Information Polity 27 (2022) 259–274
DOI 10.3233/IP-211535
IOS Press

Culling the FLoC: Market forces, regulatory regimes and Google's (mis)steps on the path away from targeted advertising[1]

David Eliot and David Murakami Wood*
Department of Sociology, Queen's University, Canada

Abstract. This paper analyzes the short history of Google's AI-driven data collation and marketing technology, Federated Learning of Cohorts (FLoC), which was designed to replace third-party cookies, the technology at the heart of "surveillance capitalism." Using publicly available data such as patents, investor calls, public filings, github accounts, and presentations, this paper explores FLoCs and its immediate replacements, The Topics API and FLEDGE, and contests claims that Google's new marketing technologies are both 'privacy-centric' and as effective as surveillance-driven targeted advertising. The paper argues that Google's parent company, Alphabet is starting on a path away from being an advertising and information company to being an "AI-first" company, and sees FLoC as one (mis)step on this path. The paper shows how an combination of interacting factors – corporate ideology, market forces, regulatory responses, and internal cultural conflict – are driving this transformation, but concludes that surveillance will continue to be at the heart of any AI-first economy.

Keywords: Platforms, Google, Alphabet, surveillance, surveillance capitalism, privacy, human rights, Privacy Sandbox, data protection, GDPR, regulation, markets, marketing, advertising, FLoC, Topics, FLEDGE

1. Introduction

In 2020, Google announced their intention to transition away from unpopular privacy-invasive third-party cookies in their market-leading Chrome browser. In their place, they proposed the use of a new AI-driven technology, "Federated Learning of Cohorts" (FLoC)[2] (Schiff, 2021), the first product of their experimental "Privacy Sandbox." They claimed that this new "privacy-centric" technology was 95% as effective as their current targeted advertising system (Schiff, 2021). However, in January 2022, barely 18 months later, Google announced that FLoC was to be dropped, to be replaced by a new system known as "The Topics API" and another known as "FLEDGE."

Our research analyzed publicly available data such as patents, investor calls, public filings, github accounts, and presentations.[3] When we began this project, no-one in surveillance studies, critical data

[1] This article received a correction notice (Erratum) post publication with DOI 10.3233/IP-229012, available at http://doi.org/10.3233/IP-229012.

[*] Corresponding author: David Murakami Wood, Department of Sociology, Queen's University, Mackintosh-Corry Hall, Kingston, Ontario, K7L 3N6, Canada. Tel.: +1 613 533 6000 74490; E-mail: dmw@queensu.ca.

[2] We use "FLoC" as it appears to be the final officially preferred acronym (see: https://github.com/WICG/floc), however "FLoCs", "FloCs", "Floc", "Flocs", "floc", and "flocs" have all appeared in news media and even on other Google sites. In quotations from sources we leave the acronym as it originally appeared.

[3] This research was partly funded by the Contributions Program of the Office of the Privacy Commissioner of Canada (OPC). The OPC project also included detailed work simulating the way in which FLoC was supposed to have functioned. We will report on this technical work, with our other research partners, in future papers.

studies or privacy studies had yet analyzed FLoC in this context, tested the claims made for it, or considered its implications for privacy and human rights more widely. Authors (2021) appears to have been the first policy paper to consider the implications, and to our knowledge, at the time of writing, only one other, largely descriptive, academic analysis of this shift has been published (Çınar & Ateş, 2022).

This is a crucial subject because it represents the cusp of a transformation of the online economy, and in particular for Alphabet/Google, a movement in process away from targeted advertising, the core of what Shoshana Zuboff (2015, 2019) identified as "surveillance capitalism," to one driven by Artificial Intelligence (AI). The FLoC debacle is not merely important in terms of the debate over surveillance and privacy online, but also in the context of the coming age of AI. This paper is therefore an early and necessarily somewhat speculative and incomplete analysis of a key moment, whose outcomes are fast-moving and uncertain.

This paper first tells the story of FLoC, beginning with its origins in the push to eliminate "third party cookies," an advertising technology (adtech) vital to Google's dominance of online advertising. We consider their response with the experimental Privacy Sandbox, from which FLoC emerged as the herald of a new apparently "privacy-centric" marketing age. We identify four broad factors that led to the overly rapid public announcement, and equally rapid termination, of FLoC: 1. corporate ideology; 2. market forces; 3. regulatory regimes, and 4. internal cultural controversies. We argue that the influence of regulatory regimes, in particular the European Union's General Data Protection Regulation (GDPR, 2016), and a proposed ban on targeted advertising in the United States Congress, was central to the demise of FLoC. However, we conclude that if FLoC was a misstep, market forces and corporate ideology are continuing to push Alphabet/Google down the path towards an AI-driven future.

1.1. Definitions

There are a number of foundational terms in this piece. We recognize that these terms are contested but exploring definitional controversies is not within the scope of this paper. Here we outline how we use each term.

Surveillance: the systematic observation, sensing or collection of data, aimed at influencing the behaviour of those observed (etc.). Often juxtaposed with privacy, surveillance has implications not just for privacy but for many other human and civil rights, social justice and equity.

Privacy: a human right that recognizes the control an individual person (or sometimes a group) should enjoy over their personal life, intimate relationships, body, mind and information or data.

Data Protection (DP): the concept of safeguarding the security, integrity and privacy of personal data. DP therefore overlaps with privacy rather than being coequal: privacy is only party of what DP involves, and in that privacy covers far more than data, data protection relates to only a portion of privacy more generally, although with ongoing digitization and datafication, it is an increasingly large portion.

Artificial Intelligence (AI): a broad definition of an artificial system (computer program) that can interpret and react to its environment in order to achieve its goals (Russell, 2019).

Machine Learning (ML): the use of big data to design and train systems to solve complex problems. A subset of AI, but AI is often casually used when referring to ML systems.

2. The challenge to targeted advertising

As Zuboff (2015, 2019) argues, Google was transformed in less than a decade from a search engine company into an advertising giant. Now, in a "digital duopoly" (Winseck, 2020), Google and Facebook together control about three-quarters of the US online advertising market. Google Ads, Google's online advertising platform, is the main source of revenue for Alphabet Inc, Google's parent company, generating US$257.6 billion in 2021 (Alphabet Inc., 2022).

2.1. Third-party cookies

Targeted advertising online relies on "cookies." A cookie is a small text file that is stored on a user's browser. Each cookie contains a unique identifier, a string of characters called a cookie ID. "Third-party cookies" are cookies saved to a user's browser by a site other than the one they are currently visiting and remember specifics about a user like login information or language preferences. Advertisers use third-party cookies to identify visitors and track behaviour, such as what sites they have visited or what items the user has viewed or added to their shopping cart. "Third-party persistent cookies," sometimes called "tracking cookies," are used to track users' online behaviour – their clicks, purchases, and geographic locations. Tracking cookies are used by advertising networks to deliver targeted, personalized ads.

