metarouter

RESPECT YOUR USERS

The #1 Way to Protect Customer Data

“You can have data without information, but you cannot have information without data.”

Daniel Keys Moran

We all know data is an invaluable but intangible asset. One that is far, far too easy to copy, keep, and repurpose.

If you share data with another person or a business, you risk losing control over how that data is used. Sharing personal information entrusted to you by your customers is a major problem, especially if you’re subject to GDPR, CCPA, or other emerging regulations.

Most Organizations Share Data More Than They Realize

The problem is, information is “shared” without organizations realizing it. Tech giants, e-commerce retailers, publishers, and advertisers have been able to collect shockingly detailed information about customers and their behavior in real life and on the Internet.

We all know the obvious aggregators of our information—Facebook, Google—but the roots go much deeper. The average enterprise marketing team uses 120 third-party martech tools. The system basically works like this: Each tool requires its own browser tag to collect information.

Even when using a tag simplification tool, the tag or pixel continues to operate on behalf of the tool, making its own call for data.

Client-side tracking involves getting the user’s browser or mobile device to send data to your server. This can be done in several ways, such as UTM parameters, IP addresses, cookies, and user agents. First, browsers are committing to preventing use of third-party cookies. Secondly, ad blockers on the client side or interrupted connections can interfere with the data you receive. Finally, once the data is collected, it is passed to an analytics service. Unless you’re using home-grown analytics, you’re sharing data with a third-party, and you’ve lost some control over it.

That means the average enterprise organization might disseminate each individual customer’s information to more than one 100 third parties.

Until recently, customers seemed to accept this system—or they simply didn’t realize what was happening behind the scenes every time they visited a company’s website. Organizations, too, trusted the tools they needed to do their jobs well.

Now, however, much attention has been given to the misuse of information, and even privacy policies. Businesses and individuals alike are discovering just how common-place the sharing of sensitive data really is.

The Old System Has to Change

“Data that is loved tends to survive”

Kurt Bollacker, Data Scientist

More and more, people will turn on businesses that allow data to be misused. Regulators are also piling on privacy regulations that will subject businesses to costly fines if they allow personal information to be misused or exposed. We need to get the data ecosystem under control.

Of course, that doesn’t mean we should stop tracking user behavior. E-commerce businesses have a valid reason to collect some sensitive information from their customers—payment information, for example, to provide goods and services. And every successful retail business, whether brick and mortar or online, has paid attention to customer buying preferences and behavior to try to figure out how to get their customers to buy more from them and to attract new customers. That’s good business, and most people accept that willingly.

But programmatic advertising, tracking technology and analytics have allowed companies to collect and aggregate a seemingly inordinate amount of data about individual consumers and specific audiences that are shared too freely across the ecosystem. For many e-commerce businesses, the risk may not be worth the results.

Bad for Business

Allowing sensitive data beyond your own walls without any ability to track it presents obvious compliance risks. GDPR, for example, specifies that a user can go in and request that an organization purge everything they’ve ever collected on that individual. That’s impossible if they’ve, say, used a Facebook tracking pixel or sent information to Mixpanel. However, if they’ve kept the data in a first-party context and remained compliant from ingestion, the user is protected.

The complexity and lack of transparency of the programmatic supply chain, too, are enabling massive fraud. In January 2017, for example, Uber discovered that one of its vendors was placing Uber ads on Breitbart, a site that Uber had blocked. When Uber dropped the vendor, reducing their ad spending, the company braced for new rider numbers to go down. There was no change.

After auditing other vendors and inspecting log files again in 2020, Uber uncovered pervasive fraud – phantom traffic, phantom clicks, and even phantom sales. Uber has sued some of the vendors, alleging that the defendants purchased ad placements on behalf of Uber, which were in fact not real ads, or were illegitimate or prohibited ads, such as “autodirects,” or ads placed on prohibited sites such as pornographic websites. By placing fewer ads through better partners, Uber was able to cut its ad spending by nearly ⅔ (or $100 Million!) with no adverse effect on its business.

