Ari Kronen

Ad-Filtering Dev Summit 2024

Ad-Blocking as a Reclamation of Agency in Digital Spaces & Beyond

Roughly 3,775 years ago, a Sumerian man dictates the following to his scribe: *Take cognizance that from now on, I will not accept here any copper from you that is not of fine quality. I shall select and take the ingots individually in my own yard, and I shall exercise against you my right of rejection, because you have treated me with contempt*.[1] This man's name was Nanni, and he bears the honorable distinction of being responsible for what is, perhaps, the first written consumer complaint in human history. A number of additional complaints sent to the merchant who sold him substandard copper – Ea-Nāṣir – have been uncovered by archaeologists, with one beleaguered writer – Imgur-Sin – asking, 'Do you not know how tired I am of this?'.[2]

The cache of grievance letters (tablets, rather), discovered at one of Ea-Nāṣir's long-abandoned properties, were composed by individuals who, apparently, fell prey to the false promises of this unscrupulous monger of metals. As Nanni himself explicates, 'When you had arrived, you claimed that you would give good ingots to Gimil-Sin, but you have not done so'.[3] This is to say, that Nanni and the other disgruntled customers were victims of deceptive advertising, which is made further evident by the desperation in Ea-Nāṣir's replies.[4] I share this abbreviated *Tale of Ea-Nāṣir* because it neatly exemplifies two fundamental elements of the thesis I present: **1**. Advertising is ubiquitous, and humans have been confronted with nefarious advertising practices since the dawn of civilization. **2**. Advertising, when it works at least, is a self-replicating phenomenon, which makes it all the more rife for serious misuse and abuse.

1 A. Leo Oppenheim, *Letters From Mesopotamia* (Chicago, US: The University of Chicago Press, 1967), 83.
2 Kristina Killgrove, "Meet The Worst Businessman Of The 18th Century BC", *Forbes*, 2018, https://forbes.com/sites/kristinakillgrove/2018/05/11/meet-the-worst-businessman-of-the-18th-century/.
3 Ibid.
4 Erin Blakemore, "Think customer service is bad now? Read this 4,000-year-old complaint letter", *National Geographic*, 2024, https://nationalgeographic.com/history/article/ea-nasir-copper-merchant-ur.

Ea-Nāṣir's correspondence also reveals that he belonged to an ancient coalition of merchants known as *the Dilmun Traders*, illustrating that, much as we do now, the peoples of 18th century BC Mesopotamia had to deal with predatory business conglomerates.[5] The parallels run deeper still, in that Ea-Nāṣir and his trading group had clearly cultivated a good reputation – however undeserving – by self-promotion and word of mouth, what some *marketeers* these days might call viral marketing. Humorously, the exploits of Ea-Nāṣir live on via image macros (or *memes*) that have been spread about him for going on a decade[6], but what most loudly rings through the ages here, is the exasperation felt by his customer base, which many of us can identify with today. As Imgur-Sin was, we too are, so very tired of being treated like rubes by advertisers and corporations. Most importantly, like Nanni, we have chosen to demonstrate agency, to exercise our *right of rejection*, which is truly the crux of the issue.

Indeed, advertising has been around in some shape or form since humans first started congregating together in towns and cities, yet at no point in history have we been so exposed to it, as we are in the postmodern era. For anyone who is not living off the grid in a substantial way, advertising is everywhere; On billboards, in magazines, newspapers and mailboxes, at subway stations, bus stops and gas pumps, on the radio and TV, even via unsolicited phone calls and text messages, but nowhere is it more preponderant than the internet, and the devices which are regularly connected to it (unless, of course, an ad-blocking solution is in-place).

What I aim to elucidate through this exploration, is that a major byproduct of pervasive digital advertising, and telemetry – with which it has become inextricably linked – is reduced agency; A subversion of our natural rights to exercise control over our own lives, and our own

5 Kristina Killgrove, "Meet The Worst Businessman Of The 18th Century BC", *Forbes*, 2018, https://forbes.com/sites/kristinakillgrove/2018/05/11/meet-the-worst-businessman-of-the-18th-century/.