Third-party cookies were identified as a privacy hazard almost as soon as they were invented in the 1990s (see e.g. Bennett, 2001), but more recently have become the subject of serious political pushback (Fou, 2020). In response, most major players in the browser industry have, belatedly, announced they will no longer support them (Bohn, 2020). For some time, Google has been announcing plans to phase out third-party cookies from their Chrome browser by late 2023 (Goel, 2022).[4]

The problem is that third-party cookies are the foundation of Google's enormous profitability. The platform is currently built on cookies and keywords, allowing Google Ads to display targeted ads on pages that they believe might be relevant. Advertisers pay Google Ads when a user clicks on their ad, making targeted ads the foundation of the business model. And despite the announcement of the future demise of third party cookies, targeted advertising will remain a major source of revenue for Google. However, without the ability to track users using third-party cookies, they needed to develop new methods of targeting advertising to specific users but without the privacy issues that had dogged third-party cookies from the start.

2.2. The Privacy Sandbox

To operationalize both this strategy and a movement away from targeted advertising, Google created an open-ended development environment known as "Privacy Sandbox," (The Chromium Projects, n.d), designed "to overcome in that mission is the pervasive cross-site tracking that has become the norm on the web..." They "plan to introduce new functionality to serve the use cases that are part of a healthy web that are currently accomplished through cross-site tracking," and "as that functionality becomes available [...] will place more and more restrictions on the use of third party cookies."

The Privacy Sandbox is an experimental software development environment, with three overall themes and an evolving number of number of sections, with different use-case focii. The three themes are: Replacing Functionality Served by Cross-site Tracking; Turning Down Third-Party Cookies; Mitigating Workarounds. The third section is specifically aimed at preventing the return of user-tracking by other means and maybe the most difficult and least developed at this point. It includes projects to deal with digital fingerprinting, one of the main objections to FLoC (see below) and other obfuscation mechanisms.

Several sections have already gone through two or more iterations, including TURTLEDOVE, from which FLEDGE emerged, and some exist only as proposals without any firm timeline for testing or release, like the The Topics API. For this research, we concentrated on the Cross-Site Tracking theme, and in particular on the first announced prototype released for live testing, FLoC.

[4] As we were revising this paper, Google announced that third-party cookie technology would also be removed from Android products (Chavez 2022).

2.3. What was FLoC?

FLoC stands for “Federated Learning of Cohorts”, and it was supposed to be powered by a relatively new process called “Federated Learning” (FL) (Google-Research, n.d). The technique has been championed as proof of Google’s dedication to privacy, as it challenges the notion that intensive data harvesting and storage is necessary to train competitive AI/ML systems (Alphabet Earnings Call, 2019).

FL addresses concerns over the mass collection and storage of personal data, but it does not address concerns about how data is used. The impetus for mass data collection in AI comes from the need to have centralized datasets to train ML algorithms. A system needs direct access to a large database of examples (data) from which to learn (Truong et al., 2020). An AI intended to suggest email responses would need access not only to a large dataset of emails and responses, but also to what responses users choose, to identify issues and improve its suggestions. The ethical concern is that the company training the AI has extracted users’ personal information – their emails – from their device, and stored them, enabling possible data breaches or misuse of that data for personal, commercial or political ends.

However, in an FL system, instead of data being centralized and used to train an AI model, the AI model is trained decentrally on the user’s device (McMahan & Ramage, 2017). The user’s device downloads the current ML/AI model and improves itself by training on the device’s localized data. Once the training is complete the improved model is encrypted and sent back to the cloud where it is averaged with other models that have gone through the same process on other devices, to create a global model to be pushed as a new update (Truong et al., 2020). This is presented as both effective and privacy-centric, as one can get the same results as with a centralized server, without needing to extract data from the user’s device (Truong et al., 2020).

According to its description, FLoC went even further, using temporal, localized data, stored on the user’s Chrome browser to segment a user into a predictive customer type: a “cohort” of users sharing similar traits (Google-Research, n.d.). Google claimed cohorts would preserve privacy, as the individual traits of users within a cohort would not be revealed, only the shared traits. Further, the cohort would be big enough that no personally identifiable information could be interpreted from a user’s cohort (Google-Research, n.d.). Marketers would then be invited to advertise to cohorts identified as sources of potential customers, not individuals (Google-Research, n.d., Bindra, 2021). Only the user’s cohort ID would be exposed, with the data used to construct it, “secure” on the browser (Google-Research, n.d.). This action would be continuously repeated, with the user being regularly sorted into new cohorts reflecting the most recent data on the user’s device that the FL model trained on (Google-Research, n.d.).

Google stated that in trials, FLoC performed at least 95% as well for advertisers as the third-party cookies approach (Bindra, 2021). But not all was as it appeared. While Google had planned to use FL, in practice the version of FLoC used in trials did not include FL or indeed any kind of AI, instead simply an on-device SimHash algorithm, a technique long used by Google in categorizing websites for Search (Manku et al., 2007), that would supposedly be updated to a machine learning algorithm in the future (The Topics API, 2022).

FLoC did not move away from mass data collection as much as promised either. FL systems require massive amounts of centralized data in order to construct the original AI/ML model, so how could Google have collected the necessary quantity of data to fuel an FL-driven system without third-party cookies? One increasingly common technique is “web beacons.” A web beacon is a first-party cookie installed on a host site, that allows a third-party to surveil the user’s actions on the site. Unlike third-party cookies, the host site must *voluntarily* attach the first-party-cookie to their website. To achieve this, a desirable free or cheap service is offered to host sites in exchange for placing the cookie. For Facebook, the most common form is the Facebook "Like" button (Facebook, n.d). When a host site installs a Like button onto their page, it automatically provides Facebook with the ability to extract visitor information including time of visit, userID, and other browser information (Facebook, n.d). Facebook receives this information even if the user is not logged into Facebook, or does not interact with the Like button (Facebook, n.d).

Google's version of the web beacon is its Google Analytics system. Google Analytics is a website analytics platform that comes in free or paid versions. It allows a host site to be able to gain valuable information about their website's visitors, and their behaviour on their site. This can aid website owners in improving their sites for a better user experience, or learn about their customers for marketing purposes. Although there is no official count of how many websites use Google Analytics, one analysis claims to have identified 28,832,505 live websites using Google Analytics (BuiltWith, 2021).

2.4. Would FLoC have protected privacy?

According to Google, FLoC protected privacy by eliminating third-party-cookies and making users anonymous members of a cohort (Bindra, 2021). We concede that eliminating the practice of cross-web tracking via third-party cookies would be better for privacy. However, there were two further related issues: the first concerns the meaning of privacy; the second is whether FLoC could have ensured anonymity and prevented re-identification, with or without FL.

Being tracked is not the only or most basic aspect of online advertising that breaches privacy. The fundamental privacy problem is the ability of a third party to infer information about a person that the user did not willingly divulge. This stems from the ability to make precise predictions about a user by collating numerous disparate data points. Google collects large amounts of non-identifiable data through techniques like web beacons and can use contemporary ML systems to produce powerful correlations. It can therefore make highly accurate predictions about the user with very little personal information. In the case of FLoC, Google required access to only a little data (e.g. most recently visited URLs). But combined with other data, the most private information – sexual desires, political views etc. – can be inferred. Ethically, we argue, this inference constitutes a privacy breach, even if the process of generating this information conforms to privacy and data protection laws.

