Prepared for the 2022 Workshop on the Economics of Information Security. Please do not cite without the authors' permission.

Exploring the role of data enclosure in the digital political economy

Brenden Kuerbis, Georgia Institute of Technology

Milton Mueller, Georgia Institute of Technology

Abstract: This exploratory research analyzes the impact of data enclosure initiatives on market competition. *Data enclosure* is the process by which the information about user activity generated by digital operations are withdrawn from an open or shared arrangement with other operators and made more exclusive to the service providers whose operations generate the data. We make the case that data enclosure is emerging as a significant feature of the multi-sided markets of digital platform providers, by looking empirically at, 1) the encryption of DNS query data using the DNS over HTTPS (DoH) protocol, and 2) Apple's and Google's enclosure of mobile identifiers used in digital advertising and cross-app user tracking. These efforts are not only privacy-enhancing moves, but also a means by which service providers compete with each other over the value and security of data. We assess the degree to which exclusivity of data fosters or forecloses competition in the relevant markets, and find mixed results. DoH, apparently a more disruptive form of data enclosure, has had little impact on industry shares so far, primarily because it was embraced by a small-share, declining actor, but the growing use of DoH and other encrypted DNS protocols does indicate a market-driven response to privacy-enhancement. In mobile identifiers in adtech, the shift in the default from opt-out permission to opt-in permission had both strong privacy effects and major effects on the distribution of revenues in the industry. But the changes are recent and the situation remains unsettled.

Introduction and research question

This exploratory research is intended to analyze the impact of data enclosure initiatives on market competition. *Data enclosure* is defined here as the process by which the information about user activity generated by digital operations are withdrawn from an open or shared arrangement with other operators and made more exclusive to the service providers whose operations generate the data. We make the case that data enclosure is emerging as a significant feature of the multi-sided markets of digital platform providers. It reflects ongoing competitive struggles over the value, utilization and protection of the vast amounts of user behavior data generated by the digital infrastructure. Enclosing data turns what was once a data commons (and a privacy problem) into a resource that a defined set of actors in the digital ecosystem have more control over, and from which competitors (as well as hackers or unwanted surveillance) can be excluded. Conceptual development and preliminary analysis of the economic impact of data enclosure will facilitate a better understanding of the relationship between privacy policy and competition among digital platforms. It also challenges key premises

of leftist privacy scholars' critique of 'Big Tech' and 'informational capitalism' (Cohen 2017; Zuboff, 2019; Pistor, 2020) and can incrementally contribute to established literature in privacy economics (e.g., Acquisti, Taylor and Wagman, 2016), modeling and legal analysis of the relationship between privacy and antitrust and competition (e.g., Bergemann and Bonatti, 2022; Economides and Ioannis, 2020; Argenziano and Bonatti, 2020; Ohlhausen and Okuliar, 2015; Shy and Stenbacka, 2015), and data markets (e.g., Arrieta-Ibarra et al., 2018; Spiekermanm et al., 2015; Laudon, 1996).

The issue of data exclusivity is fundamental to current Internet policy debates. It is relevant not only to privacy policy and data protection law and regulation, but also to concerns about platform competition. Firms in the internet ecosystem are now using enhanced confidentiality of user data as a selling point to their customers. But data enclosures do not just respond to users' and governments' privacy concerns, they may also provide a competitive advantage to a platform by excluding their competitors or other players from access to data generated by their users. Internalizing the costs of protecting privacy can also privatize the economic benefits of data. Any realistic appraisal of the platform economy must look at both sides of this equation.

Part 1 of this paper situates the data enclosure phenomenon in an ongoing theoretical debate about property rights and markets for data in the context of platforms. Part 2 describes empirically two instances of data enclosure: 1) the encryption of DNS query data; and 2) Apple's and Google's enclosure of mobile identifiers used in digital advertising. Encrypting DNS queries or restricting usage of advertising identifiers in cross-app user tracking are not only privacy-enhancing moves, but also a means by which service providers compete with each other over the value and security of data. Part 3 assesses the degree to which exclusivity of data fosters or forecloses competition in the relevant markets.

1. Theory: Political Economy of Data/Platforms

'Data' is often reified as the resource of the digital economy, but this can be misleading. It implies that the platform economy's value stems from a recorded and stored pile of bits and bytes that, like oil ("data is the new oil"), can be "mined" for its economic value. This view of data as a static commodity obscures the operational and business reality of the platform economy. Platforms are multi-sided markets (Evans and Schmalensee, 2016). That means they function as an intermediary between different groups of users to facilitate value-creating exchanges. In this business model, digital data is "co-generated by individuals through platform interactions,

and channeled to and from networked actors on the other side of the platform who use it in real-time." (Benthall and Goldenfein, 2021, p. 5) More precisely, user behavioral data is an *input* into a *service production process* which contributes to the matching and monetization algorithms of the platform. The business value of the platform depends less on "lots of data" and more than anything else on *lots of users* (just as traditional advertising-funded services do); the behavioral data just makes matching the different sides of the market more efficient.

Contrary to the popular critique characterizing users as exploited "unpaid data producers" (Pistor, 2020), a mutual economic benefit underlies the user-platform interaction. Consumers are "paid" by the platforms' provision of free information services and matches. Many of these services are incredibly valuable but now seem to be taken for granted, perhaps because of the platforms' success at making them ubiquitous: search engines, email, informational and entertainment content, document storage, and thousands of connections to products, other individuals and groups. Economists working out the logic of multi-sided markets have repeatedly demonstrated how it makes business sense for one side to subsidize entry or participation costs of another side (Rochet and Tirole, 2006; Parker, Van Alstyne & Choudary, 2016). It is also misleading to suggest that the users alone are the "producers" of the data, or that data is being "extracted" from them. While their activities do provide content, without the platform infrastructure itself there are no data and no useful applications for the data. Even severe but realistic critics of the digital market economy (Benthall and Goldenfein 2021) admit that the data is co-produced.

1.1 Exclusivity in data

Data enclosure is a way to create exclusive access to data, and thus raises the issue of property rights in information. In political economy, a property right denotes a form of control over a resource that assigns to the controller the right to benefit from it, the right to exclude others from those benefits, and the right to transfer. (Alchian, 1965; Demsetz, 1974; Barzel, 1997) As we will argue below, exclusivity is the most fundamental feature of a property right; without it, the other two features are less meaningful. Exclusion allows the owner to capture the value, either by using it or by trading it.

