICAL ADS.....</b>	<b>19</b>
	5.1 EXISTING RESTRICTIONS ON POLITICAL ADS .....	19
	5.2 MODALITIES OF REGULATION .....	20
	5.3 INTERMEDIARIES RESEMBLING PUBLIC UTILITIES.....	21
	5.3.1 A collective endeavor.....	21
	5.3.2 Intermediaries and the Swiss « <i>service public</i> » standard .....	22
<b>6</b>	<b>SUMMARY .....</b>	<b>25</b>

## 1 INTRODUCTION

This paper discusses the collection and usage of data for advertising purposes on the Internet. We focus on Google<sup>1</sup> specifically, as it is leading the market and has introduced far-reaching changes to the online advertising business.<sup>2</sup>

As in the following pages various downsides of the usage of user data will be discussed, it seems proper to start with acknowledging the numerous benefits it brings to the Internet: targeting and personalization algorithms are necessary, or at least extremely useful. Just on the side of search engines, there has to exist a proper organization, considering the vastness of data available on the Internet: Google (Search) has hundreds of billions of webpages indexed.<sup>3</sup> On YouTube, there are over 30'000 hours' worth of content uploaded every hour.<sup>4</sup> To organize search results into a meaningful order, Google has to know what users want to search for in general and also what is of interest for a specific user – depending on their location, time of day, language, and many other things.

It stands to reason that the tech companies in Silicon Valley profited highly from the recent shift towards Big Data in their industry. On one hand, they could now use the new technologies to improve their recommendation-systems, content filters, advertisements (ads), and search engines. On the other hand, they were in the prime position to collect user data that they could sell in the newly forming market. Maybe unsurprisingly, user data became one of the most valuable resources on earth.<sup>5</sup> The handling of these resources in relation to digital advertising is the main concern of this paper. Its first part is primarily focused on facts: how does the technology surrounding Google's advertising business work and how much money is involved? What is the PSI and how is it connected to existing limitations on advertising? In the second part, we take the example of targeted political ads to assess the risks they pose for democratic structures. How potent are these ads and what are their effects? How are they regulated and under which premises should discussions about further regulations take place? Finally, we open the discussion to reassess the role that intermediaries<sup>6</sup> should play in a democracy by comparing them to public utilities. Throughout this paper, we focus on the EU as well as the U.S. for references as both are western democracies that contribute greatly to intermediaries' revenue and host significant parts of their assets.

---

<sup>1</sup> Google is used as a summary term that means to specifically include YouTube and Google's numerous web-based services like Gmail, Google Maps, and the Android system.

<sup>2</sup> A fact that has been noted by EU and U.S. officials alike, see the EU Commission's «Impact assessment of the Digital Markets Act», SWD(2020) 363, p. 104, as well as Sen. Mike Lee, 'CDTA Overview' (2022), p. 1, available at <https://www.lee.senate.gov/services/files/5332FC38-76F0-4C8B-8482-3F733CF17167>.

<sup>3</sup> Google LLC., 'How Google Search organizes information', available at <https://www.google.com/intl/en/search/howsearchworks/how-search-works/organizing-information>.

<sup>4</sup> James Hale, 'More Than 500 Hours Of Content Are Now Being Uploaded To YouTube Every Minute' (2019), available at <https://www.tubefilter.com/2019/05/07/number-hours-video-uploaded-to-youtube-per-minute>.

<sup>5</sup> The Economist picked up on this notion about half a decade ago. Then, it considered a combined yearly net profit of 100 billion stemming from the «Big Five» (Alphabet, Facebook, Amazon, Apple, and Microsoft) a huge amount: The Economist, 'The world's most valuable resource is no longer oil, but data: The data economy demands a new approach to antitrust rules' (2017).

<sup>6</sup> (Internet-)intermediaries are Internet platforms that provide no or almost no content themselves but instead let users create content on their platform. Apart from Google, other prominent examples of intermediaries would be social intermediaries like Facebook, Instagram, and Twitter.

## 2 GOOGLE'S BUSINESS MODEL

### 2.1 ADVERTISEMENTS ON GOOGLE

Google is mainly a search engine: it searches for websites on the Internet, so that users can find them without knowing their specific address. Functionally, Google works as an intermediary for websites: while it does not host them on its servers, it provides access to them. These main features make it not clear what role the PSI plays. We should thus present the *status quo* of the digital advertising business that Google dominated over the last decade. This includes how Google makes its money and how much revenue it creates. A core component of using Google is being exposed to ads, a lot of which are tailored to make them as interesting as possible to the user.<sup>7</sup> They seem to be a side occurrence of browsing and a slight annoyance. For Google, however, they are in fact its main source of revenue. Subsequently, the development and improvement of ads is in the center of its efforts. Algorithms can use behavioral targeting, the process of an ad finding its designated audience by examining the online behavior of users, e.g., their browsing history.<sup>8</sup> A very similar concept is personalization<sup>9</sup>: here, content gets tailored towards the behavior of the user on the website itself. It must be noted that there are different definitions and overlaps in the terminology.<sup>10</sup> To keep it simple, we will refer to all kinds of ads as «targeted» if they are enabled by artificial intelligence (AI) to appeal to a user. To shed some further light on the inner workings of Google's business, we will look at the different advertising services it provides.

The possibility to advertise with Google began with the service «Google AdWords» in 2000.<sup>11</sup> In 2018, the service was rebranded to «Google Ads», now using improved machine learning for ads, and was connected to the newly formed «Google Marketing Platform».<sup>12</sup> Here, interested parties can pay Google to put up their ads on Google's search results and websites. For this, Google usually charges in the pay-per-click format, meaning that only if a user clicks on the ad, the advertiser is billed.<sup>13</sup> To enable advertisers to work with targeted ads, Google Ads can be linked to Google Analytics, their tracking tool.<sup>14</sup> A similar tool is Universal Analytics: it does not pro-

---

<sup>7</sup> See CHRISTOPH B. GRABER, 'Legal Sociology', in MARC THOMMEN (ed.), *Introduction to Swiss Law*, 2<sup>nd</sup> ed., Zürich, 2022, at p. 106.

<sup>8</sup> See JIANQING CHEN/JAN STALLAERT, 'An Economic Analysis of Online Advertising Using Behavioral Targeting' (2010) *SSRN Journal*, at p. 2.

<sup>9</sup> The term is closely related and overlapping with «customization» and «preference matching».

<sup>10</sup> See KAR Y. TAM/SHUK Y. HO, 'Understanding the Impact of Web Personalization on User Information Processing and Decision Outcomes' (2006) *MIS Quarterly*, at p. 866; ALAN MONTGOMERY/MICHAEL D. SMITH, 'Prospects for Personalization on the Internet' (2008) *SSRN Journal*, at p. 131; with further references VILLE SALONEN/HEIKKI KARJALUOTO, 'Web personalization: The state of the art and future avenues for research and practice' (2016) *Telematics and Informatics*, at pp. 1089–1090.

<sup>11</sup> Google LLC., 'Google Launches Self-Service Advertising Program' (2000), available at <https://googlepress.blogspot.com/2000/10/google-launches-self-service.html>.

<sup>12</sup> Google LLC., 'Google AdWords is now Google Ads' (2018), available at <https://support.google.com/googleads/answer/9028765>.

<sup>13</sup> Google LLC., 'Set a budget that works for you', available at [https://ads.google.com/intl/en\\_us/home/pricing](https://ads.google.com/intl/en_us/home/pricing).

<sup>14</sup> Google LLC., 'Product Linking: Link a Google Analytics 4 property or Firebase project to Google Ads', available at <https://support.google.com/googleads/answer/6333536>.

vide tracking on one device but provides cross-device-tracking.<sup>15</sup> According to estimates, Google Ads is now used by around 90% of all websites displaying ads.<sup>16</sup> Created in 2003, Google Network and AdSense are expanding Google Ads to also reach the owners of specific websites for advertising purposes.<sup>17</sup> They show ads from the advertisers that already use Google Ads.<sup>18</sup> With this, they earn about two thirds of what the advertisers pay per click; Google takes the remaining third.<sup>19</sup>

To assess the resulting earnings, we consult Alphabet<sup>20</sup> Inc.'s Annual Report for the fiscal year of 2021. All in all, revenue generated by Google's ads makes up about 80% of Alphabet's income. Google Search (149 billion U.S. dollars), YouTube (29 billion) and Google Network (31 billion) generate about 209 billion.<sup>21</sup> The total revenue of Alphabet is about 257 billion dollars while the net profit is about 76 billion dollars.<sup>22</sup> To put this into perspective, we can equate revenue with GDP, as they both measure the total worth produced in the respective company or state. For 2022, this would put Alphabet at rank 50 out of 196 countries, sitting between Portugal and Finland.<sup>23</sup> Google Ads and AdSense generate vast amounts of money, making Google at the same time heavily dependent on efficient and far-reaching advertising.

## 2.2 USER TRACKING

### 2.2.1 Cookies and fingerprinting

Efficient and far-reaching advertising relies on AI technology to target users. But tech companies like Google need first to collect user data before processing it into a usable

<sup>15</sup> Google LLC., 'Comparing metrics: Google Analytics 4 vs Universal Analytics', available at <https://support.google.com/analytics/answer/11986666>.

<sup>16</sup> Web Technology Surveys, 'Usage Statistics and Market Share of Google Analytics for Websites, September 2022' (2022), available at <https://w3techs.com/technologies/details/ta-googleanalytics>; see European Publishers Council, 'Executive Summary Complaint of the European Publishers Council' (2022), p. 1–1, available at [https://www.epceurope.eu/\\_files/ugd/33c303\\_3f950f2c94e142dca89e579c03a93e55.pdf](https://www.epceurope.eu/_files/ugd/33c303_3f950f2c94e142dca89e579c03a93e55.pdf).

<sup>17</sup> Google LLC., 'Google Expands Advertising Monetization Program for Websites' (2003), available at <https://googlepress.blogspot.com/2003/06/google-expands-advertising-monetization.html>; Google LLC., 'Google Network', available at <https://support.google.com/google-ads/answer/1752334>.

<sup>18</sup> Google LLC., 'How AdSense works', available at <https://support.google.com/adsense/answer/6242051>.