6 Andrew Gardner and Louise Rayner, "The Legend of Ea-Nasir: how a Babylonian businessman became an internet meme", *Institute of Archaeology – University College London*, 2023, https://ucl.ac.uk/archaeology/events/2023/jan/legend-ea-nasir-how-babylonian-businessman-became-internet-meme.

thoughts. Furthermore, that along with undermining self-ownership, these forces work in tandem to minimize the avenues by which we demonstrate ownership of property, namely our devices, and our data. I also seek to highlight how the commodification of attention and personal information facilitates developments such as vendor or platform lock-in, and to address oft-overlooked contexts in which these phenomena have manifested in a most problematic way. Finally, I will discuss proven solutions that are available to us, and challenging areas that may require new ones to be devised.

Over the past two decades, global spending on digital advertising has seen a significant increase every year.[7] Estimates show an expenditure of more than 700-billion dollars on this particular form of marketing, from across a wide variety of sectors, in the past year alone.[8] This trend has been painfully evident on platforms and operating systems that are integral to the work and recreational activities of billions, which are transforming into ever more efficient vehicles for ad-delivery, and its nastier cousin, telemetry (which is frequently difficult to differentiate from spyware).

It is important to emphasize here, that digital advertising has become inseparable from tracking, which is best exemplified by what we know as targeted advertising.[9] Implementing telemetry in order to serve customers more effective advertisements has come to form a vicious, never-ending cycle, which has resulted in bulk personal data becoming a valuable commodity, now being traded on open and clandestine markets. This has led to serious legal proceedings surrounding what news media likes to call *big tech*, and *big data*.[10]

---

7 Statistia Research Department, "U.S. Online Advertising Revenue 2023", *Statistia*, 2024, https://statista.com/statistics/183816/us-online-advertising-revenue-since-2000/.

8 Statistia Research Department, "Digital Advertising - Worldwide", *Statistia*, 2024, https://statista.com/outlook/dmo/digital-advertising/worldwide.

9 Naif Mehanna, *Intrinsically Inseparable: Investigating Novel Tracking Practices and Assessing the Carbon Footprint of Ads* (Lille, FR: Université de Lille, 2024), https://theses.hal.science/tel-04647367v1/document.

10 Nicholas Confessore, "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far", *New York Times*, 2018, https://nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

With the release of Windows 10 to consumers in 2015, Microsoft began integrating advertising and telemetry into their desktop operating system at unprecedented levels. Adverts began to appear on the login screen, on the desktop post-login (via notifications of varying sizes), in the start menu, in the search UI, and even through pop-up dialogues.[11] The categories of data collected by and transmitted to Microsoft were greatly expanded past the usual diagnostic and personal information to include: Handwriting and voice recognition; Text selections; Search queries; Auto-completed terms; Running process names; URLs visited in their Edge browser, and more.[12] Along with the aforementioned, Microsoft rolled out what is, for all intents and purposes, a compulsory Windows Update policy, rendering all updates unavoidable for the average consumer, including those responsible for deploying these undesirable elements onto Windows installations.[13] The trend of increased ad-delivery, tracking, and arbitrarily limiting user freedom, continues with Windows 11.[14]

If one wishes to use a recent version of Windows, freed from Microsoft's bombastic brand of user-hostility, they will either have to build a custom image of the OS, heavily modify a fresh install[15], or acquire editions that are not available to consumers through legal means, with many of these approaches being known to break crucial components of the operating system, such as the entire Windows Update mechanism.[16] Sure, there are lightweight third-party utilities which can be used to mitigate some of these issues on active installations, but their efficacy

---

11 Whitson Gordon, "How to Remove the Most Annoying Ads From Windows", *PC Magazine*, 2024, https://pcmag.com/how-to/how-to-remove-most-annoying-ads-from-windows.

12 Joel Hruska, "Microsoft finally reveals exactly what telemetry Windows 10 collects about your PC", *Extremetech*, 2017, https://extremetech.com/computing/247311-microsoft-finally-reveals-exactly-telemetry-windows-10-collects-pc.