In a purely abstract sense, digital data seems to resist exclusivity. Digital data is nonrival in consumption (i.e., one person's use of it does not consume or "use up" the resource). Because of the rapid, practically costless way it can be duplicated and transmitted, it is also notoriously difficult to contain. For those reasons, digital data seems to meet both criteria of a

public good: it is both nonrival in consumption and difficult or impossible to make exclusive. (Samuelson, 1954) But this attempt to remove data resources from a market economy framework fails on two counts. First, in a digitized world, treating data as a public good poses a huge problem for privacy. It would mean that large amounts of PII and users' behavioral data are unprotected and freely appropriable. Even the most rabid critics of informational capitalism recoil at this prospect.[1] Any argument for privacy in the digital world necessarily involves some form of exclusion from access to data. Second, exclusion from data resources can and does happen all the time. Exclusion can be achieved by legal means, e.g., the European Commission's Data Governance and Data Acts, which seek to define rights (including exclusion) associated with co-generated data.[2] But it can also be done technologically or operationally. A simple example is the way encrypting TV signals changed satellite television from an open-access broadcast service to a paid, subscription service. (Kuerbis and Mueller, 2020) Third, even in resource regimes where exclusion is difficult, such as the common pool resources explored by Ostrom (1990; 1994), governance can be achieved by establishing collectively binding rules governing access and appropriation. But this requires the governance institution to establish boundaries of exclusivity around the collectivity in control of the common pool.[3] Most of the platform critics are arguing for some kind of data trust or collective governance approach which would rely on exclusivity.

In their data enclosure initiatives, platforms and other digital service providers are establishing de facto control over the data by *technological* means. Platforms withhold from others operational data generated by their users, instead of sharing it. The term "enclosure" can have negative connotations[4], but we use it in a scientific not normative sense, to describe a

[1] Indeed, a data "commons" - the ability to freely appropriate the footprints and records generated by users of the vast digital infrastructure - is the ultimate foundation of so-called surveillance capitalism (see Zuboff, 2019, Chapter 3) because it allowed the early tech giants a huge first-movers advantage in appropriating unprotected resources.

[2] See the proposed Data Act at https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113 and 2020 Data Governance Act at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

[3] Only pure open access regimes lack exclusion, and they are known to foster inefficient allocations (the tragedy of the commons).

[4] These stem from a quasi-Marxian interpretation of the enclosure of agricultural and grazing land in England in the 17th and 18th centuries. (Wordie, 1983; Mingay, 1997) The English enclosures were part of a long-term evolution of an industrial market economy. Private and exclusive property rights supplanted a system of small-scale shared or informally-defined land rights. It was a transformation of property structures that established a resource allocation mechanism more suited to larger-scale production, a greater specialization and division of labor in commodities such food and wool, and markets for land and its products. In the quasi-Marxian spin, the term "enclosure" connotes something being grabbed and stolen from the public. But this is only "quasi-Marxian" because while these negative interpretations characterize propertization as a destructive departure from a pre-existing idyllic, communal society, Marxist theory itself characterized the emergence of private property as both historically necessary and as a major enhancement of society's "productive forces." So the negative take reflects more a kind of vulgar Marxism or anti-market sentiment than Marxist political economy.

transformation of property relations that emerges as an institutional byproduct of market interactions. Note that the platforms' control of the infrastructure allows them, not individual users, to assert the property right. They are the parties best positioned to gather and put to use the patterns generated by user behavior. Indeed, it is hard to conceive of what users themselves would do with data about their own online activity.

1.2 Enclosure and competition in data markets

A significant number of legal scholars concerned with privacy (Cohen, 2017; Pistor, 2020; Viljoen, 2020; Benthall and Goldenfein, 2021; Zuboff, 2019) argue that platforms usurp the entire notion of a liberal market economy and use this assertion as the springboard for proposals for radical transformations of the information economy.[5] In our view, the emergence of data enclosure is a reconfiguration of property rights that is fully consistent with the operation of a liberal market economy. Moreover, it addresses some of the concerns privacy advocates have expressed and does so without the *a priori*, top-down and likely unimplementable reforms proposed by the critics.

An analysis of data enclosure suggests that in a contested, multi sided market, a digital platform provider competing for users would have two distinct incentives: 1) an incentive to use the privacy and security of their users' data as a product differentiator; 2) an incentive to assert or maintain exclusivity over the data co-generated by its users and its infrastructure to maintain or increase a competitive advantage in the provision of intermediation. The product differentiation incentive and the exclusion incentive can reinforce each other, but sometimes they can work at cross-purposes.

In the first case (better privacy as competitive advantage) a provider would advertise superior data security for users, propose better privacy policies, or offer more secure operational techniques. Apple has clearly chosen this path, publicly branding its products and services as more privacy-protective than its major platform rivals. There is also substantial evidence of privacy/security as a product differentiator in the DNS resolution market. Cloudflare, Google and Mozilla all touted the enhanced security of their encrypted DNS resolution services. However, the privacy differentiation incentive might also push them toward limiting potential ways of monetizing the data/users to which they have exclusive access. We provide examples of both in the empirical section of the paper.

[5] Pistor (2020) is typical of the sweeping and in some cases obviously inaccurate claims: platform-generated data is a "tool for governing others that rivals nation-states with their law" and "consumers are [not] free to choose which services they use, or which goods they buy. Big Tech has taken over the process of selecting and choosing."

In the second case, a platform may achieve a competitive advantage by generating and/or acquiring data that is different from, and somehow more useful than, the data possessed by its competitors. As the earlier analysis suggested, the best way to do this is to attract users that the other platforms don't have, and secondarily to expand the types of services bundled into the platform (e.g., by linking a mobile operating system that delivers search and app store to a home Internet of Things (IoT) service). In this case, the business would not have an incentive to share that data. It would deny its rivals access to data and users that it uniquely possesses. This does not seem to be what is happening with the DNS query data, but it may describe what Apple is doing by withdrawing IDFA - both discussed in the empirical part of the paper.

2. Instances of Data Enclosure

This research identifies two digital data markets, DNS query data and mobile adtech identifiers, where data enclosure activity is occurring among firms. We try to assess the motives and incentives of the companies engaged in enclosure, and assess its effect on competition in the market. A complete study would need to: a) identify instances; b) measure the deployment or scope of data enclosure in the relevant markets over a defined period of time; c) examine the distribution of revenue and market share before and after the data enclosure measures; and d) assess the impact of the enclosure on market concentration and the firm's business (revenues, market share, growth or decline).

This paper constitutes a first pass reliant on what is anachronistically called "desk research" but which really means "Internet search" and "reliance on publicly available data." Some data sources are incomplete or unsatisfactory. Some of our interpretations of the actors' incentives and intentions are tentative, and could benefit from interviews with the business firms themselves. Still, there is sufficient data to fulfill the two objectives of this research: 1) to document that data enclosure is in fact happening in significant parts of the platform market, and 2) to demonstrate that it poses an interesting trade-offs or interactions between privacy policy and competition policy.

2.1 Encrypting DNS

Under traditional DNS, the queries and responses needed to resolve domain names move between the end user and their local ISP over Port 53 using Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). This transmission takes place in clear text.

Under this arrangement, neither the queries nor the responses are encrypted when they are transported between the parties, nor are the endpoints of communication authenticated. That makes the data visible to anyone capable of monitoring the traffic. This is more than just a privacy concern, it is also a political and economic issue. Many censorship and organizational security policies have been predicated on the use of open, freely available DNS query data. Examples include the United Kingdom's Digital Services Act requiring blocking of domains associated with certain content, or organizations implementing split-view DNS to restrict DNS data to different network segments or hosts.

