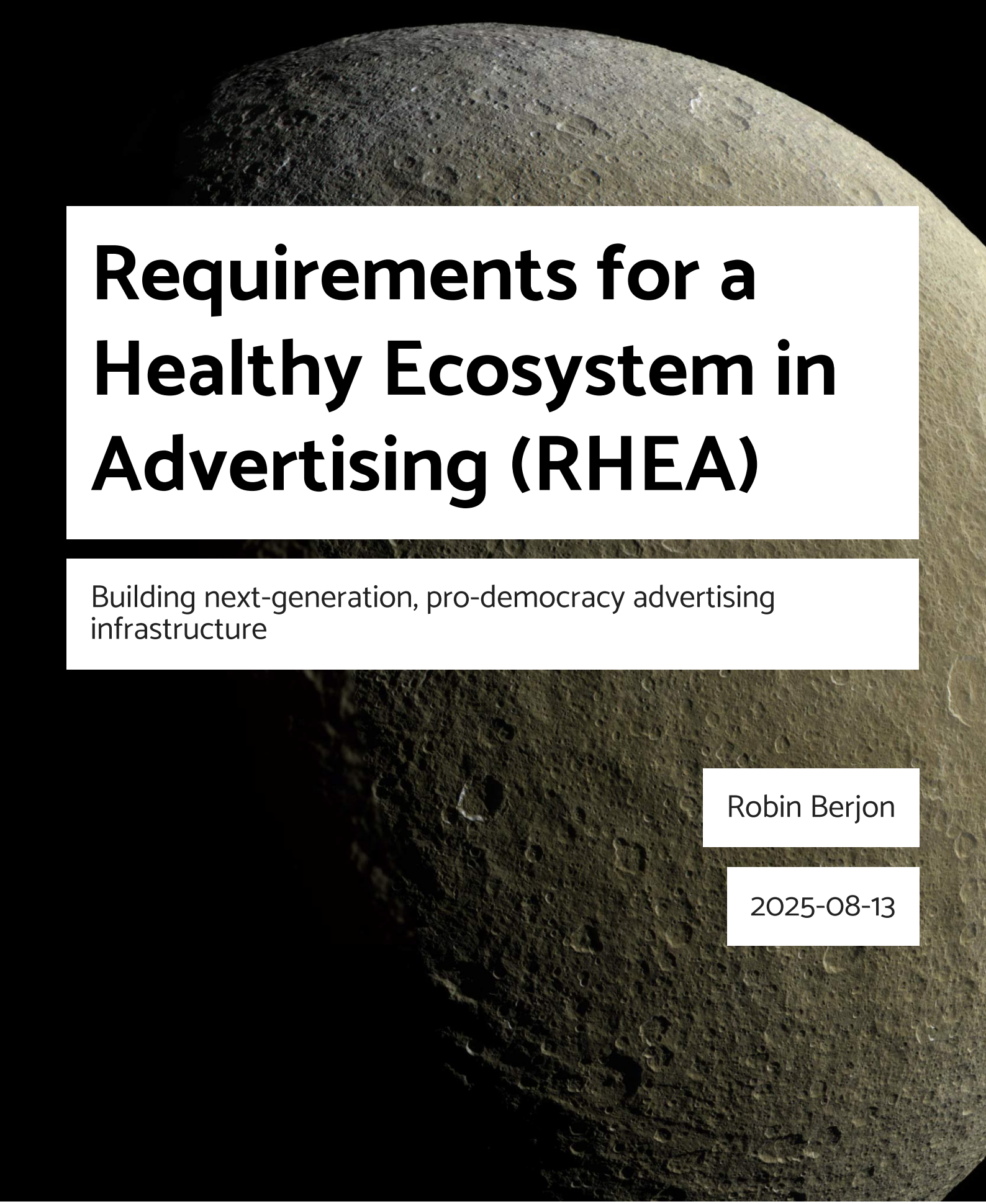

Requirements for a Healthy Ecosystem in Advertising (RHEA)

Building next-generation, pro-democracy advertising infrastructure

Robin Berjon

2025-08-13

supramundane *agency*.

Advertising is a critical input to much of the digital economy, not least of which media. In fact, it has proven essential to the point of being described as "the business model of the internet." Unfortunately, however, advertising has not been governed with the care that such an important piece of infrastructure deserves. Advertising is unpopular with technologists who want to do good, activists and civil society organisations often simply propose to eliminate it or limit themselves to superficial proposals that don't engage with the technology or economics (e.g. "just use contextual"), and regulators have found the advertising system highly opaque and complex to engage with. It is common that publishers and marketers would only partially understand the system they use, which in turn stokes fear of what may happen if anything were to change. The field is highly concentrated around a Google/Meta duopoly and fraught with a long list of ills, but a comprehensive vision for a stakeholder-centric alternative has yet to emerge.

This document outlines what an alternative could be. It doesn't claim to be complete and certainly not detailed, but it offers a path forward that can hopefully be iterated upon and deployed.

An Ecosystem Of Multifaceted Problems

There is extensive literature about issues in digital advertising, and summarising it is beyond the scope of this paper. Instead, we offer a list of the more salient problems in the space so as to inform both the urgent need for reform and the shape of the solution space we consider further down.

Taxing The Media to Subsidise Disinformation

Legacy digital advertising is a system that, at the scale of the entire internet, taxes high-quality contexts (often the media) and redistributes that money to slop farms and disinformation operators, while advertising intermediaries take a cut.

To understand how that works, it is important to understand that today's digital advertising shares data in such a way that the same person will be recognised by intermediaries across completely unrelated contexts. Crucially, this means that a person can be observed in one context and targeted in another.

