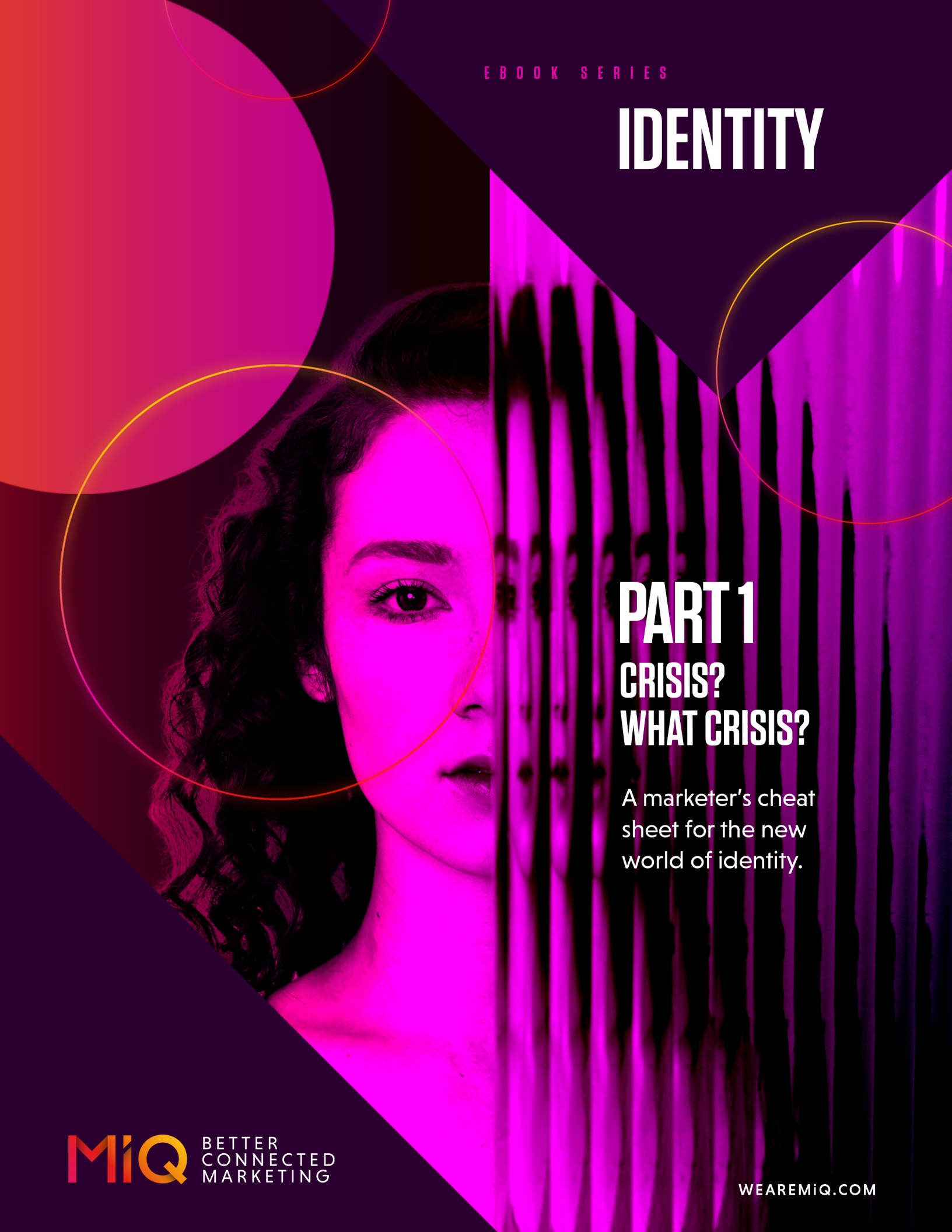
EBOOK SERIES

IDENTITY



PART 1

CRISIS? WHAT CRISIS?

A marketer's cheat sheet for the new world of identity.

MiQ BETTER CONNECTED MARKETING

WEAREMiQ.COM

KEY TAKEAWAYS:

In this short ebook you'll find out:

- What's changing in the world of identity and why it matters to marketers
- Why there's no single silver bullet solution for a world beyond personal identifiers
- What the different options are for identity in the future - and how you can make them work together
- A cheat-sheet for all the terms you need to know to navigate the world of identity

INTRODUCTION

We're currently in the midst of the biggest shift in the way digital advertising works since its inception. And that's all because of what's changing in the world of identity.