Previous work by Kuerbis et al. (2020) explains how DNS query data is economically valuable. Among other things it can contribute to user profiling or play a role in network security services, traffic management and content delivery networks. In the last 10 years, the lack of confidentiality of DNS query data began to be seen as a privacy problem. (Bradshaw and DeNardis, 2016) Motivated by a heightened commitment to privacy and security in the post-Snowden era, the IETF has since 2014 developed three different standards for encrypting DNS query data: DNS over Transport Layer Security (DoT), DNS over QUIC (DoQ) and DNS over HTTPS (DoH). It is useful to analyze the adoption of these technologies and the way each of these standards distributes control over DNS query data.

DoT, standardized in 2016, uses an assigned, dedicated port (Port 853) to encrypt the network path between the Internet Service Provider (ISP) to the domain's resolver. This means that the data available to the ISP and the domain's resolution service doesn't change, as they must both be able to decrypt the data. This technique leaves the existing relationship between the customer, the ISP, and the domain resolution service structurally unchanged, and does not exclude those existing players from access to DNS query data. DoT allows the user's network administrator (a commercial ISP or enterprise network) to monitor and block DNS queries.

The DNS over HTTPS (DoH) standard, in contrast, has more radical effects. The existing order of user - supplier contractual relations is rebalanced, and the implementation of encryption in this case excludes more actors from query data. DoH runs the DNS resolution protocol out of an application on the end user's device. It is no longer a service bundled with the user's Internet access, it is a service bundled in a browser. The choice of a resolver can be embedded in an application which is controlled by the browser producer. Another power-rebalancing effect of DoH is the deliberate mixing of DNS resolution traffic with all other Web traffic. DoH queries do not have a dedicated port like DoT; they go through port 443 with all the other HTTPS traffic. This means that DNS queries and responses cannot be messed with, either by "good guys" (LEAs or well-meaning censors who want to block certain bad domains) or by "bad guys"

(authoritarian governments, cybercriminals, nation-state military hackers). For this reason, only DoH can be considered an act of data enclosure by our definition.

However, the ability of DoH to shift control of query data depends on its implementation and the policies of the browser application. DoH was enabled in two of the main browsers (Chrome and Firefox) in September 2019[6] and September 2018[7], respectively. On Feb 25, 2020[8], Firefox's owner, Mozilla, began the rollout of encrypted DoH by default for US-based users, pointing them to Cloudflare's name server by default, but also allowing users to specify other name servers in their Trusted Recursive Resolver program. On the other hand, Google's launch of DoH in Chrome, which occurred in May 2020[9], did not do this, instead switching users over to DoH if their current DNS provider supported it, and providing manual configuration options for users that wished to use a specific name server.

In early 2021, a fourth standard, Oblivious DoH (ODoH), took the protection of the privacy of DNS queries even further. (Saha, 2021; Verma and Singanamalla, 2020). Noting that even with DoH, "the resolver can still link all queries to client IP addresses," and that some users may not be willing to trust Cloudflare with sensitive query information, Cloudflare began working with Apple and Fastly to develop a new IETF standard that introduces a proxy that obfuscates the link between DNS queries and IP addresses.[10] As of this writing ODoH is still an Internet-draft, and since it has not been implemented it is not discussed any further in this paper.

2.2 Enclosing mobile identifiers

Apple and Google are developing mechanisms governing the use of identifiers within their mobile platforms, and their deployment provides an inflection point potentially impacting broader adtech market competition. Similar to the use of unique cookie identifiers in browser applications to facilitate user tracking and ad placement across websites (also a technology which Apple and Google have sought to influence[11]), the iOS IDentifier For Advertising (IDFA)

[6] https://blog.chromium.org/2019/09/experimenting-with-same-provider-dns.html

[7] https://wiki.mozilla.org/Trusted_Recursive_Resolver

[8] Mozilla blog. https://blog.mozilla.org/en/products/firefox/firefox-continues-push-to-bring-dns-over-https-by-default-for-us-users/

[9] https://blog.chromium.org/2020/05/a-safer-and-more-private-browsing-DoH.html

[10] It is an organizational separation, query data privacy depends on the proxy and the target server operators not colluding.

[11] Specifically, Apple and Google moved to block third party cookies in the Safari and Chrome browsers used on desktops and laptops. Third party cookies are set in a browser by a party other than the website the user is visiting and used to track users across websites. Apple implemented this change in March 2020, with Google set to do the same in 2023. Google has several proposals for replacing cross-site tracking functionalities accomplished by

and Android Advertising ID (AdID) have been used to identify and track users' mobile devices across different apps installed on the device. This permits advertisers to deliver personalized and targeted ads, measure campaign performance, control the frequency of ads, and attribute impressions and clicks to app installs, among other things. (ClearCode, 2020). Apple and Google control who uses the IDFA and AdID and how they are used through their respective platforms including App Stores and mobile devices. They do this by means of their contractual arrangements with users and application developers, as well as enforcement of data use within the operating system.

Apple announced its decision to limit tracking across apps in September 2020 as part of iOS 14[12], and it's AppTracking Transparency (ATT) framework was launched in the iOS 14.5 release in April 2021.[13] It requires that app developers explicitly ask users to opt-in to developers' use of the IDFA to track and target users with personalized ads across apps. In place of using the IDFA for tracking, Apple is now offering its SKAdNetwork (Store Kit Ad Network), a set of internally developed protocols and standards to "help advertisers measure the success of ad campaigns while maintaining user privacy."[14] Google's Android, on the other hand, allows users to opt out from ad personalization based on cross site tracking using the AdID, or to reset their AdID when desired.[15] Google launched its Privacy Dashboard as part of Android 12 in October 2021. The Privacy Dashboard essentially provides the same level of cross app tracking control to users, however it requires the user to dig into the OS settings and make several decisions.[16]

---

third-party cookies, see its Privacy Sandbox initiative (https://www.chromium.org/Home/chromium-privacy/privacy-sandbox) which has been met with some resistance, although in February 2022 Google announced it was extending the Privacy Sandbox to Android as well. https://www.blog.google/products/android/introducing-privacy-sandbox-android/

[12] Details for app privacy questions now available, September 3, 2020. https://developer.apple.com/news/?id=hx9s63c5

[13] Asking Permission to Track, https://developer.apple.com/app-store/user-privacy-and-data-use/

[14] SKAdNetwork. https://developer.apple.com/documentation/storekit/skadnetwork

[15] Google's AdID tracking policy is the focus of a legal action taken under the EU's GDPR, see Moody (2020).

[16] Android 12's new privacy settings draw a clear line between Google and Apple, May18, 2021.https://www.macworld.com/article/346892/android-12s-new-privacy-settings-draw-a-clear-line-between-google-and-apple.html

3. Adoption and competitive effects of data enclosure

This section attempts to place data enclosure efforts into a descriptive analysis of its competitive effects, drawing on quantitative data when possible.

3.1 Adoption of Encrypted DNS

In order to measure the level of data enclosure taking place in the DNS query process, we need to measure the degree to which DoH has been implemented. The availability of DoH as a standard (RFC 8484) does not mean that everyone instantly uses it. Many end users and ISPs continue to use legacy unencrypted DNS, while others may implement the two other query encryption standards (DoT or DoQ). Further, signs of accelerating, declining or static levels of DoH adoption can provide evidence of the incentives for DNS query data enclosure among the relevant parties.