Not all contexts are equal. Quality publishers (of all sizes) develop specific audiences over time and through hard work. These audiences are valuable for advertisers because they correspond to a meaningful group of people that can correlate well with brand goals or a given purchase intent. Slop farms and disinformation networks, on the other hand, do not produce valuable, well-developed audiences. Instead, they try to drive traffic up through any means available. In addition to the low quality of the context they offer, they also have amorphous audiences without clear advertising value. When contexts are isolated (and also when advertisers have better control over where their advertising ends up), it is more challenging for slop and disinformation to be profitable.

This all changes when people can be targeted across contexts. A given person can be observed as being part of a high-value audience and later targeted in a low-value context. This both decreases the valuation of the quality context — since it is getting fewer, lower bids for its own audience — and increases the revenue that flows to slop and disinformation, what is

known as *Made For Advertising (MFA)* sites. It is a distributional arrangement that takes money from hard-working media to subsidise disinformation. This is detrimental to the media, to democracy, and to the information ecosystem overall.

A few additional details add some colour. First, slop is profitable on volume (of which there is a lot) and also provides an outlet for lower-quality ads. There is an equilibrium point that blends a given proportion of quality and slop contexts at which an advertising marketplace such as Google's is maximally profitable. Since the marketplace controls data distribution and prices, they are in a position to ensure this equilibrium is maintained.

Second, it's tempting to believe that marketers may benefit from lower prices thanks to this but it's not obvious that they do — they often have poor visibility into the contexts in which their advertising reaches their intended clients.

And finally, it's important to keep in mind that what policy documents from Google or Meta describe as "publishers" is a large undifferentiated group that almost always includes active disinformation networks and slop farms.

A pro-democracy solution must put an end to this subsidy system, both to make quality publishers more profitable and disinformation a less attractive business.

Privacy

Issues of surveillance in digital advertising are well established. The loading of one single ad typically involves broadcasting someone's interaction with a given page or system to hundreds of additional parties, and after the ad has been loaded yet more parties are contacted. All of these actors obtain identifiers that enable them to track people's behaviour across their entire online presence. Both publishers and marketers are typically unable to provide a reliable list of who has seen any given person's data, and are even less able to account for processing purposes. Regulatory interventions have produced very little impact and consent-based approaches often inconvenience people without affecting data collectors much.

There is at best only limited evidence to support the idea that this data collection and processing is needed. Not one single reproducible study has been produced, results point in different directions depending on method and data set, and many studies are conflicted (or don't declare conflicts), fail to test meaningful counterfactuals, and some commonly-cited ones are preposterously wrong.

There is, however, an advantage to surveilling people in many contexts: it's an effective way to predict that a given person is about to purchase a specific product (or carry out a similar action), show them an ad right before they buy it, and claim the conversion. This is worth unpacking. Marketers are keen to measure the effectiveness of their campaigns by attributing conversions — a specific action taken by a person, often a sale but not necessarily — to whoever showed that person an ad that "triggered" this conversion. But deciding what ad might *cause* which given person at what given time in which specific context to buy something is inordinately hard. It is *a lot* easier to detect that a given person is about to make a purchase no matter what — especially if you have data about what they search for through a search engine, their entire browsing history through your browser, their location through your mapping application and a mobile OS, and access to what they are emailing about.

Showing an ad for a product that someone is about to buy anyway is a net loss for the advertiser: that is literally the *last* person who should be seeing that ad. But the advertiser doesn't know that, and it makes it possible to claim the conversion, which means greater advertising dominance and more future spend. There is evidence that this practice is taking place ([*hbr-targeting*]) and no study has eliminated the concern. The massive data leak that is digital advertising is therefore not known to be better for advertisers and, as deployed, might be worse for them. We already know from the previous section that it does not help publishers.

Fraud

In addition to intermediary practices that are detrimental to people, publishers, and marketers, the digital advertising environment is riddled with fraud. A report from the World Federation of Advertisers speaks for itself ([*wfa-ad-fraud*]). They predict ad fraud to be worth USD $50bn in 2025 at the conservative end of the spectrum (and up to almost three times that), potentially making it second only to the cocaine and opiates market as a form of organised crime.

Interestingly, the WFA estimates that whenever ad fraud is committed, less than half of the money goes to the fraudster, with the rest flowing to "legitimate" intermediary actors. One doesn't need to be cynical to note that the revenue amounts and the widespread nature of fraud do not incentivise intermediaries to crack down on it.

To make matters more interesting, the suggested cure for these problems can often make the problem worse, for instance when Invalid Traffic (IVT) or brand safety vendors (who are supposed to keep ads from appearing in wrong, including fraudulent, contexts) systematically defund climate reporting or use their tooling to index publishers' content and compete against them for contextual targeting.

Security

The technical practices of adtech and martech are also intrinsically insecure. The entire edifice is built on top of unverified third-party code injection. When (not if) a marketing vendor is compromised, the attacker becomes able to run code on often tens of thousands of websites as if they were the website operator, allowing them to interact with backend APIs or to capture data entered by users, up to and including username/password combinations.

This is a direct consequence of the open-ended promiscuity of the adtech stack, as empowered by browser vendors. It is, in a very concrete sense, strictly impossible for a publisher to abide by their legal obligations to be diligent with cybersecurity if they also wish to display advertising from today's industry.

This additionally makes data breaches impossible to audit after the fact. In many cases, there is simply no way to know which third parties had code injected into a page as a breach was ongoing.

Whenever a security bug is uncovered in a browser, advertising provides an excellent delivery mechanism for it. And because code is injected dynamically, it is possible for an attacker to inject malicious code for a time, attain a given objective, and then remove the malicious code without leaving any trace.

Espionage

It is tempting to lump all issues downstream of data collection under privacy, but when you combine the scale of the surveillance, the sensitive nature of the data including all online activity and geolocation, and a technical architecture that entirely obfuscates who is listening you obtain a system with societal and geopolitical concerns that exceed privacy issues typically more centred on furthering individual agency.

