Making Data Private - and Excludable:
A new approach to understanding the role of data enclosure in the digital political economy

Brenden Kuerbis, Georgia Institute of Technology
Milton Mueller, Georgia Institute of Technology

Introduction

This exploratory paper links the economics of privacy and data (e.g., Acquisti et al, 2016; Jones & Tonetti, 2020) to an analysis of the industrial organization and governance of the internet (e.g., Kuerbis, Mueller and Panday, 2020). Its goal is to understand the impact of market-driven encryption and privacy initiatives on the political economy of data. Our work highlights how encryption and the major platforms' limitations on adtech are part of a much broader competitive struggle over the economic value of data. Encrypting DNS queries, for example, is not only a privacy-enhancing move, but also a means by which service providers compete with each other over the value and security of data. Encryption encloses data, turning what was once a data commons (and a privacy problem) into a resource that a defined set of actor(s) in the digital ecosystem have more control over, and from which competitors can be excluded.

This push for the exclusivity of data is fundamental to current Internet policy debates. It is relevant not only to privacy and data protection law and regulation, but also to concerns about platform competition, cybersecurity, and content regulation. Firms in the internet ecosystem are

using confidentiality of data as a selling point to their customers.[1] But they are not just selling privacy, they are also gaining a competitive advantage by excluding their competitors or other players from access to data generated by their users. The costs and benefits of producing privacy and protecting data are being internalized by internet service firms. Exclusivity allows actors to more precisely understand the value of the underlying data and negotiate varying governance structures (e.g., standardization, contractual arrangements, etc.), potentially leading to different distributional outcomes.

The paper proceeds by first situating our analysis in the institutional economics literature on property rights, enclosures, and data. We then describe 1) some historical cases of enclosure using encryption; 2) the introduction of the DoH protocol as a way of enclosing DNS query data; 3) the enclosure of Apple and Google mobile identifiers used for advertising. The institutional economic framework is shown to provide analytical traction for understanding and anticipating the public policy problems associated with this trend.

Property rights, enclosures and data

Political economists from Marx to Coase to Ostrom have recognized the importance of property relations in shaping the way an economy works. In the words of one member of the New Institutional Economics (NIE) school, “Property rights institutions underlie the performance and income distribution of all economies.” (Libecap, 1986) They do this by defining the rules for the appropriation, use and exchange of resources, as well as defining the boundaries of rights.

A key and enduring aspect of the concept of property is exclusion. (Alchian, 1965) The owner of a resource can exclude others from using or benefiting from the resource. This allows the owner to capture the value, either by using it or by trading it. Even in resource regimes where exclusion is difficult, such as the common pool resources explored by Ostrom (1990; 1994), collective rules for appropriation can be defined, and boundaries of exclusivity around the collectivity in control of the common pool must be established. Only pure open access regimes lack exclusion, and they are known to foster inefficient allocations (the so-called tragedy of the commons).

Property regimes are not static. They evolve in response to socio-economic development, and they can be consciously modified in line with notions of public policy or justice. In Marx’s historical determinism, the transformation of feudalism into capitalism was

[1] E.g., Google announces plan to tackle privacy issues in online advertising, The Guardian, Jan 25, 2011. https://www.theguardian.com/technology/2021/jan/25/google-announces-plan-to-tackle-privacy-issues-in-online-advertising

analyzed as the emergence of a new set of property relations more suited to the “material forces of production” required by emergent industrialism. In NIE theory, competitive forces alter institutions that are not congruent with economic growth. “Changing market conditions exert pressure for dynamic adjustments in the existing rights structure…” (Libecap, 1986) There are many examples of the enclosure of resources that were once part of an open-access commons, just as there are many examples of the erosion of exclusivity in resources that were once more private and exclusive (Boyle, 2003; Mueller, 2010). Transformations of property regimes signal consequential disruptions in economic structures.

But what is the role of property in data? Digital data is notoriously nonrival in consumption (i.e., one person’s use of it does not consume or “use up” the resource); it is also notoriously difficult to contain for purposes of exclusion. For those reasons, digital data is sometimes seen as a public good, which is defined as a good that is both nonrival in consumption and difficult or impossible to make exclusive. But in a digitized world, treating data as a public good poses a huge problem for privacy advocates, because it makes data freely appropriable. Data protection and privacy law could be characterized as an attempt to assign exclusive property rights in personal data to the individuals to which the data refers. (Lessig, 2002) Other legal scholars have resisted classifying privacy as a data property right, because the replicability and many potential uses of data make it impossible for the seller to know exactly what they are giving away, and/or because a property rights regime makes it too easy for individuals to transact their privacy away. (Samuelson, 2000) Yet even if the complex notification and consent regimes of data protection law are not intended to facilitate exchange, they rest on the creation of an artificial, legally mandated exclusivity, just as copyright protection does. Encryption on the other hand is a *technological* means of creating exclusivity in data; it erects a fence around digital data that restricts access, making the public good a private good. While legal scholars continue to debate the applicability of the property rights approach to data and privacy (e.g., Zech, 2016), Julie Cohen (2017) importantly recognizes that modern information economy platforms are fostering “a quiet revolution in the legal status of data as (*de facto* if not *de jure*) proprietary informational property. (154)

Institutional economics provides precise and useful distinctions between four broad classes of goods: public goods, private goods, club goods, and common pool resources. As Figure 1, based on Elinor Ostrom’s (1994) institutional analysis and design framework shows, distinctions hinge on the degree to which resources are rival in consumption (i.e., one person’s

consumption does not prevent anyone else from using it) and excludable (i.e., the degree to which an owner or appropriator of the resource can prevent others from appropriating it.)