Identity is at the core of digital marketing. It's the USP of programmatic. It's what makes it all possible. As advertisers, we didn't used to know anything about the people who saw our ads on billboards, on the sides of buses, in the pages of newspapers. But, now that everyone and everything is online, we do.

Identity is the whole shebang.

But identity is changing. High profile, negative stories about consumer data - from major data breaches through to the Facebook/Cambridge Analytica scandal - mean that people are, understandably, more concerned about the security and use of their personal data than ever. And so, the biggest tech companies and government regulators have responded, making changes and bringing in new rules that mean the way we understand consumer behavior and use that understanding to increase the effectiveness of online advertising is going to be very different from how it has been up to now.

And that's what this ebook series is all about.

We know that keeping track of all the changes, the innovations, and the new solutions isn't easy. And working out exactly what's right for your brand or agency is tougher still. That's why, across the series, we're looking at what the new identity landscape means for marketers who still want to get all the good things that online targeting and measurement can deliver for their ad campaigns, as well as giving practical advice as to what you need to do to start making changes now and what you need to be aware of to be ready for what's coming next.

In this first book, we'll start off by giving an overview of how we got here, what the landscape looks like now, and give you a framework for thinking about what identity will mean in the future.

Let's get into it.

THE IDENTITY CHEAT SHEET

Before we get started, here's a glossary of all the terms you need to know to navigate the future of identity, all in one handy place...

Accessibility - The measure of how easy or difficult it is to collect different types of data. Generally, the more consent someone has to give for data to be collected, the less accessible it is.

Anonymity - The measure of how possible it is to identify an individual consumer based on the data collected from them.

Anonymous data - Data that's based on contextual data, such as website type or geolocation data, rather than the identity, device or behavior of an individual. Also, includes data that's been 'de-identified', such as permanently hashed email addresses.

Authenticated data - Data that's obtained by someone logging in to a site or platform, usually based on long-lasting identifiers like email addresses and phone numbers.

Clean room - A secure location for connecting, cross-referencing, and analyzing first-party data with data owned by walled gardens, publishers or even other brands.

Closed web - A term used to describe the walled garden environments that tech giants like Amazon or Facebook use to monetize their owned and operated data and inventory.

Cookies - Little bits of data stored in your browser that allow consumers to be tracked around the web - to remember where they've been and what they've looked at. Soon to be a thing of the past.

Data aggregation - The process of combining data from multiple individuals and analyzing it as a whole, rather than basing insights on personal details.

Data bunker - A secure location for two or more brands to combine their first-party data to find insights for mutual benefit.

Device graphs - A map that links together all the devices used by an individual, such as their computer at work, laptop at home, tablet and smartphone.

Edge computing - This means that any processing and data analysis of a consumer's online behavior (for advertising use) takes place on their device itself, so none of their personal information is passed on to third parties.

First-party data - The data that a brand owns about its customers or people who are interested in its goods and services. The most valuable commodity a marketer owns.

Geo-location data - A form of anonymous data usually based on using zip or postal codes, and things like census data.

Identity - The overarching term for the technologies and techniques advertisers use to differentiate between people on the internet so they can understand and target them more effectively.

Identity spine - A method for stitching together identity profiles from recognized data which can then be matched up with authenticated data to discover better insights.

ID resolution - Technology that can gather and 'match' multiple IDs - both online and offline - to create a single view of individual consumers, so advertisers can replicate the effect of cookies. See also authenticated data.

Open web - The areas of the internet that aren't controlled by gatekeepers like walled gardens. In advertising terms, the space where all publishers are able to monetize their inventory and data by selling it to advertisers.

Personal data - Anything that can be used to identify a specific individual. Obvious examples include email addresses and phone numbers, but things like cookie IDs, and device IDs are also included as personal data by eg GPDR.

Recognized identity - Pseudonymous identifiers that let advertisers identify someone but are not explicitly provided or declared by that person, such as cookies and device IDs. Rapidly becoming less used.