13 Sean Hollister, "Microsoft won't fix the most frustrating thing about Windows", *CNET*, 2017, https://cnet.com/tech/computing/microsoft-windows-10-forced-updates-auto-restarts-are-the-worst/.

14 Greg Farough, "Life's better together when you avoid Windows 11", *Free Software Foundation*, 2021, https://fsf.org/news/lifes-better-together-when-you-avoid-windows-11.

15 "FAQ." *Revision*, 2024, https://revi.cc/docs/category/faq/.

16 "Windows 10 Ameliorated - the Most 'Barebones' Version of Windows 10." *Tonymacx86.com*, 2020, https://tonymacx86.com/threads/windows-10-ameliorated-the-most-barebones-version-of-windows-10.303463/.

varies greatly[17], and it has been shown[18] that some of the policies and settings which such programs modify, are not respected by the OS, and bypassed.[19]

While Apple's own desktop operating system, macOS (or OS X, as some of us still prefer), has a much cleaner track record, being orders of magnitude less flagrant in these departments, it still has a unique set of privacy and advertising pitfalls.[20] The consistently diminishing means through which users are able to service or repair their Apple products[21], certainly constitutes a loss of agency as well, though hardware freedom and right-to-repair issues are too deep of a tangent for this presentation.

We have seen Google, one of the long-time worst offenders in this space, continue along a similarly troubling trajectory with Android. With each new release it becomes more and more challenging to decouple your data from Google. Application usage, typing habits, SIM card serial numbers, WiFi MAC addresses, auto-correct, voice, location, and contact data, are all shared with Google by the average Android device, with evidence showing that many of these metrics are still being transmitted when the user is not logged into their Google account.[22]

If you wish to use Android without this rampant and invasive misbehavior from Google or an OEM, you may find yourself installing third party utilities from an alternative source like F-Droid, entering ADB commands to remove preinstalled software, or, going through the process

---

17 Ars Staff, "Even When Told Not to Windows 10 Just Can't Stop Talking to Microsoft", *Ars Technica*, 2015, https://arstechnica.com/information-technology/2015/08/even-when-told-not-to-windows-10-just-cant-stop-talking-to-microsoft/.

18 "Windows 10 Privacy Settings", *IT Security Office | Virginia Tech*, 2024, https://security.vt.edu/resources/win10privacy/.

19 Gordon Kelly, "Microsoft Admits Windows 10 Automatic Spying Cannot Be Stopped", *Forbes*, 2015, https://forbes.com/sites/gordonkelly/2015/11/02/microsoft-confirms-unstoppable-windows-10-tracking/.

20 Arin Waichulis, "Apple addresses privacy concerns around Notification Center database in macOS Sequoia", *9To5Mac*, 2024, https://9to5mac.com/2024/09/01/security-bite-apple-addresses-privacy-concerns-around-notification-center-database-in-macos-sequoia/.

21 Georgia Young, "The Apple is still rotten", *Free Software Foundation*, 2017, https://fsf.org/blogs/community/the-apple-is-still-rotten-why-you-should-avoid-the-new-iphone.

22 Douglas Leith, *Mobile Handset Privacy: Measuring The Data iOS and Android Send to Apple And Google* (Dublin, IRL: Trinity College Dublin, 2021), https://scss.tcd.ie/doug.leith/apple_google.pdf.

of unlocking your phone or tablet's bootloader, finding a variant of android – a *ROM* – that is compatible with both your device and carrier, then copying firmware partitions, and flashing said ROM in a recovery environment.[23] This is prohibitively complicated for the average user, can also lead to breakage of fundamental device features[24], and hampers users from accessing commonly used services outside of the Google ecosystem.[25]

No such alternative options even exist for Apple's mobile devices, and, though they are a bit less brazen with how advertising and telemetry have been implemented on iOS, both are still very much parts of the platform. Apple serves ads throughout a number of core iOS applications, collects much of the same data about iOS customers that Google does from its Android users[26], and in-fact, disabling some of the telemetry categories which *are* exposed to the user on iOS, has no effect at all.[27] While network and content-filtering can, to an extent, mitigate OS behavior like this, it is an uphill battle.