Uber is not alone. Many companies have found that reducing ad spending does not necessarily lead to decreased revenue. A great deal of programmatic advertising is wasted on low quality or fraudulent ad placement. That annoys consumers, may tarnish your brand, and puts customer data shared with fraudsters at unnecessary risk.

Even if a business works only with well-established partners, sharing the data the business collects directly from its customers can reduce its competitive edge. For example, if you carefully track your customers’ data and send it to Facebook to create ads targeting specific audiences, your competitors can then use Facebook’s look-alike audiences to benefit from the data you collected. For small businesses, this may be helpful at first. For enterprise organizations, it’s a huge liability from the start.

E-commerce businesses rely heavily on access to consumer data, but if they suffer data breaches or allow third parties to access and misuse—or possibly even use—that data, they will lose customers, damage their reputation, and may incur fines for violating one or more privacy laws. The risk is high, and businesses need to be extremely cautious about sharing the customer data entrusted to them.

Bad for Individuals

Irresponsible data collection is, of course, also bad for customers. In the last few years, we've seen too many examples of unprincipled companies abusing access to consumer data.

Facebook, for example, lost many users over the Cambridge Analytica scandal. In that case, an app that paid Facebook users to fill out surveys for academic research purposes, harvested the survey takers' personal information as well as that of their contacts and then used the data to create psychographic profiles of the data subjects and sold the data to political campaigns.

Researchers have also found unprotected, publicly exposed databases with profile information collected by data brokers. Last year, researchers found one with 235 million profiles scraped from social media. And just last month a hacker published personal information of over 500 million Facebook users. This information, which was apparently scraped using a flaw in Facebook's contact importer, included full names, phone numbers, Facebook IDs, locations, birthdates, and email addresses of over 500 million Facebook users.

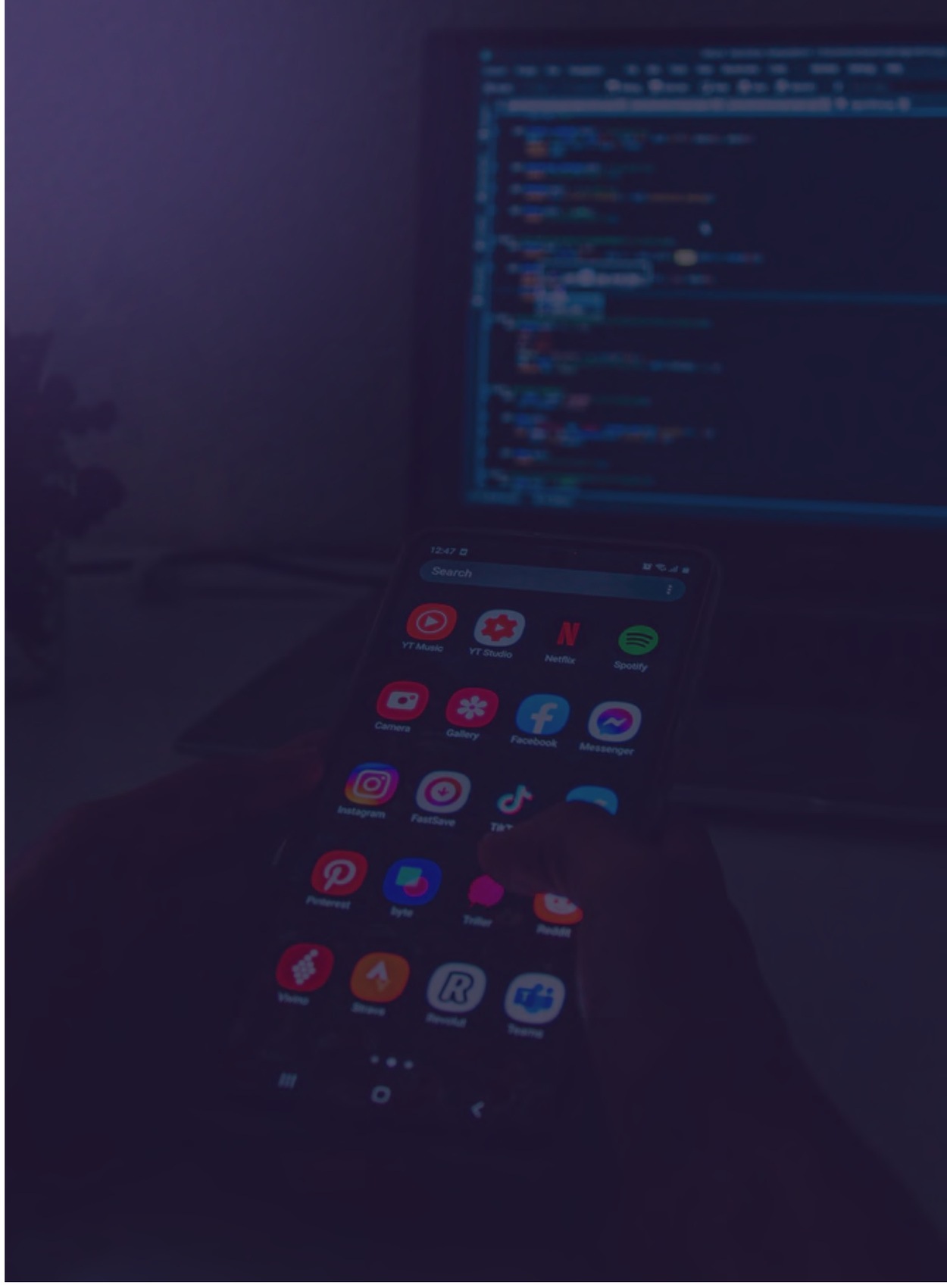
Brokers would not be collecting this data if it weren't valuable, and neither the social media platforms nor the data subjects can control how the data is used, once a data broker gets it. Aggregated, it can provide enough information for identity theft, phishing attacks against a user's company, or insurance fraud. It could be sold to hackers, stalkers or law enforcement agencies, all without the users' consent.