Indeed, it is possible to buy information off the shelf about military and intelligence workers who attend brothels and visit nuclear vaults ([*wired-nuclear-brothels*]) and thanks to the wide sharing of identifiers between data brokers the U.S. government can create a one-stop-shop for sensitive personal data provided by the private sector ([*spy-one-stop-shop*]). This confirms earlier work from The New York Times in which reporters, with access to only a *tiny* subset of the data that brokers have were able to track people to nuclear plants, church, family planning ([*nyt-last-night*]).

Nothing about this data limits its use to the espionage of nation-states, it is perfectly applicable to corporate espionage as well. Listing all the people who work in a given building during the day and leave digital trails that expose them to blackmail is trivial. As is knowing what employees are reading about on the internet, what they are buying, or where they are travelling to.

While not specific to advertising, this issue is almost entirely driven by advertising-related data collection.

Opacity

The digital advertising environment is so opaque that very little evidence-based decision-making is possible. Marketers track campaign performance as best they can and make the most informed decisions that they are able to (e.g. using mixed-media modelling) but by and large they lack the ability to sufficiently understand which levers are really effective and where their campaigns are really shown.

The biggest impact from this is risk aversion. Actors will have an ad strategy that delivers *something* and any major change feels like it could bring everything down. It is so difficult to meaningfully attribute causality — even if experienced practitioners know how to make localised improvements — that it is impossible to assess changes without tests and very difficult to create meaningful tests.

Advertisers are often in the dark about where their ads were placed. Publishers are often in the dark about which impression drove which income, and completely in the dark about most ads they carry or how much the buyer paid for them. Calculating the adtech tax is at best challenging and some of the better attempts at tracing money from buyers to sellers failed to account for very significant sums.

Concentration and Governance

There is little need to expand on problems of concentration in the advertising market now that Google has been convicted as a monopolist in *both* digital advertising in general and search advertising. The overall digital advertising market has a large number of small actors because there are plenty of services — many of them of dubious value — that can be overlaid atop the core money-makers, but there is no doubt as to who dominates the market and makes the rules. Even Meta, the other arm of the duopoly, takes second place to Google's global empire.

While this situation is well documented, it is worth underlining a couple of specificities that should guide efforts to fix the advertising market.

First, as explained at length by Dina Srinivasan, "*Google dominates advertising markets by engaging in conduct that lawmakers prohibit in other electronic trading markets: Google's exchange shares superior trading information and speed with the Google-owned intermediaries, Google steers buy and sell orders to its exchange and websites (Search & YouTube), and Google abuses its access to inside information.*" ([*why-google-dominates-ads*])

That is possible because, unlike other electronic markets (and, in fact, markets in general) advertising trading markets are largely unregulated or operate under unenforced regulation. This is possible in part because the digital advertising industry was granted the leeway to self-regulate for 25 years (which it largely did not do), and in part because Google controls and sets the rules for the marketplaces, data ingress points (browsers and operating system), and largest market participants. Google is the actor with the most power and the most to lose from sharing governance over advertising markets.

A second consideration is that it isn't possible to completely separate the already-complex digital advertising system from related considerations involving browsers, operating systems, and search.

Part of the issue has to do with privacy. For one, Google Chrome is not only the only remaining significant browser to offer no privacy protection but it also deploys an impressive array of deceptive patterns to trick its users into disclosing their entire browsing history to Google — something which Google then uses to optimise its search engine, an advertising business. Google isn't the only one to blame: Apple also invented mobile ad IDs so that people would be tracked in apps and markets privacy but defaults to Google Search.

But, more importantly, the manner in which Google's search business maintains its dominance has a direct impact on the value of advertising across the digital sphere, defunding other actors. In a nutshell, money that is spent on search advertising isn't spent elsewhere in the advertising system. But, as established in the U.S. Google Search case, Google's

monopoly in search allows it to charge supracompetitive prices in search, and the centrality of search means buyers cannot easily switch to spending elsewhere. This means that Google Search is depreciating ad prices for the rest of the digital sphere. In turn, that search monopoly is enforced by browser vendors and mobile operating systems, who get a cut of that revenue in exchange for the service. The system operates as a de facto cartel, making money by artificially driving up the value of Google Search ads and defunding ad revenue for the rest of the web.

Sustainability

The real-time nature of ad bidding requires having every ad request processed by hundreds of parties. This is highly inefficient. The vast amounts of data being collected, stored, access, and processed for this system also incur energetic costs.

Additionally, ad creatives are often exceedingly heavy (in bytes), which uses up bandwidth and processing power. Since they are typically seen thousands if not millions of times, the effect adds up.

What's more, some types of ad fraud can be particularly processing-intensive.

Overall, while sustainability considerations in advertising have rarely been foregrounded, there is meaningful room for improvement along this dimension as well. ∎

Who To Improve Advertising For?

Today's legacy system puts advertising intermediaries at the centre, with marketers a very distant second, then publishers, and finally people. This proposal inverts that order entirely.

Better for people. No one likes advertising, but under this systems the entire advertising environment will be far safer, with much higher privacy, and much more stringent security. Ads will allow use fewer resources and will better support publishers. It will be possible to use the internet without an ad blocker. This new system also comes with protections for children and vulnerable people built in.

Better for publishers. Quality publishers will no longer have to give away their hard work in order to subsidise slop farms and disinformation providers. With a more equitable market, their revenue will go up. It will also be safer to operate a site or app, and those will offer a faster, more pleasant user experience. You will make money for knowing your audience.

Better for advertisers. This system makes it easier to stamp out fraud and offers traceability for all spend. It helps shake bad actors out of the market — and let's face it, we all know that many marketing options that we have to use are bad products from untrustworthy actors. It offers more credible financial reporting on spend.

Better for legitimate adtech actors. Legitimate adtech actors face the unpleasant task of having to promote themselves in an industry in which flat-out lying and fraudulent behaviour goes unpunished and where the rules are set by tech monopolies in their own exclusive interest. By eliminating much of the cruft and the fraud, we can make it easier for good actors to operate and innovate.

