PRIVACY

Towards A New Ecosystem

SEPTEMBER 2020

TAPTAP

Confidentiality

TAPTAP

I. Introduction. A context for privacy

We are living in a world where more data than ever is available —both for us to use but also about us— especially as smartphones are nearly ubiquitous in many countries and 5G is making a formal entrance. We benefit from this data on a daily basis when we for instance check the weather or use navigation to get from A to B. We also benefit by seeing offers relevant to our interests at any given moment and through access to free services and content in exchange for our information or engagement.

As the volume of data continues to climb, users generating this data are becoming increasingly educated about how and why their data is being used and beginning to develop opinions about this use. Data privacy and security are top of mind for people worldwide, and the focus is intensifying[1].

We owe much of their education to data controversies like Facebook and Cambridge Analytica and the subsequent regulations and measures cropping up to protect privacy rights around data. We have seen how these measures have changed the landscape of digital advertising in just a few years, and they are clear indications that we are transitioning to a world where data protection and privacy is paramount and typical identifiers (like cookies and advertising IDs) are fading —all of which will continue to affect the industry.

While there may be new consumer data protections, the emergence of these measures does not precipitate the end of targeted media or measurement, but it does push every industry player, especially media vendors, to declare a position on data privacy and begin to look to the future for novel and creative ways to achieve targeted, relevant communications —a challenge we have taken up at TAPTAP.

While consensual 1:1 or addressable targeting, measurement and optimization are still a viable option, TAPTAP provides unique tools that accomplish it, like a persistent identifier, the Sonata ID, and an open ecosystem DMP, while prioritizing user privacy and transparency around data. This is because we were early adopters of implementing and prioritizing data protections, so our products and policies guiding these products are data safe by design.

Likewise, complying with data protection laws like GDPR has been a smooth process, and preparing for the eventual reality of fewer identifiers —for a time when 1:1 targeting is not scalable, not available or simply not preferable —is well underway through our product and technology development. As experts in the ultimate contextual signal, location, we have built a technology based in location intelligence that allows us to harness data and carry out our methodology of planning and profiling, media activation and measurement in new ways without necessarily having to rely uniquely on user generated data.

1. eMarketer | Digital Marketing In Today's Privacy-conscious World

II. Industry Changes

In support of further transparency and privacy rights, governments and regulatory agencies around the globe have created new laws and practices for any entity that processes or stores data. Similarly and opportunistically, the most influential names like Google and Apple are evolving their platforms in favor of their strategic business interests and proposing fundamental changes that will transform digital marketing as we know it.

The following is a brief list of the most far reaching policies.

GENERAL DATA PROTECTION REGULATION (GDPR)

GDPR redefines what is considered personal data - expanding the term to cover more - and imposes obligations to organizations anywhere if they target or collect data related to people in the European Union. It views "data protection as a pillar of citizens' empowerment and is the EU's approach to the digital transition."[2]

GDPR mandates that publishers must—

- Explain to users what data is being collected
- For what purpose
- Receive consent from end users (in most cases)
- Delete data upon request

UNITED KINGDOM DATA PROTECTION ACT (UK DPA)

The updated UK DPA contains nearly the same principles as GDPR but is adapted to local UK laws which will be most relevant locally as BREXIT is implemented. The UK DPA has been committed in the use of consent and not legitimate interest as the only privacy standard under which personal data can be obtained. The Information Commissioner's Office (ICO) is responsible for enforcing the UK DPA.

CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

The CCPA applies only to residents of California in the United States. It grants users the right to:

- Know which personal information (PI) is collected, and how it is used and shared
- Delete PI
- Opt-out of the sale of their PI

2. European Commission | Communication From The Commission To The European Parliament And The Council.

SAFARI INTELLIGENT TRACKING PREVENTION (ITP)

There have been several iterations of ITP but the most recent expires browser cookies every 24 hours on the Safari browser. Third party cookies are blocked by default, but users have the option to opt-in.

