1-26-2022

Privacy Considerations for Online Advertising: A Stakeholder’s Perspective to Programmatic Advertising

Dylan A. Cooper
California State University, Channel Islands

Taylan Yalcin
California State University, Channel Islands

Cristina Nistor
Chapman University, nistor@chapman.edu

Matthew Macrini
California State University, Channel Islands

Ekin Pehlivan
California State University, Channel Islands

Recommended Citation

Cooper, D.A., Yalcin, T., Nistor, C., Macrini, M. and Pehlivan, E. (2022), "Privacy considerations for online advertising: a stakeholder’s perspective to programmatic advertising", *Journal of Consumer Marketing*. https://doi.org/10.1108/JCM-04-2021-4577

Privacy Considerations for Online Advertising: A Stakeholder's Perspective to Programmatic Advertising

Privacy considerations for online advertising: A stakeholder's perspective to programmatic advertising

Cooper, Dylan; Yalcin, Taylan; Nistor, Cristina; Macrini, Matthew; Pehlivan, Ekin[*]

Forthcoming in Journal of Consumer Marketing (DOI 10.1108/JCM-04-2021-4577)

Purpose

Privacy considerations have become a topic with increasing interest from academics, industry leaders, and regulators. In response to consumers' privacy concerns, Google announced in 2020 that Chrome would stop supporting third-party cookies in the near future. At the same time, advertising technology companies are developing alternative solutions for online targeting and consumer privacy controls. In this paper, we explore privacy considerations related to online tracking and targeting methods used for programmatic advertising (i.e., third-party cookies, Privacy Sandbox, Unified ID 2.0) for a variety of stakeholders: consumers, AdTech platforms, advertisers, and publishers.

Design/methodology/approach

We analyze the topic of internet user privacy concerns, through a multi-pronged approach: industry conversations to collect information, a comprehensive review of trade publications, and extensive empirical analysis. We use two methods to collect data on consumer preferences for privacy controls: a survey of a representative sample of US consumers and field data from conversations on web-forums created by tech professionals.

Findings

Our results suggest that there are four main segments in the US internet user population. The first segment, consisting of 26% of internet users, is driven by a strong preference for relevant ads and includes consumers who accept the premises of both Privacy Sandbox and UID 2.0. The second segment (26%) includes consumers who are ambivalent about both sets of premises. The third segment (34%) is driven by a need for relevant ads and a strong desire to prevent advertisers from aggressively collecting data, with consumers who accept the premises of Privacy Sandbox but reject the premises of UID 2.0. The fourth segment (15% of consumers) rejected both sets of premises about privacy control. Text analysis results suggest that the conversation around UID 2.0 is still nascent. Google Sandbox associations seem nominally positive, with sarcasm being an important factor in the sentiment analysis results.

Originality

The value of this paper lies in its multi-method examination of online privacy concerns in light of the recent regulatory legislation (i.e., GDPR and CCPA) and changes for third-party cookies in browsers such as Firefox, Safari, and Chrome. Two alternatives proposed to replace third-party cookies (Privacy

[*] Dylan Cooper is Associate Professor of Management at CSU Channel Islands. Taylan Yalcin is Assistant Professor of Marketing at CSU Channel Islands. Matthew Macrini is a graduate student at CSU Channel Islands. Cristina Nistor is Clinical Assistant Professor of Marketing at Chapman University. Ekin Pehlivan (corresponding author ekin.pehlivan@csuci.edu) is Associate Professor of Marketing at CSU Channel Islands. We thank the review team of Journal of Consumer Marketing for helpful feedback. All errors are our own.

Sandbox and Unified ID 2.0) are in the proposal and prototype stage. The elimination of third-party cookies will affect stakeholders, including different types of players in the AdTech industry and internet users. We analyze how two alternative proposals for privacy control align with the interests of several stakeholders.

Keywords: privacy, online tracking, third-party cookies, Unified ID 2.0, Privacy Sandbox, programmatic advertising

Introduction

Privacy concerns have an impact on consumer's spending habits (Maseeh *et al.* 2021; Spake *et al.*, 2011) as well as their willingness to share information online. Thus, privacy considerations are an important topic for marketers and academic researchers, who focus on online information privacy (Acquisti *et al.*, 2012; Akhter, 2014; Fehrenbach and Herrando, 2021; Martin *et al.*, 2017). Previous research has emphasized the need to analyze the separate stakeholder interests and reactions to privacy concerns (Appel *et al.*, 2020; Martin and Murphy, 2017; Mascarenhas *et al.*, 2003; Sheehan and Hoy, 1999). As tracking methods for programmatic advertising become more varied, privacy considerations affect each consumer's everyday decisions as a consumer logs onto a website or uses a search engine (Brough and Martin, 2021; Graeff and Harmon, 2002; Hong *et al.*, 2021; Phelps *et al.*, 2000).

In January 2020, Google announced that their Chrome internet browser would no longer support third-party cookies, which are unique identifiers placed on browsers by advertising technology companies (Graham, 2021) in 2022. Following industry and regulator discussions on privacy concerns, this deadline was later extended to 2023[[i]]. Regulation on privacy controls has an impact on the effectiveness of targeted advertising campaigns, as documented by Goldfarb and Tucker (2011). Cookies are an important part of targeted online ads: 52% of advertising revenue can disappear for a publisher if a customer disables these cookies (Lardinois, 2019). Chrome holds a 66% market share (StatCounter, 2021), which implies that Google's action would fundamentally change the AdTech business both for consumers and advertisers (Graham, 2021) but also for regulators who are balancing the need for consumer privacy control versus the anticompetitive effects that banning cookies may have on Google's ad competitors (Robertson and Brandom, 2021; Shields, 2021). Google's proposed solution is Privacy Sandbox, a set of software tools under development that allow individually targeted advertising while protecting user anonymity. Although welcomed by some, Privacy Sandbox has been criticized as a way to lock advertisers into Google’s online advertising ecosystem and to prevent brands from conducting in-house customer analytics and measurement of online advertising effectiveness (Glueck, 2021). Several advertising technology competitors, such as LiveRamp and The Trade Desk, are developing alternative solutions in order to give consumers more options for privacy controls and to maintain independence from Google (Graham, 2021).

Our study explores privacy considerations related to targeting and tracking methods used for programmatic advertising (i.e., third-party cookies, Privacy Sandbox, Unified ID 2.0, etc.) for a variety of stakeholders: the consumers, AdTech platforms, advertisers, and publishers. We explore this topic through a multi-pronged approach: anecdotes from a variety of industry events, a comprehensive review of trade publications on the topic, and empirical analysis of two large datasets about consumer privacy attitudes. We use two separate methods to collect data on consumer’s privacy concerns. First, we collect data on consumer attitudes on the current and projected landscape of privacy controls by using a large online survey on a representative sample of the US consumer population. We employ several statistical methods to analyze the consumer attitudes expressed in the survey. Our empirical results suggest that there are currently four main segments in the US internet user population whose widely different privacy preferences should be considered in the development of any new privacy regulation. Second, we collect a dataset of web forum (Reddit) content about privacy concerns. We use text analysis on data from subreddits on the topic, coded by two independent coders and processed using Voyant tools. This multi-pronged approach allows us to capture the privacy concerns from a variety of stakeholders, as policy makers, publishers, advertisers, and consumers navigate the changing landscape of online privacy controls.

Our work is particularly important as the online world has become more prevalent in consumer's lives in the last decade and perhaps even more so during the COVID-19 pandemic. Our contribution is three-fold. First, we use novel datasets to estimate consumers' preferences for privacy options that will be competing in the AdTech marketplace for targeting online consumers. Our study uses a large sample that is representative of the US population, thus answering the call for privacy studies that do not rely on student samples (Bélanger and Crossler, 2011). We identify four different current clusters of consumer privacy preference in the US internet user population. Second, we explore the different points of view of stakeholders in the online privacy ecosystem. We consider how proposed methods of user targeting affect the interests of internet users, advertisers, online publishers, and AdTech companies whose services make up the online advertising ecosystem. We also include anecdotal evidence of the current views of technology professionals, whose attitudes about the proposed changes will determine the success of future targeting campaigns. Third, we develop and validate a new scale for measuring privacy concerns related to current proposals to replace third-party cookies. From a managerial and policy perspective, our paper speaks to the future of the programmatic ad industry and indicates the best prediction available of what consumers want from the other stakeholders in the online market.