The second issue is technical. Critics raised questions regarding FLoC's ability to provide genuine anonymity. The threat to anonymity comes from digital fingerprinting, a process by which a third party site collects numerous small pieces of information about a user's device or browser, and combines the collected information to create a clear image of the user (Surveillance Self Defense, 2020). FLoC would have made fingerprinting easier, as users were sorted into cohorts of only a few thousand (Cyphers, 2021). The small number of users per cohort would have given fingerprinters a head start, as they would only have needed to distinguish a user's browser from a few thousand (in their cohort) rather than a few million. Google acknowledged this but only planned to address it after FLoC was implemented. Further, as advertisers would have been provided with users' cohorts, concerns were raised about cross-content exposure, which occurs when a user identifies themself to a website by logging in or registering: the website might then have been able to link the user's specific profile to their FLoC (Cyphers, 2021).

FLoC might not have been as secure as intended even if FL been fully integrated. Multiple studies have demonstrated that although the FL process is claimed not to extract any personal data from the user's device, this might not be accurate (see e.g. Truong et al., 2020). Embedded within the updated training model is information which can be reverse engineered to reveal personal information about the user (Truong et al., 2020). Although Google may not have planned to use this, the fact that it would be exported meant that personal data was still being removed from the user's device, making the user's data vulnerable to potential attacks (Truong et al., 2020).

As with the fingerprinting issue, which would be heightened by FLoC, it remains unknown if Google would have been able to solve this and other privacy issues. Heightened ability to fingerprint users was cited as a reason for FLoC's termination (The Topics API, 2022). Although FLoC may have provided comparable advertising capabilities to third-party cookies, Google's apparent inability to address these issues suggests that FLoC would *only* have been able to fulfill the advertising half of its functional promise.

2.5. FLoC and the GDPR

One of the most immediately consequential questions about FLoCs was how compatible they were with existing privacy and data protection regulations, particularly the EU General Data Protection Regulation (GDPR). We concentrate on the GDPR because first of all, as Colin Bennett (2018) states, 'The GDPR is clearly a significant extension of the global process of policy convergence and the trading up of international privacy standards.' Paul Breitbarth (2019) agrees that the GDPR is influential and 'has created a surge in privacy regulations.' Secondly, we argue that one of Google's main motivations in initiating the Privacy Sandbox was to deal with the challenge of GDPR compliance and pre-empt future EU regulatory developments.

While the previous European Data Protection Directive 95/46/EC was used with increasing frequency to punish corporate infringers of privacy and data protection rights, its small fines meant powerful platform corporations were not greatly affected (Houser & Voss, 2018). The GDPR empowered the Data Protection Authorities (DPAs) of EU member states to institute very large fines, not in fixed amounts but relative to the size of the company. The GDPR allows for fines of up to 4% of global turnover, whether or not the company has any facility in the EU.

The early general opinion within the online marketing industry held that 'GDPR will force marketers to relinquish much of their dependence on behavioral data collection' (Ghosh, 2018). Google stated that it expected FLoC to be compatible with the GDPR. However, by the first half of 2021, representatives had stated several times that the technology was still not ready to be tested in the EU (Schiff, 2021b). There were several unresolved issues. The first was whether processing of personal data to generate a cohort assignment needed consent. The second was whether the assignment of users to cohorts constituted a privacy violation (Lyden, 2021). In the latter case there were concerns about whether the data collected by Google for FLoC would be truly anonymized (and therefore not subject to the GDPR) or whether it would be merely pseudonymized, and therefore still defined as personal data, as it would be potentially re-identifiable. The digital fingerprinting issue alone would seem to put data from FLoC in the latter category. *Wired UK* reported that Johannes Caspar, Hamburg's data protection commissioner was arguing that FLoC would be covered by the could 'allow conclusions' to be derived about users' online activities and that 'Implementing users into the FLoCs could be seen as an act of processing personal data. And this requires freely given consent and clear and transparent information about these operations' (Burgess 2021).

But the question of consent is much bigger than this and is especially problematic for AI-driven systems as FLoC was intended to be. GDPR 6-1 says that

> 'Processing [of data] shall be lawful only if [...] the data subject has given consent to the processing of his or her personal data for one or more specific purposes,' with the only exceptions being the 'performance of a contract ... compliance with a legal obligation ... in order to protect the vital interests of the data subject [or others] ... the performance of a task carried out in the public interest ... [or] the legitimate interests of the data controller.'

It is difficult to see any of these necessity clauses applying to Google's training of AI, so the requirement for consent seems unavoidable. Houser and Voss (2018), Li et al. (2019), and Andrew and Baker (2021) all agree that the overall effect of these and other sections of the GDPR relating to AI might "cripple the tech companies' ability to monetize the data" (Houser & Voss 2018, p. 105). Houser and Voss conclude that this "may be an end to Facebook and Google as they currently operate, at least in the EU" (108–109). Zarsky (2016) came to a similar conclusion in an earlier paper, prior to the institution of the GDPR.

More recent analysis by Andrew and Baker (2021) disagrees. They claim that "the EU's effort to address privacy risk appears to have created space for new forms of surveillance" (570). Broadly speaking, this is because an over-focus on individual privacy might accelerate a kind of surveillance arms race and platform corporation work to develop new surveillance technologies to get around regulations, and further, this could result in "crystallizing the power of tech elites [...] which have already established vast economies of scale in the collection and analysis of behavioral data."

However, what may have been the final nail in the coffin for FLoC was the stirring of opposition in the United States. A succession of whistleblowers and hearings on corporate surveillance and social media culminated in the publication by House Democrats in mid-January 2022 of a *Banning Surveillance Advertising Act* (Eshoo, 2022). Even were it not passed, the bill marked a significant shift in the discourse about privacy and adtech in the USA from that Congressional Research Service Report of 2011 (above). The bill specifically allows for generalized targeting and contextual advertising but almost everything else is prohibited. As the Privacy Sandbox shows, Google was already moving in this direction but the bill made it clear that that ambiguous strategies like FLoC would not suffice.

2.6. *Culling the FloC*

Many reports of the demise of FLoC were triumphant and dismissive. The headline in *HowToGeek* was representative of the mood: "Everyone Hated Google's FLoC, and Now It's Dead" (2022). In trying to satisfy everyone, FLoC pleased no-one. Privacy activists, critical scholars, including ourselves (Authors 2021) and EU regulators noted the obvious privacy and data protection issues.

Simultaneously with culling FLoC, Google announced the release of "The Topics API" (hereafter just "Topics"), ostensibly a direct replacement for both third-party cookies and FLoC (Schiff, 2022). News stories discussing the cancellation of FLoC connected the cancellation to the implementation of the more "privacy-centric" Topics API, creating the perception that Google had taken criticism seriously (ignoring the fact that FLoC had also been presented as "privacy-centric").