Just visit haveibeenpwned.com to see if your data has been compromised. Mostly likely, it has.

Something must be done.

What About Regulations, Cookie Killing, Browser Restrictions?

Consumers, privacy advocates, and regulators have been calling for change. Unfortunately, regulations like GDPR and CCPA have not made much difference. They have increased the fines levied for breaches of personal information and forced us to click through innumerable cookie policy and do-not-sell-my-data pop-ups. And the data breaches continue. Governments are not well equipped to deal with cutting edge technology. Legislators rarely understand the technology, rely on industry insiders to draft the regulations, and take years to pass laws that often turn out to be ineffective. Regulation will help, but it will not fix this.



Additionally, organizations like Google and Apple have appeared to be enacting change, respectively, by restricting third-party cookies on browsers, launching new protective mechanisms like IDFA (Identifier for Advertisers), and more. These sounds good on the surface, but we cannot rely on the tech giants to self-regulate. Companies like Apple, Facebook, Amazon, Microsoft, Netflix, and Google (FANG or FAAMG or, sometimes, FAANG) control massive walled gardens of data and monopolize their industries. It is very difficult for smaller companies to compete, particularly when tech giants cooperate with each other. In 2017, for example, Google cut a secret deal with Facebook, convincing Facebook to join an alliance of companies working with Google on Open Bidding, in return for special information, speed advantages, and a guaranteed win rate in bidding auctions.

The truth is, large tech giants that comprise the core of what we're calling the old system already have a huge information advantage over most e-commerce companies—from the vast amount of data they collect from their own users and from other advertisers. They are powerful enough to act in their own self-interest, which means repositioning their brand or cutting off the data flow for others has no impact on their bottom line.

In other words, the current aren't enough.

It’s Time to Take Responsibility

“Only you can prevent wildfires.”

Smokey the Bear

Complying with the letter of regulations like GDPR and CCPA is not enough. Trusting in the policies set up by a third-party is not enough. Once you have collected personal information, you are responsible for it. You must honor consumer requests to access, amend, or delete their data, and it is almost impossible to do that if you have shared that data with third parties. Typical compliance for data shared with third parties is in the form of “requests” – consumers request that a business delete their data, and the business requests that third parties delete their copies of any shared data. It is difficult, if not impossible, to verify that a third-party has actually deleted the data.

The only way to be sure is to take responsibility for privacy and compliance is to manage customer data from ingestion. To collect it first-party and protect sensitive details from getting to a third party.