Literature review

Recent research on privacy focuses on consumers' sharing of online information (Acquisti *et al*., 2012; Akhter, 2014; Martin *et al*., 2017). Our paper builds on this stream of literature by considering the on-going debate about information sharing by consumers, first-party data collected by brands, and third-party data collection. As internet privacy controls are changing from an eco-system that is relatively open and based on third-party cookies for consumer tracking across websites, it is even more vital for researchers to analyze how consumers perceive these changes. Unlike previous research that focuses on the consumers' attitudes on the current online privacy ecosystem, we focus on the consumers' choices going forward: we obtain consumers' attitudes towards potential features of prominent technologies that will be adopted in the near future to replace third-party cookies.

We are particularly interested in the area of privacy controls that intersects with programmatic ads. Programmatic advertising has been increasing as a share of total online advertising, an increase that has coincided with cheaper and more effective methods of online tracking and targeting of consumers. The increase in programmatic advertising has also coincided with the expansion of online privacy concerns, as firms are collecting more and more information about consumer habits even though consumers are increasingly worried about such tracking (Brough and Martin, 2021; Graeff and Harmon 2002; Phelps *et al*., 2000).

Our paper also speaks to a related and important stream of research by adding to our understanding of the various shareholders in the online privacy arena. Following calls to add to research on different stakeholder views for online privacy concerns (Liyanaarachchi, 2020; Lwin *et al*., 2007; Martin and Murphy, 2017; Mascarenhas *et al*., 2003; Sheehan and Hoy, 1999), we use anecdotal evidence to suggest the separate interests for this particular industry.

Recent research has analyzed the determinants of consumers' increased privacy concerns and proposed a psychological framework to identify dimensions of privacy concerns for consumers (Stuart *et al*., 2019) and emphasized that privacy is a multi-dimensional concept that must be addressed as such across all the stakeholders (Bélanger and Crossler, 2011). In particular, Bélanger and Crossler (2011) point out that most of the privacy studies that involve customers are highly dependent on data from student populations and thus likely are not capturing the distribution of the entire US population. Moreover, Wirtz *et al.* (2007) has focused on analyzing the causes and consequences of customers' concerns about online privacy using an experimental survey approach. Our study uses a large sample that is representative of the US population, thus answering the call for more diverse and thus multi-faceted research on privacy concerns.

Our work also enhances the recent findings related to the privacy paradox (Li *et al.*, 2017). The privacy paradox refers to the discrepancy between consumers' stated preferences for privacy and their online behaviors. It has been thoroughly documented that consumers prefer to disclose less information than they actually do (Awad and Krishnan, 2006) and, so far, research has focused on behavioral factors that may explain this paradox (Hui *et al.*, 2007; Li *et al.*, 2017; Taddicken, 2014). Our paper explores an alternative explanation: the ecosystem of available privacy choices can greatly influence the consumers' stated preferences as well as their actual online behavior. Thus, in our study of the representative US consumer sample, we present consumers with plausible available options for their privacy choices with the goal of minimizing the paradoxical choice between their true preferences for privacy and what consumers can actually do to accomplish these preferences in the real world. Our study can inform further regulatory and industry positions of the choices consumers would make among the current proposed alternatives.

Industry Context

Programmatic Advertising

Programmatic advertising has come to dominate online advertising in the past decade. It has represented 83.9% of total display ad spending in 2019 (Perrin, 2021) and is expected to grow further in the future as automated data processing becomes increasingly sophisticated. Its success depends on data-driven and automated decision making to target a particular audience online, usually at an individual consumer level and in real time. Harry Harcus, managing director at Group M's programmatic agency Xaxis, in an interview for Marketing Week, explained programmatic advertising as, "The use of data and technology enabling marketers to make decisions in real time about the advert they want to deliver to the consumer" (Rogers, 2017).

Programmatic ad campaigns replace traditional ad campaigns that are conducted by managers' decisions on where and when to place the ads online, and instead rely on advanced software to target a particular type of customer according to available data on them. While there are many definitions of programmatic ads and the ecosystem for these types of ads, the main difference between programmatic ads and traditional ads has to do with how automated the technology for the ad placement is.

Programmatic ad campaigns automatically follow certain rules decided ahead of time by the managers or campaign decision makers, as advertising space is created in real time by consumers' actions such as visiting a website. These rules can include the choice of websites where ads will be published, ad space characteristics such as size and location on the website, and the maximum price of the ad space. While these are similar to decision making in traditional advertising, automation allows for making these decisions at an individual impression level, instead of thousands or millions of impressions.

Moreover, data on consumer characteristics and their online behavior, such as previously visited websites, allow targeting consumers at an individual level as well. By tracking the websites that a consumer visited previously, one can understand the interests of the consumer, which allows targeting each consumer accordingly with ads relevant to their interests. Thus, the targeting effectiveness of programmatic advertising critically depends on the amount and quality of consumer data available. Consequently, advertisers and AdTech companies build databases on individual internet users by tracking their online activity.

Stakeholders

The programmatic ecosystem is large and complex. Beyond internet users, there are many stakeholders in changes affecting this ecosystem. It is helpful to keep in mind that the commodity traded in this market is ad space. On the supply side there are publishers of websites who aim to attract consumers with interesting content. On the demand side there are advertisers who would like to buy ad space to reach these consumers. An Ad Exchange typically sits in between, facilitating transactions, that are usually resolved through real-time bidding (Rask, 2021). Some transactions also take place in private marketplaces.

Publishers are served by Supply Side Platforms (SSP) that allow them to automatically list their inventory for sale in an Ad Exchange, in real time as consumers create ad space by clicking to load web pages. Some publishers, especially smaller ones, choose to be a part of an Ad Network, that aggregate inventory to benefit from economies of scale. Advertisers or their agents are served by Demand Side Platforms (DSP) that allow them to bid on ad space as it becomes available on Ad Exchanges. These bids are automatic with pre-determined decision algorithms based on consumer data.

Large amounts of data are handled by a separate type of player in this industry called Data Management Platform (DMP), which collects, stores and supplies data to either Supply or Demand Side Platforms. DMPs are vital for programmatic ad campaigns as they help managers make automated decisions based on consumer data and adjust campaign parameters accordingly.

Advertisers can choose to hire DSPs that are integrated with a DMP, work with a trade desk to coordinate their buys or even take the entire process inhouse. The inhouse option is costly as it requires sophisticated data analysis and resources dedicated to just this type of ad buys. If done correctly, successful companies with inhouse campaign can have a greater understanding of the customer response, a quicker adaptation of the campaign and ultimately more control. For most companies, inhouse campaigns are prohibitively expensive. Thus, they rely on trade desks or DSPs to run programmatic ad campaigns.

Our description of this industry is quite simplified, but still very complex. The main benefit of this complexity is, for advertisers, targeting consumers at an individual level, and for consumers, seeing more relevant ads based on their interests. This more efficient and effective targeting also creates an economic value beyond traditional advertising that is shared by the AdTech industry, which is comprised of the technology companies that facilitate the whole process such as SSPs, DSPs, DMPs, Ad Exchanges, Ad Networks, and several specialized types of firms not mentioned here. In order for this individual targeting to work, consumer data is collected at an individual level by tracking their online behavior.

Tracking technologies

Third-party cookies are the primary method for tracking and targeting users. With this method expected to become infeasible in 2023, multiple replacement technologies have been proposed. In this section we review how tracking is accomplished with third-party cookies before describing two possible replacements, Unified ID 2.0 and Privacy Sandbox, which are likely to replace the current options due to the industry standing of the companies who have proposed them.

Third-Party Cookies

Currently the most prominent way of collecting data on consumers, especially for tracking the websites they visit, utilizes third-party cookies. Although there are other ways to track consumers used by AdTech companies, such as "fingerprinting" a device (and hence its user) by collecting information on hardware and software configuration in order to identify it later, the bulk of consumer tracking at present is done through third-party cookies.

It is important to note that cookies were not originally designed for consumer tracking and targeting. A cookie is simply a small piece of data that is stored on the user's computer by the browser. This small piece of data allows a website to remember a user and their previous activity on the website, such as the items they placed in the shopping cart in a previous visit. Normally each website has access to only the cookies they placed on the user's computer—these are called first-party cookies.