<sup>19</sup> Google LLC., 'AdSense revenue share - Google AdSense Help', available at <https://support.google.com/adsense/answer/180195>.

<sup>20</sup> Alphabet is the parent company of Google and functions mainly as a holding company.

<sup>21</sup> Alphabet Inc., 'Annual Report for the fiscal year of 2021' (2022), p. 33, available at [https://abc.xyz/investor/static/pdf/20220202\\_alphabet\\_10K.pdf](https://abc.xyz/investor/static/pdf/20220202_alphabet_10K.pdf).

<sup>22</sup> *Ibid.*, p. 50.

<sup>23</sup> IMF, 'GDP, current prices', available at <https://www.imf.org/external/datamapper/NGDPD@WEO>.

tool for tracking.<sup>24</sup> At the moment, there are innumerable methods for tracking user activity.<sup>25</sup> We will focus on the two most common categories on the Internet.

Arguably, the best-known tool is the «cookie».<sup>26</sup> Functionally, cookies are small text files that contain information about the user.<sup>27</sup> This technology was invented originally to make online shopping easier as it created a memory of the user's browser for the website. With the information in the text files, the vendor could for instance remember what the user had in their shopping-cart, even if they left the website and came back later.<sup>28</sup> Nowadays, there are many different categories of cookies.<sup>29</sup> In accordance with the original intent for cookies, websites use the available information to enable the proper functioning of their interface. These «first-party» cookies are limited to the specific website that created them. For most purposes, session cookies are sufficient, meaning that they expire as soon as the user closes their browser. Then there are other, newer types of cookies: as the name suggests, «third-party» cookies are put on the user's browser by advertisers. These cookies track user activity and are thus persistent, meaning that they do not expire when the browser gets closed.<sup>30</sup> By putting cookies on different websites, they can create a profile of the user. A limitation was that advertisers originally could not read each other's cookies due to their unique domain properties. Cookie synchronization<sup>31</sup> circumvented this problem by not reading the cookies themselves but by synchronizing the user ID that was created by using them. This way, advertisers can buy each other's knowledge about users.<sup>32</sup> Another limitation was that the user could delete cookies from their browser. This problem was circumvented by «evercookies», or «supercookies». Their purpose is to create a backup of existing cookies and even search the user's browser for remnants

---

<sup>24</sup> See KARL-HEINZ LADEUR, 'Die Zukunft der Medienverfassung', in KARL-HEINZ LADEUR, et al. (eds), *Die Zukunft der Medienverfassung*, Tübingen, 2021, at pp. 50–51; this is notably a distinct strategy from traditional media; like newspapers: smart ads get created by data that was mostly collected by other sources and is in its nature a by-product. With further references JÜRGEN HABERMAS, 'Überlegungen und Hypothesen zu einem erneuten Strukturwandel der politischen Öffentlichkeit', in MARTIN SEELIGER/SEBASTIAN SEVIGNANI (eds), *Ein neuer Strukturwandel der Öffentlichkeit?*, Baden-Baden, 2021, pp. 470–500, at pp. 491–492.

<sup>25</sup> Google states that they use «various technologies to collect and store information, including cookies, pixel tags, local storage, such as browser web storage or application data caches, databases, and server logs». They «also allow specific partners to collect information from your browser or device for advertising and measurement purposes using their own cookies or similar technologies»: Google LLC., 'Google Privacy Policy' (2022), available at <https://policies.google.com/privacy>.

<sup>26</sup> Named by its inventor, Lou Montulli, after the already existing term «magic cookie», used by programmers to describe data that enables specific operations by the receiver: Lou Montulli, 'The reasoning behind Web Cookies' (2013), available at <https://montulli.blogspot.com/2013/05/the-reasoning-behind-web-cookies.html>.

<sup>27</sup> See CHEN/STALLAERT, 'An Economic Analysis of Online Advertising Using Behavioral Targeting', supra note 7, at p. 2; TOMASZ BUJLOW, et al., 'A Survey on Web Tracking: Mechanisms, Implications, and Defenses' (2017) *Proceedings of the IEEE*, at p. 1481.

<sup>28</sup> See The New York Times, 'Giving Web a Memory Cost Its Users Privacy' (2001); Montulli, 'The reasoning behind Web Cookies', supra note 25.

<sup>29</sup> See RICHIE KOCH, 'Cookies, the GDPR, and the ePrivacy Directive', available at <https://gdpr.eu/cookies>.

<sup>30</sup> GEORG MERZDOVNIK, et al., 'Block Me If You Can: A Large-Scale Study of Tracker-Blocking Tools' (2017) *Proceedings of the IEEE*, at p. 2.

<sup>31</sup> Google's name for it is cookie «matching».

<sup>32</sup> GUNES ACAR, et al., 'The Web Never Forgets: Persistent Tracking Mechanisms in the Wild' (2014) *Association for Computing Machinery*, at p. 676.

of deleted cookies to restore them.<sup>33</sup> They can be traded cross-browser and can identify the user even on a new, previously unused, browser.<sup>34</sup>

With much of the public's attention focused on cookies, the practice of fingerprinting provides a viable alternative for tracking.<sup>35</sup> There are two main kinds, the first of which is «canvas fingerprinting»: the rendering of written text online is marginally different from browser to browser and hardware to hardware. This means that with suitable software, data about the user like the monitor, phone, keyboard settings, or even the used CPU can be observed and used for profiling.<sup>36</sup> A second method is «browser fingerprinting». By collecting information about the user's settings, it can identify the browser in use and track it over long periods of time.<sup>37</sup> Fingerprinting is functionally similar to cookies insofar as it can be used to create a digital profile of the user. But while cookies are stored on the user's browser, fingerprinting happens remotely.<sup>38</sup> The remote storage has the effect that the user cannot manually get rid of fingerprinting by clearing their cache and that its existence is nearly impossible to detect.<sup>39</sup> In one of the first landmark studies conducted in 2010, PETER ECKERSLEY found that over 80% of browsers had a trackable uniqueness to them, making them a target for fingerprinting. Although the fingerprinted browsers changed rapidly with user activity, even simple algorithms could easily link the newer back to the older versions.<sup>40</sup>

## 2.2.2 The privacy-debate

Since its implementation, tracking technology has become a central point of the ongoing debate over user privacy<sup>41</sup> on the Internet.<sup>42</sup> In this paper, our focus will be

<sup>33</sup> With further references *ibid.*; BUJLOW, et al., 'A Survey on Web Tracking: Mechanisms, Implications, and Defenses', *supra* note 26, at pp. 1491–1492.

<sup>34</sup> *Ibid.*, at p. 1492.

<sup>35</sup> NICK NIKIFORAKIS, et al., 'PriVaricator' (2015) *International World Wide Web Conferences Steering Committee*, at p. 821.

<sup>36</sup> ACAR, et al., 'The Web Never Forgets: Persistent Tracking Mechanisms in the Wild', *supra* note 31, at p. 675; MERZDOVNIK, et al., 'Block Me If You Can: A Large-Scale Study of Tracker-Blocking Tools', *supra* note 29, at p. 2.

<sup>37</sup> With further references ALEJANDRO GÓMEZ-BOIX, et al., 'Hiding in the Crowd: an Analysis of the Effectiveness of Browser Fingerprinting at Large Scale' (2018) *International World Wide Web Conferences Steering Committee*, at p. 307.

<sup>38</sup> See MERZDOVNIK, et al., 'Block Me If You Can: A Large-Scale Study of Tracker-Blocking Tools', *supra* note 29, at p. 2; see NAVPREET KAUR, et al., 'Browser Fingerprinting as User Tracking Technology' (2017) *2017 11th International Conference on Intelligent Systems and Control (ISCO)*, at p. 109; see ANTOINE VASTEL, et al., 'FP-STALKER: Tracking Browser Fingerprint Evolutions' (2018) *2018 IEEE Symposium on Security and Privacy (SP)*, at p. 2.

<sup>39</sup> NIKIFORAKIS, et al., 'PriVaricator', *supra* note 34, at pp. 821–822; KAUR, et al., 'Browser Fingerprinting as User Tracking Technology', *supra* note 37, at p. 109; ANNA KOBUSIŃSKA, et al., 'Big Data fingerprinting information analytics for sustainability' (2018) *Future Generation Computer Systems*, at p. 1323; VASTEL, et al., 'FP-STALKER: Tracking Browser Fingerprint Evolutions', *supra* note 37, at p. 2.

<sup>40</sup> PETER ECKERSLEY, 'How Unique Is Your Web Browser?' (2010) *Electronic Frontier Foundation*, at pp. 8–13; one for many: GÓMEZ-BOIX, et al., 'Hiding in the Crowd: an Analysis of the Effectiveness of Browser Fingerprinting at Large Scale', *supra* note 36, at p. 309.

<sup>41</sup> For this discussion, privacy means the control over what personal data a user wants to share with the Internet, making lasting anonymity a possible choice.



mostly on the impact of such technology on democratic structures via targeted ads. The following section is thus not going into detail on the progression of the privacy debate but should showcase its significance when discussing regulations. In the early days of the Internet, the general consensus was that users were anonymous.<sup>43</sup> This was a natural assumption, as until the middle of the 2000s, there was far fewer personal data on the Internet that could be measured.<sup>44</sup> Also, computing power was far lower, not allowing for complicated algorithms to work with user data.<sup>45</sup> Although there was some earlier coverage of cookie-related issues, DANIEL HOWE/HELEN NISSENBAUM trace the beginning of the online privacy debate back to 2005.<sup>46</sup> Around this time, the U.S. Department of Justice requested Google's records of search queries. Google denied the request arguing that it would undermine its user's trust in the company. A year later, researchers found out that the identity of individuals could be retraced with just the information that Google had about user's search queries.<sup>47</sup> In 2010, newspapers and subsequently the Federal Trade Commission (FTC) started covering tracking activity based on cookies much more intently.<sup>48</sup> The FTC saw heightened concern for privacy especially with large Internet platforms and urged for self-regulation as well as the enforcement of existing laws.<sup>49</sup>

The debate over the impact of tracking on user privacy is now well over a decade old. It showcases an obvious downside of the usage of tracking technology and remains an important issue today. As such, it acts as one of the main driving forces for regulation.