Shared ID solutions - Technology that allows vendors across the ad tech industry to access and use the same identifier for a consumer. See also authenticated data.

Third-party data - Data that brands can buy from sources that aren't the original collectors of that data to supplement their first-party data and find deeper insights.

Value exchange - The basis of the ad-funded internet. People get (most) web content for free; in exchange, brands get to advertise to them.

Walled garden - A tech giant with a massive audience that brands can only access by spending directly with that company or its platform. Examples include Facebook, Amazon, Twitter, and Google.

01

THE IDENTITY CRISIS - HOW DID WE GET HERE?

The age of the cookie

The 'value exchange' principle is one of the longest standing features of the internet.

As consumers, we get access to the vast majority of content on the internet for free. And, in exchange, we let the people who own the websites we visit make money by showing us adverts.

Since the dawn of digital, the way advertisers have made sure they're showing their adverts to the right people is through cookies.

Cookies are basically small text files stored on your web browser with a little bit of data in them. They were invented to solve the problem of remembering useful information when a person surfs the web – anything from remembering your login details to knowing your favorite pages.

And, because cookies know where you've been online, what you've looked at and what you've done, they've traditionally been instrumental for digital advertisers looking to target consumers and measure the success of their ads on desktop and mobile.

To give a really simple example, if you've visited a load of shoe retailer websites, the cookies will store that information, and a shoe brand can read that data and surmise you're a good person to show their shoe adverts to. Cookies also know what online adverts have been shown to you, so the shoe brand can see if showing you their ad led to a purchase.

The death of the cookie

Over the last few years, there have been growing concerns about internet companies exploiting individuals' data through the use of third party cookies - meaning cookies that are placed on your browser and used by companies beyond those that own the actual websites you visit.

The idea of a company you've never heard of using data about your internet browsing behavior, to most people, feels pretty invasive. And internet browsers have responded. In 2017, Firefox and Safari began to block the use of third-party cookies on their browsers. And, while they are currently still allowed on Google Chrome, the browser that takes the biggest share of web-surfing, it's been announced they will be blocking third party cookies imminently.

From that point, third-party cookies will be essentially defunct.

Other types of identifiers are being restricted too. When Apple released iOS 14 in 2020, they also presented plans to make the IDFA (ID for Advertisers) explicitly opt-in for each app installed, meaning mobile measurement companies wouldn't just get automatic data on someone's behavior.

And all of this comes at a time when broader concerns about consumer privacy and stricter regulations are on the rise. Whether it's GDPR in Europe, PIPEDA in Canada, or state-level initiatives like CCPA in the US, the direction of travel is clear. To eliminate the worst practices of the ad tech ecosystem - from mishandling data, to unscrupulous selling of data, to just being downright creepy - advertisers are going to have to adapt to a world where the use of personal data for targeting and measurement is not possible without explicit consent.

It's a really big deal. A major change. But it's also a really good thing - for consumers, advertisers and agencies. It's a chance to put an end to the lazy, murky practices that cookies have sometimes encouraged, and a chance for the whole industry to re-think the value exchange with consumers, focus on quality media and quality data, and start the process of rebuilding trust.

So, the next question is, how?

02

OVER WALLS AND INTO BUNKERS

The first thing to say - loud and clear - is that the end of third-party cookies and other personal identifiers doesn't mean the end of targeting and measurement in online advertising.

But it does mean the ad tech landscape is going to be a bit more fractured and difficult to navigate, because cookies will not be replaced with one single catch-all identifier that everyone can use. And that means advertisers are going to have to be smart, experimenting with new tools, technologies and techniques, to get the high-performing campaigns they're after.

The walls get higher

For several years now, the online ad ecosystem has been divided between the walled gardens and the open web.

Walled gardens (the likes of Facebook, Google, Amazon, Twitter etc) have masses of data on their own consumers, and they allow brands to use that data to advertise to those consumers. They're called walled gardens because all the data stays within their owned and operated system, and advertisers can only buy ad space through the company or via its tech platforms.

Everything else is on the open web, where consumer data and ad inventory can be accessed by all the various businesses that make up the ad tech lumascape. The open web has, by necessity, been where most programmatic experimentation has taken place, driving innovations like DCO (dynamic creative optimization) and custom bidding models, as well as expanding the size of the addressable universe to include new channels like digital-out-of-home (DOOH), audio and connected TV.