IOS 14 & IDENTIFIER FOR ADVERTISERS (IDFA)

Each device has a unique IDFA. Advertisers and publishers use the IDFA to track user activity for targeting and measurement. With the onset of iOS 14, users must grant each app specific permission to use this identifier for advertising purposes, without which persistent tracking in iOS is impossible. As Limit Ad Tracking (LAT) is implemented at a device level, no apps will have access to the ID without this user permission and opt-in. Just recently Apple announced it will delay the launch of the IDFA planned deprecation until early next year.

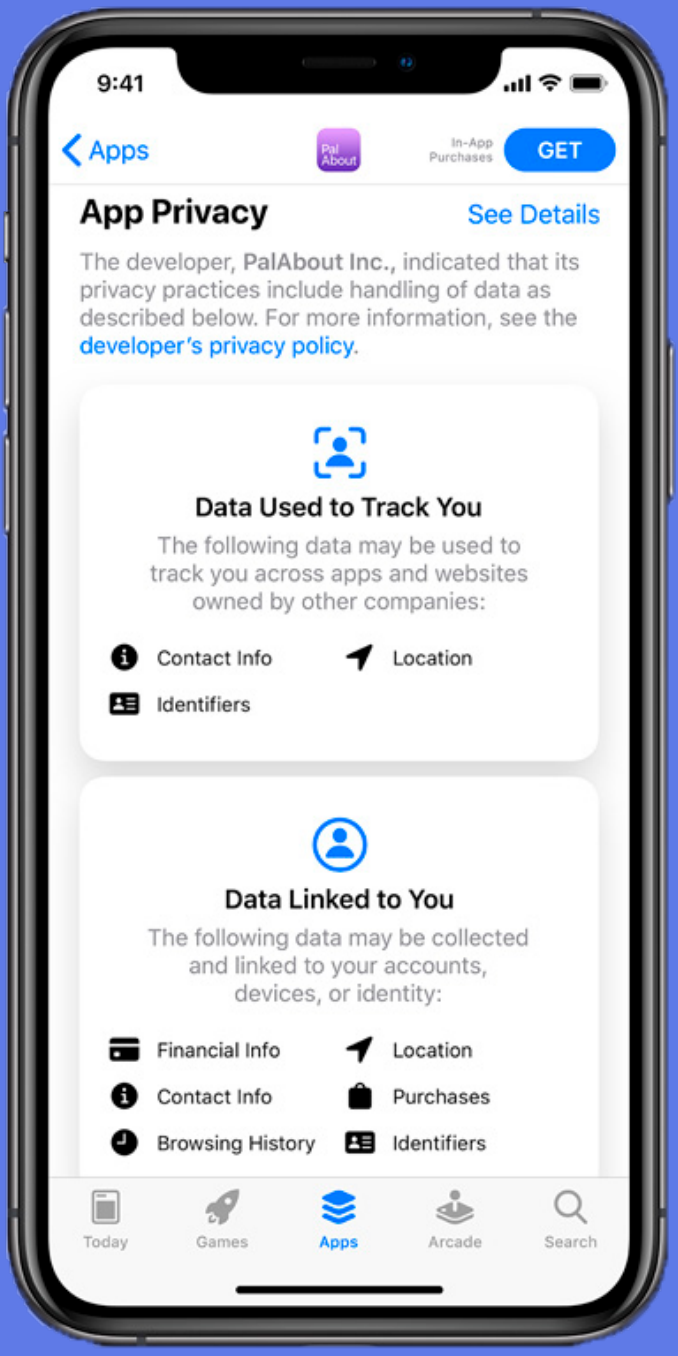
GOOGLE CHROME

In its most significant cookie policy, Google announced that it will be retiring cookies on the Chrome browser by January 2022. Chrome controls nearly 70% of the browser market share. This is one of the most disruptive initiatives we have seen and has far reaching consequences for the industry and even web innovation.

MOZILLA FIREFOX

All third party cookies are blocked by default.

Other countries, including Brazil, Mexico and China, have or are creating their own regulations, and while the CCPA applies to only residents of California, regulations at the federal level in the US are a possibility for the future.