### 3 THE «PRIVACY SANDBOX INITIATIVE»

#### 3.1 CONCEPT AND PROGRESS

For a long time, the controversies surrounding the invasive nature of cookies and fingerprinting have been a thorn in Google's side.<sup>50</sup> Google's stated goal for the PSI is

<sup>42</sup> ECKERSLEY, 'How Unique Is Your Web Browser?', supra note 39, at pp. 3–4; NICK NIKIFORAKIS, et al., 'Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting' (2013) *2013 IEEE Symposium on Security and Privacy (SP)*, at p. 541.

<sup>43</sup> See CHRISTOPH B. GRABER, 'Personalisierung im Internet, Autonomie der Politik und Service public' (2017) *sic!*, at p. 257.

<sup>44</sup> Looking at intermediaries, Facebook started its operations in 2004, YouTube and Reddit in 2005, and finally Twitter in 2006. Instagram, Snapchat and TikTok all started later, in the 2010s.

<sup>45</sup> See the mostly confirmed "Moore's law" which states the trend that computing speed doubles every two years: GORDON E. MOORE, 'Cramming more components onto integrated circuits' (1965) *Electronics*, at pp. 2–3.

<sup>46</sup> The New York Times, 'Fresh From Your Browser's Oven' (1999).

<sup>47</sup> DANIEL C. HOWE/HELEN NISSENBAUM, 'Trackmenot: Resisting Surveillance in Web Search', in IAN KERR, et al. (eds), *Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society*, Oxford, 2009, at p. 2.

<sup>48</sup> With further references HELEN NISSENBAUM, 'A Contextual Approach to Privacy Online' (2011) *Dædalus*, at p. 32.

<sup>49</sup> See Federal Trade Commission, 'Protecting consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers' (2012), at pp. 56 and 73, available at <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

<sup>50</sup> See, e.g., its latest settlement in this regard: The New York Times, 'Google Agrees to \$392 Million Privacy Settlement With 40 States' (2022).

thus to help user privacy and simultaneously to allow for content to remain free on the internet.<sup>51</sup> To achieve this, it wants to abandon third-party cookies and fingerprinting altogether. However, Google does not want to eliminate tracking of the user itself, a practice that we showed to be highly profitable. Rather, it wants to replace the existing technologies with others that should arguably be less invasive into user privacy.<sup>52</sup> Google distinguishes between different parts it wants to change, notably how to «show relevant content and ads» and to «strengthen cross-site privacy boundaries».<sup>53</sup> As we are mostly concerned with how the ads are produced, we will focus on the technologies that relate to the former statement.

Google's PSI originally wanted to establish a new kind of web-tracking-system called «FLoC», which was abandoned in the early months of 2022 due to negative feedback from users.<sup>54</sup> The successive proposal is the «Topics API».<sup>55</sup> The goal is still to learn about user interests out of their Internet activity. Up to 350 of those interests, or «topics», are stored locally on the user's browser. When clicking on a website, it then directly requests the topics, and not information about the user's browsing history. The proposed benefit of this method is that fingerprinting is made more difficult, and advertisers do not know which specific websites are visited by the user. Furthermore, Google promises an opt-out method for the «Topics API», which is not much different than their current cookie policy.<sup>56</sup> Google also develops the «FLEDGE API», which aims to remodel remarketing on websites. This means that after visiting a website of an advertiser, the website can ask the browser of the user to be added to an «interest group», basically marking it for further use. When the user visits a different website that provides ad space, an ad auction is run on the browser to determine which ad is to be displayed. The seller, mostly meaning the website displaying ads, provides the relevant criteria for each individual auction. The buyers, meaning different advertisers who have the browser in their «interest group», compete for their ad to be shown. Finally, the most desirable ad based on the relevant criteria gets displayed. Similar to the «Topics API», the focus shifts to the user's browser, as ad auctioning is now taking place there. This enables ad personalization without cross-site tracking of the user. Google wants to provide an opt-out model for this API as well.<sup>57</sup> «Topics API» and «FLEDGE API» started their respective original trials in early 2022. Google aims for the general availability of the PSI in the second half of 2023.<sup>58</sup>

---

<sup>51</sup> Google LLC., 'The Privacy Sandbox: Protecting your privacy online', available at <https://privacysandbox.com>.

<sup>52</sup> Google LLC., 'Building a more private web' (2019), available at <https://www.blog.google/products/chrome/building-a-more-private-web>.

<sup>53</sup> Google LLC., 'The Privacy Sandbox Timeline for the Web' (2022), available at [https://privacysandbox.com/intl/en\\_us/open-web/#the-privacy-sandbox-timeline](https://privacysandbox.com/intl/en_us/open-web/#the-privacy-sandbox-timeline).

<sup>54</sup> The Verge, 'Nobody is flying to join Google's FLoC: Brave, Vivaldi, Edge, and Mozilla are all out' (2021), available at <https://www.theverge.com/2021/4/16/22387492>; Electronic Frontier Foundation, 'Google's FloC Is a Terrible Idea' (2021), available at <https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea>.

<sup>55</sup> Google LLC., 'Topics', available at [https://privacysandbox.com/intl/en\\_us/proposals/topics](https://privacysandbox.com/intl/en_us/proposals/topics). API stands for «Application Program Interface».

<sup>56</sup> Google LLC., 'The Topics API' (2022), available at <https://developer.chrome.com/docs/privacy-sandbox/topics>; we will show the opt-out method for cookies to be insufficient under EU standards.

<sup>57</sup> Google LLC., 'FLEDGE API' (2022), available at <https://developer.chrome.com/docs/privacy-sandbox/fledge>.

<sup>58</sup> Google LLC., 'The Privacy Sandbox Timeline for the Web', supra note 52.

It must be noted that Google's way of presenting its project does not on all points overlap with the public's opinion: The PSI has been criticized by experts and the online community at large for a multitude of reasons. The most important is that privacy is not actually being improved significantly if one is to look at the technical details.<sup>59</sup> There have also been serious concerns from an anti-trust perspective, as the new technologies make ad-buyers even more reliant on the already dominant Google Ads.<sup>60</sup> The development of the PSI is thus surrounded by controversy: in the best-case scenario, it improves user privacy and in the worst case, it does not and it further consolidates Google's market position. In any case, it does not jeopardize Google's business model.

## 3.2 RECENT DEVELOPMENTS AROUND TRACKING TECHNOLOGY

### 3.2.1 Tearing down «cookie-walls»

The PSI is not being developed in a vacuum. Outside forces impeding cookie technology should be considered in the context of its emergence. Since the implementation of the EU's ePrivacy Directive in 2002, «well-informed consent» was required for the use of cookies, meaning that before using them, the website needed to inform users of the practice. Subsequently, websites could and did make their services dependent on accepting cookies. The problem of this «cookie-wall» became quickly apparent, prompting a regulatory response in the EU.<sup>61</sup> According to Article 6(1) (a) in conjunction with Article 7(4) of the General Data Protection Regulation (GDPR), «valid» consent is now required, meaning that users can decline cookies and still access the website. A pre-selected form allowing cookies has been deemed not sufficient by the European Court of Justice, meaning that an opt-in process is now mandatory for the EU.<sup>62</sup> Additionally, according to Article 21(2) of the GDPR, if user data is used for direct marketing, the user can opt-out of this practice at any time. The Digital Services Act (DSA) further improves on this. Article 25(1) bans confusing designs when showing a cookie banner.<sup>63</sup> All in all, reliance on cookies for tracking gets more unreliable for advertising purposes as time goes on. A specific example for

---

<sup>59</sup> Electronic Frontier Foundation, 'Don't Play in Google's Privacy Sandbox' (2019), available at <https://www EFF.org/deeplinks/2019/08/dont-play-googles-privacy-sandbox-1>.

<sup>60</sup> See The Verge, 'Google antitrust suit takes aim at Chrome's Privacy Sandbox' (2021), available at <https://www.theverge.com/2021/3/16/22333848/google-antitrust-lawsuit-texas-complaint-chrome-privacy>; see TechCrunch, 'Google's Privacy Sandbox targeted by fresh EU anti-trust complaint' (2022), available at <https://techcrunch.com/2022/01/24/germany-publishers-privacy-sandbox-complaint>.

<sup>61</sup> Data Protection Working Party, 'Working Document 02/2013 providing guidance on obtaining consent for cookies' (2013), p. 5, available at [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf).

<sup>62</sup> See ECJ, Judgment of 1 October 2019, Planet49, C-673/17, EU:C:2019:801, paragraph 65; see BGH, Judgment I ZR 7/16 of the 28<sup>th</sup> of May 2020.

<sup>63</sup> This method is also called creating «Dark Patterns».

Google is its service Google Analytics, which violates the GDPR, getting it restricted or banned in several EU states.<sup>64</sup>

### 3.2.2 Pressure from non-state actors

Google and its browser Chrome are under increased pressure from legislation in the EU, but they also increasingly compete with other private actors as well. As the usage of cookies has changed from its original intent towards marketing, the public's perception has shifted with it. An example of comparatively early and successful anti-tracking software is TrackMeNot.<sup>65</sup> It was developed to circumvent tracking by giving out random data that obfuscated the real user activity.<sup>66</sup> Furthermore, browsers like Firefox and Safari have been limiting the use of cookies and fingerprinting for several years.<sup>67</sup> Apart from these better known brands, there are also browsers and search engines like Opera, DuckDuckGo and Brave that do not track user activity at all.<sup>68</sup> Finally, even if Chrome is used, VPN-software<sup>69</sup> and Ad Blockers are increasingly wide-spread.<sup>70</sup> VPNs obscure the IP address and browsing behavior of a user by sending Internet traffic through a (usually encrypted) tunnel to their own servers before it reaches the user or the website.<sup>71</sup> Ad Blockers are a simple way to not being exposed to ads on the Internet. While they are largely effective, they are not inherently stopping tracking and compete in a constant arms race with tech-companies to update and improve their services.<sup>72</sup> All in all, however, users remain relatively complacent in their strive for less tracking on the Internet. Across several studied countries for instance, users value their personal data quite low: browser activity for instance is valued at around 4 dollars per month, and even less in the younger demographic.<sup>73</sup> Subsequently, the available options for protecting user data currently

<sup>64</sup> To varying degrees e.g. in Italy, France and Austria: Italian Supervisory Authority, 'Italian SA bans use of Google Analytics: No adequate safeguards for data transfers to the USA' (2022), available at <https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9782874#english>; Commission Nationale de l'Informatique et des Libertés, 'Use of Google Analytics and data transfers to the United States: The CNIL orders a website manager/operator to comply' (2022), available at <https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply>; see the decision of the Austrian Data Protection Office: dsb D155.027, 2021-0.586.257.