Better for democracy. With improved privacy, less espionage of our people and our businesses, cheaper enforcement of data regulation, increased protection against interference campaigns, easier auditing of political advertising, stronger protections for children and vulnerable people, improved revenue streams for the media, the benefits to democracy are not hard to find. ∎

Privacy

The approach to privacy advocated here is principled but it does not match the ideal of privacy advocated by many CSOs. Rather, it offers a messy compromise of the kind that we should expect in a democracy. (*Note: this section focuses on the GDPR because the first order of business for this project is Europe, but much of the thinking can be extended elsewhere and implemented via other legal mechanisms.*)

This kind of contested consensus is precisely what strong data governance frameworks like the GDPR should be used to. Contrary to popular but incorrect opinion, nothing in the GDPR requires that people should consent to nearly every processing in nearly every context using an uninformative, agency-reducing popup. The alternative to consent is also not a blanket nuclear option in which practically all data processing beyond serving content is obliterated. The regulation, ill-applied as it is, is mercifully more powerful than its caricature.

The central organising principle of RHEA's approach to privacy is *sole controllership*, which is to say that to the extent possible whenever a person interacts with an entity they only have to deal with one data controller in charge of determining the means and purposes of data processing. Note that this does *not* entail that said means and purposes are lawful or aligned with the expectations of the data subject. It only means that that there is a single point of accountability.

This helps multiple constituencies:

- **For people**, it means that their data does not get processed outside of the context in which it was collected and it gives them a unique point of contact for issues. It eliminates the current universal data leak of the RTB system and severely limits the amount of processing of their data. Also: it should be possible to eliminate most consent banners.
- **For publishers**, it protects their audiences such that advertising technology providers can no longer use publisher data to compete against publishers and sell targeting services to enrich slop farms.
- **For advertisers**, while it initially restricts some targeting and reporting capabilities, these can progressively be supported again with adequate data protection. In time, this will create an ecosystem that is far less fraudulent, much more auditable (particularly for publicly-traded companies that meaningfully audit their marketing

spend), and far more transparent. This will open the door to better decision-making leading to improved performance.

Supporting this approach requires multiple steps working together.

First, a number of processing exemptions must be made to ePrivacy/GDPR consent requirements, comparable (and possibly identical) to those established by the CNIL ([*cnil-exemptions*]). This makes it possible to help eliminate many consent banners for baseline, single-controller processing. Relying on consent for this kind of processing is detrimental because it makes some of the safer, more conservative, least invasive data processing look exactly like the most dangerous and invasive kind.

Second, publishers are required to support the Global Privacy Control (GPC, [*gpc*]). This is a GDPR-compatible signal that indicates that the user is exercising their data rights to enforce single-controllership by withdrawing their consent to all data processing involving other controllers and objecting to all sharing of data to other controllers made under legitimate interest. The GPC is already available in multiple browsers.

Third, targeting capabilities are driven by Seller-Defined Audiences (SDAs), which is to say that they are developed, supported, and maintained by the publishers (sellers) rather than by third parties. Note that nothing prevents a seller from carrying out invasive profiling (other than lawfulness) but they are uniquely responsible with respect to their users.

Systems to use SDAs already exist today but publishers have very little incentive to ever use them. The problem is that developing audience segments is costly but the current RTB ad systems means that the fact that a given person is part of a given segment is broadcast to every party that is listening to the RTB bidstream. In practice, under the current system, publishers are forced to offer the hard work of developing segments with every intermediary in the advertising industry, for free, knowing that they will then use that data to compete with the seller in other spaces. Single controllership and the fact that ad requests are not being broadcast (see *Marketplace* below) make SDAs worth investing in for publishers.

Note of course that this document assumes that contextual targeting is available at all times. Experience from contextual actors shows

Fourth, since not all privacy requirements can be enforced through technical means, all participants are bound by the terms of an Article 40/41 Code of Conduct. This could be the legal mechanism supporting the exemptions or the GPC requirement, for instance. This provides the grounds for the sort of trade-off that we are seeking: the Code of Conduct can offer some lenient rules for some aspects of data protection but in a balanced exchange for auditing and enforcement capabilities mandated under Article 41. Aspects that could be governed under the Code include how ad servers must respect data protection and targeting requirements set by the institution and purchased in the marketplace (both described below) or how some constrained geolocation information can be provided in order to geofence campaigns.

Fifth, in order to support smaller publishers, we could consider some limited kinds of audience sharing built around data exchanges under the Data Act. Any kind of sharing is potentially problematic so any such project would need strong independent validation.

Sixth, purpose-specific technical capabilities (e.g. attribution, fraud prevention, frequency or recency capping, retargeting) will be governed by the marketplace and institution (see below). Powerful, privacy-preserving methods have been proposed for some of these but their practical, cost-effective deployment may be some time away. In order not to let the perfect be the enemy of the good, the RHEA system will afford these capabilities in initially implementations (constrained, controlled, and governed) that may be less privacy-protecting, but will gradually shift to better implementations.

Finally, in order not to put all decisions relating to privacy in the hands of an institution that could become captured by financial interests (given that it is, after all, centred on making money), the institution

will be required to rely on systems that allow privacy decisions to be delegated to mini-publics via sortition (Lin Kyi, Asia Biega, Paul Gölz forthcoming) or on user experiences designed to support more informed decision-making in the cases when consent is necessary ([*consenter*]).■

Marketplace

Digital advertising has many components, but by far the most influential is the marketplaces that match buyers with sellers. By focusing our energy on fixing that component, we obtain leverage from which to fix other issues.

One aspect of advertising marketplaces to understand is that they are infrastructure. Marketplaces are, by their nature, two-sided markets and this in turn makes them challenging to displace. A deployed two-sided market is just as immovable as the sunk capital in a dam or port. Infrastructural systems are in a position to set rules that govern their users and this is no exception. Digital advertising is in a bad place in large part due to the structure of today's advertising marketplaces. But there is a silver lining: because it is a point of governance and rule-making, by gaining control over it we gain power to make much of the system operate much better.