Difficulty of excluding users	**Subtractability of use (rival occupation or consumption)**	
	Low	High
Low	**Club goods**	**Private goods**
High	**Public goods**	**Common pool goods**

Figure 1: Classification of goods, adapted from Ostrom (2005, p. 24)

Ostrom's framework has been applied in the field of Internet governance to the problem of managing Internet identifiers (Mueller, 2010) and to copyright (Hess and Ostrom, 2007).

Examples and evolution of data enclosure

Many communication networks have experimented with, developed, or deployed protocols using encryption or other mechanisms to make valuable data excludable with different outcomes. In this section we examine four cases: over the air (OTA) broadcast, satellite-based cable, and more recently, Internet networks and adtech. We highlight how these efforts to enclose take place in a broader context of competing economic and policy concerns, and how data may shift between being a public, club and private good.

OTA broadcast and pay TV

OTA broadcasting was used by economist Paul Samuelson (1954) as the paradigmatic case of a public good. Broadcast signals were freely available to anyone who could receive the signal. As early as 1931, however, Zenith was working on a subscription model of television signal delivery to help mitigate "the tremendous cost of bringing premium content to the living room." (Zenith Radio Corp, 1955; Leonard, Webb and Ellett, 1956) Believing that in the long term neither government nor advertising sponsorship "would be able to support an adequate number of stations and the types of programming the public would want," Zenith announced its Phonevision system in 1947, which broadcast OTA television signal that was jittered and decoded with the first set-top converter box that added a signal transmitted over a phone line.

This effort received FCC approval in 1953 and Zenith trialed the system in Chicago, New York City and locations in New Zealand and Australia. According to its inventors, “electronic coding of both picture and sound prevents unauthorized reception of premium programs, yet reserves to the subscriber the right to select either these or non-toll programmes as he wishes.” (Leonard, Webb and Ellett, 1956) Contrary to Zenith’s predictions, between 1949 and 1951 television advertising spending had increased ten-fold to $128 million putting advertiser-funded commercial OTA broadcast stations firmly in place in markets like Chicago. The demand for Zenith’s subscription-based “pay television” never materialized. (Ad Age, 2003; Jajkowski, 2013)

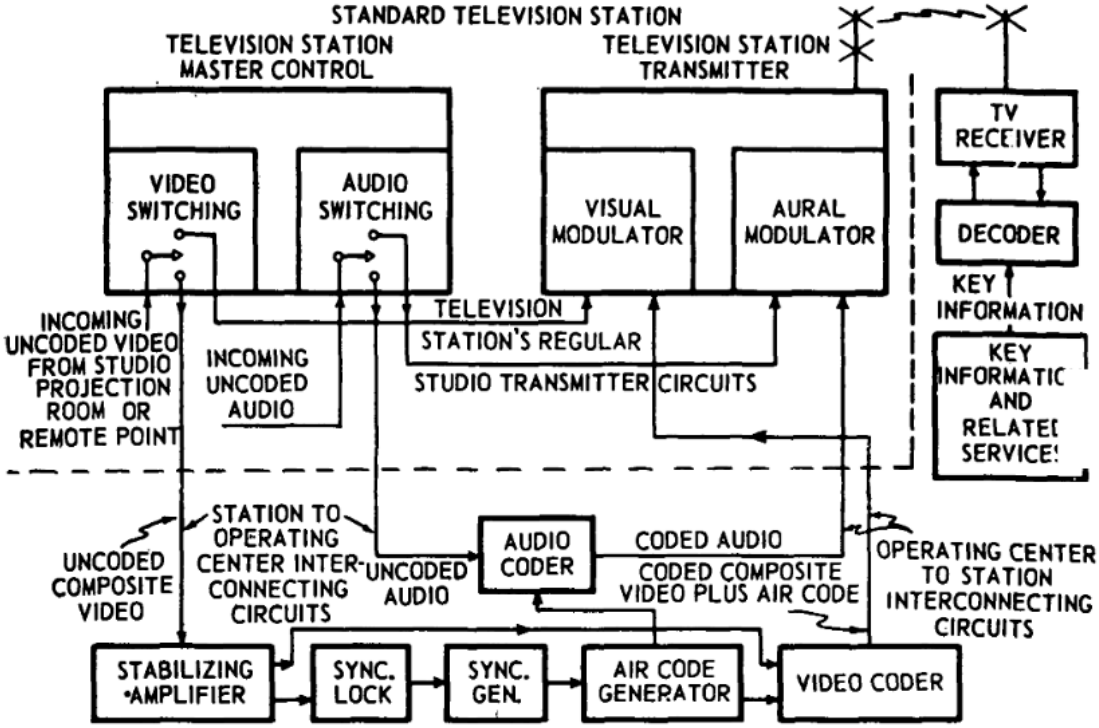

Figure 3: A simplified functional diagram of a Phonevision installation

(Source: Leonard, Webb and Ellett, 1956, 208)

Satellite-based cable and conditional access

More than 30 years later, newly-formed satellite-based cable television networks in the United States were in furious competition with one another.[2] (Johnson, 1982; Mueller, 1987) A significant problem for subscription-based cable networks like HBO was that their programs were distributed in the clear by satellite to cable system head-ends, which meant they could

[2] FCC Sets Open Sky Policy on Satellite Service, New York Times, June 17, 1972. https://www.nytimes.com/1972/06/17/archives/f-c-c-sets-open-sky-policy-on-satellite-service.html

also be received or even retransmitted by any other person with a properly tuned dish. This created a free rider problem for content producers and programmers, not only domestically, but transnationally where international copyright treaties also failed to provide adequate protection. (Yarvis, 1984) The Cable Act of 1984 permitted cable networks to encrypt their satellite feeds, enclosing the data using the VideoCipher and subsequent protocols so only end users that purchased a decoder from a satellite provider could receive the channel. In 2012, the FCC expanded the ability to enclose data, granting cable network operators permission to encrypt basic television service including public good local broadcast stations.[3] Encryption prevented signals from being observed by non-subscribers and created a burgeoning, global, multi-billion network security industry providing "conditional access" systems for networks' signals.[4]