<sup>65</sup> Released in 2006, it came shortly after the public became aware of privacy risks posed by tracking.

<sup>66</sup> See HOWE/NISSENBAUM, 'Trackmenot: Resisting Surveillance in Web Search', supra note 46, at pp. 1–2.

<sup>67</sup> Mozilla Security Blog, 'Firefox 72 blocks third-party fingerprinting resources' (2020), available at <https://blog.mozilla.org/security/2020/01/07/firefox-72-fingerprinting>; Apple Support, 'Prevent cross-site tracking in Safari on Mac', available at <https://support.apple.com/guide/safari/sfri40732>.

<sup>68</sup> MICHAEL MUNCHMORE, 'Stop Trackers Dead: The Best Private Browsers for 2022' (2022), available at <https://uk.pcmag.com/browsers/134703>.

<sup>69</sup> VPN stands for «Virtual Private Network».

<sup>70</sup> KAUR, et al., 'Browser Fingerprinting as User Tracking Technology', supra note 37, at p. 103; MERZDOVNIK, et al., 'Block Me If You Can: A Large-Scale Study of Tracker-Blocking Tools', supra note 29, at pp. 3–4; IVANA VOJINOVIC, 'VPN Statistics for 2022 - Keeping Your Browsing Habits Private' (2022), available at <https://dataprot.net/statistics/vpn-statistics>.

<sup>71</sup> See ABDULLAH ALSHALAN, et al., 'A Survey of Mobile VPN Technologies' (2016) *IEEE Commun. Surv. Tutorials*, at pp. 1177–1178.

<sup>72</sup> See MERZDOVNIK, et al., 'Block Me If You Can: A Large-Scale Study of Tracker-Blocking Tools', supra note 29, at pp. 11–12.

<sup>73</sup> JEFFREY PRINCE/SCOTT WALLSTEN, 'How Much is Privacy Worth Around the World and Across Platforms?' (2022) *SSRN Journal*, at pp. 842–845.

don't put a large dent in the dominant market position of Chrome.<sup>74</sup> Still, they pose viable alternatives should users decide to change providers due to concerns for their privacy.

A multitude of steps have been taken by regulators, users, and competitors to limit Google's invasions of privacy. This has put considerable pressure on Google to change away from established tracking technology. It has thus reacted by introducing the PSI, which is self-regulatory in nature. With this action, Google hopes to appease its customers and political forces pushing for more regulations. However, this is only one side of the equation. Even after the implementation of the PSI, Google's business model will still work largely in the same way, even if privacy protection gets improved. The second part of this paper will address specific problems that arise in the context of targeted ads.

## 4 THE EFFECTS OF TARGETED ADS ON DEMOCRACY

### 4.1 MEASURING THE IMPACT OF POLITICAL ADVERTISING

To measure the effectiveness of targeted ads, we must first choose a suitable kind to examine, as most content is permissible for ads on Google, with only a few exceptions.<sup>75</sup> For the purposes of this paper, we will only examine one specific kind of targeted ad, namely the political ad. The choice falls on this kind of ad because it relates directly to the functioning of democracies, as intermediaries like Google have a strong and now prolonged standing as information sources for voters.<sup>76</sup> After showing the effect of political ads, we will take into consideration specific (self-)regulations in this field. It must be noted that we focus on third-party automated ads and not user generated content favoring a political opinion. This leaves out an important factor that shapes public discourse, as it has been shown that AI-driven filtering technologies are demonstrated to prefer some political views and creators over others.<sup>77</sup>

The effectiveness of digital political ads is subject to debate, with some research suggesting its limitations.<sup>78</sup> Limitations can come from a multitude of sources: the messaging, the candidates, votes, but also timing and demographics. There, the benefit of targeted ads becomes apparent, as a targeted ad caters more to their interest. Measuring the impact of digital political ads is difficult, but we can look at the example of the 2016 U.S.-presidential election. This well-known case provides sufficient discussion and media coverage to give us a relatively reliable picture.<sup>79</sup> While in 2016, the advertising campaign has been mostly conducted on Facebook, and not on

---

<sup>74</sup> Statcounter, 'Browser Market Share Worldwide', available at <https://gs.statcounter.com>.

<sup>75</sup> See Google LLC., 'Google Ads policies', available at <https://support.google.com/adspolicy/answer/6008942>.

<sup>76</sup> See NIC NEWMAN, et al., 'Reuters Institute: Digital News Report 2022' (2022), at p. 12.

<sup>77</sup> MEGAN BROWN, et al., 'Echo Chambers, Rabbit Holes, and Algorithmic Bias: How YouTube Recommends Content to Real Users' (2022) *SSRN Journal*, at p. 26.

<sup>78</sup> See ALEXANDER COPPOCK, et al., 'Does digital advertising affect vote choice? Evidence from a randomized field experiment' (2022) *Research & Politics*, at p. 6.

<sup>79</sup> See the assessment of the Berkman Klein Center: ROBERT FARIS, et al., 'Partisanship, Propaganda, and Disinformation: Online Media and the 2016 U.S. Presidential Election' (2017) *Berkman Klein Center for Internet & Society at Harvard University*, at p. 42.

Google, this comparison is nevertheless suitable as the intent is primarily to measure the effect of targeted ads and not their origin.

## 4.2 CASE STUDY: THE 2016 U.S.-PRESIDENTIAL ELECTION

### 4.2.1 Timeline and Outcome

Because of platforming and enabling targeted political ads, intermediaries like Google, Twitter, and Facebook played a pivotal role in the last two U.S.-presidential elections.<sup>80</sup> Especially Facebook's role has not gone unnoticed: since it broke out in March 2018, the «Cambridge Analytica» scandal has been a symbol for the vast extent of tracking used to create targeted political ads. In short, the subsidiary of the SCL Group<sup>81</sup>, Cambridge Analytica, conducted a large-scale data collection on Facebook that was barely legal at best.<sup>82</sup> It was then used by Donald Trump's presidential campaign to create targeted political ads out of these user profiles.<sup>83</sup> A large portion of the public and academic discussion ever since has been aimed at the blatant disregard for personal information like age, sex, personal messages, likes and posts.<sup>84</sup> For our purposes, the most important takeaway is not the data collection by which the results of the 2016 election were influenced, but the election itself. While Cambridge Analytica collected huge amounts of personal data it did not directly produce and distribute political ads.<sup>85</sup> For this, the Trump-campaign used the database of «Project Alamo» in their own campaign. It worked closely with Facebook, Twitter, and Google to gain as much insight into targeting strategies as possible. They used Cambridge Analytica's vast datasets among others to create ads for social media platforms.<sup>86</sup>

The aim for the 2016 election was to improve turnout for Trump in swing states and at the same time to dissuade African Americans, young women, and idealistic white liberals, the key voter demographics of Hillary Clinton, from voting for her.<sup>87</sup> To achieve its goals, «Project Alamo» combined targeting from user data with automated personalization technologies.<sup>88</sup> Nationally, African American turnout was at a

<sup>80</sup> Twitter was not involved in advertising but was of considerable strategic importance for the Trump Campaign: *ibid.*, at p. 32.

<sup>81</sup> SCL stands for «Strategic Communication Laboratories».

<sup>82</sup> Just recently, Meta (formerly Facebook) had to settle a complaint concerning the affected U.S. population: BBC News, 'Meta settles Cambridge Analytica scandal case for \$725m' (2022), available at <https://www.bbc.com/news/technology-64075067>.

<sup>83</sup> The New York Times, 'How Trump Consultants Exploited the Facebook Data of Millions' (2018); Neue Zürcher Zeitung, 'Die smarten Datendiebe' (2018); The Guardian, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach' (2018).

<sup>84</sup> Wired, 'How to check whether Facebook shared your data with Cambridge Analytica' (2018).

<sup>85</sup> It was paid about 6 million dollars for conducting the collection of the data: Federal Election Commission, 'Disbursements: Trump Campaign to Cambridge Analytica', available at [https://www.fec.gov/data/disbursements/?data\\_type=processed&committee\\_id=C00580100&recipient\\_name=cambridge+analytica](https://www.fec.gov/data/disbursements/?data_type=processed&committee_id=C00580100&recipient_name=cambridge+analytica).

<sup>86</sup> Brat Parscale, the digital ad executive of Trump's campaign, said that they did not use the additional psychographics constructed by Cambridge Analytica because he did not believe that they worked: 60 Minutes Politics, 'Facebook "embeds," Russia and the Trump campaign's secret weapon' (2017).

<sup>87</sup> Bloomberg, 'Inside the Trump Bunker, With 12 Days to Go' (2016).

<sup>88</sup> Project Alamo used between 40'000 - 175'000 different variants of its ads every day and evaluated their effectively: Wired, 'Here's How Facebook Actually Won Trump the Presidency' (2016).

20-year low.<sup>89</sup> While the turnout from young white men was significantly up, young white women stayed about the same from 2012.<sup>90</sup> About 12% of voters for Bernie Sanders in the primary voted for Trump in the general election and another 12% voted third-party or did not vote.<sup>91</sup> On the other hand, votes for Trump came in large part from white non-college graduates.<sup>92</sup> In swing states, their turnout was up, or at least less down than the other demographics.<sup>93</sup> Looking at this data, it's apparent that the goals put forward by «Project Alamo» were met, if not surpassed.<sup>94</sup> This proved to be of significant value due to the closeness of the election. In multiple swing states won by Trump, the difference between candidates was very close, sometimes less than 1%.<sup>95</sup>

Looking at expenses, in 2016, the Trump campaign spent about 87 million dollars on digital ads or about 25% of its whole campaign budget. In contrast, the Clinton-campaign only spent about 32 million dollars or 5% of its whole budget for the same purpose.<sup>96</sup> Including outside spending, the Republicans spent about 153 million dollars for Trump on digital ads, while the Democrats only put forth 10 million for Clinton.<sup>97</sup> The effectiveness of digital advertising was capitalized on in the next presidential election: the total sum spent by all 2020 presidential candidates on digital ads easily passed the one-billion-mark.<sup>98</sup> Looking at the two main candidates in the 2020 general election, Trump and supporters spent about 160 million on Facebook and 140 million on Google Ads while Joe Biden and supporters spent about 150 million and 100 million respectively.<sup>99</sup> The total digital ad spending – including outside spending – thus amounted to around 550 million for the top two candidates. The difference in money spent on digital ads between the 2016 and 2020 cycles makes it very likely, that in 2024, the U.S. presidential election campaigns will again invest substantially in digital ads on intermediaries.

