Gaining Control Of Your Customer Dialogue -

A STEP-BY-STEP GUIDE TO IN-HOUSING YOUR ID GRAPH

adstra

the new **ideal** in data

As the world around us begins to find its footing amid the ongoing pandemic, we're seeing a new level of confidence ramping marketing spend. Supply chain disruption and shifts in consumer behaviors driven by the pandemic have led to new levels of product sampling and changes in purchase processes. Mass adoption of new media channels born from our forced isolation combined with increased use of legacy media channels such as linear TV and Direct Mail and proliferation of devices to engage these channels has further expanded the choices an advertiser has to reach their target audience.

Marketers are faced with the fragmentation of consumers' attention across multiple media channels. No single media has the scale of engagement to make many traditional marketing approaches work on their own. On top of this, consumer privacy concerns are driving a new wave of regulation that seeks to govern every interaction with a brand. The walled gardens certainly offer some of the best opportunities to engage customers within their constraints, however, the garden's terms often eliminate much of a brand's ability to effectively manage the communication journey.

As a result, marketers are realizing their need to improve the level of control in recognizing their customers and the data signals they can use to determine the ideal level of messaging with their customers. This whitepaper explores the ways brands are managing the flow of customer identity and data going forward and provides a roadmap to one of the primary answers many brands are considering: in-housing their ID graph entirely.

TOPICS:

Competing Incentives

In-House Your ID Graph

New Paradigm for Data Portability

Part I: Competing Incentives: In the 2020's, Marketers Will Have To Do More With Data, Do it Faster, and More Securely. But how?

Consumer privacy legislation, like Europe's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), reflect a true shift in attitudes about data. Consumers want more control, more transparency, and more tangible value in exchange for their information. By necessity, these new regulations place new liabilities and demands on marketer's control and governance of first-party data. The more the data flows, and the more parties are involved, the greater risk a marketer takes in tackling the data and identity challenge. Relying on multiple partners and points solutions to orchestrate data between different systems leaves marketers exposed at every handoff.

Marketers are being thrust into a new era defined by first-party data and identity - an era that requires seamless and secure maximum (and maximally secure) portability of between online and offline, known and unknown channels (in addition to security). Marketers need a way to orchestrate any form of data or identity to any endpoint, and enable effective measurement of that action, all while protecting user privacy and ensuring the proper handling of their information.

At the same time, the business of orchestrating data requires marketers to prioritize privacy and security as never before. As bad actors find new ways to interrupt or ransom data usage, marketers are increasingly curious about what more can be done behind firewalls in order to increase the overall security of data and operations. On privacy, consumer privacy legislation, like Europe's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), reflect a true shift in attitudes about data. Consumers want more control, more transparency, and more tangible value in exchange for their information.

This means that marketers are often trying to balance two competing incentives: on one hand, they must do more with first-party data to stay competitive. And on the other hand, they must perform all their data operations more securely and transparently. Additionally, marketers need to perform those operations faster than ever; Manually sharing data with third parties takes time, which represents their own cost in an era of rapid changes to consumer habits and preferences.

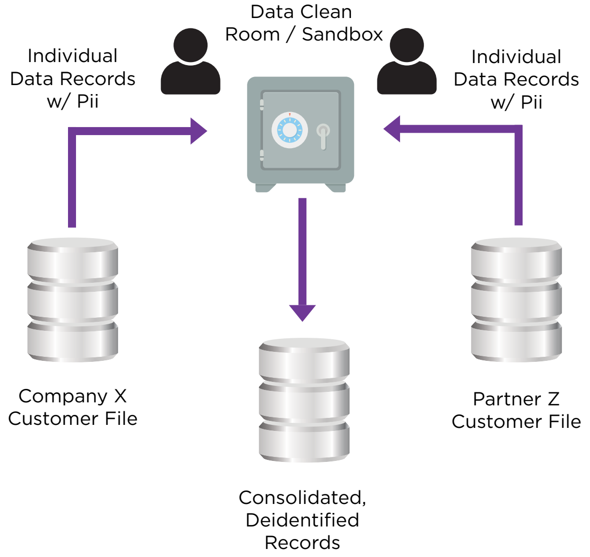
Four ways to Share Data - You Decide The Risk

A number of interesting solutions are emerging to help marketers solve that problem and balance those priorities, such as:

