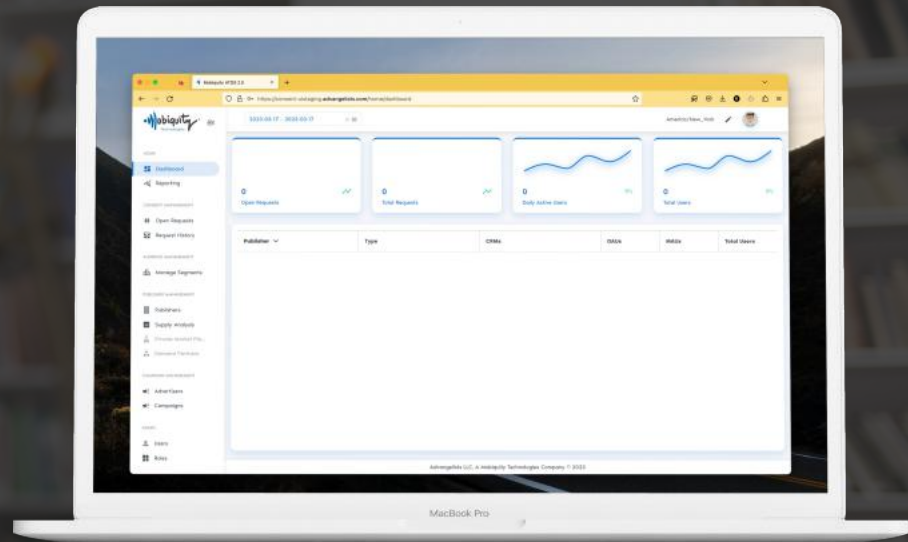
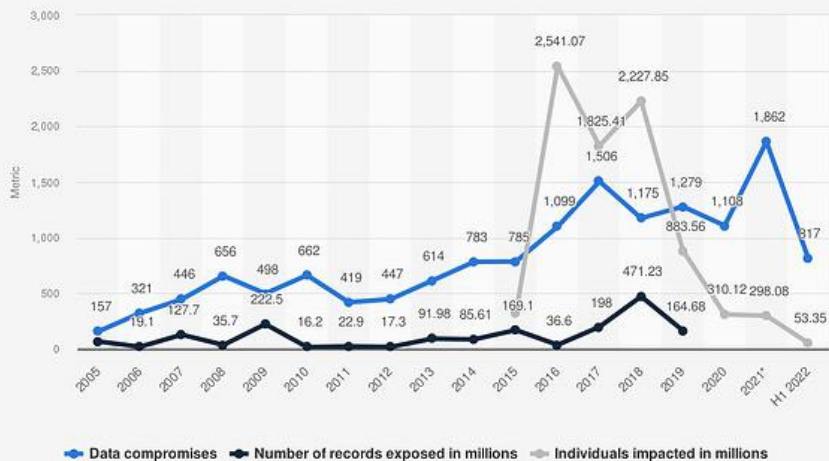


Mobiquity Technologies

Next Generation Ad-Tech Operating System for
PUBLISHER COMPLIANCE & MONETIZATION



Annual number of data compromises and individuals impacted in the United States from 2005 to first half 2022



Source
Identity Theft Resource Center
© Statista 2022

Additional Information:
United States; Identity Theft Resource Center; 2005 to H1 2022; data compromises include data breaches, data exposure
impacted may go beyond the United States

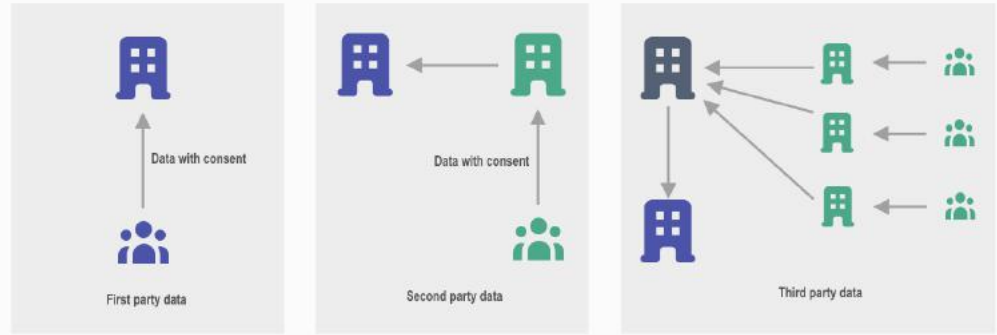
75%

Of Americans
believe their personal data is
less secure now than it was five
years ago.