<sup>89</sup> Pew Research Center, 'Black voter turnout fell in 2016 US election' (2017), available at <https://www.pewresearch.org/fact-tank/2017/05/12/black-voter-turnout-fell-in-2016-even-as-a-record-number-of-americans-cast-ballots>.

<sup>90</sup> Circle, 'Election Night 2016: 24 Million Youth Voted, Most Rejected Trump' (2016), available at <https://circle.tufts.edu/latest-research/election-night-2016-24-million-youth-voted-most-rejected-trump>.

<sup>91</sup> BRIAN SCHAFFNER, 'How Sanders supporters behaved in the 2016 general election', available at <https://sites.google.com/view/brianschaffner/public-outreach-analyses/how-sanders-supporters-behaved-in-the-2016-general-election>.

<sup>92</sup> Pew Research Center, 'An examination of the 2016 electorate, based on validated voters', available at <https://www.pewresearch.org/politics/2018/08/09/an-examination-of-the-2016-electorate-based-on-validated-voters>.

<sup>93</sup> Center for American Progress, 'Voter Trends in 2016' (2017).

<sup>94</sup> Brat Parscale expressed satisfaction over their results: *Huston Chronicle*, 'Trump's digital ad exec based in San Antonio' (2016).

<sup>95</sup> The closest states being Michigan + 0.23%; Pennsylvania + 0.72%; Wisconsin, + 0.77%; notably also Florida, + 1.20%: *The New York Times*, '2016 Presidential Election Results' (2017).

<sup>96</sup> Digital ad spending was up almost 800% from 2012: CHRISTINE B. WILLIAMS/GIRISH J. GULATI, 'Digital Advertising Expenditures in the 2016 Presidential Election' (2018) *Social Science Computer Review*, at p. 409.

<sup>97</sup> *Ibid.*, at p. 414.

<sup>98</sup> E.g., the Democratic primary candidate Michael Bloomberg spent about 280 million on digital ads alone: Open Secrets, 'Michael Bloomberg (D): 2020 Presidential Candidacy', available at <https://www.opensecrets.org/2020-presidential-race/michael-bloomberg/online-ad-spending?id=N00029349>.

<sup>99</sup> Open Secrets, 'Donald Trump (R): 2020 Presidential Candidacy', available at <https://www.opensecrets.org/2020-presidential-race/donald-trump/online-ad-spending?id=N00023864>; Open Secrets, 'Joe Biden (D): 2020 Presidential Candidacy', available at <https://www.opensecrets.org/2020-presidential-race/joe-biden/online-ad-spending?id=N00001669>.

In conclusion, we can observe that targeted political ads were used for voter persuasion and the tactical goals of the Trump campaign were met. Furthermore, the large sums of money spent by the presidential campaigns in both elections point to the huge effectiveness of targeted political ads. It's very likely that Trump was helped considerably by targeted ads provided by «Project Alamo», quite possibly even securing his presidency.

#### 4.2.2 Political advertising and democracy

Party affiliations of the winning candidate should not be the foundation for an argument against intelligent advertising strategies and the heavy use of social media for voter persuasion. There needs to be specific harm demonstrated. As the use of targeted political ads is obviously not limited to U.S. presidential elections and continues to this date, we must further examine the effects linked to targeted political ads.<sup>100</sup>

With the advent of new technologies like the radio, television and finally the Internet, there came more efficient means of reaching voters. But do targeted ads still improve efficiency fundamentally in the same way? To answer this question, we need to consider what distinguishes them from other ads. With what might be called «generalized» ads, like those on TV or radio, there are a broad range of potential voters that see them and react by discussing them with friends and family before voting. In other words, it stands to reason that they serve as a tool for communication between political interests and *all* voters.<sup>101</sup> However, if the ads reach only specific voters and cater to their specific interests, there is far less discussion as no one has the same understanding of the political situation. This is of little concern for the political parties involved as they are primarily interested in winning the election or vote at hand. For them, personalized ads provide a tool of almost surgical precision for convincing voters for their cause.

Voters on the other hand run the risk of losing political advertising as a reliable source for gathering politically relevant information.<sup>102</sup> Election ads are not only targeted but can also be loaded with conspiracy theories, fake news, and hate speech.<sup>103</sup> If ads are used as a precise instrument for influencing specific important voters, their basis of information starts to differ significantly from their constituency. Personalization technologies like targeted political ads or filtering technologies can add to the formation of so-called echo chambers, filter-bubbles, and contribute to radicaliza-

---

<sup>100</sup> The executive of Cambridge Analytica claimed that it has been active in more than a hundred elections: BBC News, 'Cambridge Analytica: the data firm's global influence' (2018); see The New York Times, 'This Ad's for You (Not Your Neighbor)' (2022).

<sup>101</sup> Ads on TV can be in some ways personalized as well: the region and the channel can be influenced. However, this kind of personalization is very much limited in its effectivity.

<sup>102</sup> See also the proposition that suggests denying fake news sites access to advertising improves democratic discourse: FARIS, et al., 'Partisanship, Propaganda, and Disinformation: Online Media and the 2016 U.S. Presidential Election', supra note 80, at p. 21.

<sup>103</sup> Global Witness, 'TikTok and Facebook fail to detect election disinformation in the US, while YouTube succeeds' (2022), available at <https://www.globalwitness.org/en/campaigns/digital-threats/tiktok-and-facebook-fail-detect-election-disinformation-us-while-youtube-succeeds>; see Sum of Us, 'Stop the Steal Part 2: How YouTube and Meta are dismantling Brazilian Democracy' (2022), available at [https://s3.amazonaws.com/s3.sumofus.org/pdf/Stop\\_The\\_Steal\\_2.0\\_Part\\_2.pdf](https://s3.amazonaws.com/s3.sumofus.org/pdf/Stop_The_Steal_2.0_Part_2.pdf); see The New York Times, 'With Ads, Imagery and Words, Republicans Inject Race Into Campaigns' (2022).



tion.<sup>104</sup> Echo chambers are communications between users that build on confirmation bias.<sup>105</sup> Similar phenomena are filter bubbles: ELI PARISER describes them as a state of isolation that gets created through an algorithm selectively guessing the interests of a user, leaving out other information.<sup>106</sup> Through this, the user does not see content that differs from their interests and only consolidates their own perceptions.<sup>107</sup> This bubble is isolating, invisible and almost unavoidable, making it highly problematic.<sup>108</sup> Consequently, society gets fragmented, and the public sphere provided by the Internet gets eroded.<sup>109</sup>

Western democracies have a strong deliberative element to them, as collective and rational discussions are cornerstones of political discourse.<sup>110</sup> They rely on a well-educated and informed citizen who first discusses political issues and then goes to vote on them.<sup>111</sup> Especially important is witnessing competing viewpoints that allow voters to make informed decisions.<sup>112</sup> As such, the access to information, especially in the form of media, is critical to the proper functioning of a democracy.<sup>113</sup> This is backed by multiple studies showing a clear connection between the quality of media and the health of democracies.<sup>114</sup>

Political ads are not only important for the contents of an election or vote but also for the process around it. Having established that targeted ads can contribute to negative effects in democracies, we can again refer to the U.S. for a specific example.

<sup>104</sup> See CASS R. SUNSTEIN, *#Republic: Divided Democracy in the Age of Social Media*, Princeton and Oxford, 2017, at pp. 15–16; see GRABER, ‘Personalisierung im Internet, Autonomie der Politik und Service public’, supra note 42, at pp. 260–261; see GRABER, ‘Legal Sociology’, supra note 7, at pp. 103–104.

<sup>105</sup> See CASS R. SUNSTEIN, *Republic.com 2.0*, Princeton, 2009, at p. 116; see MICHELA DEL VICARIO, et al., ‘The spreading of misinformation online’ (2016) *PNAS*, at p. 558; see HABERMAS, ‘Überlegungen und Hypothesen zu einem erneuten Strukturwandel der politischen Öffentlichkeit’, supra note 23, at p. 488.

<sup>106</sup> See ELI PARISER, ‘Beware online “filter bubbles”’ (2011), available at [https://www.ted.com/talks/eli\\_pariser\\_beware\\_online\\_filter\\_bubbles/transcript](https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles/transcript).

<sup>107</sup> Research suggests that content gets mostly distributed around already established social connections, i.e., echo-chambers: DEL VICARIO, et al., ‘The spreading of misinformation online’, supra note 106, at p. 558.

<sup>108</sup> ELI PARISER, *The Filter Bubble: What the Internet is hiding from you*, New York, 2011, at pp. 9–10.

<sup>109</sup> See HABERMAS, ‘Überlegungen und Hypothesen zu einem erneuten Strukturwandel der politischen Öffentlichkeit’, supra note 23, at p. 489.

<sup>110</sup> *Ibid.*, at p. 475.

<sup>111</sup> See JOHANNES REICH, ‘“Homeschooling” zwischen elterlichem Erziehungsrecht, staatlicher Schulpflicht und Kindeswohl’ (2012) *Zentralblatt* (113), pp. 576–609, at pp. 576–609; GRABER, ‘Personalisierung im Internet, Autonomie der Politik und Service public’, supra note 42, at pp. 263–266; see MATTHIAS MAHLMANN, *Konkrete Gerechtigkeit: Eine Einführung in Recht und Rechtswissenschaft der Gegenwart*, 3<sup>rd</sup> ed., Baden-Baden, 2017, at p. 114; the underlying reasoning is that being eligible to vote is the norm and not being is the exception; see BGE 146 I 20 d. 5.2.2.