While conditional access regimes emerged in response to evolving business models and market competition as well as intellectual property concerns, they also implicated policy areas like privacy and surveillance. A report by the OECD (1999) noted that a primary function in conditional access systems was management of subscriber information, particularly identifying data like names, addresses, etc. This valuable data had to be updated, stored in, and shared across network operators' databases. At the time, national regulators like the Japanese Ministry of Posts and Telecommunications established guidelines for the protection of subscribers' personal information based on the OECD's 1980 privacy protection guidelines. In the United Kingdom, regulators specified that any information gained through conditional access not be shared with other business units, and that the "secrecy of subscriber information [was] backed by a provision in the class license for conditional access services."

Conditional access systems implemented by network operators were also the target of transnational surveillance for national security purposes. By statute, Paragraph 9(1)(c) of Canada's Radiocommunication Act prohibited decoding encrypted subscription programming signals unless in accordance with an authorization from a lawful (i.e., Canadian domiciled) distributor of the signal.[5] The Communications Security Establishment (CSE) of the Canadian

[3] Commision relaxes the cable encryption prohibition, Federal Communications Commission, Oct 12, 2012. https://www.fcc.gov/document/commission-relaxes-cable-encryption-prohibition

[4] Global Conditional Access System (CAS) Market Report 2020-2025: Extensive Growth in the Telecommunication Infrastructure are Anticipated to Drive the Market, https://www.globenewswire.com/news-release/2020/12/24/2150420/28124/en/Global-Conditional-Access-System-CAS-Market-Report-2020-2025-Extensive-Growth-in-the-Telecommunication-Infrastructure-are-Anticipated-to-Drive-the-Market.html

[5] See Radiocommunication Act (Paragraph 9(1)(c)) Exemption Order for the Purposes of National Defence and Security, Department of Industry, https://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf09417.html

government applied for and received an exemption for decoding encrypted subscription programming signal transmitted by foreign distributors of programming. The exemption applied "where the signal is decoded to fulfil the mandate of CSE in respect to the acquisition and use of information for the purpose of providing foreign intelligence in accordance with the intelligence priorities of the Government of Canada." This exemption facilitated the collection of foreign intelligence from distributors of encrypted content domiciled in allied or other countries, whereas the CSE would otherwise gain conditional access by simply purchasing the content from distributors domiciled in Canada.[6]

Internet and encrypted DNS queries

Several decades later, the Internet's domain name system (DNS) became the object of data enclosure efforts. When someone (or something) uses domain names to access a web site (www.example.com) or communicate with an email address (person@example.com), a DNS query is created and forwarded to a server known as the recursive resolver. A DNS query asks what IP address must be used to send packets to the named host or email address, a process known as resolution. The recursive resolver will either have the answer for the query stored, and will respond, or it will query authoritative name servers to find and deliver the matching resource records of a domain name. Although a computer, router, or any other networked application can be configured to talk to a specific DNS resolver, users typically default to using the resolver settings provided by the network operator, which might be the Internet or telecom service provider, or their organization's IT department.

Under traditional DNS (shown in Figure 3), DNS queries and responses 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 (represented by green arrows); neither the queries nor the transport of the messages are encrypted, nor are the endpoints of communication authenticated. This data can be monitored by networks along the transmission path, and is susceptible to interception, blocking or modification. These actions could take place for a variety of reasons, including business, network security or legal requirements.

[6] This eye-opening discovery has important implications for current debates. Large recursive resolver businesses in the US could become very important to US LEAs, similar to how LEAs began to use mobile network data.

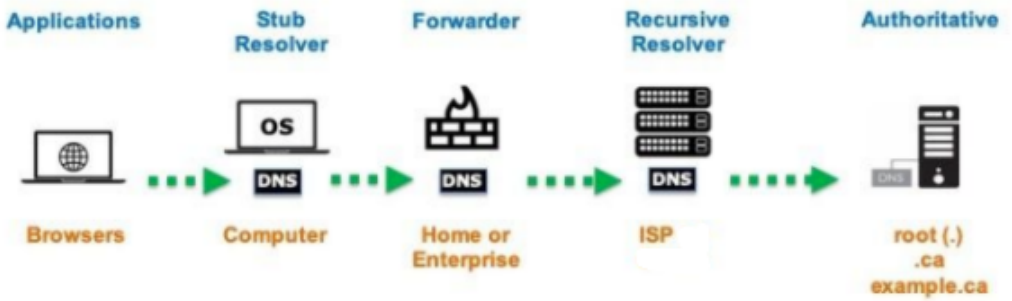

Figure 3: Traditional DNS Deployment
(Based on: ICANN Security and Stability Advisory Committee, 2020)

The DoH protocol (shown in Figure 4), uses HTTPS to transport the query between the application/stub resolver and recursive resolver, the same protocol used for secure (i.e., encrypted) web pages. This is important because:

- DoH queries and responses look like any other HTTPS traffic over port 443, making it more difficult (but not impossible) to isolate them.
- DoH provides confidentiality for DNS data while in transit between those authenticated endpoints, making monitoring, blocking or modification of the queries by intermediary actors more difficult.
- The entity providing recursive resolution might not be the local ISP. The DNS query can bypass the local ISP and be handled by a recursive resolver run by a cloud service or an application (e.g., browser) provider.