Third-party cookies, on the other hand, allow for tracking users across websites through a creative workaround. Not all content a user sees on a specific website is stored in the website's servers. For example, the ads will typically be stored in an ad server. In order to show the ad to the user, the browser needs to make a call to the ad server, which is an external party. This call allows the external party to also place a cookie on the user's computer through the browser. The creative workaround uses this same mechanism: third parties can place a cookie on a user's computer if they get a call from a website, and this allows the third party to know that the user visited the website and when the visit happened. In order to facilitate this call, data collectors make agreements with websites and place a tracking pixel (sometimes called a tracking cookie or tag) on the website.

A tracking pixel is a 1x1 pixel-sized image that is usually transparent, thus invisible to the user. The pixel image is stored in the data collector's server which requires the browser to make a call for it. Subsequently the data collector knows that the user visited the website. If the data collector has pixels over many websites, they can generate a list of websites a user visited previously. According to webcookies.org[[ii]], a scan of close to 2 billion websites shows that the average website has 5 pixels with the maximum number exceeding 500. This means that when a user visits a website, on average, 5 third parties (who are likely to be data collectors) make a note of it. The user is generally unaware this has occurred.

The browser plays a crucial intermediary role because it is the software that places the cookies in the user's computer on behalf of third parties. Thus, the browser is a gatekeeper that can block third-party cookies and pertinent consumer tracking and targeting that is vital for the programmatic ecosystem. There are several browsers that block third-party cookies, most notably Safari and Firefox. However, Chrome, the most popular browser with 66% market share, does not, at least for now. When Google announced the plans to block third-party cookies in Chrome by 2022 (later extended to 2023) citing privacy reasons, the AdTech industry was faced with the prospect of losing the most common way to track consumers and hence targeting them effectively. Consequently, several AdTech companies, including Google, started laying out plans to address privacy and targeting issues important for many stakeholders in the online advertising ecosystem.

Unified ID (UID) 2.0[iii]

UID 2.0 is The Trade Desk's proposal for replacing third-party cookies in the AdTech ecosystem. (The Trade Desk provides the leading independent Demand Side Platform used by advertisers to purchase impressions on the internet.) The Trade Desk began work on UID 2.0 in 2020 and has several partners, including LiveRamp, The Washington Post, Nielsen, and Criteo[iv].

According to Jeff Green, CEO of The Trade Desk, the goal of UID 2.0 is to "protect the *quid pro quo* of the internet, which is seeing relevant ads in exchange for free content, while at the same time protecting privacy."[v] The Trade Desk and their partners believe that user concerns about privacy are driven primarily by a failure of AdTech companies to effectively communicate the *quid pro quo* principle[vi]. Dave Pickles, CTO of The Trade Desk, said, "The basic problem is that cookies aren't understandable…consumers are just afraid but they don't really know what is happening…[the solution] has to be a conversation with consumers…driven from the value exchange."[vii] Consequently, the assumptions about user preferences that inform the design of UID 2.0 are (1) users prefer behaviorally targeted online ads and (2) users will accept data collection practices similar to what is currently done when they understand that these practices fund free access to online content (e.g., recipe websites, YouTube videos, social media). The belief that behaviorally targeted online ads are preferred by consumers is deep-rooted in the advertising industry[viii], although findings in academic research suggest this is often not the case (for a review, see Boerman *et al.*, 2017). The assumption that the *quid pro quo* of the internet is acceptable to users is also an area of debate. For example, Schumann *et al.* (2014) found that internet users were more convinced to provide personal data when websites justified the request with a *quid quo pro* argument than an argument based on providing relevant ads. Legal scholar Strandberg (2013) argued, however, that the exchange of personal information for free online content occurs in a market so stripped of typical feedback mechanisms that users' acceptance of the exchange should not be interpreted as representing their true preferences. Winegar and Sunstein (2019) come to similar conclusions based on empirical results.

The heart of UID 2.0 is a single identifier of each internet user, created by encrypting their email, which is used to track them across the internet. This identifier can be used by all AdTech companies that interact with the user, e.g., to collect information about them or target them with advertising. UID 2.0 replaces the multitude of identifiers currently constructed and maintained through the use of third-party cookies by individual AdTech companies. As a result, identifying users and sharing data about users between AdTech companies should be more efficient with UID 2.0, leading to higher data quality and increased data sharing. Unlike Google's Privacy Sandbox (discussed below) or third-party cookies, UID 2.0 is intended to be consistent across all internet browsers as well as user device types, e.g., web browsers, mobile phones, and connected TV, which would allow AdTech companies to better track users and streamline their processes across those platforms. If widely adopted, UID 2.0 would allow AdTech companies to continue much as they operate now, but with improved data and, consequently, better ad targeting, potentially leading to higher revenue. Supporters of UID 2.0 see it as a way for AdTech companies to maintain some independence from Google and Facebook, as well as Apple and Amazon, while fearing that the Privacy Sandbox would increase Google's dominant position[ix].

UID 2.0 also includes simplified privacy controls for internet users. Users would be able to set their privacy preferences for a particular web site, similarly to how they now set their cookie preferences. However, unlike cookie settings, those preferences would be automatically applied when they access the same web site with a different browser or device, reducing the burden of maintaining privacy settings. For internet users, the disadvantages of UID 2.0 are similar to the current disadvantages of user tracking through third-party cookies, because consumers will continue to be tracked and data about them will continue to be widely held within the AdTech ecosystem. Internet users will be afforded some protection because of the encryption of their email addresses and terms and conditions about UID 2.0 may be used. However, user identities can often be determined from demographic data; for example, one study estimated that 99.98% of Americans can be correctly identified based on 15 demographic attributes (Rocher *et al*., 2019; WashPostPR, 2020). If UID 2.0 increases data quality and sharing, it may make identifying internet users easier rather than more difficult.

Privacy Sandbox

Privacy Sandbox is Google's proposal to protect user privacy while supporting advertising on the internet. In particular, it is a proposal for how "the web could work without cross-site tracking,"[x] including tracking by either third-party cookies or less well-known mechanisms such as fingerprinting. Disabling of tracking internet users is a dramatic change for the AdTech industry because tracking users is currently central in developing user profiles and identifying users for targeting. The original Privacy Sandbox proposal was augmented with extensions proposed by non-Google AdTech companies (e.g., Criteo[xi]) and in-house Google units (e.g., Google Ads[xii]). In the first half of 2021, Google launched a prototype of the core functions of Privacy Sandbox to allow for limited testing by online publishers.

To stop cross-site tracking, Privacy Sandbox will need to prevent internet users from being identified in ways that can be validated in a context external to the website the user is visiting[xiii]. This will not only prevent AdTech companies from profiling users based on their browsing behavior, but also thwart much aggregation and exchange of internet user data, because these tasks require sharing user identifiers between AdTech companies. (This stands in stark contrast to the capabilities enabled by the unified identifier in UID 2.0.) However, Privacy Sandbox will allow limited behavioral targeting of internet users[xiv] because Google has estimated that eliminating would reduce advertising revenue of online publishers by over 50% (Ravichandran and Korula, 2019). These core elements of Privacy sandbox—preventing cross-site tracking and allowing limited targeting—are based on two assumptions about internet user preferences. First, users would like to substantially restrict the level of data collection by AdTech companies, especially data that allows them to be identified. Second, users would accept more limited data sharing to support targeted advertising. Research supports the assumption that internet users would like to prevent AdTech companies from tracking them (Alreck and Settle, 2007; McDonald and Cranor, 2010; Turow *et al.*, 2009, 2012). However, to our knowledge, the assumption that users would accept more limited data sharing in the ways that Privacy Sandbox proposes has not been rigorously and directly investigated in academic research.

To implement its goal of preventing cross-site tracking while supporting more limited behavioral targeting[xv], Privacy Sandbox proposes to extend Google's internet browser, Chrome, to take on many of the functions currently implemented elsewhere in the AdTech ecosystem[xvi]. This includes functions such as defining consumer interest groups, identifying which interest groups the Chrome user belongs to, running the auction for ads to place on web pages, and selecting the creatives to display. As a result, Privacy Sandbox puts the internet user's web browser (Chrome) at the center of technical process for online advertising, instead of being a relatively passive receiver of cookies and ads. The major advantage of Privacy Sandbox for internet users is that it greatly restricts the amount of information about the user available to other parties. This could provide significant protection for consumers against malicious actors, governmental surveillance, and the like.