Feature-creep has been regularly observed in the world of proprietary, commercial software, and this goes doubly so in the mobile device arena, where it is all-too-often paired with new encroachments on privacy, and new ways of delivering ads. The rise of smartphones and similar mobile devices has been an undeniable influence on the direction which commercial desktop operating systems have taken, and this is much to the detriment of our privacy.

Commercial desktop and mobile operating systems seem to have reached a point of convergence in this regard, where types of advertising and tracking that were once largely limited to the latter, have become increasingly common on the former. This is to say nothing of

---

23 "Install LineageOS on Motorola G7 Power", *LineageOS Wiki*, 2024, https://wiki.lineageos.org/devices/dre/install/.

24 "Issues - LineageOS", *Gitlab*, 2024, https://gitlab.com/LineageOS/issues/android/-/issues.

25 Chris Hoffman, "SafetyNet Explained", *How-To Geek*, 2016, https://howtogeek.com/241012/safetynet-explained-why-android-pay-and-other-apps-dont-work-on-rooted-devices/.

26 Douglas Leith, *Mobile Handset Privacy: Measuring The Data iOS and Android Send to Apple And Google* (Dublin, IRL: Trinity College Dublin, 2021), https://scss.tcd.ie/doug.leith/apple_google.pdf.

27 Ibid.

streaming boxes such as Roku, Fire Stick, and Apple TV, which are so laden with advertising and telemetry[28], that they can see notable breakages, or outright refusal to function, if they fail to communicate with certain ad and tracking servers.[29]

By now it should be apparent that advertising goes hand-in-hand with not just telemetry, but reduced user choice, or in other words, a loss of agency. If you will not view their ads, if you will not accept their routine violations of your privacy, if you will not use the software or hardware they specify, you will be locked out of their services, and potentially, the services of their partners. This is an extraordinary kind of vendor and platform lock-in, as it represents a confluence of efforts from multiple entities, resulting in our computing devices more and more being treated like managed devices in an institution, or a closed office environment. Perhaps most emblematic of these worrying trends, is Microsoft's infamous *My Computer* desktop icon morphing into *Computer*, then with Windows 8, finally graduating to *This PC*.[30]

Even beloved open source stalwarts like Mozilla, who managed to avoid this unsavory melange for years, seem to have fallen under the spell. New varieties of promotional content and telemetry are periodically integrated into Firefox[31], with some being delivered through the aptly named *Mozilla Experiments* program.[32] This has resulted in a growing number of forks, and my user.js file passing 200 lines. To be fair, Firefox was not the first, is far from the only browser to implement such *anti-features*, and there are markedly worse offenders out there.[33]

---

28 Girard Kelly et al., *Privacy of Streaming Apps and Devices*, (California, US: Common Sense Media, 2021), https://commonsensemedia.org/research/privacy-of-streaming-apps-and-devices-watching-tv-that-watches-us.

29 Thomas499, "Whitelist required for firestick to work properly - Issue #115 - anudeepND/whitelist", *GitHub*, 2019, https://github.com/anudeepND/whitelist/issues/115.

30 "My Computer is now This PC", *Microsoft Support*, 2017, https://support.microsoft.com/en-us/windows/my-computer-is-now-this-pc-ddb34f0e-85f2-1cdd-6327-02879f2360f5.

31 Martin Brinkmann, "Mozilla is investigating huge Telemetry performance issues in Firefox for Android", *gHacks Tech News*, 2024, https://ghacks.net/2024/05/30/mozilla-is-investigating-huge-telemetry-performance-issues-in-firefox-for-android/.

32 "Experimenter Docs", *Mozilla Experimentation and Feature Delivery*, 2024, https://experimenter.info/.

33 Douglas Leith, *Web Browser Privacy: What Do Browsers Say When They Phone Home?* (Dublin, IR: Trinity College Dublin, 2020), https://scss.tcd.ie/Doug.Leith/pubs/browser_privacy.pdf.