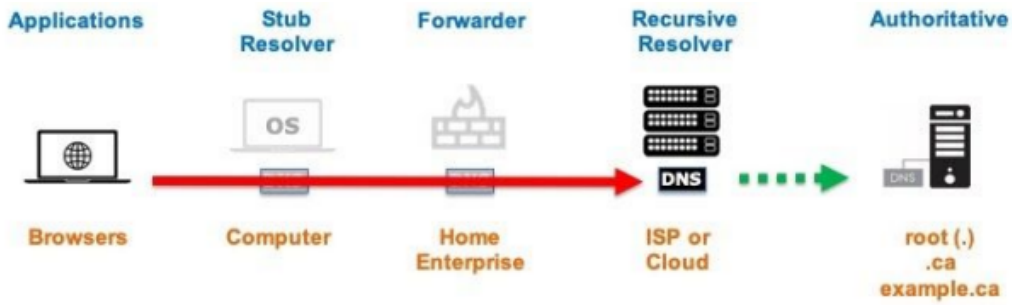

Figure 4: Possible DNS over HTTPS Deployment
(Source: ICANN Security and Stability Advisory Committee, 2020)

For most of the internet's existence, the service of resolving a domain name to obtain an IP address was bundled with an ISP's internet access service. But recently, cloud services

competing in a number of other markets have offered an alternative DNS resolution service to end users who were sophisticated enough to reconfigure their stub resolver (open resolvers). Along with major cloud providers, the browser software manufacturers (who are basically in the advertising business and compete with each other for eyeballs on the web), have learned that they can control or influence where users go for DNS resolution. With DoH, as Figure 2 indicates, the ISP can be completely bypassed in the DNS query process (depending on users' configuration). Alternatively, an ISP may decide to compete with the DoH providers and offer the service itself to retain access to DNS query data.

DNS query data and the related activity of recursive resolution can be examined using Ostrom's framework. Historically, clear text DNS query data could be viewed as a club good. Query data had low excludability being available to network operators running recursive resolvers between the user and the authoritative resolver operator. Like information generally, this data was also mostly non-rival, as it could be used repeatedly for different purposes, and even retain its value over time. These characteristics led to the creation of positive and negative externalities that accrued or were imposed on parties not involved in the original query transaction. For example, the sharing of ISP query data with network security providers and content delivery networks resulted in DNS-based protection from malicious websites, as well as the optimization of content delivery times. Advertisers' use of query data also provided users more precise and efficient search-based advertisements. Earlier work by Kuerbis et al. (2020) identified eleven market segments producing or consuming DNS query data, from DNS query generation in applications, resolution by ISPs and managed DNS services to complementary goods and services like network security, digital advertising, and content delivery, with an overall market size of more than $940 billion. But the use of query data also resulted in normative, if not legal, violations of users' privacy. For example, an ISP that provided query data to third parties serving advertisements eventually faced legal action from regulators, a European data protection authority found DNS query data processing to be illegitimate if not compliant with GDPR, and DNS query data sold to researchers has been allegedly used inappropriately for political purposes.[7]

[7] For example, when the subject of an inquiry by the German Federal Network Agency, Deutsche Telekom proactively switched off a DNS redirection service provided to its subscribers that was operated by a separate digital advertising company. (Böck, 2019) Separately, the Spanish Data Protection Agency (2019) found that unless DNS query data processing complied with GDPR "it would be an illegitimate processing of that personal data." Finally, while the sale of DNS query data is legal, a recent indictment against a former Clinton campaign lawyer suggested "private Internet records", i.e. DNS query data, were sold to researchers studying attribution and mined to help conduct opposition research. (US District Court, District of Columbia, 2021)

DoH encloses DNS query data, making non-rivalrous query data only available to and controllable by the endpoints able to encrypt or decrypt it. Conceptually, the enclosing of DNS query data shifts it from a club to a private good, reconfiguring the actors who have access to the data. Encrypting queries grants a de facto property right to the producers of that data, in this case users and application providers as well as DoH-enabled recursive resolver operators, who are able to exclude the benefits of query data from others. This creates a starting point for negotiations and laying the ground for contracts (Rusche and Scheufen, 2018) and other institutional bargaining over the use of that data.

Mobile Internet and advertising identifiers

Given the historical role of market competition and privacy policy shaping communications networks decisions to enclose protocol data, it is not a surprise to see it recurring today. The mobile Internet digital advertising market, and the variety of industry players it involves, has been consumed by efforts to enclose protocol data used in mobile device operating systems. 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[8]), the iOS IDentifier For Advertising (IDFA) and Android Advertising ID (AAID) have been used to identify and track users' mobile devices across different apps installed on the device, deliver personalized and targeted advertising, measure campaign performance, frequency cap and attribute advertising impressions and clicks to app installs, among other things. (ClearCode, 2020) Apple recently moved to enclose the user-resettable unique identifier within their operating system. Apple and Google control who uses the IDFA and AAID and how they use them through App Store and Play Store platforms' contractual arrangements with users and application developers. Beginning with Apple iOS 14, users must now opt in to app developers' requests to use the IDFA to track them across apps owned by other companies. Google, on the other hand, allows users to reset their AAID and they can opt out of ad personalization based on cross site tracking using the AAID.[9]

[8] Specifically, Apple and Google moved to block third party cookies in the Safari and Chrome browsers. Third party cookies are set in a browser by a party other than the website the user is visiting. Apple implemented this in March 2020, with Google is set to do the same in 2022. Google has several proposals for replacing cross-site tracking functionalities accomplished by third-party cookies, see https://www.chromium.org/Home/chromium-privacy/privacy-sandbox which have been met with some resistance.

[9] Google's AAID opt out policy is the focus of a legal action taken under the EU's GDPR, see Moody (2020).