Privacy Sandbox appears to have strong disadvantages for current AdTech companies and advertisers. Many types of such companies, such as Supply Side Platforms (SSPs) and Demand Side Platforms (DSPs), would continue to operate, but the information they would receive would be dictated by the user's browser and the functionality these companies could offer to their customers (e.g., advertisers and publishers) would be restricted by the functions built into Privacy Sandbox. For example, Criteo's proposal to extend Privacy Sandbox[xvii], developed after Criteo's stock fell sharply on Google's announcement of discontinuing support for third-party cookies (Graham, 2020), focused on adding basic functionality currently available in the AdTech ecosystem, e.g., support for fraud prevention methods and AB testing. Extensive recoding of other AdTech companies' software to facilitate interaction with Privacy Sandbox would likely be necessary as well. In addition, advertisers, and other companies running online campaigns, would most likely need to design their campaigns around more limited targeting capabilities. Finally, some types of AdTech companies, most notably third-party data providers, could see their role, and economic prospects, sharply diminished (Morrison and Molla, 2020). There is concern that Privacy Sandbox would strengthen Google's already dominant position in online advertising (Kelly, 2021) that has led to an anticompetitive behavior inquiry in the United Kingdom[xviii].

The current proposal only applies to Google Chrome, which has about 66% of the non-mobile internet browser market globally[xix]. Producers of other browsers such as Mozilla Firefox, Microsoft

Edge, or Apple Safari could choose to extend their own browsers to include similar functionality. If they did so, AdTech companies could operate in a similar manner across browsers. If other browsers do not support Google Privacy Sandbox functionality, AdTech companies would either implement parallel mechanisms for advertising on those browsers or abandon them. Note that, because both Firefox and Safari already block third-party cookies, AdTech companies are already dealing with this issue on those platforms.

In anticipation of these upcoming changes, we investigate the privacy concerns among US internet users first through a representative sample survey, and follow up with a supplementary study analyzing text from conversations on subreddits with various stakeholders represented in each conversation. In the next section we summarize our methods, the measure validation process, data analysis and findings for both studies.

Methodology and analysis

Study 1: Survey on Representative US Consumer Sample

We aim to determine US internet users' preferences for privacy in online advertising as related to proposals to replace third-party cookies, by surveying their support of the fundamental assumptions of Privacy Sandbox and UID 2.0. Existing measures of internet user privacy concerns (e.g., Bellman *et al.*, 2004; Buchanan *et al.*, 2007; Smith *et al.*, 1996) do not differentiate between the ways that Privacy Sandbox and UID 2.0 affect privacy, primarily because issues related to online user tracking were not as prominent at the time that these measures were developed as they are now. Accordingly, we developed measures based on public statements made by the primary proposers of Privacy Sandbox and UID 2.0, which we pretested.

Measure Development

Privacy Sandbox and UID 2.0 are based on overlapping but distinct assumptions about internet user preferences. The proposers of UID 2.0 argue that internet users prefer to see ads relevant to their interests and, if appropriately informed, would be supportive of the "*quid pro quo* of the internet" (Green, 2020), essentially the idea that users receive free online content (e.g., blogs, videos, news) in exchange for allowing data about their actions to be collected for advertising (Schumann *et al.*, 2014). In short, UID 2.0 assumes that, when internet users understand that allowing data collection by advertisers funds the free content they consume, they are accepting of the current uses of data in online advertising.

The designers of Privacy Sandbox, on the other hand, assume that laws such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) are representative of internet users' preferences (Wolly, 2020). Google states, "The Privacy Sandbox project's mission is to 'Create a thriving web ecosystem that is respectful of users and private by default'" [[xx]]. Consequently, in contrast to UID 2.0, the Privacy Sandbox emphasizes preventing advertisers from identifying users in any way that allows tracking actions across websites or building databases about interests [[xxi]]. In order to support online advertising, Privacy Sandbox assumes, like UID 2.0, that users are accepting of ads relevant to their interests and, critically, that users are willing to allow online advertisers to receive limited information about them as long as they cannot be identified.

We developed self-report measures of internet user preferences related to these assumptions in order to measure the level of support they have in the US population. The measures are internet users' *preference for relevant ads*, *acceptance of quid pro quo, desire to prevent data collection,* and *acceptance of limited information*. The first two are the foundational assumptions underlying UID 2.0's current design, while the first one and the last two are the foundational assumptions of Privacy Sandbox. The final measures are presented in Table I. The following paragraphs describe their development.

Insert Table I here

We analyzed public statements about the proposals from Google and The Trade Desk on their websites, blogs, GitHub repositories, YouTube channels, and industry events. From this information we created candidate items that present the assumptions in layperson terms, while staying consistent with the technical details. To assess the inter-item reliabilities and factor structure, we then conducted a trial with 101 adult US internet users on Prolific, an online platform for research surveys [xxii]. The order of the items in the measures was randomized and the order of the measures was varied. No order effects were found. Because the inter-item reliability was high on all measures, we eliminated some theoretically redundant items to create more concise measures. We also reworded one item to reduce cross-loading in an exploratory factor analysis (EFA) and another item to reflect changes in the Privacy Sandbox proposals, specifically the publication of FLEDGE [xxiii], after the initial candidate items were created.

We first ran a second trial (*N* = 190) on the Prolific platform to test these changes and reconfirm the measure reliabilities and factor structure. The measures had high inter-item reliability with all Cronbach's alphas greater than .90; an EFA using principal components analysis and varimax rotation revealed the expected factor structure. The factor loadings are shown in Table I. To test convergent and discriminant validity (MacKenzie *et al.*, 2011), we added the *concern for information privacy* (CFIP) measure (Smith *et al.*, 1996) as adapted for online privacy by (Bellman *et al.*, 2004). CFIP has four dimensions about concerns related to excessive data collection, unauthorized secondary use of data, improper access to data by unauthorized actors, and errors in personal data held by advertisers. We adjusted the CFIP items by replacing all instances of "Web site" with the contemporary usage "website." The CFIP correlated with our new measures in appropriate ways, with the strongest correlation being -.63 between *acceptance of quid pro quo* and data collection concerns. To create the final measures, we retained all items from this trial. The details of the measure validation analyses are available from the authors.

Privacy Sandbox and UID 2.0 are meant to replace advertisers' use of third-party cookies, so neither proposes changes to first-party use of data, that is, data collected by advertisers on their own platforms, e.g., user page view and sales data from an online store. However, internet users may not distinguish first- and third-party data uses. If they object to typical uses of first-party data, support for the assumptions of Privacy Sandbox or UID 2.0 may be undermined. To explore this possibility, we developed a measure of internet users' *acceptance of first-party data use* with one item for each of five prototypical uses of first-party data, such as retargeting users who left an item in a shopping cart and using past purchase history for targeting. See Table II.

Insert Table II here

Sample

The survey was completed by a representative (age, sex, ethnicity, geographic region) sample of 818 adult US residents on the Centiment [xxiv] market survey platform. Although Centiment pre-screened the participants, we also included one attention check question. Centiment retained only data for participants who passed the attention check. The company estimated that that 5-10% of participants failed the check. Our analysis includes only the participants who responded correctly to the attention check question. The participants were between 18 and 94 years old (*M* = 53.59, *SD* = 17.27), with 456 females (55.7%), 355 males (43.4%), and 7 others (.8%). In the sample, 628 (76.8%) participants self-identified as white, 91 (11.1%) as African American, 65 (7.9%) as Hispanic, 31 (3.8%) as Asian, 25 (3.1%) as Native American, 3 (.4%) as Pacific Islander, 12 (1.5%) as another race, and 5 (.6%) did not reveal their race and ethnicity. The percentages sum to greater than 100, because participants could select multiple categories.

Measures

After informed consent, the first page of the survey included the *preference for relevant ads* (Cronbach's α = .86), *acceptance of quid pro quo* (α = .90), *desire to prevent data collection* (α = .86), and *acceptance of limited information* (α = .86) measures described above. The next page held *acceptance of first-party data use* (α = .91). All measures elicited responses on a seven-point Likert scale with higher scores representing higher levels of agreement. The penultimate page included the *concern for information privacy* measure described above, with scores recorded on a seven-point Likert-type scale. The final page included demographic questions. The survey took approximately 6 minutes to complete.

Results

Table III presents the means, standard deviations, and intercorrelations among the variables. Overall, participants somewhat prefer relevant ads (M = 5.39, SD = 1.22), desire advertisers to be prevented from collecting data about them (M = 5.94, SD = 1.10), slightly reject the quid pro quo of the internet (M = 3.46, SD = 1.52), and are somewhat accepting of advertisers receiving more limited information about them (M = 4.89, SD =1.30). In a repeated measures t-test, participants were more accepting of advertisers receiving limited information than of the *quid pro quo* of the internet (df = 817, t = 27.06, p < .001, d = .95). The large effect size suggests that Privacy Sandbox is substantially more aligned with internet user preferences than UID 2.0. It is important to note that consumers are generally wary of data collection: the average for the variable *"Desire to prevent data collection"* is the highest among all privacy-related variables collected.