The open web is also where non-tech-giant publishers get the most control and flexibility when it comes to understanding the audiences that consume their content and maximizing revenue.

The crucial difference between the two is that the open web has, traditionally, relied on third-party cookies, whereas walled garden consumer data is 'opted-in': consumers log-in voluntarily and are identified by an email address or other persistent ID.

All of which means that, in a world without cookies, the future of identity will inevitably involve more walled gardens - with higher walls.

The walled gardens currently get about 60% of all ad spend - and that number is only going to rise due to two factors. First, the existing tech giants will benefit from being non-cookie-based by design, with brands moving spend to areas where the identity changes aren't an issue.

Second, and more importantly, what was previously the open web will start looking a lot more like walled gardens. New solutions are emerging (see below) that will offer advertisers secure access to consumer data across a whole load of sites using a shared ID.

Essentially, these shared ID companies put a bubble around a big area of the open web and make tracking and targeting possible within that bubble, while also protecting and anonymizing the data of individual consumers.

It's an ideal solution in terms of mimicking the functionality of third-party cookies, while also addressing privacy concerns. But for advertisers, navigating between these bubbles will be tricky as you don't want to waste budget targeting the same people but just in different places. And publishers too will have to make decisions about the data they ask for in exchange for access to content, whether that's a login, a paywall, a freewall and so on.

02

First-party rules

The other side of third-party cookies drifting off into the sunset is the increasing importance placed on brands' own first-party data.

In fact, the biggest thing that brands need to be doing right now to prepare for the future of identity is getting their first-party data in great condition - and making sure they have everything in place to make sure it stays that way.

Not only is good first-party data still the basis for all high-performing digital campaigns, it's also the way to take advantage of new identity solutions like clean rooms.

Clean rooms are a way to get deeper insights from your first-party data by connecting it with data from another source in a super-secure platform so you can analyze it and discover insights without any personal data leaving the safety of the closed system. There are a number of ways advertisers can use clean rooms.

1

With walled gardens

This is where you connect your data with data held by a walled garden (eg Amazon) to do things like better understand campaigns within that platform and discover audience insights.

2

With publishers

You can connect your first-party data with audience data from publishers to cross-reference your audience with the consumers actually visiting that publisher's site.

3

With other brands

This is perhaps the most innovative use of clean rooms, where they allow for one brand to connect their first-party data with the data of another brand (ie second-party data). This provides an opportunity for companies in adjacent spaces (think, airlines and car hire brands, or restaurants and food-delivery apps) to safely pool their data to discover mutually beneficial insights.

4

With third-party data providers

Enhancing first-party data with external data sets is nothing new. But using clean rooms for this connection provides an extra layer of privacy, both for your own first-party and for the data held by third-parties.

To put it simply, the end of personal identifiers isn't going to limit advertisers. Rather, it presents them with an abundance of new options: of different types of data, of different solutions, of different partners, of different ways of working. The crucial part for advertisers is knowing what options are out there, who does what, and how it can all work together to get the results they're looking for.

Which leads us neatly to...

03

THE NEW IDENTITY FRAMEWORK

The IAB has outlined a framework of the available methods for identifying online audiences, each with their own benefits and drawbacks due to differing levels of accessibility (how easy it is to obtain) and anonymity (how much they rely on personal identifiers).

Within each area, there are different potential partners with different solutions. And, again, it's important to restate: it's not a question of choosing one of these areas for your identity needs. The challenge for advertisers is finding the right mix between them.

Let's go through them one by one.

03

Recognized identity data

What is it?

Recognized identity is the most old-school identity data. It's been the basis for most digital marketing over the last twenty-something years and includes things like cookies and device IDs that allow us to literally 'recognize' a consumer without their explicit permission. With recognized identity solutions, brands, agencies and third-party partners have been able to identify, segment, target and measure digital consumers based on their browsing behavior.

Good points?

Traditionally, this has been the go-to option for advertisers because it's the easiest data to get hold of. And, because cookies aren't being removed from Chrome until 2022, there's still a window for brands to use these tried-and-tested methods that tap into recognized identity, while figuring out what combination of the others work best for them.

