CCPA Compliance made easier with Oomnitza

As new data regulations roll out, compliance has become a top priority for management of companies storing consumer data. For many executives making sure their organization is California Consumer Privacy Act (CCPA) compliant is on the top of their to do list. With CCPA's January 2020 implementation date quickly approaching organizations must adapt promptly to its new regulations. CCPA poses new challenges establishing California consumer rights including personal data request, erasures and opt-outs from organizations holding their personal information.

The scope of this regulation reaches far beyond businesses physically located in California but instead, any company that stores personal data of California consumers. The act also sets a new standard in security standards requiring IoT devices carrying personal information to be encrypted to prevent data breaches. Without an efficient way of managing and locating data carrying IoT devices as well as ensuring their encryption compliance with CCPA can be a difficult task for organizations with thousands of IT assets.

CCPA continues the trend for stronger consumer data protection regulations initiated by the European Union's General Data Protection Regulation (GDPR). As CCPA lurks in the near future and consumer data protection expansion shows no sign of slowing down, the importance of effective asset management for organizations continues to grow. Oomnitza's asset management platform makes CCPA compliance easier bringing visualization, centralization and automation to IT asset management.

With Oomnitza CCPA Compliance can be made easier by:

- Providing a single platform locating all data carrying IoT devices allowing for complete data request, erasures, and opt-outs.
- Establishing a centralized record of each asset's assigned user, installed software, and service tickets over its lifetime.
- Ensuring data carrying assets are encrypted giving organizations the confidence all IoT assets have the necessary security parameters in place.
- Automating workflows to notify when potential security risk occur. By utilizing integrations and workflows IT departments can be alarmed when a device may be unsecured or accessed by an unauthorized user.