Insert Table III here

To identify distinct segments based on their preferences regarding the foundational assumptions of Privacy Sandbox and UID 2.0, we performed an agglomerative hierarchical cluster analysis of the z-scores of the four variables, using Ward's method with a squared Euclidean distance measure. Although the scree plot of coefficients suggested a large number of clusters (~50) minimizes error, inspection of the dendrogram suggested a more parsimonious four-cluster solution is appropriate (Yim and Ramdeen, 2015). We identified the members of the four clusters with a k-means cluster analyses of the same variables, because k-means cluster analysis provides more reliable clusters than hierarchical analysis [xxv]. The resulting clusters are presented in Table IV. Once again, across all clusters, consumers on average have a high desire to prevent data collection, which should indicate to marketers that consumer privacy preferences need to be balanced against the targeting for relevant ads. While averages do not inform us about what trade-offs consumers would make in this balance, we can better understand these choices in the context of what type of privacy controls consumers would rather employ in order to achieve this data collection protection. Thus, the four clusters we identify represent different consumer preference for privacy options.

There were 209 (26%) participants in Cluster 1, who accepted the premises of both Privacy Sandbox and UID 2.0. Their preferences appear to be driven by a strong preference for relevant ads (*M* = 6.33). Cluster 1 is the only cluster that skews male (55%) and for a more descriptive reference we name the typical person in it as "Everything goes Evan." The 212 (26%) participants in Cluster 2, "Ambivalent Amy", were ambivalent about both sets of premises with the mean score on all variables between 4 (the scale midpoint) and 5 points (labeled "somewhat agree"). However, the 277 (34%)

participants in Cluster 3, “Anonymous Anna”, accepted the premises of Privacy Sandbox but rejected the premises of UID 2.0, indicating that they are driven by a desire for relevant ads (*M* = 5.69) and a strong desire to prevent advertisers from aggressively collecting data (*M* = 6.56). Finally, the 120 (15%) participants in Cluster 4, “Private Priscilla”, rejected both privacy options, due to ambivalence about relevant ads (*M* = 4.14) and, like participants from Cluster 3, indicated a strong desire to prevent advertisers from aggressively collecting data (*M* = 6.70). The last cluster, who is most conservative in privacy preferences, is also oldest (56.7 years old) and skews female the most (65%).

Insert Table IV here

Users may not differentiate between first-party uses of data (e.g., targeting users with ads for items left in a shopping cart) and tracking with third-party cookies. Thus, we asked about preferences related to first-party data uses. Overall, participants somewhat disapproved of first-party uses of data (M = 3.35, *SD* = 1.41). Consistent with their previously reported preferences, participants in Cluster 1 had a slightly positive view of first-party data uses (*M* = 4.51, *SD* = 1.11), participants in Cluster 2 were ambivalent towards it (*M* = 3.81, *SD* = 1.06), and participants in Cluster 4 were unaccepting of it (*M* = 1.81, *SD* = .88). Although the participants in Cluster 3 were generally supportive of the premises of Privacy Sandbox, they were unaccepting of first-party data uses (*M* = 2.78, *SD* = 1.15). This is important because Cluster 3 was the largest cluster and to the degree that internet users do not differentiate between first-party uses of personal data and data collected by tracking with third-party cookies, their support for the online environment created by Privacy Sandbox may be eroded.

Study 2: Content Analysis on Reddit forums

Our second data collection is aimed at exploring the contemporary conversations around UID 2.0 and Google Sandbox. We pulled comments from 26 subreddits for one month, in March 2021. These forums were chosen in one of three ways: 1) by searching the keyword “Privacy”, and “Google Sandbox” or variations of “UID 2.0” (e.g., uid, UID, unified ID, universal ID, etc.) on Reddit’s search engine; 2) by following links from other subreddits about related topics, 3) through a Google search with keywords "uid, cookie, reddit" and "sandbox, cookie, reddit". The criteria yielded 26 total subreddits and 588 comments. We cleaned, coded and analyzed this textual data using Voyant Tools. We then conducted a semantic frequency analysis to provide insight into real world privacy concerns among professionals in technology and AdTech-related areas, such as software and web development, information security, and search engine optimization (SEO).

The initial dataset included 49 subreddits, which was then narrowed by focusing on a filter of “Privacy.” The result of the filtering process yielded 26 viable subreddits. Most of these 26 subreddits explicitly identified professionals as their community members in their descriptions, while a few included mostly practitioners and enthusiasts of platform and web development, SEO, and digital advertising. The following results are based on this conservative sample focused on privacy. Two researchers independently categorized the sample based on the stakeholder categories and by the main theme (UID 2.0, Google Sandbox, or both).

Our work draws on methods proposed by earlier research on sentiment analysis (Prabowo and Thelwall, 2009) and seeks to explore any emergent themes among a specific group of people. Therefore, we investigated keyword frequencies, collocates and correlations at a corpus and individual document level. Due to the sparce amount of text on this novel topic, our findings are presented as anecdotal information and are meant to be exploratory. This exploration is intended to add to the discussion of the dominant theme and sentiment regarding the two proposed solutions among professionals in tech or AdTech related areas and offer directions for future research.

Findings

Results of our exploratory analysis of the text revealed that UID 2.0 is still in its early stages of introduction to not only the consumers, but also to tech and AdTech professionals. There is sparse discussion about UID 2.0 and many unknowns are evident in the discussion posts between the AdTech professionals we sampled. Table V lists the data sources and the categorizations determined by two coders as well as the number of relevant posts and their comments.

Insert Table V here

Anecdotal evidence suggests that discussions are focused on Google mostly. Indeed, a clear finding of our analysis is that discussions on privacy mention Google (485 times) and Google Sandbox overwhelmingly more than UID (total of all variations 37 times). Overall, Google themed discussions are an order of magnitude higher than conversations about alternatives, indicating that the industry is overwhelmingly concerned with changes that are proposed and implemented by Google, the dominant company in this space. Moreover, UID-focused subreddit posts and comments discuss Google Sandbox more commonly than they do UID, again emphasizing that all alternatives to third-party cookies will be compared to Google's proposed solution, Sandbox.

The sentiment analysis yielded heavy valence towards positive sentiments at first glance (positive to negative associations ratio 670 : 206.) Most attributions were to Google Sandbox in the overall corpus with only 7 total attributions (positive and negative) to UID. However, we also noted that sarcastic tones that contained generally positive words could have impacted our sentiment analysis. To estimate whether this error would be significant in switching sentiment towards negative, we reviewed a random sample of text in the overall corpus (n = 30 comments) and found that two out of the 30 had implicit and contrary meanings. For example, one developer wrote "Google Privacy Sandbox is a path forward to respect user privacy to the highest standard, and also support user targeting, personalization and recommendation use cases.” This association is marked as positive, however the author continues to negate that statement: “Can one be targeted, served personalized ads, and have their data privacy be respected? Hell no Google's sandbox is the opposite of 'Sandboxing' if that's how they are doing it. It is sandboxed from other third parties, not google.” This anecdotal evidence suggests that while the overall sentiment analysis seems positive, some of the positive comments may be undermined by undetected sarcasm.

While further research is still needed to confirm our initial findings, this exploration suggests that overall sentiment towards Google Sandbox solution among our sample was positive; and that the alternative proposed has yet to create awareness on the free internet content quid-pro-quo argument.

Managerial and Policy Implications

The managerial and policy related implications of this study are multi-fold. As stakeholders adjust to a new ecosystem, where third-party cookies are no longer utilized to track internet users, managers for publishing, AdTech, and third-party firms are trying to identify the winning solution to programmatic advertising while keeping privacy concerns top of mind. In addition, regulators are becoming more active in this area due to perceptions of consumer discontent, a concern for managers in the industry. We provide findings from a US representative survey to inform those discussions and decisions. We propose that a holistic stakeholder’s approach would benefit the decision makers, especially given that public sentiment is well segmented with various levels of comfort when it comes to sharing one’s data in return for more relevant ads. Although typical internet users are likely unaware of the details of actions being taken on their behalf by AdTech companies and regulators, their preferences should play an important role in shaping those actions. For example, the designers of replacements for third-party cookies can consider these consumer segments when defining levels of privacy in their solutions, making choices available that match the different segments’ desires. This applies equally to Privacy Sandbox, UID 2.0, and the other solutions that are beginning to emerge. Regulators can similarly tailor their rules and suggestions so that consumers who accept the *quid pro quo* of the internet are able to allow tracking and more personalized targeting in exchange for free online content, while users who want high levels of privacy are able to attain that.

