



Blockchain Solution for CCPA Compliance

Srinivasan Sundararajan

VP & Head, GAVS Blockchain CoE

Sri Chaganty

Chief Technology Officer

What is CCPA?

The California Consumer Privacy Act (CCPA) is a state statute intended to enhance consumer protection and data privacy rights of the residents of California, United States. It is widely considered one of the most sweeping consumer privacy laws, giving Californians the strongest data privacy rights in the U.S.

Any individual, irrespective of nationality, who qualifies as a California resident per the CCPA definition is covered under this law. CCPA empowers individuals who continue to meet the California residency requirements, with lifetime rights to ownership, control and security of their personal information and imposes new responsibilities on businesses:

- Consumers to be treated as owners of their personal information, under all circumstances
- Consumer consent, opt-in/out and delete mechanisms to be provided for data collection, its usage, sharing and/or monetization
- Complete transparency to honour fundamental consumer right to know every detail on the what and how of collection, usage, sharing and selling of their personal data
- Non-discrimination in terms of price or service irrespective of CCPA rights they may have exercised
- Privacy policy to be updated based on CCPA's requirements and made publicly available

Is it applicable to my organization?

CCPA is applicable to any for-profit organization, regardless of its physical location, that interacts with, does business with and/or collects, processes or monetizes consumer data of California residents, and meets one or more of the criteria below:

- Has gross annual revenue in excess of \$25 million USD
- Deals with the personal information of 50,000 or more California consumers, households, or devices
- Earns 50% or more of its annual revenue by monetizing such data

Why is it important for my organization to comply with CCPA?

In the increasingly complex digital landscape, data privacy and security have become major areas of concern across the globe. Legislations like GDPR (Europe) and CCPA (USA) provide a legal framework to rein in businesses that exploit consumer data and give back to consumers true control over their personal data and establish digital trust.

- Increasing occurrences of data breaches and consumer privacy violations make digital trust a major challenge. Total compliance will involve careful planning and execution for lifetime maintenance
- Organizations could find themselves embroiled in lawsuits and/or face monetary penalties if they are not careful about data security and compliance, since CCPA empowers consumers to sue the errant business, if their personal information is used without consent, or stolen due to a data breach
- Of course, any organization that truly complies with privacy laws like CCPA & GDPR in letter and spirit, and respects the consumer as the sole custodian of their data, will stand to gain their trust and goodwill

Consent Management

The first and foremost action item for an organization aiming for compliance with data privacy laws is to understand where and how they store the personal data of their customers (the terms customer and consumer are used interchangeably in this document). They should also have a thorough strategy in place to manage consumer consent. Consent management is responsible for managing consumers' consent generation, updates, withdrawals and data disposal mandates.

Blockchain Technology for Consent Management

Most Data Privacy solutions in the market help prove compliance to consumers and authorities, but are not comprehensive enough to achieve the real intent behind these legislations. In this context, **Blockchain-based Consent Management is emerging as a True Platform** to empower the consumer with full control over their personal information.

Blockchain is a disruptive technology similar to the Internet in how it is dramatically transforming the way businesses transact with one another and with the consumers. Blockchain technology supports the integrity, the non-repudiation and the versioning of consents in a public verifiable way without any trusted parties. Blockchain based solutions provide trust improvement and immutability due to impossibility of falsification.

Blockchain is a distributed ledger that consists of cryptographically signed, irrevocable transactional records, based on shared consensus among all participants in the network. A blockchain is intrinsically decentralized and consensus-based, and every transaction is signed by the transaction owner's cryptographic keys, and so it is perceived as the best way to ensure ownership of consumer private information.

Master Data Management (MDM) methodology is the industry-standard to consolidate multiple sources of master data and create a single version of truth. While MDM enables organizations to create a golden master record per consumer from the varied data sources, it has to be extended with consent management features to enable the consumer to truly own their data and exercise options like *Do Not Sell* or *Delete*. A golden record represents a unified and cleansed view of many disparate sources of information.

With the powerful combination of cryptography-based Master Data Management and Consent Management capabilities of Blockchain, organizations can provide robust data protection to their consumers. This approach overcomes the limitations of other data privacy solutions and safeguards the business and its consumers with comprehensive data privacy and security.