Programmatic Problems

Today, most digital advertising is transacted by what are known as "programmatic" channels. With the exception of direct-sold advertising in which a deal is concluded directly between people working for the buyer and seller, which is a minority of cases primarily towards the high end, advertising is bought and sold through automated means. What this document proposes is to change the dynamics of that automation.

The most well-known issue with today's programmatic advertising is that is *assumes* that you must broadcast personal data in order to work. With every bid requests, a person's identifier is sent to hundreds of bidders along with information that can retrace their behaviour. Advertising intermediaries also synchronise identifiers with one another and construct elaborate identity graphs so as to better identify people as they move from context to context. In addition to the surveillance and espionage concerns that this massive, constant, unchecked data leak raise, the system also disincentivises publishers from innovating and understanding their audiences better because any information that they share with the bidding system gets shared with all the participants in the bidding system, who can then simply reuse that information to target people elsewhere.

The structural assumptions of the programmatic system produce a structural redistribution of revenue, taking from

quality publishers and supporting slop makers. The TCF, which was proposed to afford some control over data broadcasting is at best a fig leaf: it shares the personal data along with a little flag that says "you're not allowed to use this." (Technologists call this approach a "bozo bit" because only a bozo would be deterred by it.)

This broadcasting of personal data happens because, if you want to perform *real-time* bidding then you need to be providing potential bidders with information, in real time, about what they are expect to bid on.

But the truth is that real-time processing is unnecessary. Buy-side systems don't typically determine in real time what to buy or not, or only in a limited fashion. Segments, targeting parameters, etc. are typically processed in batches.

Not only does real-time processing assume poor data protection practices but it also makes it hard for publishers to audit the quality of creatives that they serve and it grants the market operator a lot of power by playing even on some very minor (and hard to measure) differences in access to data or timing ([*why-google-dominates-ads*]).

What is valuable about programmatic is the automation. What we seek is therefore automation that may be fast (e.g. purchasing small batches of impressions) but doesn't require real-time, sell-side pull-based processing.

A Marketplace Standard

The Beckn Protocol is an OTN (Open Transaction Network) that is emerging as a standard marketplace interactions. It abstracts all the steps required in listing inventory, matching buyers and sellers, making deals, delegating payment, and various attestations and certifications that can be relevant for a given type of market.

Beckn is deployed by specialising that protocol for specific commercial areas (which has been done for retail orride hailing, and is ion the process of being applied to energy markets for instance) and then operating a network backed by server infrastructure to implement the marketplace itself. Client tools on both the seller and buyers sides then connect to that marketplace and transact there.

Specialising Beckn for advertising, sellers would make inventory available on the marketplace based on impressions that they expect to have in the relatively-near future. (Just how near and what timing-related rules apply is an operational question, but the flexibility is important.) Impressions are made available with whatever targeting information the seller has available, notably SDAs and geofencing.

Buyers bid on impressions or impression bundles based on what they wish to purchase, how soon they want the mini-campaign (if an impression bundle) they want to run, with what pacing, on which contexts they wish to appear, etc. Note that we can operate multiple mechanisms here: buyers can bid directly to publishers, or we can use match-making algorithms to optimally pair supply and demand. Creatives (detailed below) are part of bids so that sellers can factor that into pricing, reject what they deem unsafe or out of policy, etc.

Once a deal is concluded between a buyer and a seller, the mini-campaign is installed in the seller's ad server. The seller has a pre-defined window inside of which to produce the impression, after which the deal is nullified. Funds are held in escrow in the mean time.

Note that because impressions are bought without sharing data, sellers are incentivised to develop Seller-Defined Audiences (SDAs), which encourages them having a better understanding of their audience and the kind of trust relationship that makes consented profiling possible — all things that are impossible under today's arrangement. A constant risk with SDAs (that isn't specific to this arrangement) is that sellers are incentivised to lie about the segments they have. In order to avoid that, the marketplace could maintain a reputational index based on conversions per segment.

Because the protocol is standardised, people can build high-quality tools to access it (both for buyers and sellers) and compete on tool quality, without having to deal with capricious changes or risking being excluded. It means that buyers and

sellers can build their own smart automation, pace their campaigns, have more effective yield management, and generally develop fully transparent knowledge of what works for them. Accountable, evidenced-based decisions become possible for marketing and advertising executives, as well as for the finance teams that oversee them.

Standards are not, however, magical and just using an open standard for a marketplace doesn't give that marketplace good stakeholder-centric governance. This section describes the high-level technical arrangement, the governance of the network(s) is necessary as well and covered in a later section.

This foundation can provide a solid basis atop which to gradually develop solid advertising features (as outlined in the next subsection) but more generally to provide a more transparent ecosystem that can be more readily reasoned about. Everything from KYC requirements to evidence that an ad was actually served by the right entity (e.g. in part with signed origin delivery such that the server attests that a given impression was on its own server) can be put in place to govern ad markets with the same rigor that is expected from other electronic markets.

The Whole Set

Digital advertising requires more than just matchmaking between buyers and sellers, it also features a number of additional mechanisms to make the market operate more smoothly, and notably to make running a campaign more efficient. These include the likes of attribution, fraud prevention, frequency or recency capping, or retargeting.

This report does not go into detail about how all of those features can be supported. The goal here is to establish that another foundation for digital advertising is possible — on that foundation we can then layer the additional functionality. This can happen in multiple ways:

- Initially, we can support at least some of these features using the mechanisms that they rely on today. This won't provide the ideal data protection (including audience protection) properties that are called for, but continuity in transition is important.
- As an intermediate step, we can proxy or support some of these features based on infrastructure operated by the Garuda institution (see below). This is imperfect, but provides a trusted intermediary and improves on the current situation.
- The more recent privacy-preserving alternatives can be rolled out, such as Attribution.

