SOLUTION BRIEF

CALIFORNIA CONSUMER PRIVACY ACT

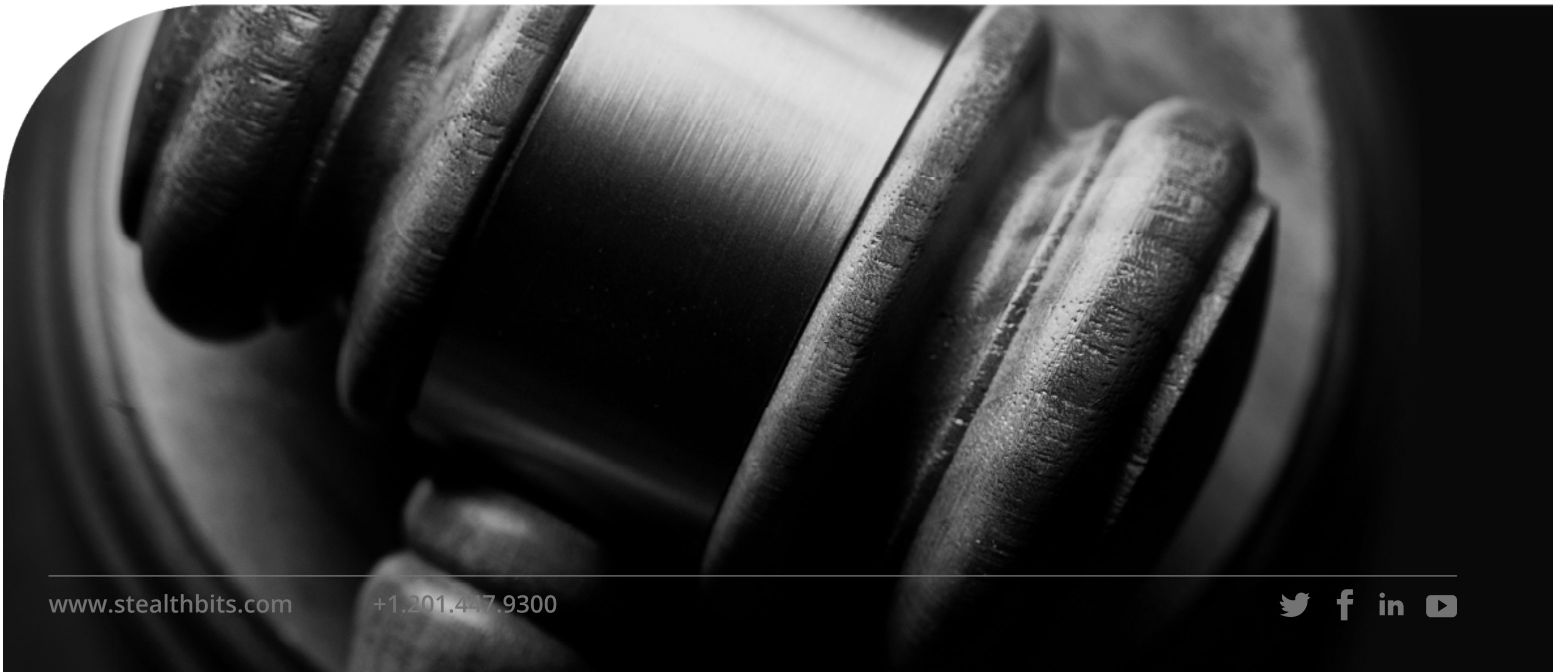
The California Consumer Privacy Act (CCPA) was designed to protect California consumers' data privacy, and reshape the way organizations doing business in the state approach "The Right to Deletion" frequently referred to as The Right to be Forgotten. The legislation – the first of its kind nationwide – aligns relatively closely with the European Union's General Data Protection Regulation (GDPR), and will require for-profit organizations to be compliant with the legislation by July 1, 2020 – with some impacts being felt sooner than that.

Under the CCPA, many for-profit organizations are required to:

- Notify consumers of the type of personal information being collected about them, what that information is being used for, and whether that information is being sold to third-parties
- Provide a public way, via their website or a toll-free number, for consumers to opt-out of the collection of their personal information
- Provide a listing of personal information collected in the past twelve months upon request

In most data driven companies, customer information is shared widely between departments and stored in a variety of databases, files shares, employee workstations and cloud storage, making it difficult to get a complete list of all privacy data throughout the organization. In order to comply with CCPA requirements, Stealthbits provides a range of capabilities that allow customer to identify, secure and report on privacy data. Features such as:

- **Host Discovery** to identify the different platforms within the network that may contain various unstructured and structured data repositories to ensure a comprehensive view of your organization's privacy data footprint
- **Sensitive Data Discovery** capabilities that analyze content for patterns or keywords that match built-in or customized criteria related to customer privacy
- **Remediation Actions** that automate all or portions of the tasks you need to perform to demonstrate compliance with CCPA and a myriad of other regulatory standards



PERSONAL DATA

The CCPA defines nonpublic information as, “information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household”. This definition includes Social Security numbers, drivers’ license numbers and, purchase histories, as well as unique personal identifiers such as device identifiers and other online tracking technologies. Stealthbits can help:

- Automatically discover where unstructured and structured data exists across your network
- Examine the contents of 400+ file types (including images using OCR) stored within Network File Shares, SharePoint Sites, Cloud Storage platforms, and Exchange, as well as Oracle and SQL Server databases
- Leverage over 350 preconfigured criteria sets aligning to Personally Identifiable Information (PII)
- Clean-up stale files that no longer need to be managed or maintained to reduce overall data scope and risk
- Classify (tag file metadata) and/or move, delete, modify permissions, and integrate with other technologies to automate manual processes

DATA PRIVACY

The CCPA grants consumers, “various rights with regard to personal information relating to that consumer that is held by a business”, and requires businesses to, “*implement and maintain reasonable security procedures and practices*” to do so. Stealthbits can help:

- Understand access rights, permissions, activity, data sensitivity, ownership, and file metadata across unstructured and structured data sources
- Automatically implement a least privilege access model, ensuring access rights and permissions are limited to only what users need at all times
- Monitor and secure Active Directory to prevent unauthorized access to data resources and mitigate risks associated with account compromise and privilege escalation
- Maintain a full, searchable audit trail of all file access activities, Active Directory changes, account authentications, and more for forensic investigations and auditors

BREACH NOTIFICATION

Under the law, medical information or protected health information that is collected by a covered entity or business associate must follow the breach notification rules issued by the United States Department of Health and Human Services. Stealthbits can help:

- Detect and alert on abnormal user behavior, suspicious activities, and attempts to compromise account or data security in real-time
- Integrate with existing SIEM solutions for consolidated alerting and advanced correlation with other network technologies

NEXT STEPS

To learn more about how Stealthbits’ solutions can help you achieve compliance with The California Consumer Privacy Act, contact us at https://www.stealthbits.com/contact.

Schedule a Demo

stealthbits.com/demo

Download a Free Trial

stealthbits.com/free-trial

Contact Us

info@stealthbits.com