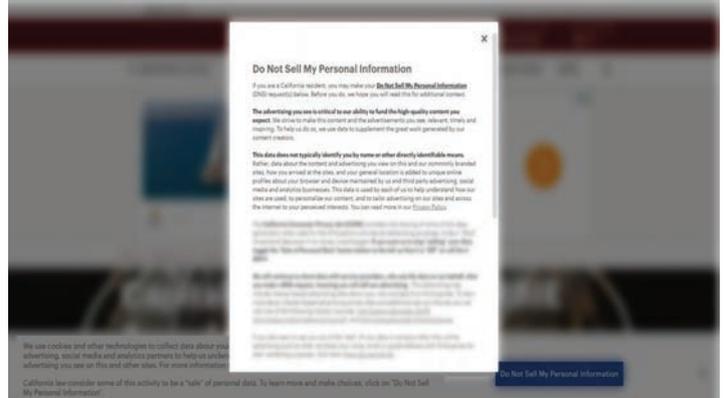
Limitations of Current Solutions for Consumer Consent Management

Existing solutions claiming to provide consent management (governance, granularity, traceability) show less suitability due to several disadvantages like:

- Consent applicability limited to the particular application/website/company providing the solution
- Consents not shareable across applications and/or information systems

- Consents not auditable by third parties
- Respect for privacy in "all or nothing" mode

Most quick-fix solutions provide a customized cookie banner with a *Do Not Sell My Info* link to get consumer preference (as seen in the image below).



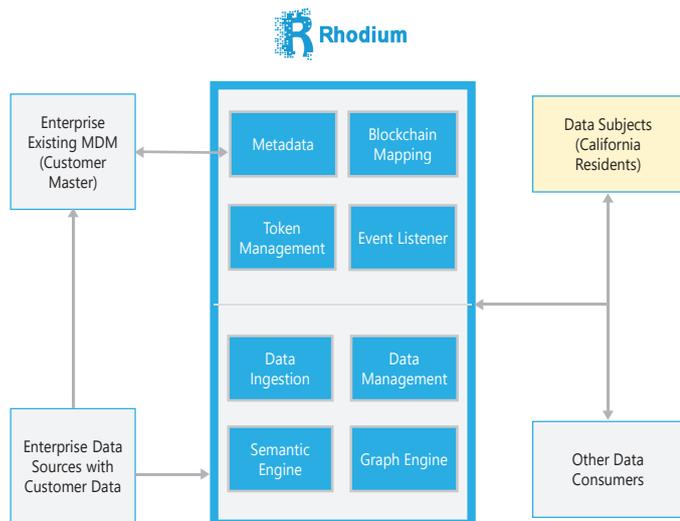
While the cookie banner solution is an easy workaround, it has the following limitations:

- Since websites are not the only points of consumer data capture, this is a partial solution that does not take care of the myriad other ways data could be obtained
- The cookie banner will accept consent from any website user and the true identity of the end user may not be verifiable unless they have a password-protected account with the business
- Even if user identity is verified, this solution does not prevent a data breach that exposes confidential information, hurting the consumer and the business in the process

GAVS' Rhodium Framework for CCPA Compliance & Extended Customer Data Management

Given the limitations of current market solutions for data privacy and also the organizational need to consolidate customer data from multiple business entities into a single golden record, GAVS addressed the problem with a blockchain based solution. The data owner can manage consent with precision & granularity. He can grant read/write access and specify duration of consent validity for each user he wants to give access to. Also, the consent management function is shareable across applications.

GAVS' Rhodium Customer MDM & CCPA Compliance Solution



PATENT PENDING - <201941046426>

GAVS' Rhodium Framework (patent pending) for Customer Master Data Management and Compliance with Data Privacy Laws like GDPR and CCPA:

- Enables consolidation of multiple customer data sources and links them to a golden record, while still maintaining the respective business entity's ownership of the data
- Provides cryptography-based access to end consumers and allows them to truly own their personal information and exercise options like Do Not Sell, Delete, Opt-in and Opt-Out
- Has extensions to monetarily compensate consumers for access to their data
- Enables organizations to accommodate consumer relationships like family, friends, and co-workers in data privacy options

- Provides rich features like Match and Merge, to perform core MDM functions like duplicate record identification & elimination using semantic search, and cleansing of incorrect data
- Stores meta data, and immutable audit trail augmented with analytics to provide complete transparency, lineage and traceability of consumer master data and data privacy related interactions

In Conclusion

Gartner has identified Transparency and Traceability as one among the top 10 strategic technology trends in their research paper on Technology Trends for 2020. According to Gartner:

- Consumers are increasingly aware that their personal information is valuable and consequently demanding control
- Organizations recognize the risk in managing and securing sensitive personal data
- Governments are implementing stricter legislations to ensure compliance. Transparency and Traceability are critical elements that stop the encroachment and support today's digital ethics and privacy needs

GAVS' Rhodium Framework (patent pending) is one of the earliest attempts to utilize the power of Master Data Management and Blockchains. This technology-led solution will truly empower organizations to be in total compliance with legislations like GDPR and CCPA and also go a few steps further in doing what is ethically right – provide all-encompassing protection for their consumers' data.

About GAVS

GAVS Technologies (GAVS) is a global IT services & solutions provider enabling digital transformation through automation-led IT infrastructure solutions. Our offerings are powered by Smart Machines, DevOps & Predictive Analytics and aligned to improve user experience by 10X and reduce resource utilization by 40%.