"With the onset of iOS 14, users must grant each app specific permission to use this identifier for advertising purposes, without which persistent tracking in iOS is impossible"

Image: https://useinsider.com/wwdc-2020-ios-14-idfa-update-and-impact-on-mobile-marketing/

TAPTAP

III. Consent Framework

TAPTAP is a global company headquartered in Spain, a member of the European Union. We comply with GDPR, but also appropriate principles of GDPR to company operations around the world. The two most common instances for processing data under GDPR (as a framework for interpreting GDPR) are Legitimate Interest and Unambiguous Consent.

LEGITIMATE INTEREST

You have a legitimate interest to process someone's personal data. This is the most flexible lawful basis, though the "fundamental rights and freedoms of the data subject always override your interests, especially if it's a child's data."[3]

UNAMBIGUOUS CONSENT

You have received explicit consent from the end user (or Data Subject) to collect and/or use their data. This is one of the strictest lawful basis.

TAPTAP strives for unambiguous consent wherever possible and is constantly evolving our policies and technology to reflect the highest standards of data protection.

WHAT DOES THIS MEAN FOR US?

For all advertising initiatives and academic studies, TAPTAP processes and applies only the data that is necessary for the activation, and nothing more. In other words, there are different levels of data precision available, especially for location data, and TAPTAP adjusts the specificity of the data according to the activation requirements. For example, if pinpoint location data is not needed, it will not be used or if we can use data at an aggregate level, we will.

All sources, composition and storage of the data in the platform is clearly outlined, and we work with data providers who have the same standards for their handling of data as well as their own consent mechanisms. We ask that all partners sign a Data Processing Agreement to supplement their own practices as an extra precaution. Finally, all data in our systems is hashed for privacy, and TAPTAP is a member of the IAB Transparency and Consent Framework 2.0, an industry GDPR consent solution. If the identifier does not meet the TCF standards, it is rejected and not used.

WHY?

Not only do we respect the right to privacy and transparency, but we also believe that the highest standards with regard to consent lead to better business for us and our stakeholders in many ways.

1. The User Perspective & Data Quality

2. The Brand Perspective

3. https://gdpr.eu/gdpr-consent-requirements/

1. The user perspective and data quality

A survey conducted by the Internet Innovation Alliance shows that 76% of internet users are concerned about how technology and social media companies are using their online data and location information for commercial purposes.[4] Further, a study conducted in select countries around the world, including but not limited to, China, Mexico, Spain, the UK, Germany & the US, found that at least 70% of respondents in all countries would cease to do business with a company that used their data irresponsibly.[5]

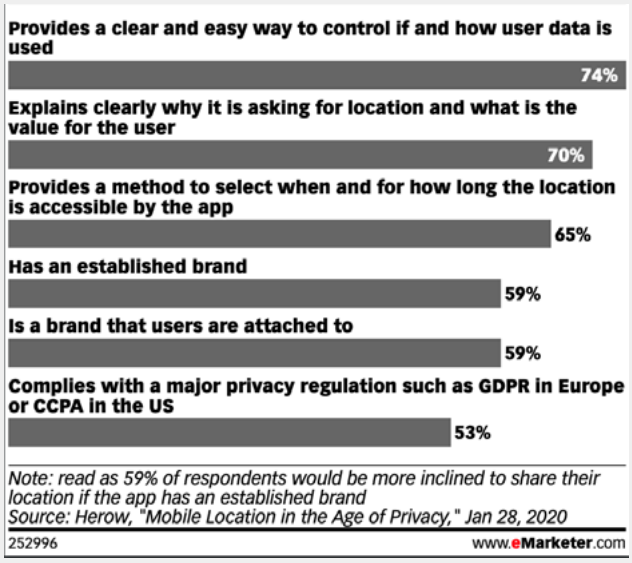
These and more statistics **can and do mean that quality data is intrinsically linked to consensual data** —safely stored and implicated— for several reasons.

First, consensual data is much more likely to be accurate. The identifiers that properly track devices or behavior require user permissions and the data generated is regulated; therefore, the only way to access this data and apply it to solutions is through a consent framework.