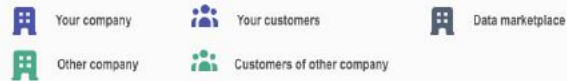
84%

Of consumers
say they want more control
over how their data is being
used

Understanding Data Types



First party data vs second party data vs third party data




Data

The Current world of Advertising

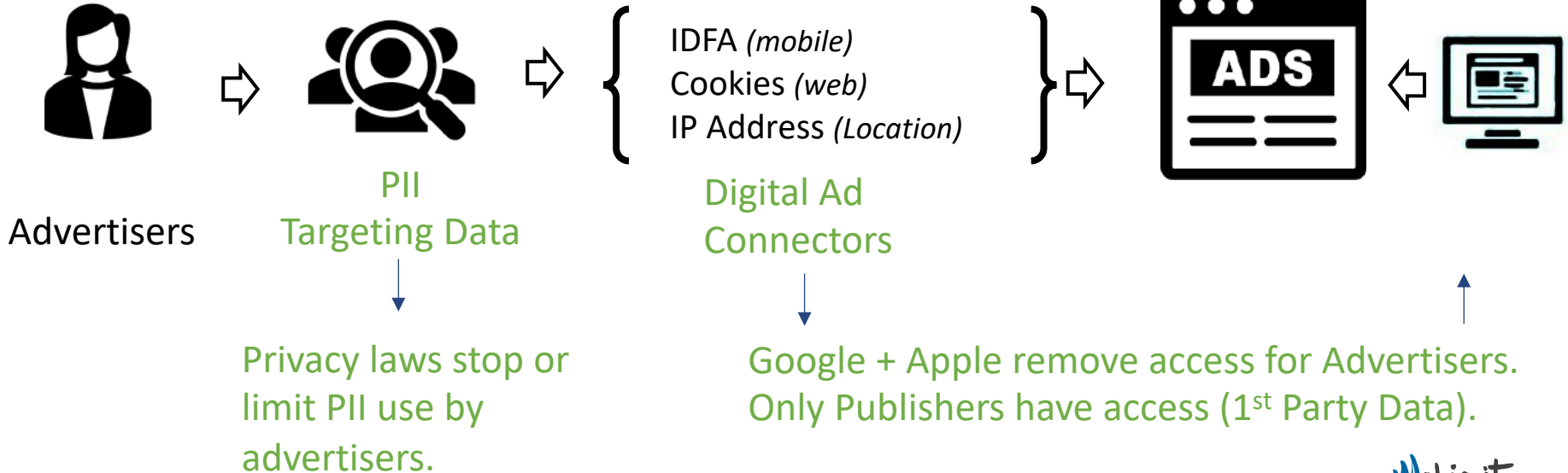


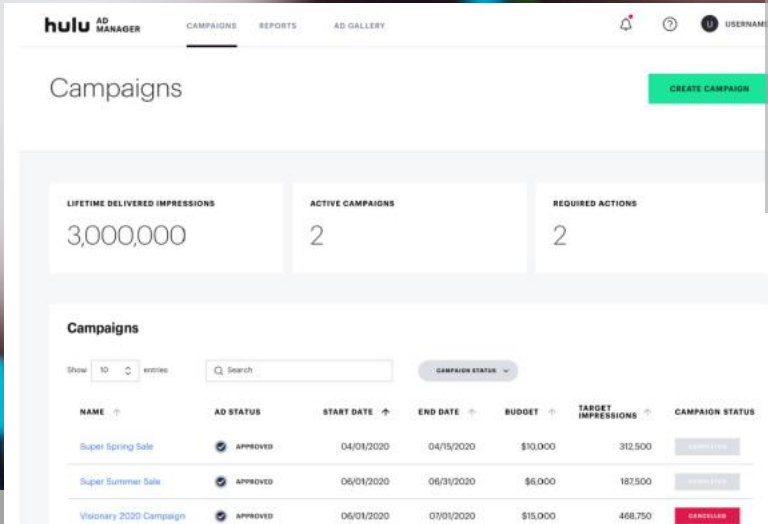
Advertisers purchase **PII** (name, address, income, etc)

PII is used to target customers by matching to **Digital Ad Connectors**

Advertiser purchase targeted Ads from **Publishers**

The Future of Advertising





Facebook feels \$10 Billion Sting from Apple's Privacy Push ~ Wall Street Journal



BIG CHANGES are coming to the world of Digital Advertising

Publishers are losing revenue due to lack of higher CPM targeted ads

Large publishers are investing in their own Ad Technology so they can use their owned 1st party data to sell high CPM targeted Ads



To maintain revenue and growth Publishers must...



Make the customer PII they own compliant with privacy laws



Provide ability for advertisers to use Publishers PII + Connectors in a privacy compliant manner



Send ad requests to Ad Networks with enhanced audience information that is privacy compliant

Why Publishers ought to consider Direct Data Management



Data Privacy and Compliance

By managing their own consent and audience management, ad tech publishers can ensure that they are in compliance with data privacy regulations such as GDPR and CCPA.



Better Control over User Data

By managing their own consent, publishers have greater control over what data they collect and how it is used, helping to build trust with their users.



Increased Revenues

By being able to target advertisements to specific audiences, publishers can increase their revenue by delivering more relevant and effective ads.



Improved User Experience

By managing their own audience management, publishers can ensure that their users have a better and more personalized experience, reducing the risk of user churn.



Increased Data Accuracy

When publishers manage their own consent and audience management, they can ensure that the data they collect is accurate, leading to better-targeted ads and improved ad performance.



Competitive Advantage

By having control over their consent and audience management, publishers can differentiate themselves, making them a more attractive option for advertisers.

How can a Publisher increase revenue in a world focused on first party data?



01. Utilizing First-Party Data

By leveraging first-party data, publishers can gain a deeper understanding of their users and their interests, which can be used to deliver more relevant and personalized advertisements, increasing the likelihood of conversion and, in turn, revenue.



02. Offering Opt-In Programs

Publishers can increase their revenue by offering opt-in programs to users, where they can share their data in exchange for a better and more personalized experience, as well as access to premium content and services.



03. Building Trust with Users

By being transparent about their data practices and giving users control over their data, publishers can build trust with their users, which can increase their willingness to engage with advertisements and increase revenue.