On the topic, we have all heard about the technical limitations placed on browser extensions, particularly effecting ad-blocking add-ons, introduced by Google's Manifest V3. Though misunderstanding of the issues surrounding MV3 abounds, decreased functionality – and increased complexity of maintaining – ad-blocking extensions for Chromium and its derivatives, is a very real consequence of this update to the WebExtensions API.[34] This is all the more worrisome, because, as AFDS attendees are well aware, once you do use an application like Firefox or Chromium to actually browse the web, if you do not have some comprehensive ad-blocking measures in place, you are in for, to quote Wesley Willis, a *real hell ride*.

The growing prevalence of advertising and telemetry is obviously not limited to for-profit entities and producers of software. Much as they do in *meatworld*, non-profits, all manner of political organizations, and – most disconcertingly – governments spanning the globe, have gotten in on the action as well.[35] [36] Digital realms enable advertisers and promoters to both amplify the effects of traditional advertising models on a much wider scale, and to far exceed the boundaries of those models. Online marketing efforts can manifest as camouflaged sponsored content, or aggressive astroturfing[37], the former of which some lawmakers have fought through legislation[38], and innovative developers have set out to mitigate with projects like SponsorBlock.

This phenomenon of sponsored content is especially concerning in the arena of journalism. So many news outlets rely on revenue from their online presence simply to stay

34 Ekaterina Kachalova, "Mozilla solves the Manifest V3 puzzle to save ad blockers from Chromapocalypse", *AdGuard Blog*, 2023, https://adguard.com/en/blog/firefox-manifestv3-chrome-adblocking.html.

35 Lori Henson, "Federal Government Advertising Spending Has Doubled to $1.8 billion since 2018", *Rebuild Local News*, 2024, https://rebuildlocalnews.org/federal-government-advertising-spending-has-doubled-to-1-8-billion-since-2018/.

36 Domen Savič, *Spreading propaganda and disinformation using public funds* (Brussels, BE: Heinrich-Böll-Stiftung, 2021), https://eu.boell.org/sites/default/files/2021-07/Spreading_propaganda_Slovenia_Domen_Savi%C4%8D_FINAL.pdf.

37 Samantha Bradshaw et al., *Industrial Disinformation – 2020 Global Inventory of Organized Social Media Manipulation* (Oxford, UK: Oxford University Internet Institute, 2021), https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/01/CyberTroop-Report20-FINALv.3.pdf.

38 Amanda Schreyer, "Beyond the Buzzwords: Sponsored Content, Native Advertising, and Consumer Protection", *American Bar Association*, 2015, https://shorl.com/darofrestusyfe.

afloat, that it has led them to increasingly employ attention-grabbing headlines and hyperbole, in other words, *clickbait*, to generate engagement. This worrying fusion of advertising and information can be seen all over more established news media, and ostensibly independent journalism platforms as well, with both mimicking the duplicitous tactics of the other.[39] Of course, the web sites associated with these outlets, are well-known for being riddled with advertising and tracking.[40]

Michael Parenti once said, 'You don't know you're wearing a leash if you sit by the peg all day'[41], and one need only visit any single high-traffic social media platform, or popular online news publication's comment section, to see just how true that is. The echo chambers of both brand loyalists and dogmatic ideologues, rabidly regurgitating the talking points, sound bytes, and slogans absorbed through overexposure to relentless promotional campaigns and advertising culture, are readily observed on such platforms. It is self-evident that many of the people who exhibit this sort of behavior do so unwittingly, or as Richard Stallman would put it, they have become *victim-coperpetrators*. In this way, advertising and propaganda are one and the same; A bludgeon that diminishes human agency, capable of endlessly replicating itself.

The advertising industry consistently grows not only because of the fertile landscape it provides on which to cultivate loyal consumers, but due to its potential for influencing the decision-making capacities, and subverting the independent thought of, a largely captive audience. As Julian Oliver noted, the overwhelming presence of advertising in our world has *created a new kind of dictatorship that one cannot escape*[42], and I could not agree more. Through

39 Anna-Katharina Jung et al., "Click me…! The influence of clickbait on user engagement in social media and the role of digital nudging", in *PLoS ONE* 17.6 (2022): https://pmc.ncbi.nlm.nih.gov/articles/PMC9242456/.