The data available without permissions or regulations is not typically as accurate or useful on its own. The increase in permissions also corresponds with a decrease in supply. In the past, opt out was more common than opt in but now the reverse is true, and several studies show that users are more likely to share their data when they have more information:

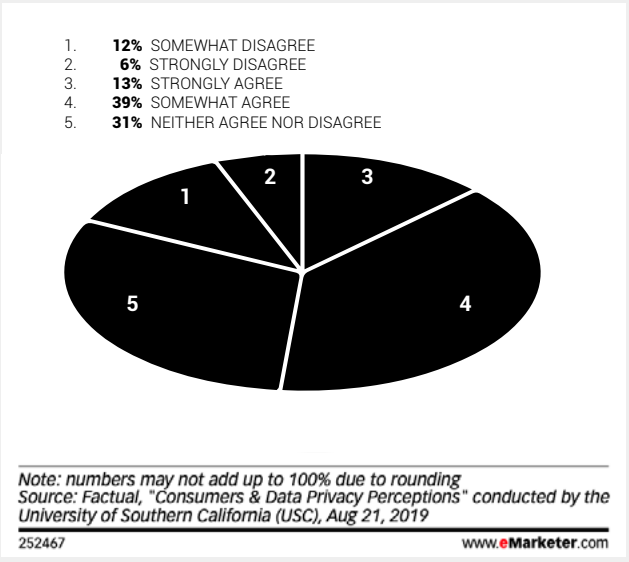
App Attributes that Make US Adults More Inclined to Share Location Data

%of respondents | November 2019



Are Use Smartphone Users Willing to Share Personal Data with Companies if the Benefits of Doing So Are Made Clear?

%of respondents | April 2019



Additionally, because many markets now have data privacy laws, a company and data processor that wants to operate on a global scale must be compliant with these regulations, even if some areas are not as regulated as others. Finally, more accurate data equates first and foremost to a better user experience, but also to more comprehensive measurement and attribution so that brands can understand what is actually driving adoption and publishers can improve their platforms.

4. https://internetinnovation.org/
5. eMarketer | Digital Marketing In Today's Privacy-conscious World

2. Brand Experience

Even if advertisers and brands are not data processors and therefore not held to the same regulations found in the various data protection laws, their consumers and stakeholders still hold them accountable to privacy rights, and they want to advertise with platforms that do not represent a risk to their doing so.

Brands are often willing to pay extra for quality data with consent files.[6]

We believe therefore that, for the good of the consumer and for the company and our stakeholders, unambiguous consent should always be prioritized.

6. eMarketer | Location Intelligence 2020

IV. Targeting With Consent

Though we may be approaching an advertising ecosystem with fewer and less specific identifiers, they are not gone just yet, and can be extremely valuable when used responsibly, with consent and in conjunction with synergistic technologies and systems.

The foundational products that make up the Sonata Platform, the proprietary platform designed by TAPTAP, are built to use data to its fullest potential for the planning & profiling, activation and measurement of an advertising or marketing initiative, for which location data is an anchor.

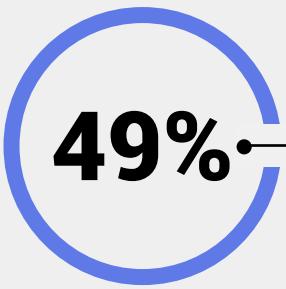
So, how do we do it? —

1. Sonata ID

As we know, there are many participants in the ad ecosystem with their own data systems and identifiers, which can lead to large quantities of data that are "fragmented and incompatible."[7]

To associate this fragmented data to the same user is a challenge, but is necessary for targeting, activation and measurement that depends on 1 to 1 targeting. A 2017 LiveRamp found that 49% of US based marketers say that bringing all data together for analysis is their number one challenge of people-based measurement.