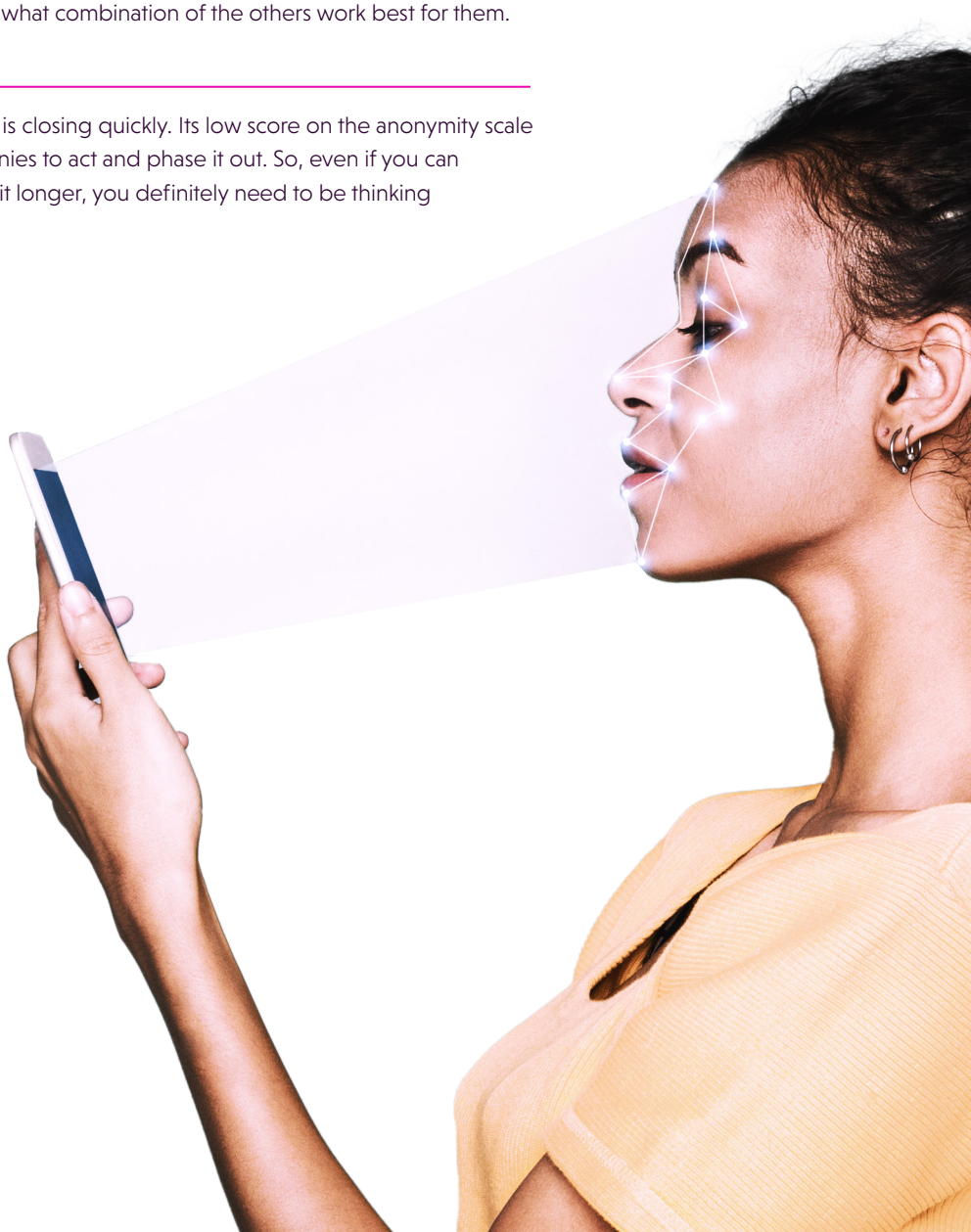
Bad points?

The window for using recognized identity data is closing quickly. Its low score on the anonymity scale is what's caused governments and tech companies to act and phase it out. So, even if you can get away with using recognized identity for a bit longer, you definitely need to be thinking outside this area now.

Potential partners?

Because recognized identity has been at the core of pretty much everything in ad tech, you'd be hard-pressed to find a partner who doesn't have solutions for using it. So, what you need to look for is a partner with a focus on what comes next.