Finally, our findings also inform marketers and advertisers in their targeting practices. Consumers desire to prevent data collection (highest mean in sample), but they also prefer ads relevant to them (second highest mean). This seemingly contradictory position can be best approached by utilizing contextual targeting, in which the ad is relevant to the content, e.g. ad for athletic equipment in a sports related webpage or ad for a kitchen gadget in a recipe video in YouTube. While this approach is less efficient than targeting depending on consumer data, it is also less likely to make privacy concerns salient, thus preserving brand equity.

Contributions to Literature

Our work is important both for managers and industry experts as well as to academic researchers, who are interested in analyzing consumer privacy concerns and preferences for privacy controls. Thus, our paper builds on previous work in this area that emphasized the need to incorporate different stakeholder points of view into research on privacy (Martin and Murphy, 2017; Mascarenhas *et al.*, 2003; Sheehan and Hoy, 1999). Moreover, our paper highlights the importance of consumers' attitudes toward changes imposed by other stakeholders in the online privacy area, which is an area of on-going research interest (Lwin *et al.*, 2007). By supplementing survey results with field data, we attempt to start a conversation regarding the trade-offs of a free and independent internet.

Our paper highlights that there is a conceptual benefit to understanding privacy concerns and data sharing preferences completely removed from any company's implementation (i.e., Sandbox or UID 2.0). Our study of US consumer privacy preferences can showcase the change in consumer privacy and provide researchers with a holistic understanding of how the socially constructed meaning of "privacy" evolves with changing structures and practices. While our current paper has a narrow focus on the effects of privacy concerns on programmatic ads, we believe it contributes to a larger body of literature on shifts of customers privacy concerns at a much higher level (Goldberg and Tucker, 2012). Consumers are aware that their preferences for privacy are often disregarded by regulators and the ad industry[xxvi]. It is thus imperative for researchers to make salient these preferences as a way to bridge the gap between consumer preferences and the current state of the market. The future of our digital lives will partially be shaped by the decisions made in these AdTech conversations, as the system chosen by a majority will likely prevail to shape the market dynamics moving forward.

Study Limitations and Future Research

As with any study our paper has several limitations. One limitation is the self-reported nature of the survey data. Previous research in the area of data privacy suggests that the self-reported attitudes and actual behaviors of consumers do not always align (Barth and Jong, 2017). As all of the data we use in our analysis is self-reported and not incentive compatible, we capture the choices consumers would make in the absence of other constraints on their privacy control choices. The attitudes reported in the study might not directly determine behavior, however, can still serve as an insight for decision making. More importantly, future research may be able to expand the analysis to specific situations where consumers face trade-offs between their privacy choices and their access to the internet using experimental methods to get at the root of the discrepancy between attitude and behavior.

Our paper also uses secondary, anecdotal evidence from stakeholders such as AdTech companies and publishers while focusing our direct data collection efforts on the consumer side. Consumers' preferences and related regulation are the presumed motivation behind the recent changes in third-party tracking online. Moreover, consumer preferences will likely influence the adoption of new proposed targeting methods (Privacy Sandbox, UID 2.0, etc.) by publishers and AdTech companies, so it is important to understand what they prefer. Future research could extend our work by collecting primary data from publishers, AdTech firms, and third parties which would provide additional context to the privacy control area.

Finally, our paper uses anecdotal evidence and initial results from sentiment analysis on web forum content to analyze the AdTech point of view on the proposed changes to privacy controls. Due to the nascent nature of discussion around UID 2.0, there was not enough data to arrive at conclusion regarding the proposed solution. Furthermore, the limitations of analyzing non-literal meaning in text analysis, suggests future research may collect data over a longer period of time as the conversation grows and control for the error any non-literal meanings may create.

This study contributes to the search for solutions to collecting valuable data without infringing on personal privacy on digital platforms. Our results suggest that understanding the perceptions of the trade-offs between receiving relevant content whether in the form of ads or non-commercial content is a strong motivator for consumers in the US. Moreover, our study furthers our understanding of the common privacy concerns among the stakeholders in this industry and thus may prove beneficial for the two privacy prototypes put forth so far, or any future proposals that may affect this industry.

References

Acquisti, A., John, L. K., and Loewenstein, G. (2012), “The Impact of Relative Standards on the Propensity to Disclose”, *Journal of Marketing Research,* Vol. 49 No. 2, pp. 160-174.

Akhter, H. S. (2014), "Privacy concern and online transactions: the impact of internet self-efficacy and internet involvement", *Journal of Consumer Marketing*, Vol. 31 No. 2, pp. 118-125.

Alreck, P. L. and Settle, R. B. (2007), “Consumer Reactions to Online Behavioural Tracking and Targeting”, *Journal of Database Marketing & Customer Strategy Management,* Vol. 15 No. 1, pp. 11-23.

Appel, G., Grewal, L., Hadi, R. and Stephen, A. (2020), “The future of social media in marketing.” *J. of the Acad. Mark. Sci.*, Vol. 48, p. 79–95.

Awad, N., and Krishnan, M. (2006), “The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization”, *MIS Quarterly*, Vol. 30 No. 1, pp. 13-28.

Bélanger, F., and Crossler, R. (2011), “Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems”, *MIS Quarterly,* Vol. 35 No.4, pp. 1017-1041.

Bellman, S., Johnson, E.J., Kobrin, S.J. and Lohse, G.L., (2004), “International differences in information privacy concerns: A global survey of consumers”, *The Information Society,* Vol. 20 No. 5, pp. 313-324.

Boerman, S. C., Kruikemeier, S. and Zuiderveen Borgesius, F. J., (2017), “Online behavioral advertising: A literature review and research agenda”, *Journal of Advertising*, Vol. 46 No. 3, pp. 363-376.

Brough, A. R., and Martin, K. D. (2021), “Consumer Privacy During (and After) the COVID-19 Pandemic”, *Journal of Public Policy & Marketing,* Vol. 40 No.1, pp. 108-110.

Buchanan, T., Paine, C., Joinson, A., and Reips, U.D. (2007), “Development of measures of online privacy concern and protection for use on the Internet”, *Journal of the American Society for Information Science and Technology,* Vol. 58 No. 2, pp. 157-165.

Caudill, E. M., and Murphy, P. E. (2000), “Consumer Online Privacy: Legal and Ethical Issues”, *Journal of Public Policy & Marketing,* Vol.19 No.1, pp.7-19.

Fehrenbach, D., and Herrando, C. (2021), “The effect of customer-perceived value when paying for a product with personal data: A real-life experimental study.”, Journal of Business Research, Vol. 137, p. 222-232.

Glueck, K. (2021), “Google’s Privacy Sandbox—We’re all FLoCed”, Oracle News Connect, 7March, available at: https://www.oracle.com/news/announcement/blog/google-privacy-sandbox-030721.html (accessed 23 March 2021).

Goldfarb, A., and Tucker, C. (2011), “Privacy Regulation and Online Advertising”, *Management Science*, Vol. 57 No. 1, pp. 57-71.

Goldfarb, A., and Tucker, C. (2012), "Shifts in Privacy Concerns.", *American Economic Review*, Vol. 102 No. 3, pp. 349-353.

Graeff, T. R. and Harmon, S. (2002), "Collecting and using personal data: consumers’ awareness and concerns", *Journal of Consumer Marketing*, Vol. 19 No. 4, pp. 302-318.

Graham, M. (2020), “Ad-tech company Criteo crashes to 52-week-low after Google said it will stop supporting third-party cookies in Chrome”, CNBC, 14 January, available at: https://www.cnbc.com/2020/01/14/criteo-stock-crashes-after-google-announces-chrome-cookie-change.html (accessed 24 March 2021).

Graham, M. (2021), “Google says it won’t use new ways of tracking you as it phases out browser cookies for ads”, CNBC, 3March, available at: https://www.cnbc.com/2021/03/03/google-says-it-wont-track-you-directly-in-the-future-as-it-phases-out-cookies.html (accessed 23 March 2021).