The Sonata ID is the persistent identifier in the Sonata Platform. The technology behind this ID-based "container" brings together device and advertising IDs, cookies, and data from third party providers (usually through an SDK) to the same identifier, which is not linked to the actual identity of the user. It gives us more visibility of the consumer journey from targeting, to activation to measurement, through a process of ID matching as well as the ability to confirm if a particular ID has been exposed to campaign ads before a particular action, which could be online or offline (store proximity or traffic). The Sonata ID draws from primarily mobile data sets, which usually provide a much richer profile of the user[8], and allows advertisers to build audiences based on multiple dimensions which bridge the gap between online and offline, including a digital and device profile, intent signals and historical or real-time location, all of which can be applied to a powerful omnichannel advertising activation.



of US based marketers says that bringing all data together for analysis is their number one challenge of people-based measurement[9]

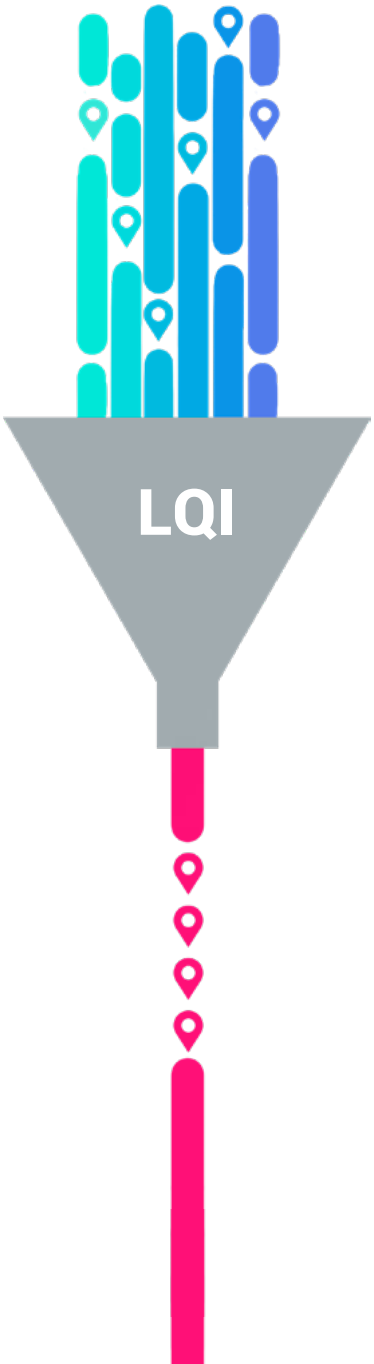
7. eMarketer | Mobile Measurement And Targeting: Eight Challenges Advertisers Face
8. eMarketer | Mobile Measurement And Targeting: Eight Challenges Advertisers Face
9. LiveRamp | The State of People-based Measurement

- OPEN ECOSYSTEM AND HIGHLY COMPATIBLE
- COLLECT FIRST AND THIRD PARTY DATA
- ELIMINATES DATA DROP OFF
- SAFEGUARD DATA TO MEET SAFETY STANDARDS

2. Sonata DMP

The Sonata ID is housed in the proprietary DMP of the platform. Creating a proprietary DMP allows us to safeguard both first party data and any data received from third parties in ways that meet data storage safety standards and laws. It also eliminates any intermediaries (and resulting data drop off) required for activation, since it is directly linked to our DSP. Any campaign events resulting from an impression served through the DSP are stored as first party data in the DMP which allows us to understand the context in which users are most likely to engage with a campaign. Having a DMP as part of the platform (and an ID-based identifier) also lets us sync our data with CRM or other custom data and other DMPs.

3. Location Quality Index



Quality location data comes from several sources, many of which are tied to identifiers that require consent - device and advertising IDs either directly or through SDKs. Other sources of location data include bid stream (from ad exchanges), WIFI, IP addresses and telecom providers.

Independent of the drop in location data supply due to consent, we know that much of location data is inaccurate, and the supply drop makes scaling difficult; therefore, companies with tools that can verify and make use of several sources of data, have a significant advantage both for real time targeting (or geo targeting/geo fencing) and building user profiles based on historical and accurate location data.

The Sonata Location Quality Index does just that by aggregating and cross referencing these multiple sources of location data and uses applied artificial intelligence to score each signal according to its accuracy, discarding erroneous or fraudulent data.

This helps us not only verify data for accuracy, but also make use of several sources that may not be reliable on their own. "For most companies, the scale of first-party data won't be enough."[10]

These technologies work in tandem to create an effective and positive user experience driven by consensual data that is only as specific as needed to be effective.