04. Investing in Privacy-Focused Ad Tech

Publishers can increase their revenue by investing in privacy-focused ad tech, such as privacy-compliant data management platforms and consent management solutions, which can help them to target their ads more effectively while still respecting user privacy.



05. Offering a Seamless User Experience

By offering a seamless and frictionless user experience, publishers can increase user engagement, which can lead to increased ad exposure and revenue.



06. Collaborating with Advertisers

By working closely with advertisers to understand their needs and target their ads more effectively, publishers can increase the value of their inventory, resulting in higher revenue.

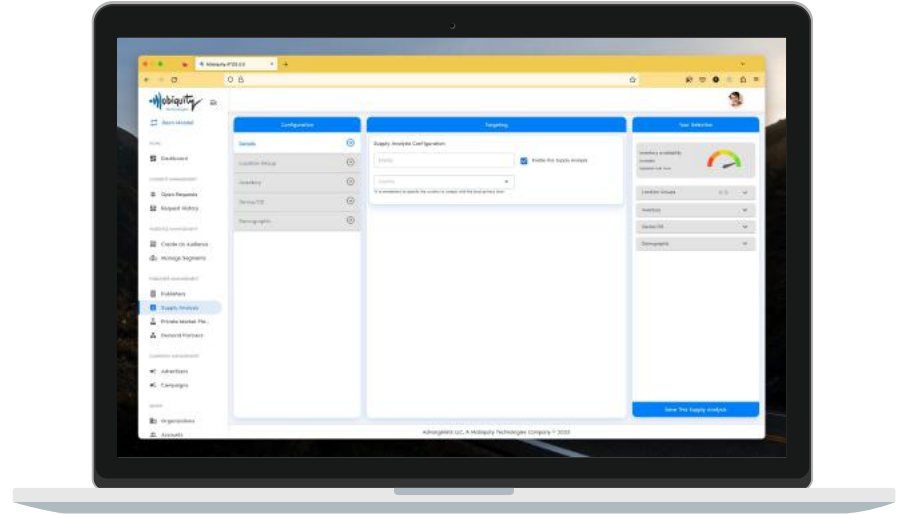
Complexities for Publishers building & managing their own buying platforms

1. **Technical Complexity:** Building and managing a buying platform requires significant technical expertise, which can be a challenge for publishers who do not have in-house technology teams.
2. **Maintenance Costs:** Running a buying platform requires ongoing maintenance and upgrades, which can be expensive and time-consuming for publishers.
3. **Lack of Scalability:** Publishers may find it difficult to scale their buying platform to meet growing demand, which can limit their ability to compete with larger players in the market.
4. **Integration Challenges:** Integrating a buying platform with other systems and technologies can be complex and time-consuming, which can negatively impact the user experience and the effectiveness of the platform.
5. **Limited Reach:** Publishers may struggle to reach a large audience with their buying platform, especially if they lack the resources to market and promote it effectively.
6. **Competition with Third-Party Platforms:** Third-party buying platforms, such as Google and Facebook, have significant reach and resources, which can make it difficult for publishers to compete.
7. **Data Privacy Concerns:** Building and managing a buying platform involves collecting and storing sensitive user data, which can raise privacy concerns and create legal and regulatory risks for publishers.

INTRODUCING ATOS4P

An Advertising OS,
reimagined for
Publishers.

An Advertising platform, engineered from the ground up for Publishers. Publishers control 100% of their inventory, their first party user data and who gets access to their ad inventory.



ATOS4P (Ad Tech Operating System for Publishers)

ATOS4P (Ad Tech Operating System for Publishers) is the new SAAS technology platform for publishers built from scratch by Mobiquity Technologies.

The benefits to a Publisher of licensing ATOS4P are:

1. Increased revenue by with high **CPM targeted ads** in a privacy compliant manner
2. Lower costs by maintaining control of inventory
3. Compliance to all Privacy laws in USA and more