At the time of writing in early 2022, Topics remains more a call to development than a finished technology. The developers say it is "coarse grained" (The Topics API, 2022), not attempting to be highly specific. This is probably not just for privacy reasons but because it is envisaged as only one modular technology that can be plugged into Google's overall emerging adtech architecture, in addition to old-fashioned contextual advertising, data from web beacons, and more. Although Topics is based on a system for assigning single-word categories to both websites and users, the numbers of categories, the way in which the categories are assigned and for how long, are still undecided. It is clear that the ultimate arbiter of categories will be Google for the vast majority of cases, with perhaps only a few privileged websites allowed to self-describe. It also seems that some random categories will be thrown into the mix to obfuscate user identity.

Some initial reactions to Topics appeared to have missed the modular aspect of the technologies emerging from the Privacy Sandbox, with one marketing pundit complaining to *AdWeek* (2022) that "Topics is a dumbed-down version of a FLoCs that people are actually able to understand ... It's the same contextual targeting capability from around 2005. It's not very sophisticated." Topics is neither stand-alone contextual adtech nor just "basically FLOC 2.0" (Schiff 2022). However Topics does share with FLoC the notion that most calculative work will occur on-browser. There will be no centralized storage of user data and site-owners will not be able to see the topics assigned to users etc. (The Topics API). The purpose of all this, of course, is to auction personalized ad space in virtually real time as users move across the Internet, but this is not now proposed to be done with Topics itself but with another adtech, FLEDGE.

"FLEDGE" (an acronym for "First Locally-Executed Decision over Groups Experiment") emerged rom out of another section of the Privacy Sandbox, TURTLEDOVE. Although its development began much earlier, FLEDGE was publicly announced just after Topics, with none of the same fanfare, and received comparatively little immediate notice. This might have been intentional as FLEDGE has greater similarities to FLoC than does Topics and presents many potential privacy concerns, and because FLEDGE had been in development for almost a year there was already substantial amount of information about it on github and elsewhere.

FLEDGE is aimed at allowing advertisers to market to users on other websites that the advertiser has deemed is interested in their product, without third-party cookies (Dutton, 2022). For example, if someone visited nike.com, and then later visited an ad-funded site, CNN.com, FLEDGE would allow Nike to identify them as a consumer interested in their product, influencing their real time ad bid (Dutton, 2022). The removal of third-party-cookies in this process would maintain the status quo of cross-site advertising (known as remarketing) while removing the ability for third parties to track users' browsing behavior across the web (Dutton, 2022).

The operation of FLEDGE is relatively simple. When a user visits a website such as nike.com, Nike requests that the user's browser be added to an interest group called "Nike shoes" (Dutton, 2022). The user's browser may remain a member of this interest group for up to 30 days (Dutton, 2022). If the website uses a third party ad-tech company, the third party company may request that the browser be added to a more general interest group such as "athletic wear" (Dutton, 2022). When the user visits CNN.com, a real-time ad auction is held on the user's browser (Dutton, 2022). When the auction begins, bidding codes are extracted from each interest group to which the browser is assigned (Dutton, 2022). The bidder receives data from their trusted server, which cannot log any information about the bidding process or user (Dutton, 2022). Each bidder then makes a bid, along with a presented ad, which are scored and ranked on the user's browser to determine a winning ad (Dutton, 2022).

3. Discussion: Surveillance capitalism and targeted advertising

We have described the short life of FLoC, and the regulatory responses to the deceased adtech. We will now consider this as a vehicle to explore a possible shift in the political economy of Google. At the conjunction of the multiple histories that one can bring to bear on Google is a logic of accumulation that Shoshana Zuboff (2015, 2019) called "surveillance capitalism." Although Foster and McChesney (2014) used the same phrase to refer to a more generalized description of contemporary capitalism underpinned by ubiquitous surveillance, Zuboff focused on what she identified as a novel technique pioneered by Google, later adopted by others particularly Facebook (Zuboff, 2019).

In contrast to earlier Autonomist Marxist scholars like Mauricio Lazzarato (1996), Tiziana Terranova (2000) and social media researchers like Nicole Cohen (2008), who considered online activity as a labor relationship, Zuboff concentrated on the "data exhaust" from human social interaction online: all the data generated in acts of communication, sharing and movement on the internet (Zuboff, 2019). Simply stated, 'Facebook and Google provide a free service to users in exchange for the use of their data' (Houser & Voss, 2018, p. 5).

Google's innovation was to find ways to link this data to individual identifiers, allowing the use of algorithms to predict users' behaviour (Zuboff, 2019). From this, Google produced profiles and secondary data products that could be packaged and sold to advertisers as "behavioral futures" (Zuboff, 2019). This allowed companies to market directly to subjects they believed most susceptible, making the marketing process far more efficient (Zuboff, 2019). Through what Callon and Muniesa (2005) term "calculative power," Google has established a dominant position over the means of production of knowledge from data so lucrative that, in addition to being the preeminent provider of online search services, it has become consistently the world's largest adtech company – challenged only by Facebook, the earliest adopter of Google's techniques (Cramer-Flood, 2021).

Zuboff was hardly the first to notice the political economic significance of these new adtech practices. For example, Christian Fuchs had produced a clear political economic account of "Google Capitalism" in 2012 which, although short, includes many of the elements later attributed to Zuboff. More generally, the encompassing power of platform corporations had already been outlined by Greg Elmer in his book *Profiling Machines* (2003), Mark Andrejevic (2007) and Tarleton Gillespie (2010) among many others. There are also other terms available that emphasize different aspects of the relationship between surveillance, data, corporate form and capitalism, for example Srnicek's "platform capitalism" (2017), West's "data capitalism" (2019) or Sadowski's "digital capitalism" (2020).

Further, the enclosure and manipulation of knowledge has always been crucial to capitalism, and indeed modernity, in general. Both the accurate identification and categorization of people were crucial to evaluation of creditworthiness in the C19th (Lauer, 2017). As advertising gave way to more complex ways of marketing, particularly Customer Relationship Management (CRM), the centrality of surveillance to capitalism became ever more obvious (Arvidsson 2003; Elmer, 2003; Pridmore & Zwick, 2011, Murakami Wood & Ball, 2013). Google only supercharged this existing trajectory and developed the tools to allow its automation online (see: Darmody & Zwick, 2020). This process continues to expand and reach into new areas as datafication intensifies (Van Dijk, 2014). As Murakami Wood and Ball (2013, p. 4) argued, building on social theorists of markets, particularly Michel Callon (1999), 'the operation of markets is underpinned by the gathering and exchange of knowledge and information, as much as it is by products and money.' Insofar as capitalism has depended upon these things, it has always been surveillance capitalism, and as Keith Breckenridge (2020) has more recently argued, it is impossible to conceive of digital capitalism without surveillance.