10. eMarketer | Location Intelligence 2020

V. User-oriented targeting, not 1:1

When we see the capabilities of ID or cookie based targeting, it begs the question about what vendors and advertisers will do once this technology is severely limited or eventually not available at all. We have several theories about what may replace IDs that include practices like fingerprinting, publisher deal IDs or the SKAdNetwork. The challenge for these methods will be more data fragmentation, GDPR compliance and industry cooperation, among others, so while they may be in our future, we think that a solution to successful advertising in a post-ID world lies in contextual targeting - but contextual targeting unlike we have seen before - the key to which is location.

Traditionally, contextual targeting simply means targeting a user based on the context, not the user himself. If we reach a user on a website or app with recipes, we assume they are interested in cooking. That said, this assumption leaves out many other possible variables or conclusions. Targeting via an ID, as mentioned, means that we can collect information and build a complete profile that includes not only contextual information but demographics, store visits, other interests and intent signals. We can measure the exposure a particular ID has had to our campaign, and tie this exposure to a successful outcome, which could be a digital or physical action. We can also profile these successful users and find more like them and even apply our predictive algorithms to offer products and services that may be of use for the end-user.

“Preparing for the eventual reality of fewer identifiers —for a time when 1:1 targeting is not scalable, not available or simply not preferable— is well underway through our product and technology development.”

Location Intelligence for new targeting possibilities

With the right ecosystem, technology and setup, we can retain many of these abilities in a way that protects individual privacy and does not rely on unique cookies or IDs. We may lose specifics about the particular individual or ID, but we retain a highly user oriented approach.

TAPTAP has developed a technology that lets us accomplish this user oriented advertising. It is a tool that aggregates several layers of data, via their location element, over a map for a geospatial analysis.

Sonata Location Intelligence Layers of Data

ONLINE & OFFLINE DATA

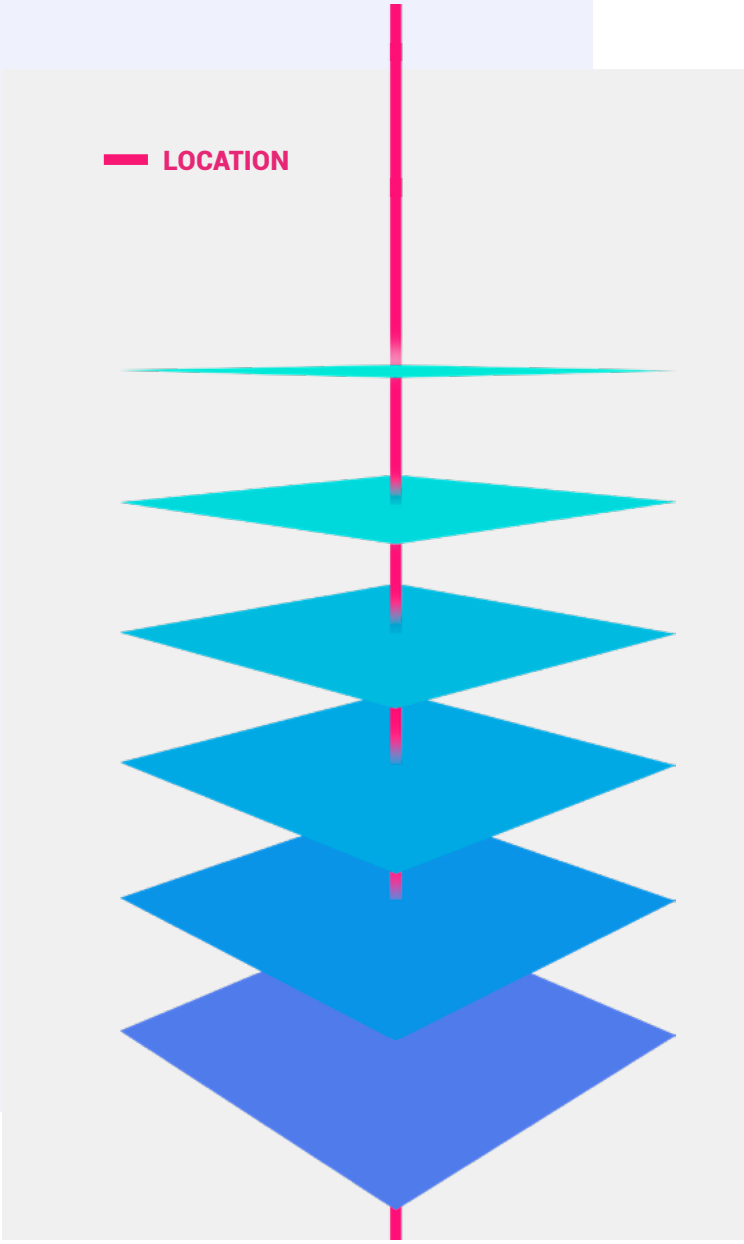
Online data is data generated and collected digitally like site and app category consumptions while offline data is the opposite like census data.