Hong, W., Chan, F.K.Y. and Thong, J.Y.L. (2021), “Drivers and Inhibitors of Internet Privacy Concern: A Multidimensional Development Theory Perspective.”, *J Bus Ethics*, Vol. 168, p. 539–564.

Hui, K., Teo, H., and Lee, S. (2007), “The Value of Privacy Assurance: An Exploratory Field Experiment.”, *MIS Quarterly*, Vol. 31 No. 1, pp. 19-33.

Kelly, C. (2021), “What Google's rejection of post-cookie identifiers means for advertisers”, Marketing dive, 4march, available at https://www.marketingdive.com/news/what-googles-rejection-of-post-cookie-identifiers-means-for-advertisers/596096/ (accessed 24 March 2021).

Lardinois, F. (2019), “Google proposed new privacy and anti-fingerprinting controls for the web”, Tech Crunch, 22August, available at: https://techcrunch.com/2019/08/22/google-proposes-new-privacy-and-anti-fingerprinting-controls-for-the-web/ (accessed 23 March 2021).

Li, H., Luo, X. ,Zhang, J., and Xu, H. (2017), “Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors.”, *Information & Management*, Vol. 54 No. 8, pp. 1012-1022.

Liyanaarachchi, G. (2020), "Online privacy as an integral component of strategy: allaying customer fears and building loyalty", *Journal of Business Strategy*, Vol. 41 No. 5, pp. 47-56.

Lwin, M., Wirtz, J. & Williams, J.D. (2007), “Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective”, *Journal of the Academy of Marketing Science*, Vol.35, pp. 572-585.

Martin, K. D., Borah, A., and Palmatier, R. W. (2017), “Data Privacy: Effects on Customer and Firm Performance”, *Journal of Marketing*, Vol.81 No.1, pp. 36-58.

Martin, K. D. and Murphy, P.E. (2017), “The role of data privacy in marketing”, J *Journal of the Academy of Marketing Science*, Vol.45, pp. 135-155.

Mascarenhas, O.A.J., Kesavan, R. and Bernacchi, M.D. (2003), "Co-managing online privacy: a call for joint ownership", *Journal of Consumer Marketing*, Vol. 20 No. 7, pp. 686-702.

Maseeh, H. I., Jebarajakirthy, C., Pentecost, R., Arli, D., Weaven, S., and Ashaduzzaman, M. (2021), “Privacy concerns in e-commerce: A multilevel meta-analysis.”, *Psychol Mark*, Vol. 38, pp. 1779– 1798.

McDonald, A. M. and Cranor, L. F., (2010), “Americans' attitudes about internet behavioral advertising practices”, *Proceedings of the 9th annual ACM workshop on Privacy in the electronic society*, pp. 63-72.

Morrison, S. and Molla, R. (2020), “Google Chrome’s cookie ban is good news for Google — and maybe your privacy”, Vox, 16 January, available at: https://www.vox.com/recode/2020/1/16/21065641/google-chrome-cookie-ban-advertisers (accessed 24 March 2021).

Perrin, N. (2021),“US Programmatic Digital Display Advertising Outlook 2021”, eMarketer, 11January, available at: https://www.emarketer.com/content/us-programmatic-digital-display-advertising-outlook-2021 (accessed 23 March 2021).

Phelps, J., Nowak, G., and Ferrell, E. (2000), “Privacy Concerns and Consumer Willingness to Provide Personal Information”, *Journal of Public Policy & Marketing*, Vol. 19 No.1, pp. 27-41.

Prabowo, R., and Thelwall, M. (2009), “Sentiment analysis: A combined approach”, *Journal of Informetrics*, Vol. 3 No. 2, pp. 143-157.

Rask, O. (2021), “What is Programmatic Advertising? The Must-Have 2021 Guide”, Match2one, 27 January, available at: https://www.match2one.com/blog/what-is-programmatic-advertising/ (accessed 23 March 2021).

Ravichandran D. and Korula, N. (2019), “Effect of disabling third-party cookies on publisher revenue,” available at: https://services.google.com/fh/files/misc/disabling_third-party_cookies_publisher_revenue.pdf (accessed 3 July 2021).

Rocher, L., Hendrickx, J. M. and de Montjoye, Y. A. (2019), “Estimating the success of re-identifications in incomplete datasets using generative models”, *Nature Communications*, Vol. 10, p. 3069.

Roberstson, A. and Brandom, R. (2021), “Google antitrust suit takes aim at Chrome’s Privacy Sandbox”, The Verge, 16March, available at: https://www.theverge.com/2021/3/16/22333848/google-antitrust-lawsuit-texas-complaint-chrome-privacy (accessed 23 March 2021).

Rogers, C. (2017), “What is programmatic advertising? A beginner’s guide”, Marketing Week, 27March, available at: https://www.marketingweek.com/programmatic-advertising/ (accessed 23 March 2021).

Schumann, J.H., von Wangenheim, F. and Groene, N., (2014), “Targeted online advertising: Using reciprocity appeals to increase acceptance among users of free web services”, *Journal of Marketing*, Vol. 78 No. 1, pp. 59-75.

Sheehan, K. B., and Hoy, M. G. (1999), “Flaming, Complaining, Abstaining: How online users respond to privacy concerns”, *Journal of Advertising*, Vol. 28 (Fall), pp. 37-51.

Shields, R. (2021), “Tension Between Privacy and Competition Exposed in Google’s Latest Regulatory Probe”, Adweek, 13January, available at: https://www.adweek.com/programmatic/tension-between-privacy-competition-exposed-google-regulatory-probe/ (accessed 23 March 2021).

Smith, H. J., Milberg, S. J., and Burke, S. J. (1996), “Information privacy: Measuring individuals' concerns about organizational practices”, *MIS Quarterly*, Vol. 20 No. 2, pp. 167-196.

Spake, D. F., Zachary Finney, R. and Joseph, M. (2011), "Experience, comfort, and privacy concerns: antecedents of online spending", *Journal of Research in Interactive Marketing*, Vol. 5 No. 1, pp. 5-28.

Spangler, W. E., Hartzel, K. S., and Gal-Or, M. (2006), “Exploring the privacy implications of addressable advertising and viewer profiling”, *Communications of the ACM*, Vol. 49 No. 5, pp. 119-123.

Strandburg, K. J., (2013), “Free fall: The online market's consumer preference disconnect”, *University of Chicago Legal Forum*, Vol. 2013 Article 5, pp. 95-172.

StatCounter (2021), “Desktop Browser Market Share Worldwide” available at: https://gs.statcounter.com/browser-market-share/desktop/worldwide (accessed 23 March 2021).

Stuart, A., Bandara, A. K., and Levine, M. (2019), “The psychology of privacy in the digital age”, *Soc Personal Psychol Compass*, Vol. 13 No. 11, pp. 12507.

Taddicken, M. (2014), “The ‘Privacy Paradox’ in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure.”, *Journal of Computer-Mediated Communication*, Vol. 19 No. 2, pp. 248-273.

The Trade Desk. (2020), “In Human Terms, Episode 15: Unified ID 2.0”, YouTube, 18 November, available at: https://www.youtube.com/watch?v=mJP2ngh0owc (accessed 23 March 2021).

Turow, J., Delli Carpini, M. X., Draper, N. A., and Howard-Williams, R., (2012), “Americans roundly reject tailored political advertising”, available at: https://repository.upenn.edu/cgi/viewcontent.cgi?article=1414&context=asc_papers.

Turow, J., King, J., Hoofnagle, C. J., Bleakley, A., and Hennessy, M. (2009), "Americans reject tailored advertising and three activities that enable it", Available at SSRN 1478214.

WashPostPR (2020), “The Washington Post adopts Unified ID 2.0 to control first party data”, The Washington Post, 16 December, available at: https://www.washingtonpost.com/pr/2020/12/16/washington-post-adopts-unified-id-20-control-first-party-data/ (accessed 24 March 2021).

Winegar, A. G. and Sunstein, C. R., (2019), “How much is data privacy worth? a preliminary investigation”, *Journal of Consumer Policy*, Vol. 42 No. 3, pp. 425-440.

Wirtz, J., Lwin, M.O. and Williams, J.D. (2007), "Causes and consequences of consumer online privacy concern", *International Journal of Service Industry Management*, Vol. 18 No. 4, pp. 326-348.