1

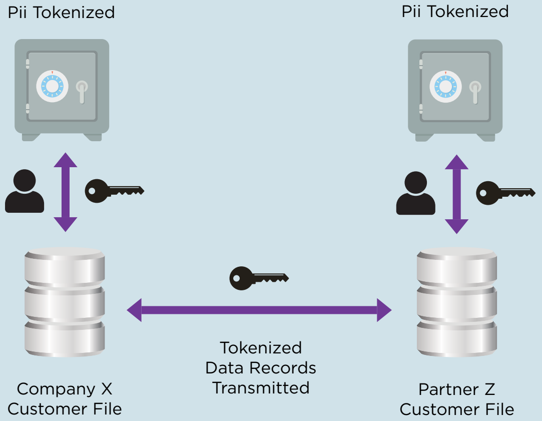
Sandboxes, Clean Rooms and Bunkers - There has been a surge of investment in creating secure environments for data matching that don't expose data to third parties. Known variously as 'sandboxes,' 'clean rooms' or 'bunkers,' they all tackle the problem of data sharing by providing a neutral and secure space for companies to share and match data without passing the data directly to their partners.

Data Clean Room / Sandboxes


Data Clean Room / Sandbox
Individual Data Records w/ Pii
Individual Data Records w/ Pii
Company X Customer File
Partner Z Customer File
Consolidated, Deidentified Records

2

Tokenized Data Transmission

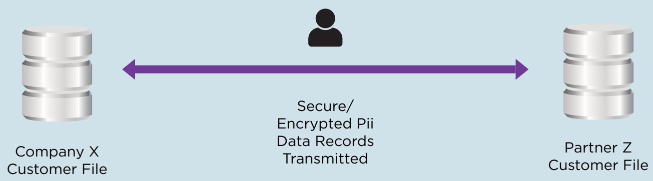


Tokens – A few companies have taken a brand new approach to securely sharing data using pseudonymized tokens to match two data sets without exposing PII. Tokens and crypto technology represent a promising new front in efforts to provide a new framework for secure data sharing.

3

API integrations - API integrations are the primary means by which brands share data today. Most of the open ecosystem is tied together via such relationships, which are brokered directly between two companies. These pathways are proven to work, but the need to manually implement each and every one takes time and effort, and can become incredibly complex for marketers to manage many at once. They also represent a higher data security risk for both parties (senders and receivers) as Pii data is often needed to enable cross platform record matching, and therefore these integrations need to be actively protecting the data transmissions.

API Data Transmission



4

Don't send your data out at all-to solve for this option, Adstra has introduced the industry's first Portable Data Module, a new technology that enables brands to leverage modular data assets and identity resolution capabilities safely behind their own firewall, eliminating the risks that come with sending PII to third parties. The PDM is built off Adstra's own identity solution - AdstraGraph - and allows clients to build out and control their own identity management capability. Rather than rely on API integrations, clean rooms, or tokens, the Portable Data Module affords brands the option of performing every action within their own environment. There's no PII to send. Clients maintain full control of the data and full transparency into its applications. Data can be easily connected and deployed to a client's various customer touchpoints, both terrestrial and digital. Even matching against external files can be conducted in the client's environment. Risks diminish, speed to execute increases, complexity drops.

All four options presented here are viable solutions for brands to pursue. The appeal of the first three options is that there is a third party stepping in to help manage the solution for you. Lower complexity and clearer implementation paths to follow also lead one to select one of these options. But none of the first three truly address the marketplace challenges that brands now face.

In today's marketplace, we see many brands starting to consider the approach of insourcing their identity management solution and Option four certainly seems appealing. But before getting there, Brands want to first get the heads around what they are signing up for in on-housing their ID solution and how to be successful in making it happen.

SIDEBAR

Outcome vs Process: Both must be considered

Outcomes are having a moment. Driven by the example of disruptive DTC brands, more and more of the ecosystem – including large, incumbent brand marketers – is driving toward a performance mindset. Marketers are thinking heuristically, focusing on ends rather than means.