<sup>112</sup> See GRABER, ‘Legal Sociology’, supra note 7, at pp. 100–101; see also HABERMAS, ‘Überlegungen und Hypothesen zu einem erneuten Strukturwandel der politischen Öffentlichkeit’, supra note 23, at pp. 476–478; see OTFRIED JARREN/RENATE FISCHER, ‘Demokratische Öffentlichkeit: Eine medienpolitische Gestaltungsaufgabe’, in Otto Brenner Stiftung (ed.), *Welche Öffentlichkeit brauchen wir?: Die Zukunft des Journalismus und demokratischer Medien*, Frankfurt am Main, 2022, at pp. 26–27.

<sup>113</sup> HABERMAS, ‘Überlegungen und Hypothesen zu einem erneuten Strukturwandel der politischen Öffentlichkeit’, supra note 23, at p. 485.

<sup>114</sup> See the discussion in PETER HETTICH/MARK SCHELKER, *Medien im digitalen Zeitalter: Neugestaltung des Programmauftrags aus ökonomischer und rechtlicher Sicht*, Zürich/St. Gallen, 2016, at pp. 69–76.

### 4.2.3 State of the political landscape in the U.S.

The political division in the U.S. is on a historic high.<sup>115</sup> Currently, many Trump-supporters have the belief that the 2020 election was influenced by Democrat-aligned actors and subsequently stolen from Trump. Claims about this «Big Lie» have been disproven and have no merit to them.<sup>116</sup> Nevertheless, the belief in the conspiracy has remained unwavering: in December 2020, about 70% of Republicans asked in a poll did not believe that Biden was the legitimate winner of the election.<sup>117</sup> Another poll puts this number significantly higher, at 84% of Republicans.<sup>118</sup> This did not change in two years, as about 74% in September 2022 still hold the same opinion.<sup>119</sup> This means that around 34 - 37% of all voters do not believe in a legitimate election. We can observe the consequences of such beliefs in the attack on the U.S.-Capitol on January 6<sup>th</sup>, 2021. After President Trump was not re-elected, thousands of his supporters marched on the Capitol with the aim of violently overturning the election.<sup>120</sup> Before and since this obviously futile endeavor, there have been numerous accounts of election deniers that have conducted threats or attacks against the perceived culprits of Trump's loss. The number of threats against members of Congress has also increased by a factor of ten over the course of one year.<sup>121</sup> Election denial is not limited to supporters of Trump, but also applies to republican politicians including Trump himself.<sup>122</sup> Looking at Congress, out of 552 republican nominees for the 2022 midterms 199 have fully denied and 61 have raised questions over the legitimacy of the 2020 election. 121 more have declined to answer when asked or have no public stance, while 93 more have accepted the results with reservations.<sup>123</sup> We can observe significant damage being done to the political process of the U.S.<sup>124</sup> There is heightened polarization in the U.S. political landscape with especially center-right voters moving

<sup>115</sup> See Pew Research Center, 'As Partisan Hostility Grows, Signs of Frustration With the Two-Party System' (2022), available at <https://www.pewresearch.org/politics/2022/08/09/as-partisan-hostility-grows-signs-of-frustration-with-the-two-party-system>.

<sup>116</sup> See ANDREW C. EGGERS, et al., 'No evidence for systematic voter fraud: A guide to statistical claims about the 2020 election' (2021) *PNAS*; Politifact, 'Joe Biden is right that more than 60 of Trump's election lawsuits lacked merit', available at <https://www.politifact.com/factchecks/2021/jan/08/joe-biden/joe-biden-right-more-60-trumps-election-lawsuits-l>.

<sup>117</sup> Quinnipiac University, 'Quinnipiac Poll' (2020), Question 9, available at [https://poll.qu.edu/images/polling/us/us12102020\\_usrn76.pdf](https://poll.qu.edu/images/polling/us/us12102020_usrn76.pdf).

<sup>118</sup> YouGovAmerica, 'Trump voters still see Biden's victory as illegitimate' (2020), available at <https://today.yougov.com/topics/politics/articles-reports/2020/11/19/trump-voters-biden-poll>.

<sup>119</sup> The Economist/YouGov, 'The Economist/YouGov Poll: September 3 - 6, 2022 - 1500 U.S. Adult Citizens' (2022), p. 204, available at <https://docs.cdn.yougov.com/t1ravwgbet/econTabReport.pdf>.

<sup>120</sup> The New Yorker, 'Among the Insurrectionists' (2021).

<sup>121</sup> For an overview see Reuters, 'Campaign of Fear: The Trump world's assault on U.S. election workers', available at <https://www.reuters.com/investigates/section/campaign-of-fear>; see The New York Times, 'Lawmakers Confront a rise in Threats and intimidation, and Fear Worse' (2022).

<sup>122</sup> CNN politics, 'Trump is doing more lying about the election than talking about any other subject' (2021), available at <https://edition.cnn.com/2021/06/12/politics/analysis-trump-election-lies-blog-post-presidency>.

<sup>123</sup> FiveThirtyEight, '60 Percent Of Americans Will Have An Election Denier On The Ballot This Fall' (2022), available at <https://projects.fivethirtyeight.com/republicans-trump-election-fraud>.

<sup>124</sup> It should be noted that division and election denial are not limited to the US. Jair Bolsonaro has stated before the 2022 Brazilian presidential election, that he will only accept a win: see Sum of Us, 'Stop the Steal Part 2: How YouTube and Meta are dismantling Brazilian Democracy', supra note 104, p. 10; the "Stop the Steal 2.0" campaign subsequently gained traction and was actively promoted by recommendation systems and smart ads on YouTube and Meta.

further right since 2016.<sup>125</sup> The Congress and the mainstream media have not had high approval levels for quite some time, and now the trust in elections is dwindling as well.<sup>126</sup> Since we have established that many of these negative effects are promoted by targeted political ads, it's thus vital that steps are taken to mitigate the effects created by them.

## 5 REGULATING TARGETED POLITICAL ADS

### 5.1 EXISTING RESTRICTIONS ON POLITICAL ADS

There are additional rules regarding political ads on Google's platforms. Before using Google for political advertising purposes, a verification process must be completed.<sup>127</sup> For election ads, encompassing most political ads, Google displays a «paid for by» message on the ad and publishes a corresponding ad report.<sup>128</sup> More importantly, Google has restricted the targeting of election ads to specific categories: geographic location, age, gender, and contextual targeting. The last one is arguably the most powerful marker, as it enables advertisers to place their ads on websites that match their specific ad.<sup>129</sup> The limitations that Google has implemented are to be welcomed, as they show significant improvements for the quality and safety of ads. Still, there are limitations of such measures. Even if an ad adheres to all rules, it can still target voters quite accurately as it is able to filter based on the allowed factors.

The EU is also implementing provisions specifically aiming at inhibiting misinformation campaigns that may involve political ads.<sup>130</sup> The entire 5<sup>th</sup> section of the DSA is predicated around limiting very large online platforms. Specifically, Article 34(1) (c) of the DSA obliges them to assess risks for civic discourse, electoral processes, and public security on their platforms. They then must take steps to implement measures to mitigate those risks. Furthermore, the EU proposed the regulation on the transparency and targeting of political ads that should come into force around 2023. The timing is not a coincidence: as stated by the EU Commission, the regulation is to be applied in the 2024 electoral cycle of the EU. Its aim is to build on the DSA and

---

<sup>125</sup> FARIS, et al., 'Partisanship, Propaganda, and Disinformation: Online Media and the 2016 U.S. Presidential Election', supra note 80, at p. 18. This is not to say that polarization exists only due to increasing use of smart technology but is enhanced by it. Trump has proven to be, mildly put, controversial, lying approximately 21 times a day: The Washington Post, 'Trump's false or misleading claims total 30,573 over 4 years' (2021).

<sup>126</sup> See HABERMAS, 'Überlegungen und Hypothesen zu einem erneuten Strukturwandel der politischen Öffentlichkeit', supra note 23, at p. 491; the U.S.-Congress has had approval-ratings in the 20% range for over a decade: Gallup, 'Congress and the Public' (2022), available at <https://news.gallup.com/poll/1600/congress-public.aspx>.

<sup>127</sup> Google LLC., 'Political content', available at <https://support.google.com/adspolicy/answer/6014595>.

<sup>128</sup> Google LLC., 'Election advertising verification', available at <https://support.google.com/adspolicy/troubleshooter/9973345>.

<sup>129</sup> It is the reverse model to the behavioral method of targeting: Google LLC., 'About contextual targeting', available at <https://support.google.com/google-ads/answer/2404186>.

<sup>130</sup> See JARREN/FISCHER, 'Demokratische Öffentlichkeit: Eine medienpolitische Gestaltungsaufgabe', supra note 113, at p. 37.

expand on transparency.<sup>131</sup> Chapter II of the DSA requires record-keeping, puts forth transparency requirements for each political ad and requires different systems for reporting (Article 6 et seq.). This is of considerable importance as users face an according problem: a majority does not recognize paid ads on Google Search.<sup>132</sup> This means they do not know that a result that they view is in fact not objective but heavily influenced by the advertiser. Political ads consequently have the appearance of not being or at least be less biased because they are not connected to a party affiliation. Even more interesting for our purposes is Article 12(1) of Chapter III of the DSA: it prohibits targeting and amplification techniques that involve the processing of specific personal data like race, political opinion, union membership or religious beliefs. A possible Achilles' heel of the new provision in Article 12 is that the restrictions can be circumnavigated by getting the consent of the user.

If these transparency requirements are met, they will provide an efficient mechanism for counteracting foreign influence. However, the main problem with targeted political ads is not who creates them, but rather whom they target. On the other hand, in the EU regulation on political ads, including the GDPR, consent of the user is vital for tracking software. The rules against «cookie-walls» as laid out in the GDPR will apply to the new rules on political ads as well, requiring informed consent of the user.<sup>133</sup> Protection of this caliber is vital. Otherwise, a user who wants to use the Internet would have to agree to all terms of services of an intermediary. If not, intermediaries would be free to not provide their services to the user. However, for the new provisions to make a meaningful difference, courts will have to strictly enforce the new regulations, as intermediaries will try to circumvent such restrictions.