A really good starting point is to ask if your partner has a strong strategy for building device graphs or identity spines. Both are methods for building identity profiles from recognized data which can then be matched up with authenticated identity data (see below) to give you a headstart when cookies are finally gone.



03

Authenticated identity data

What is it?

Authenticated identity is when a consumer has logged into a website or platform, explicitly verifying their identity (usually via an email address) and providing their consent so advertisers can build a profile of their actions within that ecosystem.

Good points?

Authenticated identity data is generally very high quality. It's collected when websites and publishers become small walled gardens, processing and using a person's data based on direct consent or, depending on local privacy regulations, providing clear methods to opt-out of data collection or personalized advertising.

And, within that mini-walled garden, it's powerful stuff. The identifiers are long-term (based on things like mobile numbers or email addresses) which makes it easier to match up to other datasets (like a device graph, from above) to work out what a consumer is interested in beyond that one website they're on.

Bad points?

Unsurprisingly, authenticated data is among the hardest to come by. On the open web, people aren't used to logging in to websites to access content or save items. So, if publishers and website owners want to generate authenticated data, they have to educate consumers and show them tangible benefits as to why they should. That may be easier for major news outlets with access to masses of premium content or ecommerce sites that have the ability to make generous offers in return for data, than for smaller retailers, niche blogs or regional news channels. And, even for the larger sites, there's still likely to be a scale challenge compared to the accessibility of recognized data.

Another thing to consider with authenticated IDs is measurement and data refresh. The long-term stickability of the identifiers mean you run the risk of wasting budget by advertising to people who've already taken an action - a person who looks at a lawnmower online and then buys one in store, will not want to be hounded with lawnmower ads for the next year.

Potential partners?

You need to be aware of two main innovations in this space.

The first is shared ID initiatives. This is technology that allows for sharing the same ID across a group of websites. So, if a consumer logs into one website, that can be matched up with other logins from other opted-in websites. By doing so, a consumer can then be tracked across all of the websites within that ecosystem. The Trade Desk is leading the way in this space with their Unified ID 2.0 initiative, which is set to be picked up and scaled by Prebid, the leading open source bidding solution worldwide.

The second initiative focuses on something called 'identity resolution'. Instead of sharing identity data between partners, these ID resolution companies are working on solutions to gather and 'match' multiple IDs together. The frontrunner in this space is LiveRamp's IDL (IdentityLink), but others include Zeotap and Liveintent.

Authenticated data solutions are still evolving. The business who emerge as winners in both shared ID and ID resolution spaces will be whoever gets the partnerships to create the necessary scale, whoever builds the best methods for reducing data latency and erosion, and, of course, who can demonstrate they are protecting consumer privacy most effectively.

03

Aggregated identity data

What is it?

Aggregated identity is the newest identity kid on the block. The idea is that, rather than look at an individual's data, you gather a whole load of consumer data all together into what's commonly called a cohort. Advertisers can then analyze the grouped data and find insights based on trends, without ever exposing data about individuals or their devices to third parties.

Good points?

Aggregated data is a truly privacy-first identity solution. It protects individual consumer data by design, while still providing advertisers plenty of scope for finding insights about addressable audiences. Clean rooms and data bunkers (see above) are both methods for connecting and analyzing data within a privacy-first environment. On the open web, the use of new technologies like 'edge-computing' and 'federated learning' is being explored to group individuals into 'cohorts' for advertising purposes. In this case, individuals are placed into different interest groups based on their behavior, and that interest group information is then stored on their browser or device (literally 'on the edge'). Advertisers can use these interest-based groups for segmentation, targeting and measurement, but they never get access to the individual's data itself.

Bad points?

While aggregated data might sound like the dream solution, many aggregated methods are still in the very early stages of testing, so developers and analysts are having to learn the ropes and test the success of different ways of doing it. As yet, we don't really know what the best practices are for using aggregated identity data, what good looks like, or how it can best be used alongside other forms of identity data.

Potential partners?