Customers willingly enter into a relationship with an organization. They trust them. That organization is the only one incentivized to protect customer data. They bear the burden in the event of a breach. They benefit from customer loyalty. It starts and ends with the first party.

Fortunately, it’s not as hard as it used to be.

The Secret to Protecting Consumer Data

This does not mean that you cannot use the data for advertising purposes, you just have to do it more carefully. Client-side tracking has been used successfully for many years, but it’s not going to work for much longer.

The only option for organizations is to collect data in a first-party context and protect it from ingestion. They must track the information—without a browser tag, without a tracking pixel—process it responsibly, and deliver it to third parties in a format that is safe. Internally, they can build their own customer data platforms and use raw data, but it can’t leave their secure walls.

A Quick Guide to Server-side Data Integration

Server-side data processing is the concept of generating an event from the server that houses your website's code, as opposed to data generated on the client, which typically relies on javascript files called from the code snippets placed in your website's HTML.

In Chrome, if you open up your Developer Tools and click on the Sources tab, you'll likely see a collection of files. If you're running common tools such as Facebook Pixel or Google Analytics that require a feed of data produced from your users, you should see the files they use to process data and send to their respective APIs here.

When data is generated via the server, on the other hand, there is no indication that anything is loading on the page at all—because it isn't! The events are produced by back-end services that power your website, like a Customer Data Infrastructure (CDI).

Common examples of events that can be generated here are log-in events, product purchases, and form submissions. Typically, they’re recorded in a database somewhere for you to access at a later date. But you can also choose to forward them along to your vendors' APIs (so long as they accept server-side events).

Server-side information relies on events produced by the services behind your website—and server-side integrations let you take back control of your customers’ data and use it to gain the insight needed to grow your business and retain your customers, without allowing third parties to accidentally or maliciously misuse it.

“Server-Side” Doesn’t Always Mean the Same Thing

Many CDIs or CDPs that offer server-side integrations have to run them in conjunction with client-side integrations. Yes, data is integrated server-side, but all the client-side insecurities and inefficiencies are also in play. A huge limiting factor is that not all vendors support APIs to process this type of data. Google, for example, generally doesn’t accept data produced server-side. They are developing a new solution for server-side eventing, but so far, the plan is to require Google's client-side tag to run.

It’s important to note that information is still being shared whenever a client-side tag is present.

Instead of relying on server-side APIs, then, the solution is to collect all the data that an event generated client-side would contain, in a first-party context, and keep it within your control. The end result is a server-side event that looks exactly the same as a client-side event, even though no third-party javascript is ever involved in the processing of data.

So is it possible to restrict all access to your data, from any third party? The only option is a full data-routing architecture on your own private cloud that restricts all access to data processing, even for the company that created the architecture. Essentially, you must own your own data router.

How does MetaRouter Work?

1. Collect all customer data from your mobile apps, websites, and servers.
2. Process it your way and integrate it with business tools server-side.
3. Send data in any form to individual partners.

Bonus Benefits of Server-Side Data Integration

Keeping data compliant from ingestion and maintaining data governance are obvious benefits of server-side integrations. What’s not so obvious is how performance is enhanced when events are no longer subject to inconsistent browser settings, extensions, and general network risks.

Since server-side events do not require any browser resources, the browser activity triggered by each customer on your website is materially lower. This makes your website faster and more performant—to a degree directly correlated with the amount of data processed by each client-side tag you move to server-side.

Additionally, directly calling one event and sending to each vendor greatly reduces duplicate and inaccurate data.

Of course, integrating with a new tool is also easy with a ready-to-use yet fully customizable data architecture.

When it comes to respecting your users, server-side integrations make it not only possible, but also easy. The time has come for organizations to invest in their customers by providing them the experience they expect while protecting their information from accidental—or intentional—re-use.

Interested in respecting your users through server-side integration? MetaRouter provides the first server-side-focused Customer Data Infrastructure. When deployed on your private cloud, not even MetaRouter has access (though we have several alternative deployment options as well). Reach out anytime.

metarouter

For a demo or free consultation, contact us directly.

hello@metarouter.io