That kind of singular focus approach won't fly if marketers intend to rely on people-based identity solutions and also comply with the demands of new privacy regulations. For brands to get the most from identity – and to manage the risks associated therewith – brands are going to need to equally concern themselves with the how. Brands can not rely blindly on 3rd parties to manage process for them. The incentives and focus are often not aligned, creating hidden risk and surprise complaints from customers and regulators who are unaware of the 3rd parties involved. Brands need to bring in people that technically understand how data is going to flow through their systems – how it's gathered, managed, orchestrated, matched, and deployed in order to realize the outcomes that everyone champions. They will need real experts dedicated to understanding the mechanics, to asking the tactical questions – not just about outcomes, but about the process itself. Because in understanding the process, marketers will uncover both opportunities worth seizing and risks worth mitigating.

Part II:

How to In-house your ID Graph:

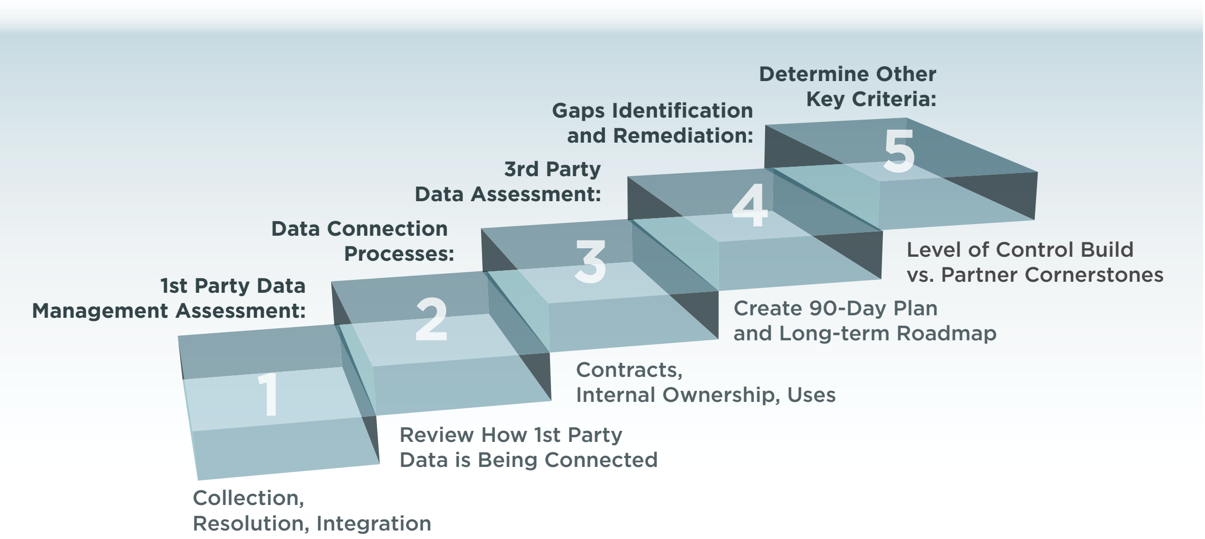
As Brands tackle the challenge of in-housing their identity operations, Adstra has laid out a 5 step assessment process that Brand can follow in establishing the foundation of their solution.

The goal is to establish a foundation that matches your business demands today and those down the road. Brands must also honestly assess the return on meeting those demands to assess the overall level of investment they should be willing to make. It is a sin to both over and under-invest. Here is a breakdown of the 5 key assessment steps:

First-party data Management Assessment:

First-party data has quickly become the “holy grail” for marketers in designing a solution that will enable their long-term ability to continue to market effectively, particularly as they face with the prospect that third-party cookies may soon vanish. The benefits of first-party data are primarily that they come with a high degree of trust and intent. The information is direct from the individual, is timely and transparent, and can be connected to an individual’s use permissions. That being said, not all first-party data has equal value. Much of the data collected today is of little incremental value to the company itself. In many instances, companies overvalue first-party data because they know it is

Adstra’s Data & Identity Framework to Set Your Identity Roadmap


Determine Other Key Criteria:
Gaps Identification and Remediation:
3rd Party Data Assessment:
Data Connection Processes:
1st Party Data Management Assessment:
5
4
3
2
1
Level of Control Build vs. Partner Cornerstones
Create 90-Day Plan and Long-term Roadmap
Contracts, Internal Ownership, Uses
Review How 1st Party Data is Being Connected
Collection, Resolution, Integration

permissible and accessible. The security of permission compliance, however, does not generate new value in the predictive or segmentation impact of any particular piece of data. That value is inherent in the data itself and

the business needs the data supports. It is for this reason that companies must provide an honest assessment of their first-party data at an

element level.