Wolly, M. (2020), “How publishers can invest in a privacy-forward future now”, Think with google, July, available at: https://www.thinkwithgoogle.com/future-of-marketing/privacy-and-trust/consumer-privacy-regulations/ (accessed 23 March 2021).

Yim, O. and Ramdeen, K. T. (2015), “Hierarchical cluster analysis: comparison of three linkage measures and application to psychological data”, *The Quantitative Methods for Psychology*, Vol. 11 No. 1, pp. 8-21.

[i] https://blog.google/products/chrome/updated-timeline-privacy-sandbox-milestones/
[ii] webcookies.org, “Web cookies scanner,” available at https://webcookies.org/number-of-cookies/ (accessed 31 March 2021)
[iii] https://www.thetradedesk.com/us/about-us/industry-initiatives/unified-id-solution-2-0
[iv] https://www.adexchanger.com/strategy/the-trade-desks-unified-id-is-gaining-steam-heres-where-things-stand/
[v] https://www.youtube.com/watch?v=mJP2ngh0owc
[vi] Dave Pickles interview 9-9:45 am Sept 24, 2020 Groundswell Identity and https://www.youtube.com/watch?v=mJP2ngh0owc&feature=youtu.be
[vii] https://www.youtube.com/watch?v=Jmmv_QLQtnQ
[viii] https://www.emarketer.com/content/do-people-actually-want-personalized-ads
[ix] AdWeek Zoom Presentation August 18 Identity 2020: The Future of Addressable Digital Adverting & Dave Pickles 9-9:45 am Sept 24, 2020 Groundswell Identity
[x] https://github.com/michaelkleber/privacy-model
[xi] https://github.com/WICG/sparrow
[xii] https://github.com/google/ads-privacy/tree/master/proposals/dovekey
[xiii] https://github.com/michaelkleber/privacy-model

[xiv] https://github.com/WICG/turtledove, https://github.com/WICG/turtledove/blob/master/FLEDGE.md, and https://github.com/jkarlin/floc

[xv] https://privacysandbox.com/

[xvi] https://github.com/WICG/turtledove, https://github.com/WICG/turtledove/blob/master/FLEDGE.md, and https://github.com/jkarlin/floc

[xvii] https://github.com/WICG/sparrow

[xviii] https://www.gov.uk/government/news/cma-to-investigate-google-s-privacy-sandbox-browser-changes

[xix] https://github.com/WICG/sparrow

[xx] https://www.chromium.org/Home/chromium-privacy/privacy-sandbox

[xxi] https://github.com/michaelkleber/privacy-model

[xxii] http://www.prolific.co/

[xxiii] https://github.com/WICG/turtledove/blob/main/FLEDGE.md

[xxiv] https://www.centiment.co

[xxv] https://www.mvsolution.com/wp-content/uploads/SPSS-Tutorial-Cluster-Analysis.pdf

[xxvi] https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/pi_2019-11-14_privacy_0-02-2/

Tables

Table I: Study 1 - Items and factor loadings from measure validation trial.

		Factor Loadings			
Preference for relevant ads		1	2	3	4
	I would rather see ads that are relevant to me than generic ads.	.31	-.20	.14	**.86**
	The ads I see on websites should be for things that interest me.	.33	-.11	.14	**.88**
	I prefer to see ads for things I might buy than for things I wouldn't buy.	.26	-.12	.12	**.89**
Acceptance of quid pro quo					
	It is OK for advertisers to know what websites I visit if that means the websites are free.	.29	-.26	**.81**	.08
	Letting advertisers know who I am is a fair exchange for websites being free.	.16	-.30	**.79**	.19
	Allowing advertisers to collect detailed information about my interests online is a fair price to pay for keeping the internet free.	.17	-.21	**.84**	.20
	If selling information about the pages I visit allows a website to be free, I'm okay with them selling that information.	.26	-.29	**.81**	.00
Desire to prevent data collection					
	Advertisers should be prevented from knowing what websites I visit.	-.16	**.86**	-.22	-.12
	Advertisers should be prevented from making databases about what I do online.	-.11	**.86**	-.21	-.18
	Websites should not be allowed to sell information about me.	-.02	**.86**	-.29	-.07
	Advertisers should not be allowed to trade information about me.	-.03	**.89**	-.23	-.08
Acceptance of limited information					
	It is okay if online advertisers get some information about me, but not enough to figure out who I am.	**.79**	-.13	.25	.22
	Online advertisers should be able to learn my broad interests, but not interests that are specific to me.	**.76**	-.00	.05	.31
	Advertisers on the internet should receive only enough information to know if they want to show me an ad but no more.	**.82**	.00	.11	.21
	It's alright if online advertisers know I am interested in buying a product they sell, as long as they don't know who I am.	**.84**	-.12	.27	.20
	If they cannot identify me, it is OK for advertisers to know that I have visited their website in the past.	**.75**	-.18	.31	.14

Table II: Study 1 - Items for measure of acceptance of first-party data use.

Acceptance of first-party data use	
	I don't mind when websites use my page view history to sell ads on their website.
	It is OK when social media platforms use information about the posts I made to sell ads.
	It is alright when search engine websites use my search history to sell ads.
	It is alright when online stores use information about my past purchases to sell ads.
	I don't mind when websites where I left an item in the shopping cart show me ads for that item on other websites.

Table III: Study 1 - Descriptive statistics and correlations.

	M	*SD*	1	2	3	4	5
Preference for relevant ads	5.39	1.22	(.86)				
Acceptance of quid pro quo	3.46	1.52	.28***	(.90)			
Desire to prevent data collection	5.94	1.10	.02	-.43***	(.86)		
Acceptance of limited information	4.89	1.30	.40***	.44***	-.05	(.86)	
Acceptance of first-party data use	3.35	1.49	.27**	.71***	-.41***	.41***	(.91)
Age	53.59	17.27	-.09	-.05	.05	-.01	-.23***

Note. *N* = 818. Cronbach's alpha values on the diagonal. ** *p* < .01; *** *p* < .001.

Table IV: Study 1 - Clusters with variable means.

	Cluster 1 *N* = 209 "Everything goes Evan"	Cluster 2 *N* = 212 "Ambivalent Amy"	Cluster 3 *N* = 277 "Anonymous Anna"	Cluster 4 *N* = 120 "Private Priscilla"
Preference for relevant ads	6.33	4.80	5.69	4.14
Acceptance of quid pro quo	5.13	4.08	2.46	1.76
Desire to prevent data collection	5.77	4.86	6.56	6.70
Acceptance of limited information	5.95	4.61	5.16	2.87
Acceptance of first-party data use	4.51	3.81	2.78	1.81

Note: The first four variables were used to define the consumer clusters.

Table V: Study 2 - Reddit content analysis summary

Subreddit	Category	Stakeholder	# or Relevant posts (Total Comments)
/r/Adblock	Google Sandbox	General (tech)	1 (3)
/r/adops	UID 2.0, Google Sandbox	Digital advertising professionals	15 (361), 1 (14)
/r/bigseo	General Privacy	Info (marketing)	21 (500)
/r/chrome	Both	General (tech)	1 (1)
/r/cybersecurity	General Privacy	General (security)	24 (500)
/r/degoogle	General Privacy	Tech enthusiasts	18 (500)
/r/europrivacy	General Privacy	General (privacy)	14 (500)
/r/Frontend	Google Sandbox	Web developers	1 (37)
/r/google	Google Sandbox	General (tech)	1 (64)
/r/hacking	Google Sandbox	Security enthusiasts	1 (19)
/r/hackernews	Google Sandbox	Security enthusiasts	1 (2)
/r/netsec/	General Privacy, Google Sandbox	Info security professionals	21 (500) 1 (2)
/r/privacy	General Privacy, Google Sandbox	General (privacy)	33 (500) 2 (32)
/r/privacy tools	General Privacy	General (privacy)	23 (500)
/r/programming	Google Sandbox	Software developers	1 (39)
/r/security	General Privacy	Info security professionals	40 (500)
/r/seo	General Privacy	AdTech	25 (500)
/r/tech	General Privacy, Google Sandbox	General (tech)	9 (500) 1 (1)
/r/technewstoday	General Privacy	Tech enthusiasts	6 (500)
/r/technology	Google Sandbox	General (tech)	1 (8)
/r/techolitics	General Privacy	Tech enthusiasts	93 (500)
/r/techsupport	General Privacy	IT professionals	53 (500)
/r/webdev	General Privacy	Web developers	43 (500)
/r/web_design	Google Sandbox	Web designers	1 (1)