Crucially, as we transition advertising to RHEA, not everything has to land on day one — only enough that it's useful at least for initial users. We can plan and prepare a gradual switch, including one that initially supports programmatic access so that publishers can drop it into their site without much work.∎

Creatives

An underappreciated problem in digital advertising is the role of creatives, the trade name for those bundles of markup, code, and images that render as ads. Because of how open-ended creatives are and of how insecure their implementation is — they primarily work by injecting code from arbitrary sources that can change at will or upon compromise — they render auditing near-impossible, are a major malware vector, are a privacy free-for-all, and obfuscate attempts at tracing the origin of given attacks. Because there is very little in the way of incentives to build them efficiently, they also tend to be highly wasteful in bytes and code execution, which hurts both user experience and publisher revenue, and is wasteful of energy.

Under RHEA creatives use a different system that is compatible with existing web technologies but much safer.

First, creatives are locked down in terms of what they can access from the network. They can *only* load resources from their origin ad server (which must comply with a number of privacy and security requirements). This means that they cannot load unexpected code or exfiltrate data other than through pre-determined and controlled channels.

Second, all of their dependencies are loaded in a content-addressed manner (which is to say that they are located by a cryptographic hash of their content) and the root manifest that lists these dependencies is itself transmitted with a hash. This has multiple benefits. One is that the user agent (e.g. browser) is able to verify when loading an ad that it is getting untampered content. This makes it impossible to modify a dependency while a campaign is in flight in order to replace it with malicious code. Another is that during post-mortem auditing, it is possible to know with certainty all the content that was involved in rendering an impression. This also makes it easier to scan content prior to setting up an ad campaign to ensure that it is safe and adheres to policy. (Note that content-addressed loading can lead to some privacy attacks but 1) that is still a substantial gain over what exists today and 2) there isn't much to do with that data since it can't be exfiltrated.)

Creatives as a content-addressable tree also renders the work of accountability by third parties easier. It is possible for researchers or journalists to recognise the same creative loading in multiple places and to be able to reproducibly analyse its

behaviour. This can help, for instance, with ad driven foreign interference campaigns.

Third, creatives are attested, which is to say that the content is cryptographically signed by the buyer. This makes it possible to trace them to their originator. This information can be used to ensure that only legitimate political actors buy political ads (which can be surfaced and reported for instance in the browser) or to support the auditing of better-business practices.

Fourth, the content-addressed manifest offers a convenient place to capture metadata about the creative. This can be used for instance for regulatory purposes such as requiring that all political ads be flagged or that ads indicate their age appropriateness. Ads for sensitive topics such as gambling or alcohol could be required to be flagged as such in their metadata so that the user agent is able to filter them out.

Finally, because the full dependency tree that produces a creative must be provided at the time that the purchase is executed, this makes it possible to enforce policies about creative size, either to reject them or to charge more for more resource-intensive creatives.

Buyers often want to adapt campaigns in flight (e.g. to respond to better lift from a variant). We support this by encouraging buying in small batches such that campaigns can be updated over time as more impressions are gradually purchased.

All of these changes can be implemented using existing web technologies but in some cases they would benefit from more direct support from user agents. This provides a path forward: we can implement this system immediately and gradually make it more efficient by moving support for it into user agents. ∎

Governance

Today's internet governance apparatus handles many low-level technology standards from IP to HTML, but as our digital sphere has grown to encompass most human activities, internet governance has failed to grow with it and comes up short on two aspects. First, in scope: most digital governance needs sit well above low-level tech but they are hardly addressed at all, primarily left to tech monopolies. For advertising, this role could have been taken on by the IAB, but it is primarily focused on lobbying for the industry as well as heavily Google-dominated. Second, in enforcement: the enforcement mechanism used by internet standards is competition in the market — if you don't implement the standard well, you will lose to competitors. Because market-backed enforcement feels automatic or even magical, the internet governance community has largely failed to think about effective enforcement or the reckon with what would happen to standards as the primary markets they operate in ceased to be contested.

As a result, there is no existing governance structure able to take on governing digital advertising infrastructure and very little in the way of models to imitate, despite it being obvious that leaving the system to its own devices has failed. This was particularly obvious during the slow-motion wreckage of the Privacy Sandbox proposal. We need institutions that are able to govern the *runtime* operation of transnational digital infrastructures.

A useful approach to governance consists in splitting the problem into smaller ones that can be governed by simpler, more manageable entities. This is done by separating out responsibilities and creating protocols such that different components with different roles can interact with one another. This approach applies here, but because the marketplace that intermediates ad buyers and sellers has such central power, this document focuses primarily on outlining a governance model for that family of entities.

The Garuda Institution

Garuda stands for "Governance of Ad Requests by a Union of Diverse Actors," named after the deity Garuda. The institution has several responsibilities:

Shepherding the technical standards that define the marketplace and related infrastructure. Garuda convenes technical discussion around marketplace standards

as well as related ones such as attribution. It also manages the integration of the advertising ecosystem into wider technical communities that operate with similar infrastructure (e.g. the Beckn Protocol). It carries out the work in writing standards, finding consensus, and developing test suites, to ensure that the marketplace is interoperable, royalty-free, and production-grade. It also manages the core principles that drive the work and serve as a constitutional foundation to the governance.

Managing the open source implementation and maintenance of the marketplace. The marketplace software will be developed in an open source manner, but changes made to the code will need to be aligned with the objectives of the institution, which will need to be reflected in the change review process. Further, there is no expectation that software development will be entirely carried out by the community; rather the institution should provision sufficient resources to underwrite the marketplace's development.

Organising the worldwide network of marketplaces. The institution will operate a network of marketplaces with high-performance SLAs and an arrangement that enables easy auditing. This will entail delegating to local operators while ensuring that the network as a whole remains trustworthy. The institution will seek a balance between locally-devolved power so that advertising can operate the way that local jurisdictions expect it to and global interoperability so that the planetary network operates seamlessly and is able to uphold a number of core principles.