The impetus for such a change in property rights associated with mobile identifiers can be explained in part by Apple's privacy concerns. But Apple is also competing in the approximately $336 billion growing global digital advertising market[10] and advertising continues to play a role in supporting network platforms. Google's reliance on and dominance in the space is well-known, with advertising revenues generated across Google Search and other properties, YouTube, as well Google Network Members' properties participating in its adtech platforms like AdMob, AdSense, and Google Ad Manager. Its advertising revenue grew at 12.15% (CAGR) between 2017 and 2019, from $95.6 to $134.8 billion. (Alphabet Inc., 2020) In contrast, although Apple has tried to compete in digital advertising through acquisition, and its services (e.g., App Store) have been growing faster than hardware revenues, its share of advertising revenue was only $2 billion in 2020. (Keith, 2021) Apple's enclosure of IDFA data positions it to leverage the strength of its multisided App Store platform, allowing users of its iOS devices to control their privacy and targeted ad experience, while letting the Apple collect and sell aggregated or higher priced individual user and ad performance data to advertisers and agencies.

The impact of these enclosure efforts on firms who stand to lose digital advertising market share or access to valuable data could be substantial. Facebook, whose access to detailed user information makes its ad sales a growing, very lucrative business, brought in $84 billion from advertising revenues in 2020. (Tankovska, 2021) Facebook has reported that the financial impact on ad targeting revenues is expected to grow from quarter to quarter. (Facebook, 2021a) In its third quarter of 2021, Facebook revenues were up 35% to $29.01B, but it missed forecasted expectations with revenue growth declining 1.06%. (Needleman, 2021; Facebook, 2021b) Similarly, the adtech industry which sits between advertisers and publishers facilitating transactions (e.g., brokers/programmatic platforms for ads and ad space, ad networks and exchanges, ad performance measurement), will be impacted. It is difficult to know how many iOS users will opt in, but, based on when Apple eliminated third party cookies, advertisers claim they may lose as much as 50% of revenue from 80% of users. (Dolan, 2021) In light of this change, impacted actors are seeking workarounds. E.g., industry players and trade associations have announced plans for probabilistic fingerprinting of user devices which could be used for advertisement targeting, measurement and attribution. (Terlap, Higgins and Haggin, 2021) In turn, Apple has indicated it will block such efforts.

[10] See Letang and Stillman (2020)

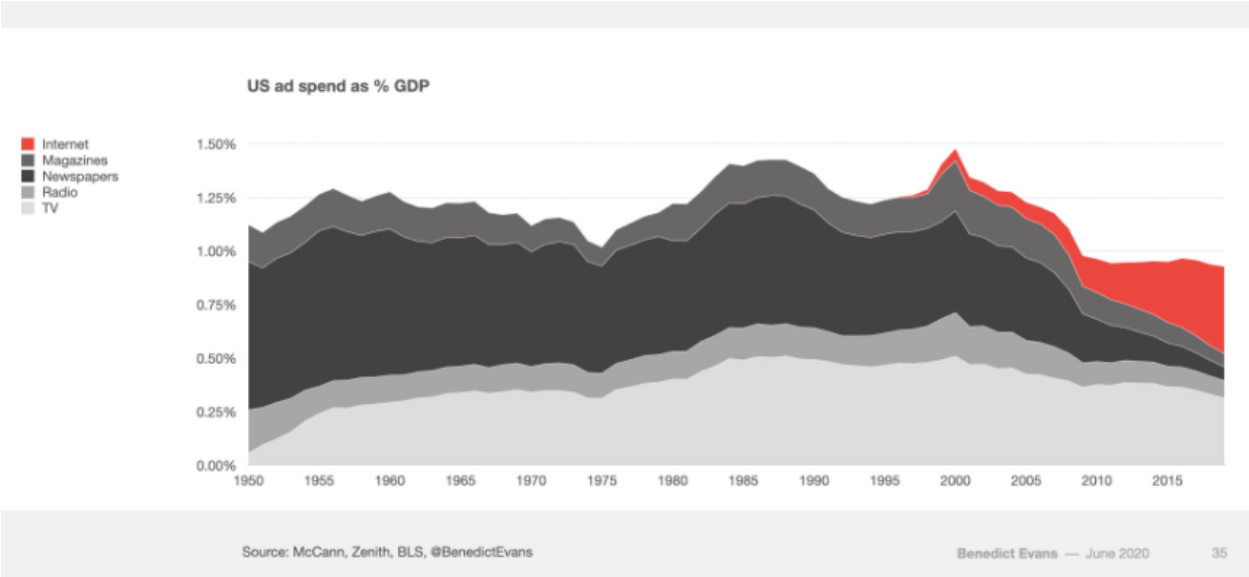

Figure 5: US advertising spend

(Source: Evans, 2020)

One might get the impression that Google and Apple are poised to dominate the mobile digital advertising market. However, that ignores broader trends and observations. As Figure 5 indicates, while digital advertising is a growing market in the US, the overall advertising market has declined as a share of GDP since 2000. As economist Eric Fruits (2020) explains,

> "Since 2000...the combination of increasing quantity, decreasing cost and increasing total revenues are consistent with a growing and increasingly competitive market, rather than one of rising concentration and reduced competition."