We maintain that FLoC was an early, small and faltering mis-step along a potential path away from Zuboff's particular model of surveillance capitalism, where the main value proposition is targeted advertising, to a system where developing AI is the main driver. We identify four factors influencing this path: 1. corporate ideology; 2. market pressures; 3. regulatory regimes; and 4. internal cultural controversies. However, we do not claim that these factors are equally influential at all times, and we have already made clear the critical role of regulatory regimes in the case of FLoC.

3.1. Corporate ideology

As one of us has argued previously with regard to Facebook, it would be a mistake to disregard platform corporations' long-term ideological drivers (Author 2019). Their founders and CEOs have goals beyond the balance sheet, and their ideologues regard themselves as being part of an accelerating civilizational transformation (see: Author, forthcoming).

From this perspective, we must take seriously Alphabet's own long-term ideological goal and the strategic movement towards becoming an "AI-first" company, involving the infrastructurization of AI and building Google's AI into the ways in which everyone uses the Internet and computing. It is only by ignoring this ideological goal that one can claim that Google is simply or primarily "an advertising company" because that is the most lucrative aspect of what they do *now*. Google is not simply an advertising company, however much of its revenue it has derived, and still derives, from adtech. It is an organization that has leveraged surveillance technologies to accumulate both big data and capital, to enable the corporation to pursue its longer term goal of embedding AI in everything, of creating a platform for the future governance of the planet. Through the development of this comprehensive deployment of AI to solve all human problems, Alphabet is intent on providing what Benjamin Bratton (2014) calls the planetary "stack" with its operating system, "planetary sapience" (Bratton, 2021).

This begins with AI in all consumer devices. During Google's 2017 I/O CEO Sundar Pichai introduced the AI-First strategy (Google, 2017). This includes a focus on integrating AI into all of their products, as well as investing in long term AI infrastructure and developing AI applications that could directly assist consumers and businesses (Google, 2017). The change in the company's goals can be further observed through Pichai's statement at the 2019 I/O proclaiming that "We are moving from a company that helps you find answers to a company that helps you get things done" (Pangambam, 2020). The transition to AI-First has since been confirmed in multiple statements ranging from Alphabet's investor calls to financial reports since their 2017 announcement.

3.2. Market pressures

Targeted advertising has produced immense wealth for tech companies, however AI is potentially *far* more lucrative, on an accelerating pace to overtake the global valuation of the advertising sector (Authors 2021). All of the adtech systems we have considered (FLoC, FLEDGE and Topics) coming out of Google's Privacy Sandbox, share an underpinning current or proposed future reliance on AI.

In the AI-driven model, instead of using consumer data to sell services to third parties, data will be used to improve AI applications that can then be sold as stand alone products, or as incentives to buy hardware products. If forced to choose between targeted advertising and AI as a service, AI would be the better economic bet. Although Zuboff considers advertising and marketing as the major economic driver of surveillance capitalism, it is impossible to ignore the fact that computer hardware generates several times more revenue, about $900Bn globally (Grandview Research, 2021). Hardware and software matter because the ability for hardware to compete in the marketplace may soon be tied to AI that enhances its user experience.

However, the proposed shift towards a focus on AI creates new surveillance pressures even as surveillance-driven advertising declines, because greater access to personal information is required to create more effective and personalized AI. In the case of virtual assistants, a product Google views as the key to their success in consumer and business hardware (Google, 2017), the data collected for the training of AIs includes all requests made to the assistant. In many cases this information is highly sensitive. Other wearable technologies such as smart watches are collecting ever greater information on their user such as their heart rate and other biometric data. The scope of data collection will expand still further as computing becomes ubiquitous, pervasive or ambient. Ambient computing, and its potential, was described by Google's head of hardware at their *Made by Google* event in 2019:

> It's super useful to have a powerful computer everywhere you are. But it's even more useful when computing is anywhere you need it, always available to help ... that helpful computing can be all around you: ambient computing. Your devices work together with services and AI, so help is anywhere you want it, and it's fluid. The technology just fades into the background when you don't need it. So

> the devices aren't the center of the system, you are. That's our vision for ambient computing. (Made by Google 2019)

The extent of data that may be collected in such a system, and Google's hardware ambitions, both appear to be unlimited.

3.3. Regulatory regimes

Google's surveillance marketing power did not simply spring from internal innovation or some ideological will-to-power. The particular regulatory environment in which it emerged is crucial. For some time now, there has been debate over different national forms of capitalism (see: Radice, 2000), and how these, and other historical, political and cultural differences produce different "regulatory regimes" (see e.g. Eberlein & Grande, 2005). Google's techniques were developed in the permissive neoliberal capitalist legal environment of the USA, and the historical unwillingness of government in the USA to intervene in the market, especially in ways which would disadvantage American success stories. As Houser and Voss (2018, p. 22) observe, the USA creates a unique situation for platform corporations to flourish:

> 'While the European Union focuses on protecting human rights and social issues, the U.S. seems to be concerned with providing a way for companies collecting information to use that information while balancing the privacy rights that consumers expect.'

But even that supposed balance is tilted towards business: a 2011 Congressional Research Service Report stated that 'the large-scale collection, analysis, and storage of personal information is central to the Internet economy; and that regulation of online personal information must not impede commerce' (Stevens, 2011 in Houser & Voss, 2018, p. n86). This is even more true when the issue of geopolitical competition with China is factored in, and AI is at the heart of future strategic considerations in this area, which has made Eric Schmidt, Google's former CEO, one of the most influential behind-the-scenes movers in US government in areas from national infrastructure to military procurement (Wolfe, 2021).

The largest platform corporations are now often considered powerful enough to exist alongside rather than inside particular jurisdictions, and constitute their own category of regulatory regime, as Karen Yeung argues with her development of the concept of regulation through the design process (Yeung 2017, see also Pasquale 2017), and Geradin et al. (2021) go further to argue that the Privacy Sandbox itself shows Google operating as a privacy regulator. Inasmuch as Zuboff has a theory of regulation, it would appear that her position is one of extreme 'regulatory capture', (see: Dal Bó, 2006), wherein the regulatory authority simply sees the interests of corporations as their own. But, as as we have already argued in the case of FLoC, this is challenged by the crucial role of the EU GDPR, and by an emerging American cross-party alliance around the need to control social media companies and targeted advertising.

As Linnet Taylor (2021) argues, 'The current challenges of governing technology demonstrate that data policy is not only economic policy: it is social policy that belongs in the political sphere.' and that this should involve re-regulation rather than deregulation and privatization, 'to make government explicitly responsible for what happens to data with effects on the population level' bolstered by 'thick forms of legitimacy.' As data collection has become ever more intrusive and intimate, and despite platform corporate mystification, surveillance and personal data privacy issues have indeed become major concerns in the USA (Auxier, 2020). Recent studies on AI assistants have also demonstrated that privacy concerns and lack of trust are a barrier for user adoption (Vimalkumar et al., 2021).