Data sources about DoH adoption levels are insufficient.[17] Currently the best available indicator of the current take-up rate of encrypted DNS is a written statement by APNIC's Chief Scientist, Geoff Huston. APNIC has set up measurement apparatus for DNS traffic dating from August 2020 to the present. In a recent blog post Huston writes: "The query volume for DoT and DoH [over the past 15 months] has increased 5-fold, from 2.5% of queries to 12% of queries. The split between DoT and DOH is approximately even these days." (Huston, 2021). However, these observations are again limited to a single network, in this case Google's Public DNS service. Thus we conclude that encrypted DNS is still a minority of DNS traffic. Hence, our assessment of its competitive effects is going to be moderated by its still-emerging presence.

3.2 Competitive effects in DNS query

Encrypted DNS is still in its early stages of adoption. Its effects on competition, if it has had any at all, are thoroughly entangled with a larger shift toward the concentration of users and

[17] Internet measurement topics necessarily lag implementations by a couple of years. DoH is too new to attract much attention from the IMC community. We know of one internet measurement study that attempts to identify the amount of encrypted DNS traffic (Garcia, Hynek et al, 2021) The study's results showed miniscule levels of encrypted DNS as a portion of all DNS-related flows (0.01% to 0.033%). This may be true or it may be because they are measuring the wrong things (e.g., it did not disambiguate browser based requests from non browser requests, creating a possibility that queries generated by automated processes were overwhelming actual user activity in their measurements. We rely on APNIC measurements instead.

advertisers on a few major platforms. One the other hand, the backers of the standardization process from which it emerged and implementation decisions indicate that data enclosure figured prominently in the DoH story.

We find that enclosure and exclusivity moves are being used by two smaller competitors as a tactic against the data-dominance of their bigger rivals. The smaller competitors are Mozilla (which develops and supports the Firefox browser) and Cloudflare (an open resolver, cloud and security platform). Mozilla was a key backer in getting DoH through the IETF, and it was a leader in default implementation of it in their browser. As Google's Chrome browser's user share has peaked, Firefox's share has declined. Measures detecting browser use find only about 4% of the users reaching them via Firefox.[18] Mozilla faced layoffs and shrinking revenues in 2019 and 2020. Cloudflare is also a runner-up to Google in the DNS open resolver market.

DoH was promoted to the public as a privacy and security advance. Mozilla denied any economic motives or benefits: on its website about DoH, Mozilla wrote, "No money is being exchanged to route DNS requests to our default resolver partners."[19] And while the company recognizes the value of the data DoH could steer towards it, it claims "our policy explicitly forbids monetizing this data." Likewise, Cloudflare publicity also explicitly distances the company from any additional monetization or even use of DNS resolution data. It is developing and promoting Oblivious DoH (ODoH) as an even more privacy-protective alternative to DoH. ODoH is a protocol that would undercut many data advantages.

However, there is more to this than privacy-differentiation. DoH was a means by which Cloudflare and Mozilla tried to undercut one of Google's competitive advantages. Mozilla has openly stated that in addition to user privacy protection, "Our goal with this feature [DoH] is to … make it harder for existing DNS resolvers to monetize users' DNS data."[20] Privacy-protecting technologies, in other words, not only provide boasting rights for their implementers, but also chip away at the data exclusivity of Google, one of the dominant platforms in DNS resolution. This would explain why Firefox, a smaller browser share, was willing to implement DoH in a way that defaulted traffic to Cloudflare.

For its part, Google did not come up with the idea for DoH, did not promote it as part of its competitive strategy, nor did it implement it in a way that could have reinforced its advantages. Google could have leveraged the dominance of its Chrome browser to implement

---

[18] Google Chrome browser market share has peaked at around 60% globally https://gs.statcounter.com/browser-market-share

[19] DNS-over-HTTPS (DoH) FAQs, https://support.mozilla.org/en-US/kb/dns-over-https-doh-faqs

[20] DNS-over-HTTPS (DoH) FAQs https://support.mozilla.org/en-US/kb/dns-over-https-doh-faqs#w_is-mozilla-getting-paid-to-route-dns-requests-to-its-default-resolvers

DoH in a way that defaulted DNS resolution to its own DoH resolver service. It refrained from doing so. Google went along with DoH, but did not lead it. But then, it did not need it. As a platform with multiple services, Google is in a position to share the end-user's query data with its subsidiary advertising services like AdWords and Double Click. Adoption of DoH does not undermine their access to this data as long as users rely on the Chrome browser. With its dominant positions in browser software, search and open resolver service, Google has no real incentive to rebalance the industry in this way. Besides, aggressive enclosure of data might trigger political reaction and legal (antitrust) scrutiny.

3.3 DoH and market share

According to APNIC measurements of DNS resolver use,[21] Cloudflare has increased its share of worldwide DNS resolver usage from 2.5% to about 4% from August 2020 to December 2021. (APNIC measurement data begins in August 2020) However, this user share gain has not come at the expense of Google, whose Public DNS usage share worldwide grew from roughly 15% to 23%. According to Huston, "the number of users passing queries through Google's resolution service has grown by 50% over the past 15 months."

We see no positive effects that DoH has brought to Firefox. Its share of browser usage in the U.S. (where it first implemented DoH by default), has declined from roughly 4.6% in February 2020 to 3.9% in December 2021.[22] A full econometric test of these effects is outside the scope of this paper, but the available data shows no discernible change in the long term decline in Firefox share that could support a conclusion that DoH had an impact - positive or negative. Even if the privacy benefits of DoH was a feature that attracted more users, Google could easily neutralize those gains by matching Firefox's and Cloudflare's support for DoH and DoT, which it did.

3.4 Adoption of iOS 14.5 and Android 12

To measure the level of data enclosure taking place with mobile identifiers, we need to measure the degree to which the operating systems implementing the policy change have been adopted. Given the substantial change in data access with Apple iOS 14.5, one might have expected to see rapid adoption. However, as Figure 1 shows, adoption of iOS 14+ doesn't look substantially different from adoption patterns of iOS 13 (in shades of red) or previous versions.