STATIC & DINAMIC DATA

Dynamic data is data that continually changes in nature like mobility whereas static data does not frequently change. An example of static data would be points of interests.

ADVERTISING & NON ADVERTISING DATA

Advertising data is related to a campaign like formats with top engagement in a particular area. Non Advertising data is noteworthy because media activations usually only generate campaign related data which is a more narrow perspective.



Location Intelligence for new targeting possibilities

More data means more possibilities

—

We link not only items typically associated with location advertising like points of interest mapping or out of home placements, but also other data like digital events, census information and proximity measures, the collective geospatial analysis of which gives us an extremely thorough picture.

Even without an ID, we are still able to gather device locations, so mobility continues to play a key role in the analysis. We can normalize these offline points and digital data - some of which is user generated (meaning it depends on the behavior of the user) and some of which is entirely independent (like density of schools in a given area) through a statistical index to make them actionable.

Aggregated data layers

—

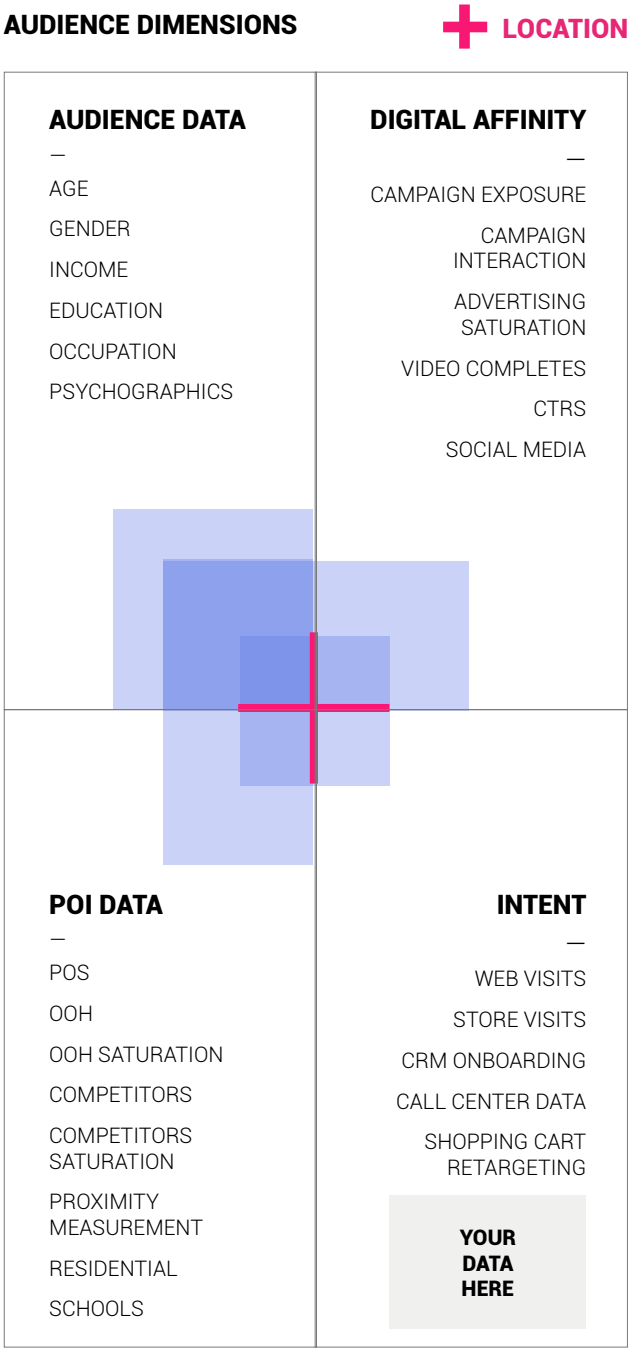
We can then use these various layers to analyze the area and create maps of audiences based on customizable variables like in the image to the right. This not only introduces new audience and geographic variables but also enables more versatility than traditional 1:1 targeting as users can adjust the amount and type of data needed for each strategy.