Google has a significant advantage over other platform corporations with regards to trust. A recent (US-based) survey from The Verge magazine awarded Google a 90% approval rating from the public, even more than Apple or Amazon (Lopatto 2021). However any new law to control surveillance advertising, like that proposed by the US House of Representatives (see above), would still hit Google harder than any other platform corporation. And this will not be compensated for entirely by Google's current direction: with the forthcoming EU AI Regulation (see: Veale & Borgesius, 2021, for an analysis of the draft proposal), further controversy is inevitable even for an "AI-First" company.

3.4. Internal cultural conflict

In their book, *How Google Works* (2014) Eric Schmidt and Jonathan Rosenberg emphasized the Darwinian innovation principles deployed by the company, particularly "the freedom … to succeed (or fail) on their own" granted to the many spin-off companies under the Alphabet umbrella. Like much development within Google, the Privacy Sandbox is explicitly such a Darwinian experiment. So, perhaps no-one should be surprised about the demise of one piece of adtech even one, like FLoC, which was announced with such fanfare.

However, this self-confidence in the process of innovation has been severely damaged lately not just by external regulation response, but by internal conflict over sociocultural assumptions and biases that Alphabet, like almost all platform corporations, has so far failed to deal with. This has involved disputes over unionization (CWA, 2021) and the engagement of Google with the US military (Shane & Wakabayashi, 2018), and a bitter struggle over Google's failure to develop genuine AI Ethics, that has, at the time of writing, led to five of the most senior AI ethicists and tech developers in this field, led by Timnit Gebru, leaving Google and creating the explicitly anti-Big Tech, Distributed AI Research Institute (DAIR).

There are also indications that adtech itself is not the cutting-edge draw into the industry that it once was. In the course of our research, we have heard from anonymous insiders in platform corporations that new recruits are increasingly dubious about surveillance-based programs.[5] This seems to back up tech media reports of both lower recruitment and higher attrition in adtech firms (Hersher 2019).

4. Conclusion

Google is attempting both to comply with diverse and increasingly restrictive regulatory regimes and celebrate privacy gains by moving away from third-party cookies, but simultaneously to continue surveillance-based marketing using the AI-driven products of their Privacy Sandbox. FLoC was important as a first, albeit failed step towards allowing Google to maintain a pretense of privacy, while still profiling subjects at a deep level, and may come to represent Google's last ditch effort to maintain their competitive advantage in the online ad space through "behavioral futures." As public perception and regulation have shifted against targeted advertising, market forecasters have perceived a corresponding industry shift towards contextual advertising, accelerated by the proposed end of third-party cookies (Winterberry Group, 2021).

Topics and FLEDGE are new steps on the same path. Neither FLEDGE nor Topics produce "behavioral futures" instead revealing users' most recent past, or almost-real-time interests, and neither require the large scale collection of user data to function. However, there are significant surveillance concerns.

First, like web beacons, with enough independent websites deploying FLEDGE, Google could continue to track users across the web, even though the user's data would be more secure from third parties. We

[5] We are, for obvious reasons, unable to name either the individuals or the corporations concerned.

should be very wary of any claims about anonymization. Second, technologies like FLEDGE would also accentuate Google's information dominance and are aimed at making Google the sole trusted guardian (and therefore exploiter) of user data. This alone presents a compelling reason in itself why Alphabet needs to be contained and perhaps even broken up. Third, categorization systems like Topics and FLEDGE could easily potentially perpetuate or even intensify socially unjust practices such as "digital redlining" (Gilliard & Culik, 2016) whereby, for example, Black and low-income users could be placed into stereotypically constructed interest groups by third parties geared towards advertising predatory products such as payday loans. Fourth, given the recent announcement of the Topics API for Android (Chavez, 2022), it is unclear if topics assigned from users' browsing histories will be used in selecting advertising within Android applications, which would be a significant departure from current practices. Data used for targeting advertisements should not be shared across technological ecosystems.

Regardless, targeted advertising will not cease immediately, and while regulatory regimes may determine the fate of particular adtech innovations like FLoC, they do not constitute overall farming conditions for Alphabet/Google. The market is not yet generating incentives to shift focus *entirely*, especially in regulatory regimes that are more permissive than the EU and USA. Advertising is however likely to become a decreasingly significant segment of Alphabet's portfolio as bets on AI open lucrative revenue streams in sectors such as hardware, healthcare and education. But in the immediate term, Google is likely to leverage its AI advantage to generate competitive advantage in the new "privacy-centric" ad-space, even as it moves away from advertising in the long-term.

In the longer term, if FLoC was a misstep, market forces and corporate ideology are continuing to push Alphabet/Google down the path towards an AI-driven future. Their surveillance and data collection practices will continue, but less for advertising and more to build AI-driven products and services, and this is likely to require far more data than targeted advertising, and collected with far greater frequency. In this context, we have not seen the last of federated learning. It is possible that federated learning could present a privacy-centric way to develop useful ML algorithms on end-user data, but much of the data for the most attractive potential markets (e.g. health care and education) are also more intimate and sensitive. By shifting economic and ideological rationales for surveillance and data accumulation towards an "AI-first" position, an intensified and extended set of ethical, legal, political and social challenges will emerge around surveillance, security, privacy and data protection, that are not yet adequately addressed in current debates and regulations, either singularly or in their cumulative social and political effects. Certainly, no invasion of privacy or over-intrusive collection of personal information is in itself better or more justified just by virtue of being for training AI.

Acknowledgments

The Open Access publication of this paper was supported by the Panelfit project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

References

Alphabet Earnings Call. (2019). Alphabet Inc (GOOG) (GOOGL) Q2 2019 Earnings Call Transcript, *The Motley Fool*. [accessed 6 January, 2022] https://www.fool.com/earnings/call-transcripts/2019/07/25/alphabet-inc-googl-q2-2019-earnings-call-transcrip.aspx.

Alphabet Inc. (2022). *Alphabet Announces Fourth Quarter and Fiscal Year 2021 Results*. Retrieved from https://abc.xyz/investor/static/pdf/2021Q4_alphabet_earnings_release.pdf.

Andrejevic, M. (2007). Surveillance in the digital enclosure. *The Communication Review*, *10*(4), 295–317.

Andrew, J., & Baker, M. (2021). The General Data Protection Regulation in the age of surveillance capitalism. *Journal of Business Ethics*, *168*(3), 565–578.

Arvidsson, A. (2003). On the 'Pre-History of The Panoptic Sort': Mobility in Market Research. *Surveillance & Society*, *1*(4). https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3331.

Author (2019).

Author (forthcoming).

Authors (2021).

Auxier, B. (2020). How Americans see digital privacy issues amid the COVID-19 outbreak, *Pew Research Center*, 4 May. [accessed 4 February 2022] https://www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/.

Bennett, C.J. (2018). The European General Data Protection Regulation: An instrument for the globalization of privacy standards? *Information Polity*, *23*(2), 239–246.

Bennett, C.J. (2001). Cookies, web bugs, webcams and cue cats: Patterns of surveillance on the world wide web. *Ethics and Information Technology*, *3*(3), 195–208.

