

Brand Engagement, Data Currency and You

Data. It's everywhere. Whether we are referring to health data, lifestyle data, location or demographic data people are becoming more aware and concerned about their data privacy rights. At first, companies promised that by freely sharing our data we are building a symbiotic, harmonious and healthy online utopia. Some claimed that by combining our data with AI they can make our lives easier by letting hardware and software machines handle the more mundane tasks of daily life for us. The data they seek is gathered and used (sometimes without our knowledge) in exchange for access to services. The winner of this data rights debate will eventually decide who is the ultimate arbiter/owner of the digital data we generate. In general, most data collection and web tracking is done to create an advertising profile.

In the early days, the Internet existed to exchange ideas, entertain and inform. But now in order to exist, most online businesses collect or use personal data to market products and services to you in the form of targeting advertising on social media platforms, search results or when loading an ad supported website. Naturally, nefarious parties have caught on to this and have incorporated malware into the ads. Persistent tracking cookies that map your browsing habits and location are now ubiquitous. Our smartphone contain apps

with the ability to grab and track your entire life just by accessing the phone's data and capabilities.

Visiting or using a web site or mobile App often means surrendering the rights to your data and accepting the ads. The data is collected to better target and entice you to "interact" with advertisers. Algorithms use the surrendered data to create a user experience based on what you want to see (or so they think). In response, you load the browser up with ad blockers to make the experience less irritating or delete the free App entirely. You avoid clicking on anything that looks like an ad and apply "banner blindness" to whatever slips through. Consumers do not want to interact with ads if they think they are going to be tracked, or pestered for their business. Why? Nobody likes a pushy salesman.

Now if you created the data, you own it - right? Maybe, maybe not. Your data has become the new currency in the online universe and we lose the right to privacy when we utilize our data as currency. Increasingly, our collective data currency is concentrating online wealth, power and control into the hands of a few companies.

I will now stop and allow for the dissenting views.

- "Digital advertising is forecasted has become a \$500B+ industry this year. How can you say it's not working?"
- "If they see it, it counts!"
- "We show ads to the people most likely to be interested in your products"
- "Why would companies be spending this much money if it wasn't working?"
- "People have expressed an interest in my products already."
- "People are willing to trade ads for access."
- "People click on my ads all the time."

In 2015, HubSpot¹ conducted a survey on how digital advertising is viewed by the "intended" targets:

- Ads are annoying and intrusive (64%)
- Ads are disruptive (54%)
- Ads create security concerns (39%)
- Ads affect load time and bandwidth usage (36%)

In 2019, a Network Advertising Initiative² survey found that attitudes have moved from annoyance to fear.

- Data collection by Hacker (56.2%)
- Data collection by website or mobile app (12.1%)
- Data collection by ad tech companies (11%)
- Data collection by the US government (9.9%)
- Data collection by foreign governments (7.8%)

https://www.networkadvertising.org/sites/default/files/final_nai_consumer_survey_paper_22oct2019.pdf

¹ Source: https://research.hubspot.com/reports/why-people-block-ads-and-what-it-means-for-marketers-and-advertisers

²Source:

In 2021, Apple announced that its Safari browser will prevent cross-site tracking and apps downloaded from its App Store must get permission in order to track the user.

• Social media companies reportedly lost \$9.85B³ in advertising related revenue following Apple's change in policy.

It is worth noting that in the four years between the two surveys users have moved from annoyance with ads to outright fear of them. Another point is people are now more concerned with hackers and ad tech companies collecting their data than government's collection and use of their data. Do brands realize that their messages are being avoided due to fear?

Do the terms Ad Blockers, banner blindness, mute buttons and "Skip Ad Now" sound familiar? Has anyone heard of people visiting a web page just to see the ads? When was the last time you intentionally clicked on an ad? People now view online advertising the same way they view a car salesman – something to be avoided.

Mobile advertising gets more marketing dollars due to the dominance in smartphone ownership. The phone screen is too small for effective banner ads, so the accepted mantra is that video and social media will power the customer engagement. The mobile ad market is predicted to hit over \$500B this year so what could go possibly wrong? With the recent iOS updates allowing users to stop app and websites from tracking users, the major online advertising platforms are now posting earning warnings. Social media sites are reporting declining user engagement and people don't share ads. Location based advertising (and the merging of online and offline activities) was a hot trend for retail business marketing until the recent release of the new iOS app tracking options. Yet again, privacy concerns are driving people to deny mobile Apps access to their location function.

So let's recap. Companies are spending big bucks on well-researched and targeted advertising they know their consumers want to see. These consumers in turn block, ignore or abandon the ads. Increasingly, people are avoiding web sites and apps that demand access to their data in exchange for access. A psychologist would diagnose this market behavior as Cognitive Dissonance. With so much at stake, what can brands and advertisers do to prevent a possible meltdown with their customers?

Granted, websites and apps cost money and must be compensated in order to exist. What if there was a way to use one's personal data to control the world around them, hide their interactions with advertisers and for advertisers to dynamically reach out to targeted demographics all at a much lower cost?

Such a concept would involve four components an individual's data, the advertiser, the interaction itself and an Infomediary™ service. The Infomediary service is the intermediary between the individual's information and the advertiser. This new model allows the individual to store their data with the Infomediary service. The Advertiser decides what demographic they want to reach, the intended message and provides the Infomediary with the ad target. When the individual interacts with the ad target they get the demographically powered message generated by their data. Once the message is displayed

 $^{^3} Source: https://www.theverge.com/2021/10/31/22756135/apple-app-tracking-transparency-policy-snapchat-facebook-twitter-youtube-lose-10-billion$

the interaction is completed. That is, unless the individual wishes to interact further with the advertiser. The interaction's end result is the user's data never leaves the Infomediary.

So what about the Infomediary service? What privacy guarantees does the individual get if a company decides to offer a huge payment in exchange for the Infomediary service's data? In order to work, the service would have to present an absolute offer. The data belongs to the person, the data owner controls if anyone can see it, and the platform itself must not have access to the data in any format. In essence the Infomediary service has to be a black hole data system where data can enter, but never escape.

The Infomediary solution would lead to a change in the current marketing business model. Instead of viewing potential customers as heavily tracked, researched and predictable targets, potential demographic groups would become brand audiences. It would also change the ad buy methodology. Just determine what message to try with a demographic group and where to trigger the ad message. Then monitor the ad campaigns uptake and adjust the demographic and/or message in real time. However, the ad must now provide something that a consumer wants to see or interact with.

This is the vision of the Cosmos Continuum™ Augmented Reality platform. Cosmos Continuum is an immersive experience delivering an intended brand message with no tracking and complete privacy providing a much more beneficial relationship between the advertiser and the consumer. The platform protects the consumer's data and identity and the advertiser gets to send the correct message to the intended audience. No longer does the advertiser need to collect data, invade privacy and create a hostile relationship with the person they wish to do business with.

The future of brand marketing will be led by privacy enhanced brand engagement. That means advertisers and marketers will have to respect the privacy of those they wish to do business with to earn their trust. People do business with those they like and respect, not those that stalk them.