Audience affinity maps instead of cookies

—

To put together these mappings, we still leverage existing data sources like bid streams or SDKs, which give us plenty of specific information, like the type of app used, formats, time stamps, and locations that comprise the data inputs.

Therefore, if we target a geo instead of an ID or a cookie, we can, with high accuracy, reach the right users even if we do not reach them on a 1:1 scale. Based on these mappings, we can implement capabilities typically only possible with IDs like sequential targeting or dynamic creative synching, especially in connection with OOH exposure.



VI. Conclusion

As levels of specificity fade, it is crucial to build ecosystems that open brands up to new kinds of advanced targeting and optimization. By making so many variables newly visible, we can see much more of what actually affects a campaign like proximity to a school by bike versus by car, omnichannel ad saturation in a given area or content consumption, to name a few. We can not only create a highly customizable audience using an array of new inputs to locate our target, but can also count on recommendations like which format would work best for this particular audience segmentation based on its saturation and levels of engagement in a particular geo. These new techniques are made possible through the universal connector of location, our ability to verify its accuracy through Sonata LQI and aggregate data through the Sonata ecosystem. We can make decisions and optimizations in real time with technology that uses machine learning and artificial intelligence.

In close, while the various identifiers still exist in the digital ecosystem, we will continue to use them to enrich our Sonata ID to reach more of the right users in a safe way, but the new techniques we can achieve with technology offer different possibilities that even many ID-based solutions cannot.

Sources

- eMarketer, Digital Marketing In Today's Privacy-conscious World
- European Commission, Communication From The Commission To The European Parliament And The Council
- https://useinsider.com/wwdc-2020-ios-14-idfa-update-and-impact-on-mobile-marketing/
- https://gdpr.eu/gdpr-consent-requirements/
- https://internetinnovation.org/
- eMarketer, Location Intelligence 2020
- eMarketer, Mobile Measurement And Targeting: Eight Challenges Advertisers Face
- LiveRamp, The State of People-based Measurement
- eMarketer, Consumer Attitudes On Marketing 2019
- eMarketer, Mobile Year In Review: The Launch Of 5g Is The Biggest Story In A Busy Year For Mobile
- eMarketer, App Attributes That Encourage Location Sharing Usa Chart 2019.Pdf
- https://www.theverge.com/2020/1/14/21064698/google-third-party-cookies-chrome-two-years-privacy-safari-firefox
- https://adage.com/article/digital/behind-googles-decision-remove-third-party-cookies-chrome/2227126
- https://www.forbes.com/sites/johnkoetsier/2020/06/24/apple-just-made-idfa-opt-in-sending-an-80-billion-industry-into-upheaval/
- https://mobiledevmemo.com/mobile-advertising-without-the-idfa-a-comprehensive-overview/
- https://www.singular.net/blog/mobile-marketing-measurement-privacy-idfa/
- https://aithority.com/guest-authors/death-of-the-cookie-future-of-online-marketing/
- https://docs.adobe.com/content/help/en/target/using/implement-target/before-implement/privacy/apple-itp-2x.html
- https://www.blog.google/products/chrome/building-a-more-private-web/
- https://web.dev/digging-into-the-privacy-sandbox/
- https://digiday.com/marketing/wtf-googles-privacy-sandbox/
- https://www.legislation.gov.uk/uksi/2019/419/contents/made
- https://www.cookiebot.com/en/uk-gdpr/
- https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf
- https://ico.org.uk/about-the-ico/who-we-are/


TAPTAP