Bindra, C. (2021). Building a privacy-first future for web advertising. 25 January. [accessed 4 February 2022] https://blog.google/products/ads-commerce/2021-01-privacy-sandbox/.

Bohn, D. (2020). Google to 'phase out' third-party cookies in Chrome, but not for two years. The Verge. 14 January. [accessed 4 February 2022] https://www.theverge.com/2020/1/14/21064698/google-third-party-cookies-chrome-two-years-privacy-safari-firefox.

Bratton, B. (2021). Planetary Sapience. *Noema*. 17 June. [accessed 4 February 2022] https://www.noemamag.com/planetary-sapience/.

Bratton, B. (2016). *The Stack: On software and sovereignty*. MIT Press.

Breckenridge, K. (2020). Capitalism without surveillance? *Development and Change*, *51*(3), 921–935.

Built With. (2021). Google Analytics Usage Statistics. [accessed 4 February 2022] https://trends.builtwith.com/analytics/Google-Analytics.

Burgess, M. (2021). Google's Grand Plan to Eradicate Cookies Is Crumbling, *WIRED UK*, 30 April. [accessed 4 February 2022] https://www.wired.com/story/googles-grand-plan-to-eradicate-cookies-is-crumbling/.

Callon, M. (ed.) (1998). *The Laws of the Markets*. Blackwell.

Callon, M., & Muniesa, F. (2005). Peripheral vision: Economic markets as calculative collective devices. *Organization Studies*, *26*(8), 1229–1250.

Chavez, A. (2022, February 16). *Introducing the Privacy Sandbox on Android*. Google. Retrieved March 29, 2022, from https://blog.google/products/android/introducing-privacy-sandbox-android/.

Çınar, N., & Ateş, S. (2022). Data Privacy in Digital Advertising: Towards a Post Third-Party Cookie Era, in Filimowicz, M. (Ed.) *Privacy: Algorithms and Society*, Routledge.

Communication Workers of American (CWA). (2021). Google Workers, Demanding Change at Work, Are Launching a Union With the Communications Workers of America. Press Release. 4 January. [accessed 4 February 2022] https://cwa-union.org/news/releases/google-workers-launch-union-with-cwa.

Cramer-Flood, E. (2021). Duopoly still rules the global digital ad market, but Alibaba and Amazon are on the prowl. *eMarketer*. 10 May. [accessed 4 February 2022] https://www.emarketer.com/content/duopoly-still-rules-global-digital-ad-market-alibaba-amazon-on-prowl.

Cyphers, B. (2021). Google's Floc is a terrible idea. *Electronic Frontier Foundation*. 9 April. [accessed 4 February 2022] https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea.

Dal Bó, E. (2006). Regulatory capture: A review. *Oxford Review of Economic Policy*, *22*(2), 203–225.

Darmody, A., & Zwick, D. (2020). Manipulate to empower: Hyper-relevance and the contradictions of marketing in the age of surveillance capitalism. *Big Data & Society*, *7*(1), 2053951720904112.

Dutton, S. (2022). *The Fledge API*. Chrome Developers. [accessed 4 February 2022] https://developer.chrome.com/docs/privacy-sandbox/fledge/#interest-group-detail.

Eberlein, B., & Grande, E. (2005). Beyond delegation: transnational regulatory regimes and the EU regulatory state. *Journal of European Public Policy*, *12*(1), 89–112.

Elmer, G. (2003). *Profiling Machines: Mapping the personal information economy*. MIT Press

Eshoo, Congresswoman Anna G. (2022) Eshoo, Schakowsky, Booker Introduce Bill to Ban Surveillance Advertising. Press Release. 18 January. [accessed 4 February 2022] https://eshoo.house.gov/media/press-releases/eshoo-schakowsky-booker-introduce-bill-ban-surveillance-advertising.

Facebook. (n.d). What Information Does Facebook Get When I Visit a Site with the like Button?: *Facebook Help Center* [accessed 4 February 2022] www.facebook.com/help/186325668085084/.

Foster, J.B., & McChesney, R.W. (2014). Surveillance capitalism: Monopoly-finance capital, the military-industrial complex, and the digital age. *Monthly Review*, *66*(3), 1.

Fou, A. (2020). No more third party cookies, no Problemo. *Forbes*. 31 August. [accessed 4 February 2022] https://www.forbes.com/sites/augustinefou/2020/08/31/no-more-third-party-cookies—good-or-bad-news/.

Fuchs, C. (2012). Google capitalism. *tripleC: Open Access Journal for a Global Sustainable Information Society*, *10*(1), 42–48.

Geradin, D., Katsifis, D., & Karanikioti, T. (2021). Google as a de facto privacy regulator: Analysing the Privacy Sandbox from an antitrust perspective. *European Competition Journal*, *17*(3), 617–681.

Ghosh, D. (2018). How GDPR will transform digital marketing. *Harvard Business Review Digital Articles* 21 May. [accessed 4 February 2022] https://hbr.org/2018/05/how-gdpr-will-transform-digital-marketing.

Gillespie, T. (2010). The Politics of "Platforms". *New Media & Society*, *12*(3), 347–364.

Gilliard, C., & Culik, H. (2016). Digital redlining, access, and privacy. *Common Sense Education*, *24*.

Google. (2017). *Google I/O keynote (google I/O '17)*. YouTube. Retrieved January 26, 2022, from https://www.youtube.com/watch?v=Y2VF8tmLFHw.

Google-Research. (n.d). *WICG/FLoCs*. GitHub. Retrieved December 8, 2021 https://github.com/WICG/floc.

Herscher, J. (2019). Is It The End Of An Era For Ad Tech OGs? *AdExchanger* 2 May. [accessed 4 February 2022] https://www.adexchanger.com/online-advertising/is-it-the-end-of-an-era-for-ad-tech-ogs/.

Houser, K.A., & Voss, W.G. (2018). GDPR: The end of Google and Facebook or a new paradigm in data privacy. *Rich. JL & Tech.*, *25*, 1.

Lauer, J. (2017). *Creditworthy*. Columbia University Press.

Lazzarato, M. (1996). Immaterial labor. In *Radical Thought in Italy: A Potential Politics*, *1996*, pp. 133–47.

LeClair, D. (2022). Everyone Hated Google's FLoC, and Now It's Dead, *HowToGeek*, 25 February. [accessed 4 February 2022] https://www.howtogeek.com/781793/everyone-hated-googles-floc-and-now-its-dead/.

Li, H., Yu, L., & Wu, H. (2019). The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management*, *22*(1), 1–6,

Lopatto, E. (2021). Verge Tech Survey 2021. *The Verge*. 6 October. [accessed 4 February 2022] https://www.theverge.com/2021/10/6/22702798/verge-tech-survey-2021-trust-privacy-security-facebook-amazon-google-apple-pandemic.

Lyden, C. (2021). Google's current FLoC tests aren't GDPR compliant. *SearchEngineLand*, 23 March. [accessed 4 February 2022] https://searchengineland.com/googles-current-floc-tests-arent-gdpr-compliant-347168.