Benefits of ATOS4P for Publishers

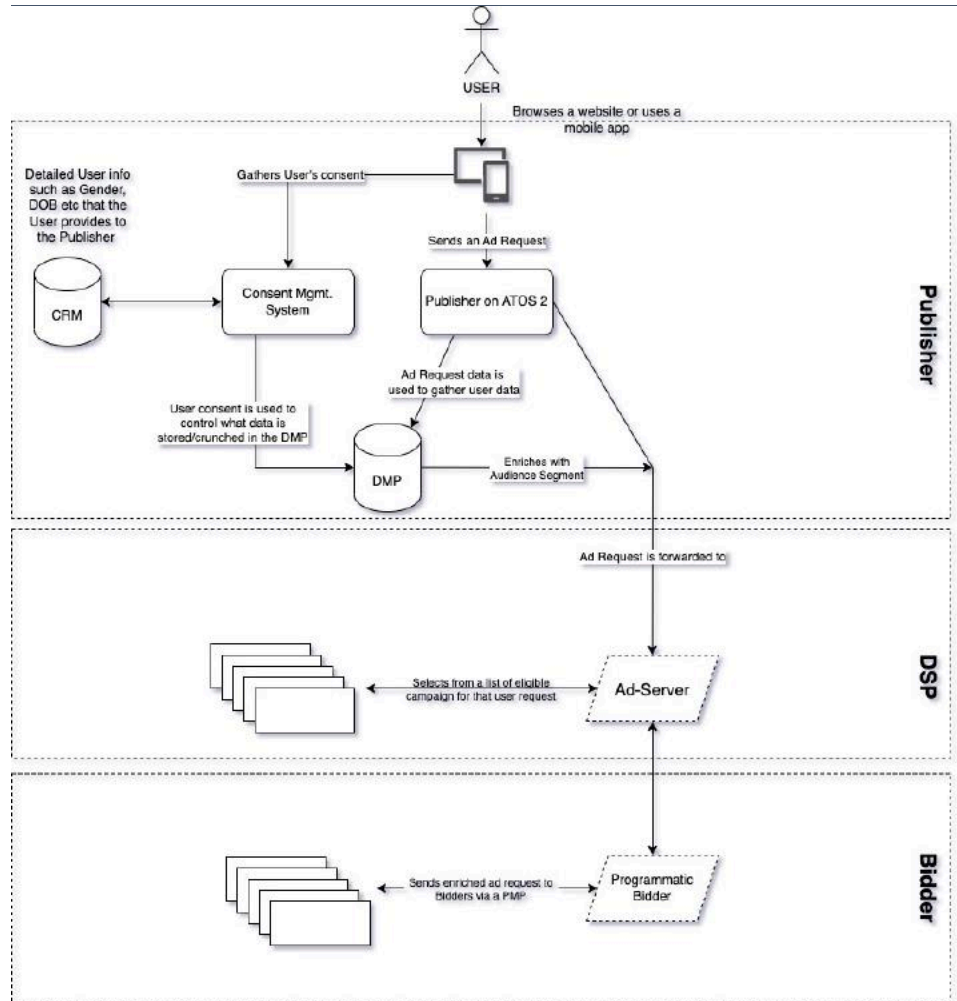
1. **Reduced Technical Complexity:** By licensing ATOS4P for consent and audience management, publishers can reduce the technical complexity associated with building and managing their own solution.
2. **Lower Maintenance Costs:** By using ATOS4P, publishers can reduce their maintenance costs and focus on their core business activities.
3. **Access to Advanced Features:** Publishers can access advanced features, such as robust data privacy controls and audience targeting capabilities, which can improve the effectiveness of their advertising efforts.
4. **Improved User Experience:** By integrating consent and audience management with a DSP and PMP creation module, publishers can improve the user experience and increase the value of their inventory.
5. **Better Data Management:** Publishers can benefit from improved data management capabilities, such as data collection, storage, and analysis, which can inform their advertising efforts and increase revenue.
6. **Faster Time to Market:** By licensing tech, publishers can get up and running more quickly, allowing them to start generating revenue faster.
7. **Reduced Legal and Regulatory Risks:** By using a licensed solution that is compliant with data privacy regulations, publishers can reduce their legal and regulatory risks and protect their reputation.

Architecture of ATOS4P

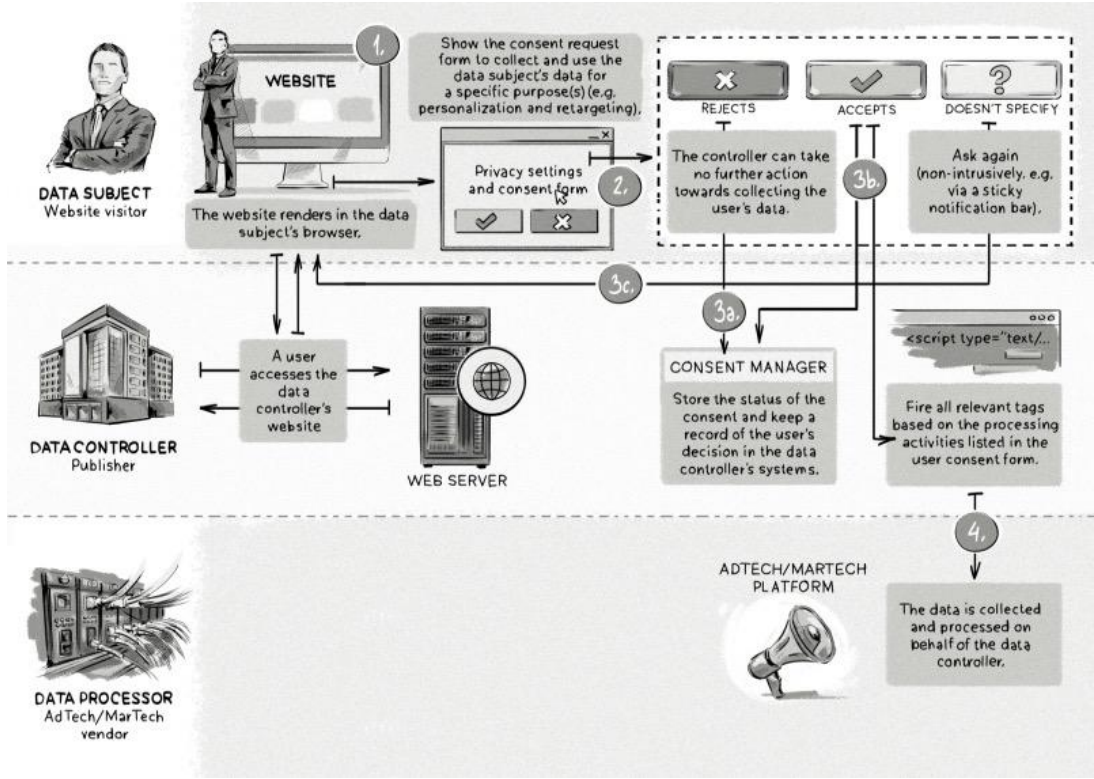
The architecture of MOBQ consent-compliant Data Management Platform (DMP) built specifically for publishers and supply-side platforms (SSPs) includes the following components:

1. **Consent Management System:** A system for collecting and storing consumer consents for the use of their personal data for advertising purposes, such as Logins and persistent ID CRM Solutions.
2. **Data Collection Module:** A module for collecting personal data from various sources, such as website interactions, mobile applications, and third-party data providers, in accordance with the obtained consents.
3. **Data Processing Module:** A module for processing the collected data, such as de-duplication, normalization, and enrichment, to ensure its accuracy and relevance.
4. **Data Storage:** A secure and scalable storage solution for storing the processed data, such as a data lake or a database.
5. **Data Access and Usage Control:** A system for controlling access to and usage of the stored data, ensuring that it is only used in accordance with the obtained consents and relevant privacy regulations.
6. **Data Analytics:** A module for analyzing the stored data to gain insights and support effective advertising campaigns.
7. **Data Export:** A module for exporting the processed data to other systems, such as ad servers, demand-side platforms (DSPs), and data partners, in accordance with the obtained consents.
8. **Privacy Management:** A system for managing privacy-related processes, such as handling access, erasure, and opt-out requests from consumers, and ensuring compliance with relevant privacy regulations.
9. **Ad Server Integration:** An integration with ad servers to enable the use of the collected and processed data for advertising purposes.
10. **DSP Integration:** An integration with demand-side platforms (DSPs) to enable the use of the collected and processed data by advertisers.
11. **Partner Integration:** An integration with data partners to enable the exchange of data in accordance with the obtained consents and relevant privacy regulations.

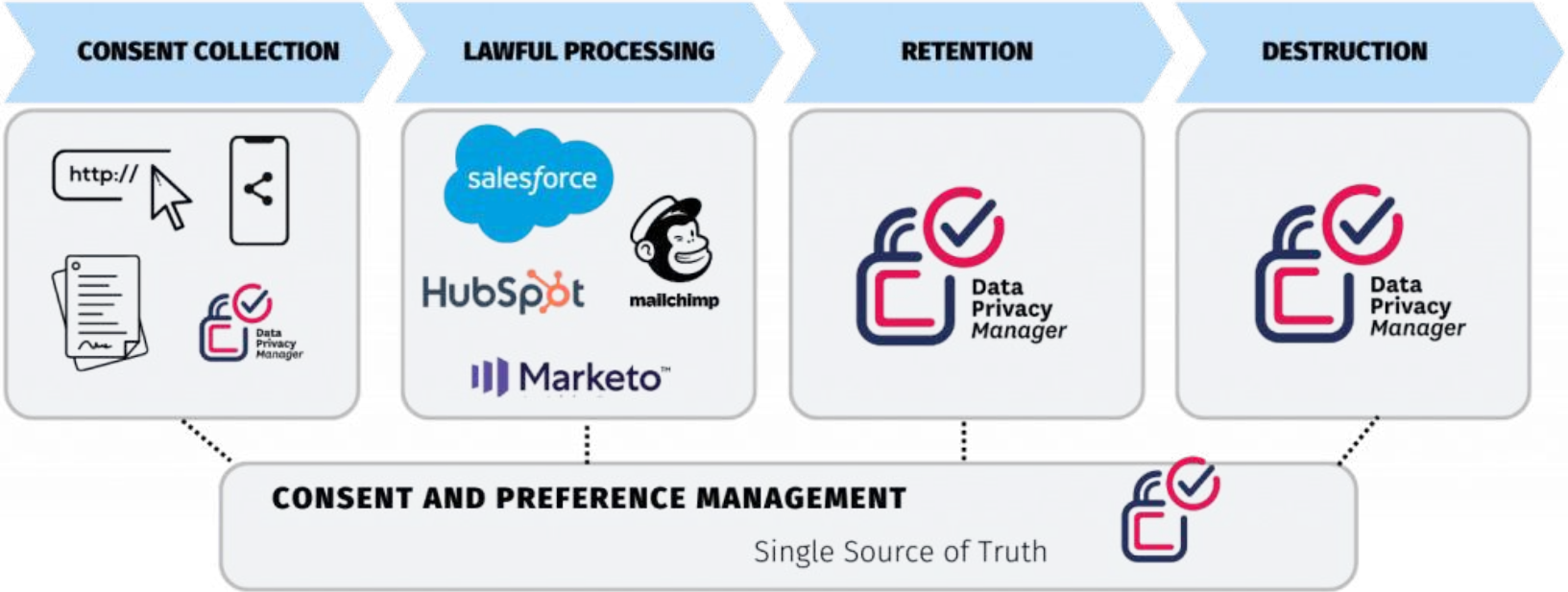
System Design



Consent Management – Flow of data visualized



Consent Management – a single point of Consent and Data management





CONTROL

Your site, your app, your rules on how they are monetized



DATA

All user data is siloed and stored in hardened caches, which only you access

Benefits



MONETIZE

Bring onboard your Agency and Direct Advertisers, while overseeing their activities



FORESIGHT

You can choose to expose your inventory Programmatically without exposing any user data