## 5.2 MODALITIES OF REGULATION

We should thus consider further how to best conceive of regulation, how it should work and what its aim should be. With the EU advancing its regulations in the field of politics, circumvention measures from Google become more relevant. A first potential circumvention tactic might be the PSI itself: by phasing out cookies and fingerprinting, Google can potentially render multiple existing and upcoming regulations around these technologies useless. Observing the interplay between Google and the EU from a systems theoretical perspective would support this assumption.

NIKLAS LUHMANN divides society into functionally differentiated systems that constitute themselves by their distinction to their environment.<sup>134</sup> As systems, like the political and economic, are operatively closed, they cannot directly change each other's structures.<sup>135</sup> They can only accomplish change through the bias of their own operations. These create «noise», which in turn could get picked up by another sys-

---

<sup>131</sup> European Union: European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the transparency and targeting of political advertising, 25. November 2021, COM(2021) 731 final, at pp. 3–4.

<sup>132</sup> Varn, 'The latest Google Ads Research from Varn 2022' (2022), available at <https://varn.co.uk/09/22/latest-google-ads-research-2022-varn>.

<sup>133</sup> European Union: European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the transparency and targeting of political advertising, 25. November 2021, COM(2021) 731 final, at p. 23.

<sup>134</sup> NIKLAS LUHMANN, *Social Systems*, Translated by John Bednarz, Jr. with Dirk Baecker, Stanford, 1995, at pp. 16–17.

<sup>135</sup> See NIKLAS LUHMANN, *Theory of Society, Volume 1*, Translated by Rhodes Barrett, Stanford, 2012, at p. 49.

tem. This can result in an «irritation», meaning that the other system might be confronted with the decision whether to change its own structures and adapt.<sup>136</sup> Apart from strong structural couplings between systems,<sup>137</sup> this makes the enforcement of precise changes difficult.<sup>138</sup> The described can be observed in the actions of Google, an actor of the economic system. The PSI is an adaption of Google's structures to the regulatory advances from the EU.<sup>139</sup> The shift to more concrete regulations has prompted Google to react by using its own operations aimed at maintaining as much profit as possible. For us, the main takeaway is that regulation is neither easy to accomplish nor is it reliably effective. The effect of well-meaning regulation can be unexpected and even undesirable.

Connecting this thought to targeted political ads means that a one-size-fits-all solution is an illusion. Still, we have established that such ads can undermine the democratic process, so thought-out regulations like the ones stemming from the EU should be welcomed. Restricting the use of targeted ads stops them from contributing to the dangers for the democratic process. It should be reiterated that this discussion should be first and foremost about targeted ads. It is the usage of AI technology that makes these ads so powerful, as it allows management at scale for the content and distribution of the ads. This means that when regulating such ads, we should differentiate between different levels of technical sophistication. It is reasonable that a political campaign can target the region that they want to show ads in or filter out non-voters like children. Furthermore, even different variations of ads depending on the current messaging might be appropriate. This leads to the conclusion that from a democratic perspective, restrictions should predominantly target ads that possess unreasonably strong targeting.

### 5.3 INTERMEDIARIES RESEMBLING PUBLIC UTILITIES

#### 5.3.1 A collective endeavor

We now open the discussion on how to treat intermediaries as objects of regulations in general. Google is a private company and as such it does not adhere to the same standards that state institutions or companies tasked with fulfilling public interests must respect.<sup>140</sup> This means that it is only limited by mandatory rules and regulations from state- and interstate actors. It does not have to respect human rights in the same way, can have a profit motive and users are less able to access legal processes.<sup>141</sup> This *status quo* should be challenged: Google provides a service that gets used and is re-

---

<sup>136</sup> See NIKLAS LUHMANN, *Theory of Society, Volume 2*, Translated by Rhodes Barrett, Stanford, 2013, at pp. 116–117.

<sup>137</sup> This interplay is especially strong between the political and the legal system with the constitution acting as a structural coupling, see NIKLAS LUHMANN, *Law as a Social System*, Translated by Klaus A. Ziegert, Oxford, 2004, at p. 404.

<sup>138</sup> Building on LUHMANN, ALAIN POTTAGE describes the observational limitations of regulators in 'Biotechnology as Environmental Regulation', in ANDREAS PHILIPPOPOULOS-MIHALOPOULOS (ed.), *Law and Ecology: New Environmental Foundations*, Oxford, 2011, at pp. 106–107.

<sup>139</sup> Regulation means the attempt of the political system to influence the operations of other systems through the medium of law, as defined by JULIA BLACK, 'Critical Reflections on Regulation' (2002), *Australian Journal of Legal Philosophy*, 27, at p. 32.

<sup>140</sup> See BGE 2C 1023/2021 d. 2.1, 2.2.1 and 2.3.1.

<sup>141</sup> See ULRICH HÄFELIN, et al., *Allgemeines Verwaltungsrecht*, 8<sup>th</sup> ed., Zürich/St. Gallen, 2020, at p. 57.

lied upon by billions of people, be they active users or people affected by them. There should thus be more discussion on what helps users navigate the Internet more securely and how they can benefit as much as possible from their time online. This means looking at the Internet and intermediaries like public affairs, not private ones – because *de facto* they already are: intermediaries are commonly used as essential infrastructure for states and their representatives.<sup>142</sup> Official websites, legal texts, and political news are accessed via Google Search. Heads of States, legislators, but also first responders like police- and fire departments use Twitter, Facebook, and Instagram to communicate in real time with the population. These services rely on intermediaries as infrastructure, going beyond a mere convenience, making them ultimately serve a public function. Subsequently, it comes as no surprise that private users also spend a lot of time on the Internet, between 6 to 8 hours per day.<sup>143</sup> Regarding the health of a democratic society, PARISER proposes that tech platforms should thus work primarily in favor of the public.<sup>144</sup> It stands to reason that more direct public control would achieve this goal, as such a concept is neither unreasonable nor new. Going back in time to the ancient city of Rome, the water supply was enabled by aqueducts built by the state, because the roughly one million people in Rome could not provide for sufficient water themselves.<sup>145</sup> In the Golden Age of Islam, in the 13<sup>th</sup> century, hospitals were completely free of charge.<sup>146</sup> Under Otto von Bismarck, the first state-led social security systems were developed in the second half of the 19<sup>th</sup> century to mitigate the financial risks posed by injury, sickness, and death.<sup>147</sup> Nowadays, public funding for streets, transit, museums or emergency services is widespread and largely accepted. We should thus examine why certain sectors are under state control, for if we want to look at intermediaries like public utilities, first we must define what the latter are.

### 5.3.2 Intermediaries and the Swiss «*service public*» standard

For the purposes of this discussion, we take the Swiss system of «*service public*»<sup>148</sup> as a baseline of understanding. The definition of the Swiss Federal Council reads about as follows: *service public* encompasses a politically defined basic supply of infrastructure goods and services that should be available in good quality and at reasonable prices for all sections of the population and regions of the country according to the same

<sup>142</sup> See GC, Judgment of 10 November 2021, *Google and Alphabet v Commission (Google Shopping)*, T-612/17, EU:T:2021:763, paragraph 224. However, the Court does not fully recognise Google as an essential facility.

<sup>143</sup> SIMON KEMP, 'Digital 2022: April Global Statshot Report' (2022), available at <https://datareportal.com/reports/digital-2022-april-global-statshot>; e.g., with an Internet penetration in the total population of around 94%, about 90%, Swiss people almost all use Google Search: NIC NEWMAN, et al., 'Reuters Institute: Digital News Report 2022', supra note 77, at p. 6; Statcounter, 'Search Engine Market Share in Switzerland' (2022), available at <https://gs.statcounter.com/search-engine-market-share/all/switzerland>.

<sup>144</sup> See The Verge, 'Filter Bubble' author Eli Pariser on why we need publicly owned social networks' (2019).

<sup>145</sup> See the numerous accounts of FRONTINUS detailing different roman officials commissioning the waterways: MANFRED HAINZMANN, *Wasser für Rom: Die Wasserversorgung durch Aquädukte*, Zürich/München, 1979, at pp. 11–19.

<sup>146</sup> DAVID TSCHANZ, 'The Islamic Roots of the Modern Hospital' *AramcoWorld*, at p. 22.

<sup>147</sup> BSV, 'Versicherung als neues Modell: Rechtsanspruch statt Bedürftigkeit' (2014), available at <https://www.geschichtedersozialversicherung.ch/synthese/1883-1884-1889>.

<sup>148</sup> Also called «*service universel*», and in German «*Grundversorgung*» or «*Universaldienst*»: with further references HETTICH/SHELKER, *Medien im digitalen Zeitalter: Neugestaltung des Programmauftrags aus ökonomischer und rechtlicher Sicht*, supra note 115, at p. 99.

principles.<sup>149</sup> Therefore, a public utility in the Swiss legal system is infrastructure that is legally seen as a public good – in other words that provides a public service. This entails a political decision to define such services, varying from issue to issue. While the term *service public* is not explicitly written down in the Swiss Constitution, several provisions derive their meaning from this concept.<sup>150</sup> For the purposes of comparing intermediaries to public utilities, the best suited provision is Article 93 of the Swiss Constitution. In essence, it defines the legislation of radio and television (RTV) to be under federal control and adhere to a *service public* mandate.<sup>151</sup> The consequences of a *service public* mandate can be shown when looking at the existing regulations on RTV. Namely the Federal Act on Radio and Television (RTVA) and the corresponding Ordinance on Radio and Television: according to Section 2 of the Act, there are minimal requirements for program service content. All programs are required to adhere to human rights (Article 4(1) RTVA), and not to jeopardize Swiss national security (Article 4(3) RTVA). They are notably also barred from advertising for political parties, candidates or officials and matters which are subject of a popular vote (Article 10(1) (e) RTVA). The largest provider, the Swiss Broadcasting Corporation (SRG) is further restricted on ads and sponsoring (Article 14 RTVA).<sup>152</sup>

Imposing such obligations on intermediaries entails a discussion over whether there currently exists the Swiss Constitution, namely in Article 93.<sup>153</sup> However, this would limit the scope to Switzerland, so we rather focus on the arguments for the already existing mandate of RTV and apply them to intermediaries. For this purpose, we will compare four different justifications brought forward for regulating broadcast companies. A *first* argument would be the importance of RTV for a democratic functional background of society.<sup>154</sup> The argument is that broadcast services contribute greatly to the distribution of political information and the functioning of the heavily deliberative democratic system of Switzerland.<sup>155</sup> Because of this, the state needs to be actively involved in prohibiting risks for the discourse. Solely addressing the RTV sector might be outdated considering the rising importance of the Internet and interme-

<sup>149</sup> Translated from German: Federal Council, 'Bericht des Bundesrates "Grundversorgung in der Infrastruktur (Service public)" (2004), p. 2, available at <https://www.news.admin.ch/news/message/attachments/9238.pdf>.