Ensuring the general health of the advertising ecosystem. By providing a common space where stakeholders must reach some form of consensus in order for the system to operate, the institution is taking on some responsibility for the health of the broader digital advertising ecosystem.

Governance Outline

This section provides only an outline of the governance model for the Garuda institution so as to give a general sense for it.

The Garuda institution is comprised of two primary bodies: the Governance Board and the Legal Entity.

The Governance Board is tasked with the oversight of the institution and the slow-moving aspects of governance. All Board deliberations are public with rare, motivated exceptions. Board terms are limited. It concerns itself primarily with the fundamentals:

- Oversight of the Executive Director's work.
- Standard and implementation process.
- Core principles of the institution.
- What can be decided by local operators (subsidiarity) versus what must be upheld at the planetary level.

The Legal Entity takes care of day-to-day operations. It is responsible for maintaining, deploying, and operating the network and marketplace at requisite Service Level Agreements (SLAs) and at reasonable cost, as well as of research into future technology that Garuda could use, with organising the various groups that will bring stakeholders together to help evolve Garuda over time, and with the elaboration of policy positions which Garuda will cooperate with regulators on. It is run by the Executive Director. The Board selects (by consensus) an Executive Director every three years or whenever the post becomes vacant.

There are three primary constituencies: user agents (e.g. browsers, operating systems, generally systems that control the conditions of ad rendering), sellers (often known as publishers), and buyers. For each of them, there are inclusion criteria designed to prevent gaming the system by spawning multiple entities. Votes are not necessarily prorated by volume, or if they are then a discount must be applied to avoid skewing too heavily in favour of larger actors. Governance Board seats are apportioned to constituencies. (The Board may then extend itself by inviting additional members.) No company can have more than one representative, even if it participates in different constituencies.

The institution is financed through a very small tax on advertising. Multiple models are possible: a flat fee per bid, a percentage of effective CPM transacted, or a flat fee per unit time that one is buying or selling on the marketplace are all possible. The amount and type of the tax is determined by the Board.

Part of the tax should further be set aside to provide financial support to stakeholders who cannot afford to pay someone to spend time in Board discussions, so as to ensure that participants from companies of all sizes, and from all backgrounds the world around can participate with equity. Another fund can be set up to support user agents that agree to abide by a given covenant (e.g. for privacy) so as to support the implementation of high-quality client software that is aligned with the needs of its users.

Subsidiarity

One challenge which this document only addresses briefly is that of the interplay between a planetary system — that must be interoperable and that should adhere to a minimal set of principles so as to be predictable in its operation — and the need for locally-anchored governance, reflective of local preferences and jurisdictions.

It is important to support both and not just global interoperability because the latter, operating alone, eliminates the agency that people are afforded through their local governance arrangements. We can only have democratic technology if it is designed and governed to be responsive to local jurisdiction.

There is a corollary to that choice: it also means that wherever the local regime is undemocratic we must accept that, for the most part, the local deployment of the digital infrastructure will also be undemocratic. This is because when globally interoperably digital infrastructure has the power to impose certain values, then it has the power to impose unethical, dangerous, or detrimental values. With subsidiarity — the arrangement according to which decisions that can be made locally are — we may lose democratic governance in some places but we gain democratic potential everywhere. We have to accept that liberation must be locally-led and not imposed from the outside.

A globally interoperable network that delegates infrastructural operations to entities in local jurisdictions has strong benefits in decreasing the cost of compliance and increasing the ease of regulatory enforcement. If, for instance, you know that your advertising infrastructure is GDPR-compliant then you can limit yourself to worrying only about your own data processing. Simultaneously, regulators have a partner with which to develop viable, sustainable enforcement. This means that that you liberate more energies for innovation while having credible regulation at the same time — an eat-your-cake-and-have-it-too arrangement. ∎

Public Policy

The RHEA system is not built on recent innovations in technology or governance, and even when a given component hasn't existed for a long time it wouldn't have prevented the emergence of this arrangement earlier. If this system has so many promising properties, why doesn't it exist already?

Several aspects have conspired to make it challenging:

- **Convening**. Making this system works requires convening support from a range of actors who have no convenor in which they can all meet.
- **Monopolies**. States have largely abandoned the governance of the digital space to tech monopolies, and they have no interest in making it work in ways that align with democracy and public interest.
- **Scale**. Advertising systems live or die on scale. Deploying an entirely new advertising system needs access to significant scale on both the buy and sell sides in order to stand a chance.
- **Regulatory environment**. The regulatory environment, including in Europe, does nothing to improve digital advertising and in many cases worsens the situation.

Most of these hurdles can be cleared using public policy (scale is harder, but investment and procurement can help sustain the system until it has grown enough). Discussions with regulators and policymakers has shown that one driver of their continued lack of intervention is that they don't see potential alternatives to the current system and worry about harming an industry that is essential to the media at a time when media companies are already on life support. But the benefits that RHEA offers can become a floor for policy, regulation, and enforcement even before RHEA is big. It can be the tide that lifts all boats and drowns all bad actors. Several policy interventions could help transition to this better system:

Break. Google is already a convicted monopolist in advertising (twice if you count that the search conviction includes search ads) and there are additional cases, notably in Europe. Google's rule-setting power in advertising makes improving this infrastructure highly challenging. Their influence power is also not to be discounted: much of the time they have a desk right inside major agencies, are in constant contact with larger buyers and sellers, and control most industry bodies.

A break-up would make a big difference in diminishing that power. It is not a solution on its own because, barring better-built alternatives designed from the ground up to work in the interest of multiple stakeholder groups, the market will just tilt again. The power of intermediaries in n-sided markets simply cannot be contained with simple markets supported by antitrust intervention every other decade. But not being a solution on its own does not mean that it cannot create space in which a broader strategy can flourish.