ACCESS

Have a large team? Set access control rights and abilities at a user level

ATOS4P – Services for Publishers

Consent
Management
Platform

Collect and manage 1st party data from customers in a manner that meets all Privacy Laws

Audience Builder

Build Targeting audiences from 1st party data
For example “Coffee Drinkers”

Self Serve Campaign
Manager

Directly Sell advertisers Publishers Ads that utilize 1st Party Data
For example, purchase Ads directed at “Coffee Drinkers”

Supply Side Server

Send publisher ads to other networks enhanced with 1st Party Data
For example, Ads directed at “Coffee Drinkers”

ATOS4P – a Privacy First Platform

1. Obtain informed consent from consumers before collecting and using their personal data for advertising purposes.
2. Implement appropriate security measures to protect collected data.
3. Be transparent about data collection and usage practices.
4. Allow consumers to access, delete, or opt-out of data collection.
5. Comply with regulations to avoid fines and legal repercussions and more importantly,
6. **BUILDS USER TRUST**

ATOS4P – the unison of Consent & Data Management

1. A Consent Management Platform (CMP) is used to manage the collection and storage of consumer consents for the use of their personal data for advertising purposes.
2. The CMP integrates with a Data Management Platform (DMP) to ensure that the DMP only collects, processes and uses personal data for which valid consent has been obtained.
3. The CMP provides the necessary interface for obtaining and recording consumer consents and tracking their status.
4. The CMP ensures that the DMP is only activated when valid consent has been obtained and updates the DMP with the latest consent status.
5. The CMP can also assist in managing the right to access, right to erasure, and right to opt-out requests from consumers.
6. This integration ensures that companies are in compliance with GDPR and CCPA regulations and reduces the risk of potential legal and financial consequences.

ATOS4P

Let's dive deeper

ATOS4P – THE DASHBOARD

The dashboard interface for ATOS4P is displayed. It features a dark blue sidebar on the left with navigation options: Dashboard, CRM, Consent Mgmt, Audience Mgmt, Create an Audience, Manage Segments, and User Mgmt. The main content area is white and includes a top navigation bar with 'Account_I', a date range '12/14/2022 - 02/08/2023', and a user profile 'Hi Admin'. The dashboard contains several key metrics: Open Requests (3), Total Requests (8), Daily Active Users (0, +20%), and Total Users (28, +30%). A 'Top Publishers List' table is shown with columns for Pub ID, Name, and Users, but it contains no data. A 'CRM Wise Users Data' section is partially visible on the right. At the bottom right, there is a blue 'UPGRADE NOW' button.

Account_I 12/14/2022 - 02/08/2023 Hi Admin

Open Requests 3

Total Requests 8

Daily Active Users 0 (+20%)

Total Users 28 (+30%)

CRM Wise Users Data

Top Publishers List

Pub ID ↑	Name ↑	Users ↑
Filter...	Filter...	Filter...
No data		

UPGRADE NOW

ATOS4P – CRM INTEGRATION

The screenshot displays the Mobiquity CRM integration dashboard. At the top, the account name is 'Account_1' and the date range is '12/14/2022 - 02/08/2023'. The user is identified as 'Hi Admin'. Three summary cards are visible: 'Total users' with a count of 30, 'Total Connected PII' with a count of 30, and 'Total Connections' with a count of 3. Below these is a 'Connections List' table with columns for Data Sources, Integration, PII Source, and Users. The table lists three data sources: Firebase (Enabled, PII Source checked, 10 users), Google (Disabled, PII Source -, 10 users), and Instagram (Enabled, PII Source checked, 10 users).

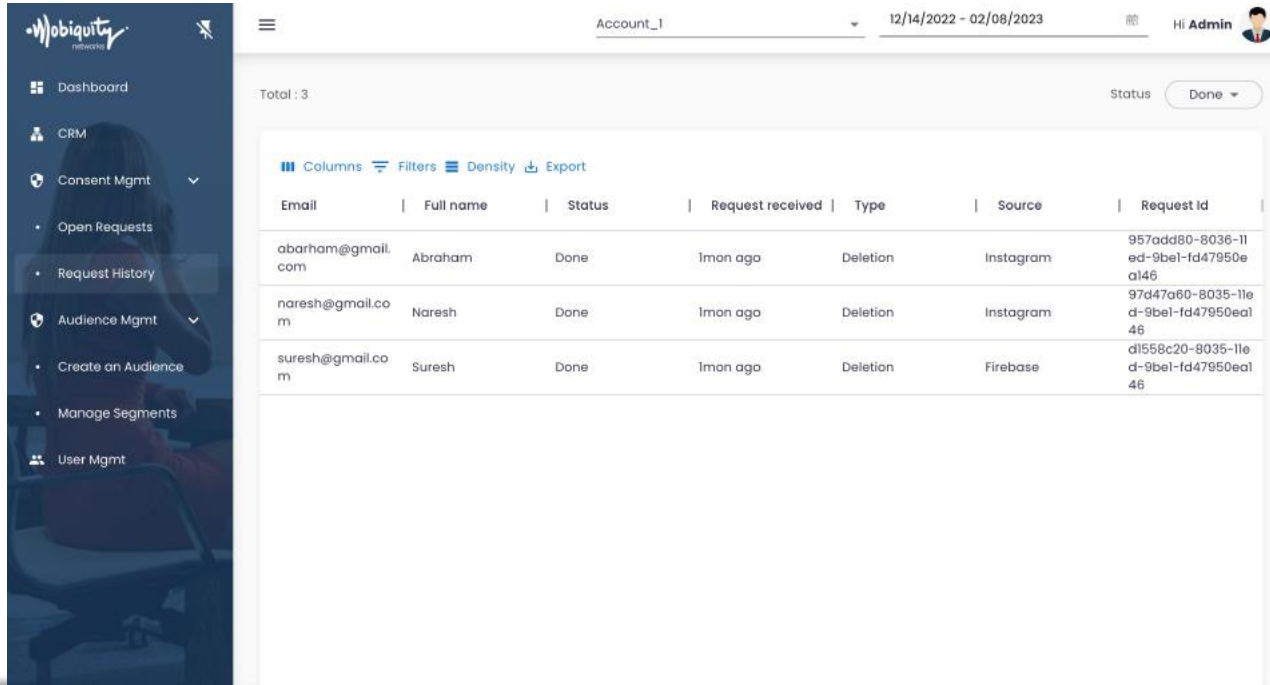
Data Sources	Integration	PII Source	Users
Firebase	Enabled	<input checked="" type="checkbox"/>	10
Google	Disabled	-	10
Instagram	Enabled	<input checked="" type="checkbox"/>	10