40 Sarah McQuate, "UW researchers clicked ads on 200 news sites to track misinformation", *University of Washington News*, 2020, https://washington.edu/news/2020/09/28/uw-researchers-clicked-ads-on-200-news-sites-to-track-misinformation/.

41 Michael Parenti, "Inventing Reality", 17 Oct. 1993, https://youtube.com/watch?v=9g3kRHo_vpQ.

42 Tomás Laurenzo, *Decoupling & Context in New Media* Art (Montevideo, UY: Universidad de la República, 2013), 97.

sheer ubiquity, advertising has become a – if not *the* – driving force shaping our cultural zeitgeist, yet, the online variety is so remarkably effective that it is now a pernicious threat.

The psychological, ideological, and social dimensions of advertising are myriad, and have received much treatment in academic circles, being the subject of sizable theses and peer reviewed research papers. Along with a reduced sense of agency and critical thinking skills[43], our attention spans suffer[44], and in some cases, our abilities to recall memories are disturbed by this war for our attention.[45] Many advertising agencies and marketing departments are well aware of the deleterious effects on individuals and society at large, yet they cynically persist in the expansion of their efforts.[46]

Slovenian philosopher Slavoj Žižek sees advertising, and popular media itself, as both products of, and delivery systems for, the dominant ideologies and narratives within the societies which produce them: *I already am eating from the trashcan all the time. The name of this trashcan is ideology. The material force of ideology makes me not see what I'm effectively eating*.[47] This insight is a most prudent juncture for me to segue into solutions for the onslaught of digital advertising with which we are faced, as it is great food for thought, and doing so will prevent me from getting too far out-of-scope.

As highlighted in eyeo's most recent report on ad-filtering, there is a vast selection of ad-blocking and general content-filtering solutions available to us.[48] The array of choices covers

43 Aimee S. Riedel et al., "Dealing with intrusive ads: a study of which functionalities help consumers feel agency", in *The Review of Marketing Communications* 43.2 (2024): https://tandfonline.com/doi/full/10.1080/02650487.2023.2197778.

44 Jessica Packer et al., "Advertising and Young People's Critical Reasoning Abilities: Systematic Review and Meta-analysis", in *Pediatrics* 150.6 (2022): https://publications.aap.org/pediatrics/article/150/6/e2022057780/189944/Advertising-and-Young-People-s-Critical-Reasoning.

45 Tim Wu, "The Crisis of Attention Theft", *Wired*, 2017, https://wired.com/2017/04/forcing-ads-captive-audience-attention-theft-crime/.

46 "The Shrinking Attention Span & What It Means for Marketers", *Boston Digital*, 2024, https://bostondigital.com/insights/shrinking-attention-span-what-it-means-marketers.

47 Sophie Fiennes et al., *The Pervert's Guide to Ideology*, Zeitgeist Films, 2014.

48 Jan Wittek et al., "2023 eyeo Ad-Filtering Report", *Eyeo GmbH*, https://info.eyeo.com/adfiltering-report.

manifold use-cases, and is so dizzying, that a deep dive into the wild variety of ads and tracking which they are used to combat, is unnecessary.

We have relatively simple and time-tested methods like using the hosts file, or a proxy auto-configuration file, as a black hole to prevent resolution of unwanted domains. There are ad-hiding user style-sheets; Caching and non-caching proxies which can strip pages of unwanted elements, like Squid and Privoxy; Recursive local VPN applications like AdAway and Rethink; Router firmware like OpenWrt, which sports a number of plugins for ad-blocking. There is software for network appliances dedicated to the task, like PiHole and AdGuard Home, along with a growing number of public ad-blocking DNS resolvers, like DNS Warden or Control D. Now, web browsers like Brave and Vivaldi have eminently configurable ad-blockers built right in too. Most popular, however, are the extremely flexible ad-blocking browser extensions; with Adblock Plus, AdGuard, and uBlock Origin leading the pack.