Companies need to take stock of what first-party data they have accessible and what they can generate or collect on a current basis. From that list, companies must then assess the true value of the data in driving business decisions and actions and what liability the ownership and handling of that data creates in terms of risking consumer perception or financial penalties. A company may know for example that a customer typically makes purchases with a Visa card. While this data may be valuable to a credit card company as third-party data, does it offer any real value as first-party data? It might if the company has worked with Visa to offer a special purchase incentive to customers that would help generate more sales. If the knowledge that the customer uses Visa does not affect any marketing or messaging activity, then it is hard to assign any value to that piece of information. For every piece of first-party data you have, it is important to understand where and how that data is being used to drive value (and at what level of value) and assess what the cost is to acquire and maintain the data, including assigning an expected penalty cost to match the risk of using and storing the data. From there, marketers can do an ROI calculation to determine if the first-party data is of value and worth investing in your technology and processes to take advantage of it. Once you have a complete first-party data assessment you should know 4 things:

1 The data you have worth keeping

2 The data you have that is not worth keeping

3 The data you would like to have and it's associated value

4 A proposed method to capture/collect the desired data and associated costs

Data Connection Processes:

The challenge with collecting and managing first-party data is integration and consistency at a

level that matches customer expectations. Once a customer agrees to share information with a company, they expect that information will be used consistently across the company's portfolio and customer touchpoints. It is for this reason that it is critical for companies to have a clear first-party data connection and management solution.

What data can be shared across internal technology and business silos, and what must be held in confidence? How will companies manage data capture and sharing permissions across these silos? And once these questions are answered, there are the tactical components on how to execute against these answers. Following closely on the heels of understanding a company's first-party data comes the need to address 2nd and third-party data. What data is easy and low-cost to access that need not be managed centrally, and what data is higher cost to acquire and should be managed in the same way as first-party data?

In earlier days, companies invested in large centralized "Data Lakes" or CRM technology. The idea was that all the information on an individual would be stored as a single record to be accessed by all other systems within a company. Hit with the challenges of technology access and flexibility, the desire to build one customer "record of truth" became an unwieldy and costly reality. Security access concerns and the need to present data closer to customer touchpoints because of response time concerns forced companies to create numerous duplicate data records across systems that had to be updated and maintained. Many have since evolved to more flexible approaches that involve developing an internal customer PIN and use of decentralized cloud-based technologies that enable consistent cross-business silo access.

Regardless of the infrastructure, it requires thoughtful consideration around linking the data collected to a defined individual with associated use permissions. What identity data is needed at each point to assign a PIN and enable downstream connection and activation or use by purpose? Is the PIN something that will be assigned internally, or will a third party be needed to resolve the identity of an individual and return a PIN? In many cases, the answer may vary based on the customer interaction.

Finally, once a complete approach has been defined, companies must consider the issue of their data security. A company's first-party data is not only a valuable asset, but also a sacred promise to the customer to protect it. At Adstra, we are strong proponents of separating the storage of Pii from other collected first-party data, using your internal PIN as the connection between the two when required. Think of the PIN linked to Pii as the key and the PIN connected to your first-party data as the safe deposit box. Always best to keep the two separated. Once you have completed your data connection assessment process, you should know 6 things:

1 Where in you marketing and customer management process data connection is required

2 Where you need to resolve a customer identity by platform/ touchpoint and link across platforms

3 Where Pii linked vs anonymous individual data is required

4 Where customer data needs to be shared across platforms

5 Where customer data needs to be shared externally

6 If your are planning on managing ID resolution and data PINing within your data ecosystems or through and external ID resolution provider

Third-party data Management:

We touched on the idea of third-party data briefly in the past section, but it warrants a bit more depth of understanding before moving forward with a company's overall Identity management approach. Much like your first-party data assessment, Companies need to understand the value and cost associated with their third-party data. What data do you have, what is needed, what can be discarded, and what are the associated costs?

The big differences in assessing the third-party data you use are twofold. First, there is the assessment of the third-party data provider. Is the data accurate, consistent, at scale, accessible, and is the provider themselves reputable and stable? Second is the assessment of purchasing and storing the data as you would first-party data vs purchasing the data potentially multiple times when being used at the end decision points.