ATOS4P – REQUEST MANAGEMENT INTERFACE

The screenshot displays the ATOS4P Request Management Interface. On the left is a dark blue sidebar with the Mobiquity logo and navigation menu items: Dashboard, CRM, Consent Mgmt (with sub-items Open Requests and Request History), Audience Mgmt (with sub-items Create an Audience and Manage Segments), and User Mgmt. The main content area has a header with 'Account_1', a date range '12/14/2022 - 02/08/2023', and a user profile 'Hi Admin'. Below the header, it shows 'Total: 3' requests and a 'Status' filter set to 'Pending'. A table lists the requests with columns for Email, Full name, Status, Type, Request received, Source, and Request Id.

Email	Full name	Status	Type	Request received	Source	Request Id
chaitanya@gmail.com	Chaitanya	Pending	Deletion	1mon ago	Instagram	31a0e250-8036-11e4-d-9be1-fd47950eal46
james@gmail.com	James bond	Pending	Get a copy	1mon ago	Firebase	e48002cd0-8035-11e4-d-9be1-fd47950eal46
broad@gmail.com	Stuart broad	Pending	Get a copy	1mon ago	Instagram	f7bbb790-8035-11e4-d-9be1-fd47950eal46

ATOS4P – REQUEST LOGS FOR AUDIT TRAIL



The screenshot displays the Mobiquity dashboard interface. On the left is a dark blue sidebar with navigation options: Dashboard, CRM, Consent Mgmt (with sub-items Open Requests and Request History), Audience Mgmt (with sub-items Create an Audience and Manage Segments), and User Mgmt. The main content area is white and shows a table of request logs. At the top of the main area, it says 'Account_1' and '12/14/2022 - 02/08/2023'. Below this, it indicates 'Total: 3' and a 'Status' filter set to 'Done'. The table has columns for Email, Full name, Status, Request received, Type, Source, and Request Id. Three rows of data are visible, all with a status of 'Done' and a request received time of '1mon ago'.

Email	Full name	Status	Request received	Type	Source	Request Id
abarham@gmail.com	Abraham	Done	1mon ago	Deletion	Instagram	957add80-8036-11ed-9bel-fd47950ea146
naresh@gmail.com	Naresh	Done	1mon ago	Deletion	Instagram	97d47a60-8035-11ed-9bel-fd47950ea146
suresh@gmail.com	Suresh	Done	1mon ago	Deletion	Firebase	d1558c20-8035-11ed-9bel-fd47950ea146

ATOS4P – AUDIENCE MANAGEMENT PLATFORM

The screenshot displays the ATOS4P Audience Management Platform interface. On the left is a dark blue sidebar with the Mobiquity logo and a navigation menu including: Dashboard, CRM, Consent Mgmt, Open Requests, Request History, Audience Mgmt (with a sub-menu for 'Create an Audience'), Manage Segments, and User Mgmt. The main content area is white and features a top navigation bar with 'Account_1', a date range '12/14/2022 - 02/08/2023', and a user profile 'Hi Admin'. Below the navigation bar is a search bar and a form titled 'Enter a name for this Audience Segment' with an 'Enable this Segment' checkbox. The central part of the interface is divided into three columns. The left column, under a 'Location' dropdown, lists various geographic filters: Country, State, DMA (US Only), City, Zip, Counties (US Only), Congressional Districts (US Only), Polygons, Senate Districts (US Only), and Lat/Lon. The middle column, titled 'Users on which State should be included in this Audience Segment?', contains 'Countries' and 'States' dropdowns. The 'Countries' dropdown is set to 'United States (USA)'. The 'States' dropdown is set to 'Ohio (USA)' and 'Washington (USA)'. Below these is a world map with two red location pins on the US West Coast. The right column, titled 'Your Selection', shows a list of selected items: 'Country' with 'United States' checked, and 'State' with 'USA', 'Ohio', and 'Washington' checked. At the bottom right of this column is a blue button labeled 'SAVE THIS SEGMENT'.