Another indication of this competition is apparent in a 2020 PWC study for the UK's advertiser association which looked at 50 firms participating in programmatic digital advertising over 15 months. (ISBA, 2020) The study observed 267 million advertising impressions, but was only able to identify 31M (12%) impressions through the entire supply chain from advertiser to publisher. Nonetheless, in that subset, 290 unique supply chains were identified. Furthermore, as Figure 6 shows, 15% of advertiser spend could not be attributed to various firms in the supply chain. The takeaway is that the digital advertising market with widespread access to mobile identifiers appears to be associated with a highly competitive market with many actors

participating. The indiscriminate sharing of user data may be bad for privacy, but it seems to be good for competitive entry by many small firms. The internalization of privacy externalities through the enclosure of mobile identifiers by platforms means that competitors need their own platforms, it becomes more like facilities-based competition. This new turn in platform competition creates a tradeoff with competition; its effects on market structure will take several years to become evident.

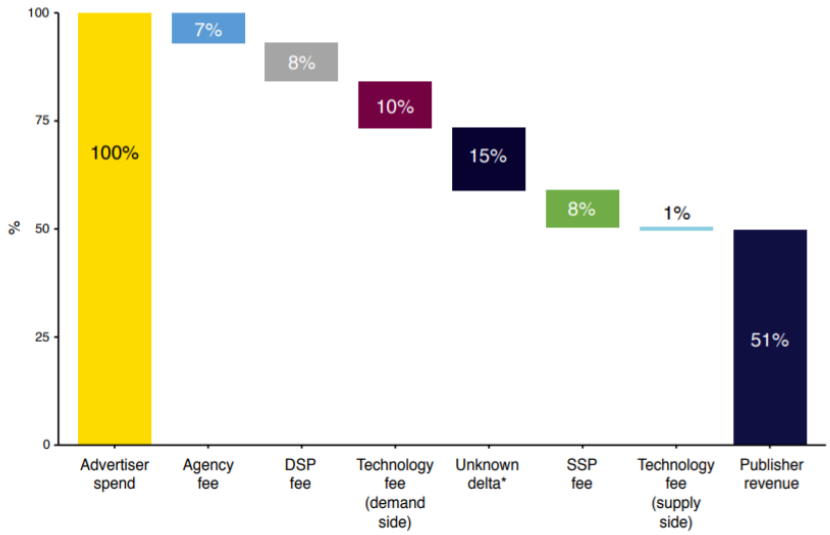

Figure 6: Industry waterfall: Advertising spend.

(Source: ISBA, 2020)

Conclusion

Competitive forces are altering data property relations in important ways. In this paper, we've examined three cases of data exclusion in networks: subscription broadcasts, Internet DNS queries, and mobile adtech. In each case we see an entanglement of economic exclusion/competitive advantage incentives with privacy or confidentiality considerations. Much like the enclosure of satellite-based cable signals transformed that industry, the creation of property rights in DNS queries and mobile identifiers stand to create highly consequential disruptions or adjustments in the existing digital economy. This is happening at the same time

as the norms, policies and laws governing data protection and privacy are undergoing dramatic, global changes and platforms are coming under increasing regulatory and antitrust scrutiny.[11]

The deployment of DoH generated a major stir in the Internet community and among certain governments. There were doomsday predictions about the centralization of DNS and its impact on Internet resilience. (Livingood, et al. 2019; eco, 2020) There were intense debates about whether DoH actually improved security, and claims that it actually undermined enterprise cybersecurity. (Vixie, 2020) There were protests against the loss of governments' ability to target domains for censorship. (UK Parliament, 2019) These concerns have waned, as market actors adjust and it becomes clearer that the production and consumption of DNS query data occurs widely across many market segments and competitors. Better defined exclusion, in essence property rights for DNS query data, is creating opportunities for (re)negotiation and wholly new contractually-enforced arrangements between producers and consumers of DNS query data. ISPs and cloud providers have updated their terms of service for resolver service to meet privacy, transparency, and blocking and modification prohibition requirements laid out in Mozilla's trusted recursive resolver program.[12] Importantly, browser market leader Google has launched a process for DoH providers to be added to its Chrome browser, eschewing lock-in.[13] Government agencies such as the U.S. NSA have developed recommendations or policies consistent with their cybersecurity objectives. (National Security Agency, 2021) We should expect to see more deployment of DoH as firms seek to maintain or gain market share of DNS query data, a valuable underlying resource to many products and services. It appears that enclosure has shifted market relations without undermining competition.

The situation with adtech mobile identifiers is more unsettled. The enclosure of adtech data forces upon us a more direct consideration of the trade off between privacy-enhancing

---

[11] Most notably, Epic Games, Inc v. Apple Inc., see https://cand.uscourts.gov/cases-e-filing/cases-of-interest/epic-games-inc-v-apple-inc/ as well a recent European Commission letter to Apple, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2061

[12] See https://wiki.mozilla.org/Security/DOH-resolver-policy, https://support.mozilla.org/en-US/kb/dns-over-https-doh-faqs and 2020 Internet Governance Forum *Workshop 73 DNS over HTTPS (DoH): Human Rights, Markets, and Governance* https://www.intgovforum.org/multilingual/content/igf-2020-day-8-ws-73-dns-over-https-doh-human-rights-markets-and-governance and Comcast's Xfinity Internet Service Joins Firefox's Trusted Recursive Resolver Program, Jun 25, 2020, https://blog.mozilla.org/blog/2020/06/25/comcasts-xfinity-internet-service-joins-firefoxs-trusted-recursive-resolver-program/