[21] https://stats.labs.apnic.net/rvrs/

[22] https://gs.statcounter.com/browser-market-share

With the launch of any “0” version (e.g., iOS 13.0) there is fairly rapid adoption with less adoption of subsequent followup releases; iOS 14 appears to follow the same pattern. In fact, the highest level of adoption (iOS 14.4) appears to occur prior to the launch of the ATT framework (iOS 14.5+ in shades of green) in April 2021. One mobile adtech measurement firm reported 21% of observed users opting in to allow cross app tracking using the IDFA, a number which has remained consistent since.[23]

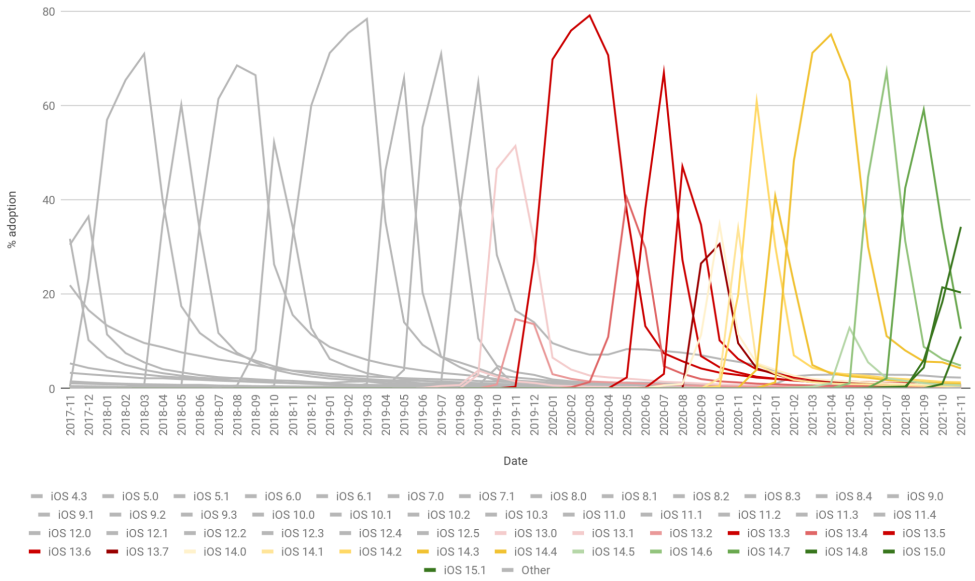

Figure 1: iOS version adoption curves (Source: Statcounter Global Stats, 2022)

Google releases Android version adoption stats to app developers. However, at this time there is no data published about Android 12 uptake.

3.5 Competitive effects in adtech

Like other modern industries, adtech is complex with multiple actors producing and consuming services. These include advertisers procuring ad agency services, ad distribution and campaign/customer data management, and advertising space using demand side platforms, as well as the publishing side providing content publication, ad inventory management, and advertising space inventory using sell side platforms, with ad exchanges and networks connecting the two sides as well as direct transactions between advertisers and

[23] iOS 14 Opt-in Rate - Weekly Updates Since Launch, September 6, 2021. https/www.flurry.com/blog/ios-14-5-opt-in-rate-idfa-app-tracking-transparency-weekly/

publishers. While there is no authoritative statistic for the number of firms participating in the market, we estimate 400-500 firms across the ecosystem.

The competitive impact of Apple's IDFA change appears to be far reaching and varied. While it doesn't establish any causality, Table 2 highlights the performance and related developments in firms from one part of the adtech ecosystem particularly impacted by the change. Customer data management (CDP) platforms collect and store different types of data from various sources and can be dependent on Apple's IDFA and other identifiers to help create a single consumer profile that can be monetized. While no definitive list of CDPs exists, adtech development group Clearcode identifies more than 60 firms active in that role.[24] Of those, 53 are privately held with limited information available. However, looking at publicly traded firms we see a variety of outcomes. Some CDP firms exited prior to Apple's change. One CDP, owned by a Canadian mass media company (Torstar) that primarily publishes newspapers, was taken private in 2020 amidst a long revenue decline. Another (Cxense), was acquired by a larger adtech firm in 2019, consistent with a widely reported consolidation trend in the industry[25]. Some firms developed CDP platforms not reliant on IDFA, with Adobe and LiveRamp seeing continuing revenue growth following Apple's change, while Neustar ended up selling its newly developed $557M CDP business. Nielsen, who's CDP was dependent on IDFA, saw a massive decline in overall revenues after the change. Other firms' revenue growth did not seem to be impacted negatively by the change, even when their CDP utilized Apple's IDFA.

Table 2:
Customer data management platforms (CDPs) revenues, developments

Firm	HQ Location	Pre IDFA revenue	Post IDFA revenue	Related developments
Adobe	San Jose, CA	$3.42B (Nov 2020)	$3.94B (Sep 2021)	Adobe Real-time CDP "has been re-architected for first-party data-driven customer acquisition. The changes come in open acknowledgment of the altered consumer privacy landscape and the deprecation of third-party cookies."

[24] Top Customer Data Platform (CDP) and Data Management Platform (DMP) Companies [Updated in 2021], August 11, 2021.https://clearcode.cc/blog/top-data-platforms/

[25] See e.g., The new titans of adtech: evolving giants, October 27, 2021. https://www.singular.net/blog/new-adtech-titans/

LiveRamp	San Francisco, CA	$119M (Dec 2020)	$127M (Sep 2021)	LiveRamp's Global Authenticated Traffic Solution (ATS), which identifies users in real time, enabling targeting without third-party cookies or IDFA, was "adopted by over 450 publishers in Jun 2021"
Nielsen	New York, NY	$1.67B (Dec 2020)	$882M (Sep 2021)	Nielsen Marketing Cloud collects data including Apple IDFA, Google AdID via third-party app SDKs
Numberly (1000mercis Group)	Paris, France	€26.1M (Jun 2020)	€32.4M (Jun 2021)	
Oracle	Marina del Rey, CA	$9.8B (Nov 2020)	$10.36B (Nov 2021)	Oracle Data Cloud Platform uses IDFA, AdID, and third party cookies
Salesforce	San Francisco, CA	$5.42B (Oct 2020)	$6.86B (Oct 2021)	Audience Studio uses and stores Apple iOS IDFA in event Customers request it to.
Neustar	Sterling, VA		$557M (Dec 2021)	Neustar's FabrickID (launched Dec 2020) "provides secure and persistent cross-media linkages between advertiser audience data and publisher media inventory" without relying on browser cookies or mobile advertising identifiers. Acquired by Transunion in 2021.
Torstar Corp	Toronto, Canada	$92.52M (Mar 2020)	N/A	Declining revenues for more than 5 5 years, taken private by NordStar Capital LP in 2020.
Cxense	Oslo, Norway	$8M (Jun 2019)	N/A	Delisted and acquired in 2019 by adtech integrator Piano.io

Another indicator of competitive effects is in performance of Apple's advertising product, Apple Search Ads, which allows advertisers to place ads within App Store search results similar to Google Ads placements displayed in Google Play Store search results. As reported by Singular, prior to the launch of iOS 14.5, mobile advertisers spend was fairly evenly split between the Android (56.16%) and Apple (43.84%) platforms. By late June 2021, spend levels on iOS ads had dropped with Android (70.29%) dramatically outpacing Apple (29.71%) and on an absolute basis, down 26%.[26] The shift could be explained by some app developers now being unable to target as effectively across apps on iOS, thus moving their resources to a competing platform. However, as industry players adjusted post-IDFA policy change, ad spend with Apple Search Ads largely recovered to around 40% as Apple rolled out its own competing advertising network. (Singular, 2021) By the fall of 2021, according to Branch, a company that

[26] $1.5B in ad spend shows iOS 14.5 is driving mobile ad spend to Android, June 23, 2021. https://www.singular.net/blog/ios-ad-spend-dropping/

measures mobile advertising effectiveness, app installs linked to Apple Search Ads had doubled in volume with about 60% of app installs on the iOS platform attributable to Apple Search Ads.[27]