It is heartening to know, that Just as digital advertising and tracking continues to grow, so do the number of people using ad-blocking software.[49] One would have to search high and low amongst those working within or adjacent to the IT sector, to find an individual who does not use at least one of the ad-blocking solutions I've mentioned thus far. The same can be said for that segment of informed consumers which tech publications once fondly dubbed *power users*. Browsers that have integrated ad-blocking components even make content-filtering accessible to our grandparents, but this is not without a concerted effort by those who have a vested interest in serving ads and harvesting personal information, to stop it.

There are a variety measures which have been employed to discourage users from blocking unwanted content, chief among them are so-called *adblock-killers*, anti-adblock scripts like BlockAdBlock. These generally consist of JavaScript inserted into web pages which verify

49 Ibid.

whether a specific file has been retrieved, or if a set of minuscule elements are loaded and displayed. If the content was not successfully retrieved, or the elements have been hidden, the user will either be forcibly redirected to a warning page as opposed to the desired content, or the content is severely obfuscated in some way.[50] Thankfully, many, many workarounds exist for these adblock-killers, rendering them mostly useless to all but the most determined webmasters.

There *are* other methods that do pose real challenges for ad-blocking, such as server-side ad injection (SSAI), utilizing randomly generated and frequently changing class names, or employing design elements that incessantly nag and annoy visitors to the point where they break down and install a dedicated application for the site, purchase a membership etc... These methods are often used simultaneously, and, though *relatively* new ad-block capabilities like procedural filters can mitigate most of these efforts to varying degrees (save for SSAI and resilience), many users opt for convenience instead. Rather than wait for a list maintainer to add a workaround, or do the digging necessary to find one themselves, they will simply whitelist that site, install that app, or buy that membership, and move on with their day. There are those who will abandon such sites, but they are expectedly in the minority (this is easily deduced from the fact that Reddit, YouTube, TikTok, and so many others, are not going anywhere anytime soon). There is another challenge that ad-blocking faces, and it is not a technical issue, but an institutional one.

There are millions of workers, and most importantly, students, who spend vast amounts of their waking lives on managed devices, in environments with a restrictive AUP, and a no-BYOD policy. They are, by virtue of their place of work or study, unable to take advantage of any content-filtering options. While this may sound like a ridiculous concern to some, as an individual who has worked as a system administrator, as a teacher, and as an entry-level support technician – who has been on both sides of the table, so to speak – I believe it is of great import.

50 "About BlockAdBlock", *BlockAdBlock*, 2019, https://blockadblock.com/adblocking/about-blockadblock/.

In schools around the world, and especially in North America, Chromebooks and Android tablets have become an all-too-common sight. Not only are students forced to use these devices in many classrooms, but they are usually provisioned with content-filtering applications that are remotely administered, and, rather than protect them from ads & tracking, double as surveillance tools. These machines are outfitted with software like GoGuardian, Bark, and Gaggle, that do a whole lot more than block inappropriate content. They are then expected to perform tasks and complete assignments using Google Apps For Education, or the Microsoft 365 Education suite.[51]

The result is that all student activity on – and in some cases, in-front of – these devices, can be remotely observed, monitored, and scanned, in real time. Additionally, their activity, and any content they produce, is subject to automated analysis, which builds profiles of students, along with flagging suspicious behavior, and reporting it to teachers, administrators, parents, or even law enforcement.[52] All the while, they are data-mined by the likes of Google and Microsoft as they do their classwork. This is a solution to content-filtering that replicates the very worst ethical and social problems of digital advertising, right in the class room. I have been required to administer such software in the past, so can tell you first hand that it is cause for great concern.

Ten years ago, before I made the questionable decision of entering a graduate program full time, I was hired by an alternative school in a dual capacity, as their computer teacher and system administrator. Due to a push from some of the parents, this school had, after years of eschewing computers for students, instituted a computer class for the third grade and up. While the school had to honor agreements to use Windows on the student PCs, and some specific educational titles, as their first computer teacher – and only line of on-site support – I was free to

51 Jason Kelley, "How GoGuardian Invades Student Privacy", *EFF*, 2023, https://eff.org/deeplinks/2023/10/how-goguardian-invades-student-privacy.