McMahan, B., & Ramage, D. (2017). Federated Learning: Collaborative Machine Learning without Centralized Training Data. *Google AI Blog*, 6 April. [accessed 4 February 2022] https://ai.googleblog.com/2017/04/federated-learning-collaborative.html.

Manku, G.S., Jain, A., & Das Sarma, A. (2007). Detecting near-duplicates for web crawling. In *Proceedings of the 16th International Conference on World Wide Web*, pp. 141–150.

Murakami Wood, D., & Ball, K. (2013). Brandscapes of control? Surveillance, marketing and the co-construction of subjectivity and space in neo-liberal capitalism. *Marketing Theory*, *13*(1), 47–67.

Pangambam, S. (2020). Sundar Pichai at Google I/O 2019 Keynote (Full Transcript). *The Singju Post*, 13 June. [accessed 4 February 2022] https://singjupost.com/sundar-pichai-at-google-i-o-2019-keynote-full-transcript/.

Pasquale, F. (2017). From Territorial to Functional Sovereignty: The Case of Amazon. *Law and Political Economy*, 6 December. [accessed 4 February 2022] https://lpeblog.org/2017/12/06/from-territorial-to-functional-sovereignty-the-case-of-amazon/.

Post, R.C. (2017). Data privacy and dignitary privacy: Google Spain, the right to be forgotten, and the construction of the public sphere. *Duke LJ*, *67*, 981.

Pridmore, J., & Zwick, D. (2011). Marketing and the rise of commercial consumer surveillance. *Surveillance & Society*, *8*(3), 269–277.

Privacy Sandbox. (n.d.). *Technology for a more private web*. The Privacy Sandbox. Retrieved March 29, 2022, from https://privacysandbox.com/.

Radice, H. (2000). Globalization and national capitalisms: Theorizing convergence and differentiation. *Review of International Political Economy*, *7*(4), 719–742.

Russell, S. (2019). *Human compatible: Artificial intelligence and the problem of control*. Penguin.

Sadowski, J. (2020). *Too Smart: How digital capitalism is extracting data, controlling our lives, and taking over the world*. MIT Press.

Schiff, A. (2022). Meet Topics API, Google's Latest Addition To The Privacy Sandbox (It's Basically FLoC 2.0) *AdExchanger*, 25 January. [accessed 4 February 2022] https://www.adexchanger.com/privacy/meet-topics-api-googles-latest-addition-to-the-privacy-sandbox-its-basically-floc-2-0/.

Schiff, A. (2021a). Google Claims FLoCs Can Be Nearly As Effective As Cookie-Based Ads. *AdExchanger*, 25 January. [accessed 4 February 2022] https://www.adexchanger.com/online-advertising/google-claims-flocs-can-be-nearly-as-effective-as-cookie-based-ads/.

Schiff, A. (2021b). Google Will Not Run FLoC Origin Tests In Europe Due To GDPR Concerns (At Least For Now) *AdExchanger*, 23 March. [accessed 4 February 2022] https://www.adexchanger.com/platforms/google-will-not-run-floc-origin-tests-in-europe-due-to-gdpr-concerns/.

Schmidt, E., & Rosenberg, J. (2014). *How Google Works*. Grand Central.

Shane, S., & Wakabayashi, D. (2018). 'The business of war': Google employees protest work for the Pentagon. *The New York Times*. 4 April. [accessed 4 February 2022] https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html.

Southern, L., & Perloff, C. (2022). Google's FLoC 2.0, Topics, Trade Effectiveness for Privacy Compliance. *AdWeek*. 25 January. [accessed 4 February 2022] https://www.adweek.com/programmatic/googles-flocs-2-0-topics-trades-effectiveness-for-privacy-compliance/.

Srnicek, N. (2017). *Platform Capitalism*. Polity.

Surveillance Self Defence. (2020). What is Fingerprinting? 14 July. [accessed 4 February 2022] https://ssd.eff.org/en/module/what-fingerprinting.

Taylor, L. (2021). Public actors without public values: legitimacy, domination and the regulation of the technology sector. *Philosophy & Technology*, 1–26.

Terranova, T. (2000). Free labor: Producing culture for the digital economy. *Social Text*, *18*(2), 33–58.

The Chromium Projects. (n.d.). *The Privacy Sandbox*. [accessed 4 February 2022] https://www.chromium.org/Home/chromium-privacy/privacy-sandbox.

The Topics API. (2022). Jkarlin/topics. *GitHub*. [accessed 4 February 2022] https://github.com/jkarlin/topics.

Truong, N., Sun, K., Wang, S., Guitton, F., & Guo, Y. (2021). Privacy preservation in federated learning: An insightful survey from the GDPR perspective. *Computers & Security*, *110*, 102402.

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197–208.

Vimalkumar, M., Sharma, S.K., Singh, J.B., & Dwivedi, Y.K. (2021). 'Okay Google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants. *Computers in Human Behavior*, *120*, 106763.

Veale, M., & Borgesius, F.Z. (2021). Demystifying the Draft EU Artificial Intelligence Act – Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International*, *22*(4), 97–112.

West, S.M. (2019). Data capitalism: Redefining the logics of surveillance and privacy. *Business & Society*, *58*(1), 20–41.

Winseck, D. (2020). Vampire squids, 'the broken internet' and platform regulation. *Journal of Digital Media & Policy*, *11*(3), 241–282.

Winterberry Group. (2021). The Outlook for Contextual Solutions in Data Driven Advertising & Marketing. *Winterberry Group Insights Library*. [accessed 4 February 2022] https://www.winterberrygroup.com/insights-library/the-evolution-of-customer-journey-management-2021-pxe9t.

Wolfe, F. (2021). Eric Schmidt to Helm National Artificial Intelligence/Emerging Technologies Project, *Defense Daily* 10 May. [accessed 4 February 2022] https://www.defensedaily.com/eric-schmidt-to-helm-national-artificial-intelligence-emerging-technologies-project/advanced-transformational-technology/.

Yeung, K. (2017). 'Hypernudge': Big Data as a mode of regulation by design. *Information, Communication & Society*, *20*(1), 118–136.

Zarsky, T.Z. (2016). Incompatible: The GDPR in the age of big data. *Seton Hall L. Rev.*, *47*, 995.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The fight for a human future at the new frontier of power*. Profile Books.

Zuboff, S. (2015). Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, *30*(1), 75–89.

Authors biographies

David Eliot is an MA student in the Department of Sociology, Queen's University at Kingston, Canada. From September 2022 he will be a PhD student in the Department of Criminology at the University of Ottawa. His work examines the advent of AI-driven platform economies.

David Murakami Wood is Director of the Surveillance Studies Centre and Associate Professor in the Department of Sociology, Queen's University at Kingston, Canada. From July 2022, he will be the Professor of Critical Surveillance and Security Studies at the University of Ottawa. His work covers planetary surveillance, smart technologies and smart cities, the future of platforms, security intelligence agencies, and global cities, particularly Tokyo.