Looking more generally at industry pricing in Figure 1, the US Bureau of Labor Statistics has produced price indices since 2010 for Internet Publishing and Web Search Portals, which consists of firms primarily engaged in exclusively publishing and/or broadcasting content on the Internet. As shown in Figure 1, Pricing for Display and Other Advertising Sales and Subscription, Content Access and Licensing Sales has remained steady or increased, while pricing of Search and Textual Advertising on these portals (like Google's Play or Apple's App Store) has steadily declined since 2010, indicating an overall competitive market that is beneficial for advertisers. In October 2020, the BLS discontinued discrete tracking of Search and Textual as well as Display Advertising, aggregating them into Advertising Sales (the blue line). It is notable that the Search and Textual Advertising index started to increase in mid 2020. The trend has continued with the aggregated data and coinciding with the launch of Apple's ATT initiative. The upward tick in pricing including Search and Textual Advertising could be, ceteris paribus, indicative of consolidation of pricing power for search-based advertising, although it could alternatively be explained by an American economy experiencing a period of inflation.

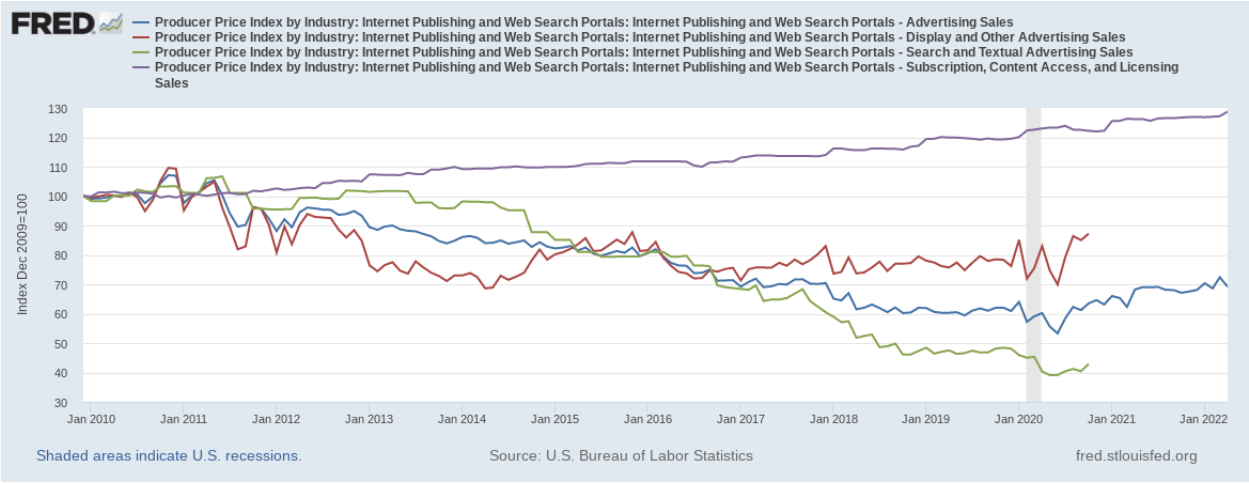

Figure 1: Producer Price Index by Industry: Internet Publishing and Web Search Portals (Source: US Bureau of Labor Statistics, 2021)

[27] Apple's privacy changes create windfall for its own advertising business, October 17, 2021. https://www.ft.com/content/074b881f-a931-4986-888e-2ac53e286b9d

3.6 IDFA and market share

The most recent report by the Interactive Advertising Bureau (2020) puts the overall US Internet advertising market at $139.8 billion, experiencing 12.2% YoY growth. Two other highlights from that report are worth noting. First, mobile Internet ad revenues continue to outpace desktop ad revenues, accounting for 70.3% of the $139.8 billion market in 2020, growing 13.4% YoY. Second, the top 10 firms continue to account for the largest share (78.1%, $109.2 billion) of the overall market. While the IAB report looks at overall trends in US Internet advertising, Table 1 provides a broader picture of the much larger global market with firm level digital advertising revenue share data for 2020 from GroupM. We also collected estimates of 3Q 2021 advertising revenues for the top ten firms, from public reports, allowing us to observe any market differences after Apple's policy change in Spring 2021.

Importantly, the overall global market is much bigger, with the top 10 firms accounting for three times as much revenue ($353.6 billion) as the IAB's survey, and including other segments like traditional television networks that continue to shift content and advertising to online streaming services. The top 10 firms are well known US and Chinese companies, competing

Table 1: Global media digital advertising revenues (Based on: GroupM, 2021)

Digital Advertising Revenue in bn $USD	2020	2020 Market share	3Q 2021	3Q 2021 Market share	Share growth
Google	131.9	37.30	53.1	40.38	8.25%
Facebook	86.7	24.52	28.2	21.44	-12.54%
Alibaba	28.6	8.09	11.7	8.88	9.80%
Bytedance	28	7.92	14.3	10.91	37.78%
Amazon	20.3	5.74	8.1	6.15	7.17%
Comcast (PF)	12.8	3.62	1.3	1.00	-72.42%
Tencent	12.6	3.56	7.1	5.37	50.66%
Disney (PF)	11.2	3.17	2.0	1.55	-51.05%
Baidu	11.2	3.17	3.0	2.30	-27.50%
Microsoft (PF)	10.3	2.91	2.7	2.02	-30.66%

with each other in multiple segments in addition to adtech. While Google is in a familiar spot and climbing in terms of market share, Apple is not in the top 10 (nor in the top 25). Looking at market concentration, the Herfindahl–Hirschman Index is 2,208 in 2020, rising slightly to 2368 in

3Q 2021, thus indicating an increasingly moderately concentrated market. The upward shift appears influenced by substantial declines in several firms' (Comcast, Disney, Microsoft and Baidu) market shares as well as a smaller decline in Facebook's second largest revenue share, along with concurrent rapid growth in market share of Tencent and Bytedance (Tiktok), and to a lesser extent Alibaba and Google.