GDPR. It is no secret that GDPR enforcement is a failure. Legitimate small businesses bend themselves out of shape to adhere to meaningless bureaucratic compliance while the biggest data brokers just leak data all around with impunity. There is active discussion in Brussels about "re-opening the GDPR" and thus reforming the text of the regulation itself. This is both cumbersome — not to mention risky — and unnecessary. Why go through such a painful process when many of the GDPR's biggest issues can be fixed with lighter-weight interventions?

Leaning more into standardised data processing, relying more on Articles 40/41 to establish meaningful baselines, seeking consensus about exemptions, supporting automated signals like GPC, shifting harder to decisions to collectives, improving data processing risk signalling are all examples of ways in which the GDPR, as a powerful legal framework, can be deployed in ways that make sense to people and businesses.

And as part of this, the GDPR needs to be enforced against the most egregious violations. The RTB system is one, the manner in which mobile operating systems or Google Chrome track people are others. In most online contexts, there is simply no justification for having more than one controller involved at any given time. There no justification for your browser to provide your entire browsing history for further processing. It is highly challenging for good actors to emerge when the industry is organised as a race to the bottom and regulators sit by watching anxiously.

DMA. The DMA is another unused or underused powertool. It was designed to shape digital markets so that they would operate in ways that are aligned with the needs of society, but so far it has only been used to have gentle conversations with monopolies, non-binding public workshops, and a couple of parking tickets.

One component of the DMA that has a meaningful impact on advertising systems is the ability for monopolies that provide more than one service to blend data from several of those services together. As explained above, this ability gives them an edge in advertising in that using data extracted from a very broad surveillance area they can detect purchase intent, show an ad for a purchase that was going to happen, and claim the conversion. The DMA should be used to enforce strict separation of those data sets and (since it unfortunately has a consent-to-monopoly exemption) impose strict requirements on consenting to cross-context data mixing. Like the rest of the DMA, this has yet to mobilised in any meaningful way.

Beyond that, the DMA has a real market-structuring toolbox and market-structuring is what is needed here. It could for instance be used to impose conditionalities on for instance search engines, browsers, etc. in terms of how they allow data to circulate.

DFA. The Digital Fairness Act (DFA) is still being shaped, but it could provide a promising vehicle for advertising-related consumer protection. A good avenue of further work is therefore taking the time to understand which provisions would most help people and support establishing a RHEA-like system.

Of particular interest is the idea that user agents — software that works on behalf of a person and represents them in their interactions with other software systems — should be regulated and required to operate in a trustworthy manner. It has already been suggested that the DFA include requirements for AI agents to be trustworthy, but there is no reason to make this so restrictive and fashion-specific — user agents hold huge power and that power is being used to deceive people and shape markets with or without AI. The W3C Privacy Principles already support such a notion ([*privacy-principles*]) and earlier work on the fiduciary responsibilities of agents offers further details ([*fiduciary-ua*]). ∎

Acknowledgements

In earlier iterations, Aram Zucker-Scharff, Max Gendler, Mihir Kshirsagar, and Reuben Binns provided much invaluable feedback. Many thanks to Juan Ortiz Freuler for organising a discussion session around Garuda at the Berkman Klein Center for Internet & Society before it was even public, as well as to Levin Kim, Crystal Lee, Sahar Massachi, Tom Zick as convenors of the *Ethical Tech* and *Big Tech Governance* groups, and the attendees of the session for a spirited and constructive discussion. Erik Bugge is always there to prove that contextual works better than everyone expects, and to suggest the simplest, no-nonsense solution.

Heartfelt thanks as well to *The New York Times* for supporting earlier versions of this work. While there, Allison Murphy, Sasha Heroy, Jackie Lee, and Danielle Racioppi very, *very* patiently explained to me how advertising and marketing work.

Finally, my deep thanks to Vera Franz and Cori Crider for long discussion and convening the group that this document is for. ∎

References

[cnil-exemptions]
Délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux «cookies et autres traceurs») et abrogeant la délibération n° 2019-093 du 4 juillet 2019. CNIL. 2020-09-17. https://www.cnil.fr/sites/default/files/atoms/files/lignes_directrices_de_la_cnil_sur_les_cookies_et_autres_traceurs.pdf

[consenter]
Consenter. Max von Grafenstein. https://www.consenter.eu/

[fiduciary-ua]
The Fiduciary Duties of User Agents. Robin Berjon. 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827421

[gpc]
Global Privacy Control (GPC). https://globalprivacycontrol.org/

[hbr-targeting]
Does Personalized Advertising Work as Well as Tech Companies Claim?. Bart de Langhe; Stefano Puntoni. 2021-12-16. https://hbr.org/2021/12/does-personalized-advertising-work-as-well-as-tech-companies-claim

[nyt-last-night]
Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret. Jennifer Valentino De Vries, Natasha Singer, Michael H. Keller And Aaron Krolik. 2018-12-10. https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

[privacy-principles]
Privacy Principles. Robin Berjon; Jeffrey Yasskin. 2025-05-15. https://www.w3.org/TR/privacy-principles/

[spy-one-stop-shop]
U.S. Spy Agencies Are Getting a One-Stop Shop to Buy Your Most Sensitive Personal Data. Sam Biddle. 2025-05-22. https://theintercept.com/2025/05/22/intel-agencies-buying-data-portal-privacy/

[wfa-ad-fraud]
Compendium of ad fraud knowledge for media investors. World Federation of Advertisers; The Advertising Fraud Council. 2016. https://swa-asa.ch/wAssets/docs/publikationen/de/branchenempfehlungen-swa/WFACompendiumofAdFraudKnowledge.pdf

[why-google-dominates-ads]
Why Google Dominates Advertising Markets. Dina Srinivasan. 2019-12-09. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3500919

[wired-nuclear-brothels]
Anyone Can Buy Data Tracking US Soldiers and Spies to Nuclear Vaults and Brothels in Germany. Dhruv Mehrotra; Dell Cameron. 2024-11-19. https://www.wired.com/story/phone-data-us-soldiers-spies-nuclear-germany/