[13] See Google's requirements, DoH providers: requirements process for Chrome, https://docs.google.com/document/d/128i2YTV2C7T6Gr3I-81zlQ-_Lprnsp24qzy_20Z1Psw/edit#heading=h.dqx6rvawuuro

technology and competition policy concerns - although, as was the case with DoH, these concerns may be inflated by interested actors in the early stages of the adjustment. Just as ISPs said DoH would make the sky fall and should be stopped, the incumbents who thrived on a more open data sharing regime are attacking the change. Trade groups in France filed an antitrust complaint against Apple, asking the competition authority to prevent it from applying its IDFA change. (Barker, McGee and Abboud, 2020) Germany's largest media, tech and advertising companies, including Facebook and publishing conglomerate Axel Springer, have also filed a complaint accusing Apple of antitrust abuse due to its IDFA change, predicting a 60% fall in advertising revenues. (Espinoza, 2021) It's too early to tell how much the enclosure of ad-relevant data by platforms like Apple will support their growth and protect their users' privacy. But it likely will reduce the number of players in the advertising ecosystem, providing advantages to players with their own user base and data collection and processing infrastructure (just as FCC policies toward broadband interconnection eliminated reseller ISPs and promoted facilities-based competition). But looking at integrated firms like Apple and Google that combine hardware, operating systems and software markets into dominant platforms in isolation ignores emerging threats that could eventually topple them. Much like Google's path of leveraging its search dominance to acquire and develop open-source Android and launch the Play Store in 2012 to counter Apple's meteoric platform growth since 2008, we now see Huawei leveraging itsiOS to build a competing platform combining its devices, open-source Android-like HarmonyOS, and Huawei AppGallery.

The most interesting questions about the future, however, arise from the degree to which data enclosures succeed in responding to consumer and government demands for better privacy protection. Google's refusal to leverage its dominant browser market share to capture all the DNS query data, allowing Chrome users to access any secure (DoH-enabled) resolver indicates that it is motivated more by cybersecurity and confidentiality than by a desire to have exclusive control of all the data.[14] Apple is also clearly catering to consumer concerns about privacy and treating it as a reputational competitive advantage in the sale of its devices and services. Privacy protection that is achieved in this way might be both more reliable and more

[14] Google can still see the unencrypted query data at the browser end point, so they can still serve relevant ads. For instance, in its recent FLoC proposal (https://github.com/WICG/floc), Google plans to "explore ways in which a browser can group together people with similar browsing habits" which may involve clustering based on hashed domains of sites visited or on-device classification of the full path of the URL. So its allowance for other DoH resolver providers does not mean it loses data, but it does forego exclusion.

effective than protection achieved by law and regulation. While some legal scholars (e.g., Pistor, 2020) have gone as far to say that data governance by large platforms could replace law and markets, we take a more subtle stance. Legal penalties and liability should, do and will continue to play an important role in the background, but the attempt by governments to assign data exclusion rights to individuals and enforce them entirely by means of litigation and fines runs counter to the reality of a pervasive, digitized environment. Service operators and equipment vendors are directly connected to the users and the networks; governments cannot be without becoming more intrusive and a greater threat to privacy than the companies themselves. Data that informs product and service provision in ways that are unique and exclusive will not completely overcome the massive amount of open data generated by internet ~~and social media~~ users, but its value might encourage platforms and other service vendors to husband the resource more carefully.

References

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature* (Vol. 54, Issue 2, pp. 442–492). https://doi.org/10.1257/jel.54.2.442

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

Ad Age. (2003, September 15). *History: 1950s*. https://adage.com/article/adage-encyclopedia/history-1950s/98701

Alphabet Inc. (2020). *Form 10-K*. https://www.sec.gov/Archives/edgar/data/1652044/000165204420000008/goog10-k2019.htm

Barker, A., McGee, P., & Abboud, L. (2020, October 28). *Apple hit with antitrust complaint in France over privacy controls*. Financial Times. https://www.ft.com/content/9b032f02-d6fe-45a5-b936-dadcff3ceca7

Böck, H. (2019, May 20). *T-Online-Navigationshilfe: Telekom beendet DNS-Hijacking*. Golem.De. https://www.golem.de/news/t-online-navigationshilfe-telekom-beendet-dns-hijacking-nach-strafanzeige-1905-141370.html

Boyle, J. (2003). The second enclosure movement and the construction of the public domain. *Law and contemporary problems*, *66*(1/2), 33-74.

ClearCode. (2020, September). *Apple's changes to IDFA in iOS 14*. https://clearcode.cc/wp-content/uploads/2020/09/Apples-Changes-to-IDFA-in-iOS-14-updated-September-2020-By-Clearcode.pdf

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

Dolan, C. (2021, January 29). *How IDFA Being Targeted Will Affect Ad Tech*. Advertising Week 360. https://www.advertisingweek360.com/how-idfa-being-targeted-will-affect-ad-tech/

eco - Association of the Internet Industry. (2020). *Discussion Paper: DNS over HTTPS*. https://international.eco.de/dns-over-https/

Espinoza, J. (2021, April 26). *German groups file Apple antitrust complaint as it makes privacy changes*. Financial Times. https://www.ft.com/content/0a48d9aa-244b-4945-b2a0-01c68683544a

European Commission. (2021, April 30). *Antitrust: Commission sends Statement of Objections to Apple on App Store rules for music streaming providers*. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2061

Evans, B. (2020, June 15). *News by the ton: 75 years of US advertising*. Benedict Evans Blog. https://www.ben-evans.com/benedictevans/2020/6/14/75-years-of-us-advertising

Facebook Inc. (2021, July 28). Second Quarter 2021 Results Conference Call. https://s21.q4cdn.com/399680738/files/doc_financials/2021/q2/FB-Q2-2021-Earnings-Call-Transcript.pdf

Facebook Inc. (2021, October 25). *Facebook Reports Third Quarter 2021 Results*. https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Third-Quarter-2021-Results/

Fruits, E. (2020, December 17). *The Case Against Google Advertising: What's the Relevant Market and How Many Are There?* Truth on the Market. https://truthonthemarket.com/2020/12/17/the-case-against-google-advertising-whats-the-relevant-market-and-how-many-are-there/

Hess, C., & Ostrom, E. (Eds.). (2007). *Understanding Knowledge as a Commons*. The MIT Press.