<sup>150</sup> Notably public transport in Article 87 Const. as well as postal and telecommunication services in Article 92 Const.

<sup>151</sup> CHRISTOPH B. GRABER/THOMAS STEINER, 'SG Komm. BV, Art. 93', in BERNHARD EHRENZELLER, et al. (eds), *Die Schweizerische Bundesverfassung: St. Galler Kommentar*, 3<sup>rd</sup> ed., St. Gallen, 2014, at paragraph 2.

<sup>152</sup> HETTICH/SHELKER, *Medien im digitalen Zeitalter: Neugestaltung des Programmauftrags aus ökonomischer und rechtlicher Sicht*, supra note 115, at pp. 148–151.

<sup>153</sup> A majority of scholars see the Internet and intermediaries implicitly addressed in Article 93: see GRABER/STEINER, 'SG Komm. BV, Art. 93', supra note 153, at paragraph 5; FRANZ ZELLER/MARTIN DUMERMUTH, 'Art. 93', in BERNHARD WALDMANN, et al. (eds), *Basler Kommentar zur Bundesverfassung*, Basel, 2015, at paragraph 13; critical URS SAXER, 'Die Online-Zuständigkeiten des Bundes' (2017) *Aktuelle Juristische Praxis*, at pp. 338–349.

<sup>154</sup> HETTICH/SHELKER, *Medien im digitalen Zeitalter: Neugestaltung des Programmauftrags aus ökonomischer und rechtlicher Sicht*, supra note 115, at p. 104; see GRABER, 'Personalisierung im Internet, Autonomie der Politik und Service public', supra note 42, at p. 268; JARREN/FISCHER, 'Demokratische Öffentlichkeit: Eine medienpolitische Gestaltungsaufgabe', supra note 113, at pp. 26–27; GRABER/STEINER, 'SG Komm. BV, Art. 93', supra note 153, at paragraph 4; see BGE 134 II 260 d. 6.2 – 6.4 and BGE 2C 1023/2021 d. 3.3.6.

<sup>155</sup> For an overview of the various deliberative elements in Switzerland, see EVA M. BELSER, 'Direkte und deliberative Demokratien der Schweiz: Vom Volk, das nicht nur mitredet, sondern entscheidet – und dennoch nicht immer das letzte Wort haben sollte', in ELISABETH ALBER/CAROLIN ZWILLING (eds), *Von Government zu Governance: Nomos*, 2021, at pp. 150–158.

diaries.<sup>156</sup> News consumption nowadays happens to a far greater extent on and through the bias of intermediaries, making them the dominant actors in the media space.<sup>157</sup> *Secondly*, it is argued that market failures exist in the media space for news of high quality.<sup>158</sup> The argument is that private actors are not sufficiently incentivized to produce quality content if it does not generate enough profit. In the case of intermediaries, they do not produce content themselves but host content of on-platform creators. They do, however, prioritize content that creates lots of engagement, which is an unreliable metric for quality at best.<sup>159</sup> As a *third* argument, special effectiveness of television and radio is brought forward. The argument is that audio-visual forms of distributing information are more potent and thus more convincing than the written form found in newspapers.<sup>160</sup> How URS SAXER/FLORIAN BRUNNER point out, this is fundamentally a paternalistic view that has also been overtaken by the shifted use of the modern media landscape.<sup>161</sup> It has to be pointed out though that at least some protection of the population from harm is a core function of states, while balancing it with personal freedom.<sup>162</sup> In the wake of the high popularity and the use of targeted ads on intermediaries there is a renewed case to be made for this argument. Being limited by the number of radio frequencies was historically the *fourth* element in favor of the *service public*:<sup>163</sup> signals were transmitted by radio waves to televisions and radios. However, there were not unlimited wavelengths to choose from as they needed to adhere to certain lengths to be transmitted. With the introduction of the Internet, this mode of transmission has become mostly obsolete. This means in turn, that communication between users is not largely restricted anymore, as it now can happen freely and without any barriers on broadcasting time.<sup>164</sup> For intermediaries, this development amounts to almost unlimited browsing time and volume. The most prevalent limitation now is the attention of the user. This is precisely why providers fight for the most interesting and engaging content. Rather than seeing this new abundance of content as freeing from a *service public* mandate, it should re-enforce it. Historically, there was a limited number of providers that created content. The state

<sup>156</sup> URS SAXER/FLORIAN BRUNNER, 'Der Service public, die digitale Revolution und die Medienverfassung' (2018) *Aktuelle Juristische Praxis*, at pp. 33–34.

<sup>157</sup> See NIC NEWMAN, et al., 'Reuters Institute: Digital News Report 2022', supra note 77, at pp. 24–25.

<sup>158</sup> With further references HETTICH/SHELKER, *Medien im digitalen Zeitalter: Neugestaltung des Programmauftrags aus ökonomischer und rechtlicher Sicht*, supra note 115, at p. 32.

<sup>159</sup> Falsities tend to spread faster than truth, see DEL VICARIO, et al., 'The spreading of misinformation online', supra note 106, at p. 558; see SOROUGH VOSOUGH, et al., 'The spread of true and false news online' (2018) *Science*, at p. 1150.

<sup>160</sup> HETTICH/SHELKER, *Medien im digitalen Zeitalter: Neugestaltung des Programmauftrags aus ökonomischer und rechtlicher Sicht*, supra note 115, at pp. 33–34 and 101–105.

<sup>161</sup> SAXER/BRUNNER, 'Der Service public, die digitale Revolution und die Medienverfassung', supra note 156, at p. 33; similar arguments are now made for online news content: it's easier, more engaging, and more convenient to consume. See NIC NEWMAN, et al., 'Reuters Institute: Digital News Report 2022', supra note 77, at p. 28.

<sup>162</sup> See CHRISTINE KAUFMANN/ANDREAS GLASER, 'Der moderne Verfassungsstaat', in GIOVANNI BIAGGINI, et al. (eds), *Staatsrecht*, 3<sup>rd</sup> ed., Zürich, 2021, at pp. 23–26.

<sup>163</sup> See HETTICH/SHELKER, *Medien im digitalen Zeitalter: Neugestaltung des Programmauftrags aus ökonomischer und rechtlicher Sicht*, supra note 115, at pp. 29–31; see SAXER/BRUNNER, 'Der Service public, die digitale Revolution und die Medienverfassung', supra note 156, at pp. 32–33.

<sup>164</sup> See HABERMAS, 'Überlegungen und Hypothesen zu einem erneuten Strukturwandel der politischen Öffentlichkeit', supra note 23, at p. 487.



distributed the frequencies with quality control in mind.<sup>165</sup> In the age of Internet, no such considerations are taken into account, as intermediaries are in a highly competitive market and primarily concerned with audience engagement.

As we can observe, the arguments brought forward for the legitimacy of a *service public* mandate in the RTV sector are for one outdated and have more importantly shifted to apply to intermediaries. They have without a doubt replaced the Swiss RTV as the dominant form of media distribution.<sup>166</sup> This would strongly point to the Swiss state having enough reason to put upon intermediaries a *service public* mandate.

## 6 SUMMARY

We started this paper by assessing the business model of Google. Its cornerstone, ads, are made possible by the collection of user data through tracking software like third-party cookies and fingerprinting. These practices have been under public scrutiny for a long time, prompting different regulations by the EU to inhibit the use of established tracking tools. Google recently introduced the PSI to change the technology away from privacy invasive methods. If effective in protecting user privacy, its business model can remain largely unchanged. This has its downsides as well, as we discussed with the example of targeted political ads in the second part of this paper. Judging from the well-documented example of the 2016 U.S.-presidential election, we can assess that these ads are highly effective as means to influence the outcome of elections. However, the disadvantage is that they hinder open political discourse by selectively providing unreliable information to the voters. The effects can be seen in the U.S., as the country is facing polarization and election denialism. Prompted by the challenges facing democracy, the EU has introduced further restrictions on political advertising on the Internet. It has developed a comprehensive host of regulations: together with the DSA and the GDPR, the regulation on the transparency and targeting of political advertisements has made tracking reliant on the freely given consent of the user, while overall improving transparency requirements. Finally, we discussed rules and expectations for the existing Swiss *service public* mandate existing in the RTV sector. Comparing intermediaries to this standard, we determined that they are well suited to be considered under a *service public* mandate.

Google has the influence and power comparable to nation-states. Its decisions, values, and technology can determine the elections of powerful countries. Maybe in line with wanting to have a say in the actions of intermediaries, a large majority of EU citizens now want Big Tech and specifically cookies to be regulated.<sup>167</sup> The EU has thus made concise steps to address digital advertising in general and political ads specifically. How this regulation fairs in practice needs to be assessed but signals in any case a clear willingness of the legislator to limit intermediaries in their power.

---

<sup>165</sup> See SAXER/BRUNNER, 'Der Service public, die digitale Revolution und die Medienverfassung', supra note 156, at p. 32.

<sup>166</sup> With further references HETTICH/SHELKER, *Medien im digitalen Zeitalter: Neugestaltung des Programmauftrags aus ökonomischer und rechtlicher Sicht*, supra note 115, at p. 22; see SAXER/BRUNNER, 'Der Service public, die digitale Revolution und die Medienverfassung', supra note 156, at p. 34.

<sup>167</sup> Synopsis report of the public consultation on the evaluation and review of the ePrivacy Directive, at pp. 12-14, available at [https://digital-strategy.ec.europa.eu/en/library/full-report-public-consultation-eprivacy-directive?pk\\_source=ec\\_newsroom&pk\\_medium=email&pk\\_campaign=dae%20Newsroom](https://digital-strategy.ec.europa.eu/en/library/full-report-public-consultation-eprivacy-directive?pk_source=ec_newsroom&pk_medium=email&pk_campaign=dae%20Newsroom).