ATOS4P – SEGMENT MANAGEMENT SYSTEM

Account_1 12/14/2022 - 02/08/2023 Hi Admin

SHOW ALL ACTIVE INACTIVE Create a new segment →

Columns Filters Density Export

Audience Name	ID	Account Id	Avg Id	Advertiser ID	Status	Action
Test Segment 2	873b6473-a715-7481-a56a-fb42d772be52	3	5	6	0	OPTIONS ▾
Nagarjuna	e81ec5ab-6439-dc02-6c28-e8403a182631				1	OPTIONS Menu ✎ Edit <input checked="" type="checkbox"/> Active 🗑 Delete
cv	ee0b6516-24d3-a6e7-40e5-50ffa3b2f41	45	22	58	0	OPTIONS ▾
fdfg	94dd4ed4-8c50-712c-74ed-8950e6d07440	10	1	7	0	OPTIONS ▾
fgg	19a494eb-6a5d-321c-b377-383ea555ae1	27	25	2	0	OPTIONS ▾
fgh	bd424601-4464-db83-1578-8d96580f5de1	12	35	5	0	OPTIONS ▾
ffgh	c9005ea8-01e9-9147-9ea1-2b9a4a9dfcf9	85	4	1	0	OPTIONS ▾
tyuty	13a6d2ae-aa26-6858-a38c-8ac3603c	25	71	5	0	OPTIONS ▾

Why would it matter to Advertisers?

1. **Legal requirements:** Advertisers must comply with privacy and data protection regulations, such as GDPR and CCPA, to avoid fines and legal repercussions.
2. **Consumer trust:** Advertisers who prioritize privacy and obtain informed consent from consumers are more likely to build trust with their customers.
3. **Better targeting:** By obtaining consent and collecting data in a transparent and secure manner, advertisers can target their campaigns more effectively and avoid wasting resources on ineffective campaigns.
4. **Reputation:** Non-compliant advertisers risk damaging their reputation and losing business due to negative consumer perceptions and potential media attention.
5. **Future-proofing:** Privacy regulations are constantly evolving and becoming stricter. By being proactive and compliant, advertisers can future-proof their operations and minimize the risk of falling out of compliance in the future.

Why would it matter to Publishers?

1. **Legal requirements:** Publishers must comply with privacy and data protection regulations, such as GDPR and CCPA, to avoid fines and legal repercussions.
2. **Consumer trust:** Publishers who prioritize privacy and obtain informed consent from consumers are more likely to build trust with their audience.
3. **Advertiser preferences:** Advertisers are increasingly demanding that their partners comply with privacy regulations, and publishers who can demonstrate compliance are more likely to attract high-quality advertisers and retain existing ones.
4. **User experience:** Publishers who prioritize privacy and obtain informed consent from their audience can provide a better user experience by respecting their audience's privacy and data protection rights.
5. **Reputation:** Non-compliant publishers risk damaging their reputation and losing business due to negative consumer perceptions and potential media attention.
6. **Future-proofing:** Privacy regulations are constantly evolving and becoming stricter. By being proactive and compliant, publishers can future-proof their operations and minimize the risk of falling out of compliance in the future.

Why would it matter to SSPs?

1. **Legal requirements:** Supply-side platforms (SSPs) must comply with privacy and data protection regulations, such as GDPR and CCPA, to avoid fines and legal repercussions.
2. **Advertiser preferences:** Advertisers are increasingly demanding that their partners comply with privacy regulations, and SSPs who can demonstrate compliance are more likely to attract high-quality advertisers and retain existing ones.
3. **Publisher preferences:** Publishers are also increasingly demanding that their partners comply with privacy regulations, and SSPs who can demonstrate compliance are more likely to attract high-quality publishers and retain existing ones.
4. **Data accuracy:** By obtaining informed consent from consumers, SSPs can ensure that the data they collect and use for advertising purposes is accurate and relevant, leading to more effective and efficient advertising campaigns.
5. **Reputation:** Non-compliant SSPs risk damaging their reputation and losing business due to negative consumer perceptions and potential media attention.
6. **Future-proofing:** Privacy regulations are constantly evolving and becoming stricter. By being proactive and compliant, SSPs can future-proof their operations and minimize the risk of falling out of compliance in the future.

Why would there be a potential revenue loss for Publishers?

1. **Decreased Inventory:** If a publisher fails to obtain the required consents from consumers for the use of their personal data, they may have to limit the amount of inventory available for advertising purposes, reducing their overall advertising revenue.
2. **Ad Blocking:** Consumers who have not given their consent for the use of their personal data may install ad blockers, reducing the reach and impact of advertising campaigns, and further reducing the publisher's advertising revenue.
3. **Reduced Advertiser Demand:** Advertisers may avoid publishers who cannot demonstrate compliance with privacy and consent regulations, reducing the demand for advertising inventory and lowering the publisher's revenue.
4. **Advertiser Fines:** Advertisers who work with non-compliant publishers may incur fines and legal penalties, which could further reduce the demand for advertising inventory and lower the publisher's revenue.
5. **Negative Reputation:** Publishers who are perceived as non-compliant with privacy and consent regulations may face negative media attention, damaging their reputation and reducing their overall revenue from advertising and other sources.
6. **Increased Compliance Costs:** Publishers who need to become compliant with privacy and consent regulations may face significant costs for the development and implementation of a consent management platform and the processes required for compliance.
7. **Improved User Experience:** By obtaining informed consent from consumers and respecting their privacy rights, publishers can improve the user experience, leading to increased traffic and engagement, and potentially, higher advertising revenue in the long run.