52 Dave Maass et al., "GoGuardian: A Red Flag Machine By Design", *EFF*, 2023, https://redflagmachine.com/research/.

implement a whole lot from the ground up. Rather than have the students surveilled, I took a three-pronged approach to inappropriate content.

I configured the router for the classroom to use OpenDNS Family Shield. With the help of some third party software, I ensured that the base Windows image which I eventually deployed to student computers, had a hosts file in place that was updated every three days, pulling in entries from a variety of sources – including a personally curated list on a networked drive – to block additional inappropriate content, social media, and common ad & tracking servers (thanks to Peter Lowe, Dan Pollock, and Michael Burgess, RIP). Finally, the student PCs all had Firefox set as the default browser, complete with Adblock Plus, along with the EasyList and EasyPrivacy subscriptions enabled. When I would catch wind of undoubtedly inappropriate websites being discussed by students, I would take note of them, and ensure that the domains were blocked through hosts before the day was over.

This, and a little attention, is all it took. Children were not able to access inappropriate content in my classroom, and there was never a need for convoluted monitoring software. I could simply focus on lesson plans and actually teach my students. In that same classroom, one of the many units I did for higher grade levels was on internet safety and privacy. Through the use of Mozilla's Lightbeam extension – and temporarily disabling most content-filtering on one PC – I showed students a live visualization of how much they were being tracked as they browsed popular websites. While many were quite bored with this exercise, a few students took great interest in the topic, asking me to show them more about my computing preferences, what ad-blocking measures I used on my own devices, and a variety of related topics. I was able to parlay increased interest from students like this into an after-school computer club, where we worked together on Raspberry Pi kits, and a variety of projects under Linux.

I share this anecdote, because like so many things, our relationship with technology starts at a very young age. While we must guard children from inappropriate and harmful content, to instill in them an association of computing with draconian surveillance measures and a feeling of always being watched, is inappropriate and harmful in its own right. It is richly ironic that what passes for content-filtering and security software in so many schools and homes, would be considered malware and spyware were it to be found on any of our personal devices. Whether it is tracking and profiling for increased revenue, or tracking and profiling for a false sense of security, it is surveillance – in fact, mass surveillance – all the same, and the outcome is always a loss of agency. In the case of learning institutions, lost opportunity as well.

In 1996, the same year my father gave me my first computer, the late John Perry Barlow penned a manifesto of sorts, *A Declaration of the Independence of Cyberspace*. In it, he wrote as follows: “We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity. Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here... We will create a civilization of the mind in Cyberspace. May it be more humane and fair than the world your governments have made before”.[53]

Things obviously did not pan out that way. The internet that most people interact with now, is a far cry from Barlow’s vision; Dominated by corporate interests who desire to do the thinking for us, surveilled by an alphabet soup coalition that vigilantly monitors our interactions, and seeks to shape our opinions. Social media platforms that many in the public view as facilitating human connection, are essentially glorified sales funnels, designed to monetize our time, attention and data, while manipulating our emotions to drive engagement. Promising

53 See: https://eff.org/cyberspace-independence

technologies like machine learning are treated as naught more than an opportunity to outsource our capacity for understanding and analyzing new information, often in exchange for exorbitant fees.

In this dystopian landscape of exploitation and uniformity of thought, there are glimmers of hope that *the open web* may still be possible. Nascent decentralized platforms; A thriving community of open source contributors spread across countless endeavors; A bevy of software and hardware projects – whole operating systems and devices – whose raison d'être is user freedom and privacy; Peer-to-peer platforms that have persisted in the face of concerted efforts to shut them down; New, more ethical and consensual advertising models, wherein consumers are materially compensated if they *choose* to view ads – like the one envisioned by Brave – and of course, a wide swath of ad-blocking solutions which enable people to say “No!”, to those who are hell-bent on commodifying them. These are all vital parts of the alternative that must one day become the norm. Here’s to a truly a free internet, for truly free people.