What we see in Table 1 is consistent with the public narrative following Apple's policy change. In the first quarterly reports following the change, social media platforms Facebook and Snap immediately blamed Apple's IDFA policy for declines in revenues. Snap reported its third quarter revenue, driven almost exclusively by advertising, up 57%, but quarter to quarter growth slowed.[28] Facebook similarly reported revenues up 35% to $29.01B, but it missed expectations due to a slowdown in the growth of their ad revenues.[29] By the following quarter, these competitors' fortunes diverged, again illustrating varied competitive effects. In the most recent reporting Facebook reported continuing losses down $10B in advertising revenues, while Snap revenues rebounded with the firm reporting "first party measurement solutions are now enabled for advertisers that represent more than 75% of our Direct Response revenue." Additional industry sectors, e.g., mobile gaming, reported similar declines with iOS gaming in-app purchase revenues (attributable to ads) declining 35% since June 2021.[30]

Apple's revenues are benefitting with the IDFA change. While Apple doesn't break out advertising from overall services revenue, the share of revenues for services grew from 14.14% to 21.93% in fiscal year 2021, with its strongest growth ever recorded between the first and second quarter (33%).[31] In its most recent quarter, Apple reached an all-time revenue record of $19.5 billion, up 24%, with all-time records for…advertising…" among other services.[32] The relatively lower cost of providing services is exhibited in Apple's profit growth, where "services have experienced a notable increase in gross margins from an already high base of 55% in 2017 to 70% in 2021, and now stand at double the size of gross margins earned on Devices." (UK CMA, 2021 pgs 77-78) Within services revenues, the UK Competition and Markets Authority reports that, "at the global level the App Store is the largest contributor to services

[28] Snap Inc. Announces Third Quarter 2021 Financial Results, October 10, 2021. https://investor.snap.com/news/news-details/2021/Snap-Inc.-Announces-Third-Quarter-2021-Financial-Results/default.aspx

[29] Facebook Posts Slower Sales Growth With Apple Privacy Policy, October 25, 2021. https://www.wsj.com/articles/facebook-expected-to-post-slower-sales-growth-with-apple-privacy-policy-11635154200?mod=djemMoneyBeat_us

[30] The state of gaming app marketing, February 2022. https://www.appsflyer.com/infograms/gaming-app-marketing/

[31] Apple Reports Fourth Quarter Results, October, 28, 2021. https://www.apple.com/newsroom/2021/10/apple-reports-fourth-quarter-results/

[32] Apple (AAPL) Q1 2022 Earnings Call Transcript, January 28, 2022. https://www.fool.com/earnings/call-transcripts/2022/01/28/apple-aapl-q1-2022-earnings-call-transcript/

revenue (at [20-40]%) followed by Advertising (Third Party Licensing Arrangements) (at [20-40]%) in 2020. Digital Content and Other represent [0-20]% and [20-40]% respectively." As the privacy-protective platform, Apple is tight-lipped about income from advertising, but applying those ranges we estimate Apple's advertising revenues to be between $2.9 and $5.8 in the 3Q 2021.[33] Such a figure would place them in the lower half of global media revenues in Table 1. Within Table 1, perhaps Apple's chief competitor is Google. Google retains the benefits of its "on by default" cross app tracking identifier, its in house adtech services, and of course its search capability, which together gives them direct insight to consumer demands as well as the ability to place targeted ads in front of users. Competition from Apple doesn't appear to matter much. Google reported $53.13B in advertising revenues in the third quarter, a 43% increase since 2020, that vastly exceeded expectations.[34] Google's continued advertising success actually benefits Apple. The largest component of Apple's licensing revenue is Apple's agreement with Google in which Google pays a share of search advertising revenues to Apple in return for Google Search being the default search engine on Safari." (UK CMA, 2021 pgs 77-78)

In sum, the competitive effects of Apple's IDFA policy change are more clear. In the complex adtech space many firms relying on the IDFA for building customer profiles, targeting, etc., are feeling its impact. Some exited prior to the change, others maintained revenue growth by innovating around the need for the IDFA identifier, while others did nothing and saw their revenue decline and in some cases grow. At a structural level, Apple doesn't appear to be a factor in a moderately concentrated market at first glance. The rapid growth in advertising revenues by primarily Chinese platforms is certainly influencing the market and possibly drowning out the effects of the IDFA policy change. Predominant publishing platforms (e.g., Facebook) are ostensibly losing advertising market share because of the IDFA change. Since the policy change Apple's revenue, dominated by services including advertising, is growing at its highest levels. Search based advertising pricing industry wide is also increasing, potentially indicative of the influence that a policy change to a platform with over a billion users can have. Overall, there appears to be a direct relationship between Apple's user privacy enhancing data enclosure effort and it's own economic advantage, positioning it to compete with the other largest firms influencing the global digital advertising market.

---

[33] This is consistent with other estimates, see Apple's Advertising Business Is Bigger Than You Think. It Could Get Bigger Still, August 3, 2021.
https://www.barrons.com/articles/apples-advertising-business-is-bigger-than-you-think-it-could-get-bigger-still-51628004419

[34] Alphabet Announces Third Quarter 2021 Results, October 26, 2021.
https://abc.xyz/investor/static/pdf/2021Q3_alphabet_earnings_release.pdf

4. Conclusion

This paper identified a new phenomenon in the platform economy: data enclosure. We argue that analysis of data enclosure illuminates the raging debate about the relationship between platforms, the market economy, privacy, and competition policy. Users interacting with online infrastructures co-generate data that feeds matching algorithms in multi-sided markets. A combination of public demands for better privacy and platforms' push for competitive advantage is leading some major firms to limit the sharing of this data with competing platforms. Some form of data exclusivity is required for privacy protection, and in this case we see the market responding to the need. But data enclosure also asserts a form of exclusive ownership of the data, raising questions about the ability of this evolving new property rights structure to alter market shares, or to reinforce or undermine the dominance of the largest platforms.

The paper described two instances of data enclosure: 1) the encryption of DNS query data; and 2) Apple's and Google's enclosure of mobile identifiers used in digital advertising. We related these exclusion mechanisms to the firms' competitive strategy. Our empirical exploration found that DoH, apparently a more disruptive form of data enclosure, has had little impact on industry shares so far, primarily because it was embraced by a small-share, declining actor. Still, it is early days in terms of general adoption, with DoH registering around 6% of DNS queries by one rough estimate. Even so, the growing use of DoH and other encrypted DNS protocols does indicate a market-driven response to privacy-enhancement. We found that in adtech, the shift in the default from opt-out permission to opt-in permission had both strong privacy effects and major effects on the distribution of revenues in the industry. Here again, however, the changes are recent and the situation remains unsettled. Our preliminary work admittedly just scratches the surface by the standards of current empirical or modeling economic research, but it suggests that the ongoing impact of adtech-related data enclosure should be monitored closely for its competitive effects, and the conceptual framework we have developed for understanding the role of stronger exclusivity over platform data will be useful in that effort.

References

Alchian, A. (1965). Some Economics of Property Rights. *Il Politico*, *30*(4), 816–829. https://www.jstor.org/stable/43206327

Argenziano, R., & Bonatti, A. (2020). *Information Revelation and Privacy Protection* (No. DP15203). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3688155

Arrieta-Ibarra, I., Goff, L., Jiménez-Hernández, D., Lanier, J., & Weyl, E. G. (2018). Should We Treat Data as Labor? Moving beyond "Free." *AEA Papers and Proceedings*, *108*, 38–42.

Barzel, Y. (1997). *Economic analysis of property rights*. Cambridge University Press.

Benthall, S., and Goldenfein, J. (2021) Artificial Intelligence and the Purpose of Social Systems. Proceedings of the 2021 AAAI/ACM Conference on AI Ethics and Society (AIES'21).