In terms of clean rooms, it's the tech giants Google and Amazon that are leading the way, though Unilever are also developing a clean room that, theoretically at least, would let you see if you're duplicating reach across Google, Facebook and Twitter. Edge computing and federated learning are where the most nascent aggregated solutions are. Many of the methods proposed in the Google Chrome privacy sandbox use some version of edge computing or federated learning as their basis, such as FLoC and Turtledove. But there are also independent partners innovating in this space such as our partner Airgrid, and Permutive.

The telcos are also big movers and shakers in this space. By providing anonymous mobile data connected to their CRM, they can provide a really robust but privacy-compliant dataset for advertisers to use. Skyrise Intelligence and Environics Analytics are good examples of companies using aggregated mobile data to help advertisers do cool new things.

CLIENT STORIES

Aggregation in practice

To see how a brand can use aggregated mobile data in a real world campaign, check out this case study on how MiQ worked with Skyrise Intelligence in the UK to drive awareness for Subway.

FIND OUT MORE

03

Anonymous identity data

What is it?

As the name suggests, this is the most privacy-conscious of the four methods because a person's identity is never gathered in any form. Instead, contextual data points are collected about the context in which a consumer is browsing. This can be either online data (the kind of websites they visit) or geo-contextual data based on things like zip or postal codes and census data, rather than the identity or behavior of a specific individual or device. For those publishers who either can't or don't want to get their site visitors to authenticate, the majority of their traffic will now be anonymous.

Good points?

As you'd expect, anonymous data is completely privacy compliant, because it isn't based on individual consumer data. This makes it very attractive for brands who have a low risk threshold when it comes to potentially misusing data.

But it can also be extremely powerful, especially for 'moments' marketing, when you want to shift your messaging or increase or lower your spend based on, for instance, what the weather is doing, what the stock markets are doing, or to latch on to big sporting moments.

And, unlike the newer identity areas mentioned above, it's been around for a while. Contextual targeting has existed for as long as cookies so, as an industry, we're not starting from scratch with the best way to use it.

Bad points?

Traditionally, anonymous and contextual targeting has (perhaps unfairly) been seen as the less intelligent younger sibling of recognized identity. And, certainly, using contextual data means casting a wider net than the hyper-targeting that was promised (if not always possible) by using personal identifiers. You can't target individuals, and so have to expand your thinking to things like certain domains or postcodes.

Potential partners?

The biggest name in online anonymous intelligence right now is Oracle, who bought Grapeshot to strengthen their capacity in that area. There are also some smaller contenders in the space like Illuma, Silverbullet and GumGum. In assessing who emerges as a winner in this space, the most important factor will be how granular you're able to get with the data gathered about a page, and how easy it is to analyze that data and connect it to the rest of your programmatic strategy.

When it comes to geo-contextual data, the big movers and shakers are the telco companies. By providing anonymous mobile data connected to their CRM, they can provide a really robust but privacy-compliant dataset for advertisers to use. Skyrise Intelligence and Environics Analytics are two companies doing impressive work in this space.

04

THE SOLUTION WILL NOT BE SINGULAR

If you were hoping this ebook would end with a clear and unequivocal conclusion about where the world of identity is heading, well... we're sorry to disappoint.

As an industry, we're still very much in the midst of changing from the old system to the new one, with no clear vision of what that new system will be. And, in truth, it was never going to be just one thing to 'replace' cookies.

For advertisers, the next few years are going to be a critical period of testing and learning about the efficacy of different ways of identifying consumers for targeting, working with different partners, and connecting them all together to drive better results.

If that sounds like a daunting task, well, we'd be more than happy to help. But the most important thing is to reiterate what we said at the beginning. All of these changes are a good thing. The end of personal identifiers is a huge opportunity for us all to rebuild trust in our industry, both with consumers and among ourselves.

What replaces cookies won't be a singular, monolithic solution. But the ability to drive new value for marketers by connecting these new technologies and systems available is a hugely exciting challenge.

GET IN TOUCH

MORE FROM OUR CONTENT

THE FUTURE, FASTER PODCAST

The future is coming faster than ever...

Thanks so much for making it to the end of the ebook. Who says long-form content is dead...?

If you enjoyed reading this, maybe you'd like to check out the Future, Faster podcast, a laid back look that the trends, topics and technologies shaping the future of advertising, with some of the smartest minds in our industry.

LISTEN NOW

MiQ BETTER CONNECTED MARKETING