Hewitt, R. (2003). *Conditional Access - The Key to Private and Pay-TV Systems*. http://www.coolstf.com/mpeg/#ca

ICANN Security and Stability Advisory Committee (SSAC). (2020). *SAC109: The Implications of DNS over HTTPS and DNS over TLS*.

ISBA. (2020). *ISBA Programmatic Supply Chain Transparency Study*.

Jajkowski, S. (2013). *Chicago Television- Phonevision on KS2XBS*. http://www.chicagotelevision.com/pay.htm

Johnson, J. (1982). Direct Broadcast Satellites: FCC Adopts Open Skies Policy for Space Age Technology. *Hastings Communications and Entertainment Law Journal*, *4*(4). https://repository.uchastings.edu/hastings_comm_ent_law_journal/vol4/iss4/12

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

Keith, S. (2021, April 27). *Apple's Privacy Changes Are Poised to Boost Its Ad Products*. Wall Street Journal. https://www.wsj.com/articles/apples-privacy-changes-are-poised-to-boost-its-ad-products-11619485863

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

Lessig, L. (2002). Privacy as property. *Social Research: An International Quarterly*, *69*(1), 247-269.

Letang, V., & Stillman, L. (2020, December 7). *MAGNA Global Advertising Forecast*. https://s3.amazonaws.com/media.mediapost.com/uploads/MagnaYearEnd2020Forecast.pdf

Leonard, A., Webb, C., & Ellett, A. (1956). Phonevision - An effective method for subscription television. *Journal of the British Institution of Radio Engineers*, *16*, 205–219.

Libecap, G. D. (1986). Property rights in economic history: Implications for research. *Explorations in Economic History*, *23*(3), 227-252.

Livingood, J., Antonakakis, M., Sleigh, B., & Winfield, A. (2019). *Centralized DNS over HTTPS DoH, Implementation Issues and Risks*. https://tools.ietf.org/id/draft-livingood-doh-implementation-risks-issues-03.html

Moody, G. (2020, May 18). *It's Impossible To Opt Out Of Android's Ad Tracking; Max Schrems Aims To Change That*. TechDirt. https://www.techdirt.com/articles/20200518/02402744518/impossible-to-opt-out-androids-ad-tracking-max-schrems-aims-to-change-that.shtml

Mueller, M. (1987, January). *Dishing Out Competition*. Reason Magazine. https://reason.com/1987/01/01/dishing-out-competition/

Mueller, M. (2007). Property and commons in internet governance. *Available at SSRN 1828102*.

Mueller, M. (2010). Critical resource: An institutional economics of the Internet addressing-routing space. *Telecommunications Policy*, *34*(8), 405–416. https://doi.org/10.1016/j.telpol.2010.05.002

National Security Agency. (2021, January). *Adopting Encrypted DNS in Enterprise Environments (PP-21-0016)*. https://media.defense.gov/2021/Jan/14/2002564889/-1/-1/0/CSI_ADOPTING_ENCRYPTED_DNS_U_OO_102904_21.PDF.

Needleman, S. (2021, October 25). *Facebook Posts Slower Sales Growth With Apple Privacy Policy*. Wall Street Journal. https://www.wsj.com/articles/facebook-expected-to-post-slower-sales-growth-with-apple-privacy-policy-11635154200?mod=djemMoneyBeat_us

OECD (1999), "Conditional Access Systems: Implications for Access", OECD Digital Economy Papers, No. 42, OECD Publishing, Paris, https://doi.org/10.1787/236561160725.

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.

Ostrom, E. (2005). *Understanding Institutional Diversity*. Princeton University Press.

Pistor, K. (2020). Rule by Data: The End of Markets? *Law and Contemporary Problems*, *83*(101), 101–124.

Rusche, C., & Scheufen, M. (2018). *On (intellectual) property and other legal frameworks in the digital economy: An economic analysis of the law*. Institut der deutschen Wirtschaft (IW).

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

Samuelson, P. (2000). Privacy as intellectual property?. *Stanford law review*, 1125-1173.

Spanish Data Protection Agency (Agencia Española de Protección de Datos). (2019). *DNS Privacy*.

Tankovska, H. (2021, February 5). *Facebook ad revenue 2009-2018*. Statista. https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/

Terlep, S., Higgins, T., & Haggin, P. (2021, April 8). *P&G Worked With China Trade Group on Tech to Sidestep Apple Privacy Rules*. Wall Street Journal.

https://www.wsj.com/articles/p-g-worked-with-china-trade-group-on-tech-to-sidestep-apple-privacy-rules-11617902840

UK Parliament. (2019, May 14). *Internet Encryption*. Volume 797. https://hansard.parliament.uk/Lords/2019-05-14/debates/E84CBBAE-E005-46E0-B7E5-845882DB1ED8/InternetEncryption

United States District Court for the District of Columbia. (2021). *United States of America v. Michael A. Sussman (1:21-cr-00582-CRC)*.

Vixie, P. (2020, February 5). *The Unintended Consequences of Internet Privacy Efforts*. Dark Reading. https://www.darkreading.com/risk/vixie-the-unintended-consequences-of-internet-privacy-efforts-/d/d-id/1336985

Yarvis, L. A. (1984). Signal Piracy: The Theft of United States Satellite Signals. In *Fordham International Law Journal* (Vol. 8, Issue 1).

Zech, H. (2016). A legal framework for a data economy in the European digital single market: Rights to use data. *Journal of Intellectual Property Law and Practice*, *11*(6), 460–470.

Zenith Radio Corporation. (1955). *Zenith Story, A History From 1919*.