Bergemann, D., & Bonatti, A. (2022). *Data, Competition, and Digital Platforms*. https://conference.nber.org/conf_papers/f161630.pdf

Böttger, T., Cuadrado, F., Antichi, G., Fernandes, E.L., Tyson, G., Castro, I. and Uhlig, S. (2019). An Empirical Study of the Cost of DNS-over-HTTPS. In IMC '19: ACM Internet Measurement Conference, October 21–23, 2019, Amsterdam, Netherlands. ACM, New York, NY, USA, 7 pages. https://www.dit.upm.es/~fcuadrado/publication/imc-19-doh/imc-19-doh.pdf

Bradshaw, S., & DeNardis, L. (2018). The politicization of the Internet's Domain Name System: Implications for Internet security, universality, and freedom. *New Media & Society*, *20*(1), 332–350. https://doi.org/10.1177/1461444816662932

Chhabra, R., Murley, P., Kumar, D., Bailey, M. and Wang, G. (2021). Measuring DNS-over-HTTPS Performance Around the World. In Internet Measurement Conference (IMC '21), November 2–4, 2021, Virtual Event. ACM, New York, NY, USA, 15 pages. https://www.dit.upm.es/~fcuadrado/publication/imc-19-doh/imc-19-doh.pdf

Cohen, J. E. (2017). Law for the Platform Economy. *UC Davis Law Review*, *51*(1), 133–204.

Demsetz, H. (1974). Toward a theory of property rights. In Classic papers in natural resource economics (pp. 163-177). Palgrave Macmillan, London.

Economides, N., & Lianos, I. (2020). Antitrust and Restrictions on Privacy in the Digital Economy. *Concurrences*, *3*(94275). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3834478

Evans, D. S., & Schmalensee, R. (2016). *Matchmakers: The new economics of multisided platforms*. Harvard Business Review Press.

Kuerbis, B. & Mueller, M. (2021). *Making Data Private - and Excludable: A New Approach to Understanding the Role of Encryption in the Digital Political Economy.* Presented online at 2021 Privacy Law Scholars Conference. https://privacyscholars.org/plsc-2021/

Kuerbis, B., Panday, J., & Mueller, M. (2020). *Exploring the Privacy Trade-Offs and Industry Impacts of DNS Over HTTPS*. Presented online at 2020 Telecommunications Policy Research Conference. https://papers.ssrn.com/abstract=37497.

Laudon, K. C. (1996). Markets and privacy. *Communications of the ACM*, *39*(9), 92–104. https://doi.org/10.1145/234215.234476

García, S. Hynek, K; Vekshindmitrii, D., & Wasicek, A. 2021. Large Scale Measurement on the Adoption of Encrypted DNS. https://arxiv.org/pdf/2107.04436.pdf

GroupM. (2021). *The Global 2021 Mid-Year Advertising Forecast*. https://d2ksis2z2ke2jq.cloudfront.net/uploads/2021/06/groupmglobaladforecast_June2021.pdf

Huston, G. (2021). *ICANN DNS Resolver Symposium – The Session Had Several Interesting Presentations That I Would Like to Comment On*. Circle ID. https://circleid.com/posts/20211222-icann-dns-resolver-symposium

Interactive Advertising Bureau. (2021). *Internet Advertising Revenue Report*. https://www.iab.comwww.pwc.com/e&m

Jones, C. I., & Tonetti, C. (2020). Nonrivalry and the Economics of Data. *American Economic Review*, *110*(9), 2819–2858. https://doi.org/10.1257/aer.20191330

Mingay, G.E. (1997). Parliamentary Enclosure in England: An Introduction to its Causes, Incidence and Impact, 1750-1850 (1st ed.). Routledge. https://doi.org/10.4324/9781315842929

OECD. (2021). *Methodologies to measure market competition, OECD Competition Committee Issues Paper*. https://www.oecd.org/daf/competition/methodologies-to-measure-market-

Ohlhausen, M. K., & Okuliar, A. P. (2015). Competition, consumer protection, and the right [approach] to privacy. *Antitrust Law Journal*, *80*(121).

Ostrom, E. (1990). *Governing the commons: The evolution of institutions for collective action*. Cambridge University Press.

Ostrom, E., Gardner, R., Walker, J., Walker, J. M., & Walker, J. (1994). *Rules, games, and common-pool resources*. University of Michigan Press.

Parker, G. G., Van Alstyne, M. W., & Choudary, S. P. (2016). *Platform revolution: How networked markets are transforming the economy and how to make them work for you*. WW Norton & Company.

Pistor, K. (2020). Rule by Data: The End of Markets? *Law and Contemporary Problems*, *83*(101), 101–124. https://perma.cc/H6WA-UXJY

Rochet, J. C., & Tirole, J. (2006). Two-sided markets: a progress report. *The RAND journal of economics*, *37*(3), 645-667

Saha, A. (2021, March 12) “Oblivious DoH: Enhanced DNS Privacy,” KeySight blog, https://blogs.keysight.com/blogs/tech/nwvs.entry.html/2021/03/11/oblivious_doh_enha-bMt1.html

Samuelson, P. A. (1954). The pure theory of public expenditure. *The review of economics and statistics*, *36*(4), 387-389.

SearchAdsHQ. (2021). *Apple Search Ads Benchmarks Report Q1-Q2 2021*. 2021. Retrieved December 23, 2021, from https://searchadshq.com/apple-search-ads-benchmarks-2021/

Shy, O., & Stenbacka, R. (2016). Customer Privacy and Competition. *Journal of Economics and Management Strategy*, *25*(3), 539–562. https://doi.org/10.1111/JEMS.12157

Singular. (2022). *6th Annual ROI Index: Top Media Sources*.

Spiekermann, S., Böhme, R., Acquisti, A., & Hui, K. L. (2015). Personal data markets. *Electronic Markets*, *25*(2), 91–93. https://doi.org/10.1007/S12525-015-0190-1

Statcounter Global Stats. (2022). *Mobile iOS Version Market Share Worldwide*. Retrieved February 3, 2022, from https/gs.statcounter.com/ios-version-market-share/mobile/worldwide/#monthly-201801-202104

Statista. (2021). *Mobile Apple iOS version share worldwide 2018-2021*. https://www.statista.com/statistics/1118925/mobile-apple-ios-version-share-worldwide/

UK Competition and Markets Authority. (2021) Mobile ecosystems market study interim report. https://www.gov.uk/government/publications/mobile-ecosystems-market-study-interim-report

US Bureau of Labor Statistics. (2021). *Producer Price Index for Internet Publishing and Web Search Portals — NAICS 519130*. https://www.bls.gov/ppi/factsheets/producer-price-index-for-internet-publishing-and-web-search-portals-naics-519130.htm

Verma, T., Singanamalla, S. (2020, December 8), “Improving DNS Privacy with Oblivious DoH in 1.1.1.1. The Cloudflare Blog, https://blog.cloudflare.com/oblivious-dns/

Viljoen, S. (2020). Data as Property? On the problems of propertarian and dignitarian approaches to data governance. Phenomenal World. https://www.phenomenalworld.org/analysis/data-as-property/

Wordie, J. R. (1983). The Chronology of English Enclosure, 1500-1914. *The Economic History Review*, *36*(4), 483–505. https://doi.org/10.2307/2597236

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power: Barack Obama's books of 2019*. Profile books.