For example, it may be faster and easier to use the gender provided by a DMP vs pushing your understanding of gender out to the DMP. Because third-party data is external and often ubiquitous, it can be introduced into the marketing process at most any time. Privacy and data security concerns are not the same as first-party data and can often be managed through simple contractual language and common-sense use management. There are certainly savings by purchasing third-party data at scale only once, but there are costs associated with managing the data and more impactfully in enabling the data at the customer touchpoint at the required timeliness. For more static third-party data such as gender and income, the cost of timeliness may be low, but for dynamic or trigger data, such as new mover or recent site visit data, the cost of delay can be quite high to a marketer.

Right time, Right place doesn't have to be luck. It can be captured through the Right data in the Right offer. So like your first-party data assessment, marketers, in completing their third-party data assessment should walk away with 6 things:

1 What third-party data do you have access to today at each of your critical use points?

2 What do you spend on third-party data and where are you paying for the same data more than once?

3 What third-party data is static and what is dynamic/trigger oriented?

4 What is the value-driven by the use of the third-party data?

5 What third-party data would you like to have access to but don't, and what is the associate cost of not having that data?

6 What is the consistency of the third-party data you are using and stability of the source over time?

Gaps Identification & Remediation:

Having now built an understanding of one's 1st and 3rd Party data and the ability to connect (or not connect) that data across the marketing ecosystem, you are now in a position to define and prioritize the gaps that exist. Simply put, where are you now and what is preventing you from getting the point you want to be. At a first pass this may sound simple. The challenge comes in assigning the value of closing the gap and identifying the barriers to closing the gap. These barriers can come in multiple forms. 1- Technological; 2 - Organizational; 3 - Financial; 4 - Customer engagement; and 5 - the reality of a solution to closing the gap. Some might say that #5 doesn't really exist if you can invest enough in the first 4, but we are trying to stay practical here and so should you. Often #5 manifests itself in the desire to have specific data that fundamentally does not present itself at the needed time.

Once the gaps have been identified and prioritized, then it is about putting together the appropriate remediation plan. Often the simpler the remediation plan the better chances of success. In the plan design however, it is important to establish high level principles of design. What matters most to you as a company and does the remediation plan fit within those principles. This is where sometimes simple may be confused with easy and may not be the answer. Outsourcing everything may seem simple at first, but it is really just easy. In the long run it may add complexity as you look to adjust technology and marketing approaches. Simplicity is more about the design itself, not the execution choice. Fewer steps, fewer pieces doing the work, fewer people having to make decisions are what simple looks like and leads to faster remediation and longer term use.

Other Key Criteria:

As company's think through their eventual Data and Identity management approach, there are a few additional criteria that we think are important to consider. Most of these are focused on two business considerations; 1- the value of direct individual engagement in your marketing and experience management; and 2 - your organization's ability to change processes to match new business objectives.

Here are some of the added key criteria to consider:

1. Value of personalization

2 Degree of existing customer self-identification

3 Degree of separation between consideration and purchase

4 Level of collaboration between internal marketing channel teams

PART III:

A New Paradigm for Data Portability

Adstra's Portable Data Module is a new offering that enables brands to leverage modular data assets and first-party data orchestration capabilities safely behind their own firewall, eliminating the risks that come with sending PII to third parties. The Portable Data Module represents a new technological infrastructure for safeguarding privacy and promoting transparency without sacrificing data-driven capabilities.

With Adstra's Portable Data Module, every operation performed on a brand's data, including matching, can be conducted 100% in the brand's own environment. Brands are able to access the full scope of Adstra's capabilities, including its proprietary ID Graph while maintaining total control of their data and complete transparency into all of its applications.

As Brands build out their new Identity Management solution, it is not just about security and privacy, but also about maintenance. Any solution that a Brand develops will require a consistent and reliable flow of the raw identity data required to enable their solution. For some, the data is simple updates of new mover data from the US Postal Service, but for most, it will require email, device ID, IP address, cell #, etc data that needs to be current and updated within their end solution.

With the Portable Data Module and Adstra's ID Graph, brands can extend the value of their first-party data much further than with other solutions.

To learn more, visit adstradata.com