ZIMPERIUM®

CCPA & Mobile Devices

The Facts About Mobile Security & Compliance

Fact #1: CCPA has included mobile since the day it took effect in 2020

Enterprises conducting business in California should be familiar with the California Consumer Privacy Act of 2018 (CCPA). Although it differs from the EU General Data Protection Regulation (GDPR), CCPA has been characterized as "the beginning of America's GDPR," enhancing privacy rights and consumer protection for residents of California. Businesses subject to CCPA must meet strict requirements relating to the use and protection of their customers' personally identifiable information (PII).

It is important to note that CCPA requirements apply to mobile. This is vital because mobile is near-universal in today's enterprises, and mobile apps are a significant conduit for PII. With trends in mobile technology such as incorporating wearables, IoT and apps to stream real-time personal data about the user, apps pose tremendous challenges to CCPA compliance for enterprise mobile app developers.

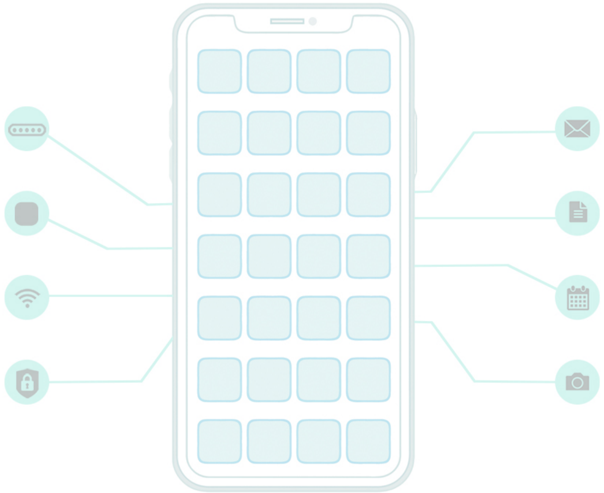
In short, if your CCPA compliance measures do not include protecting mobile devices and apps, you will be out of compliance.

Fact #2: Mobile devices are 60% of CCPA-covered endpoints

In preparing for CCPA compliance, businesses may invest significant resources to attain the level of governance of, and control over, consumer data that will enable them to meet CCPA requirements. Problems will arise if enterprises focus on protecting endpoints without realizing that **mobile devices are endpoints**, both with respect to CCPA and in general.

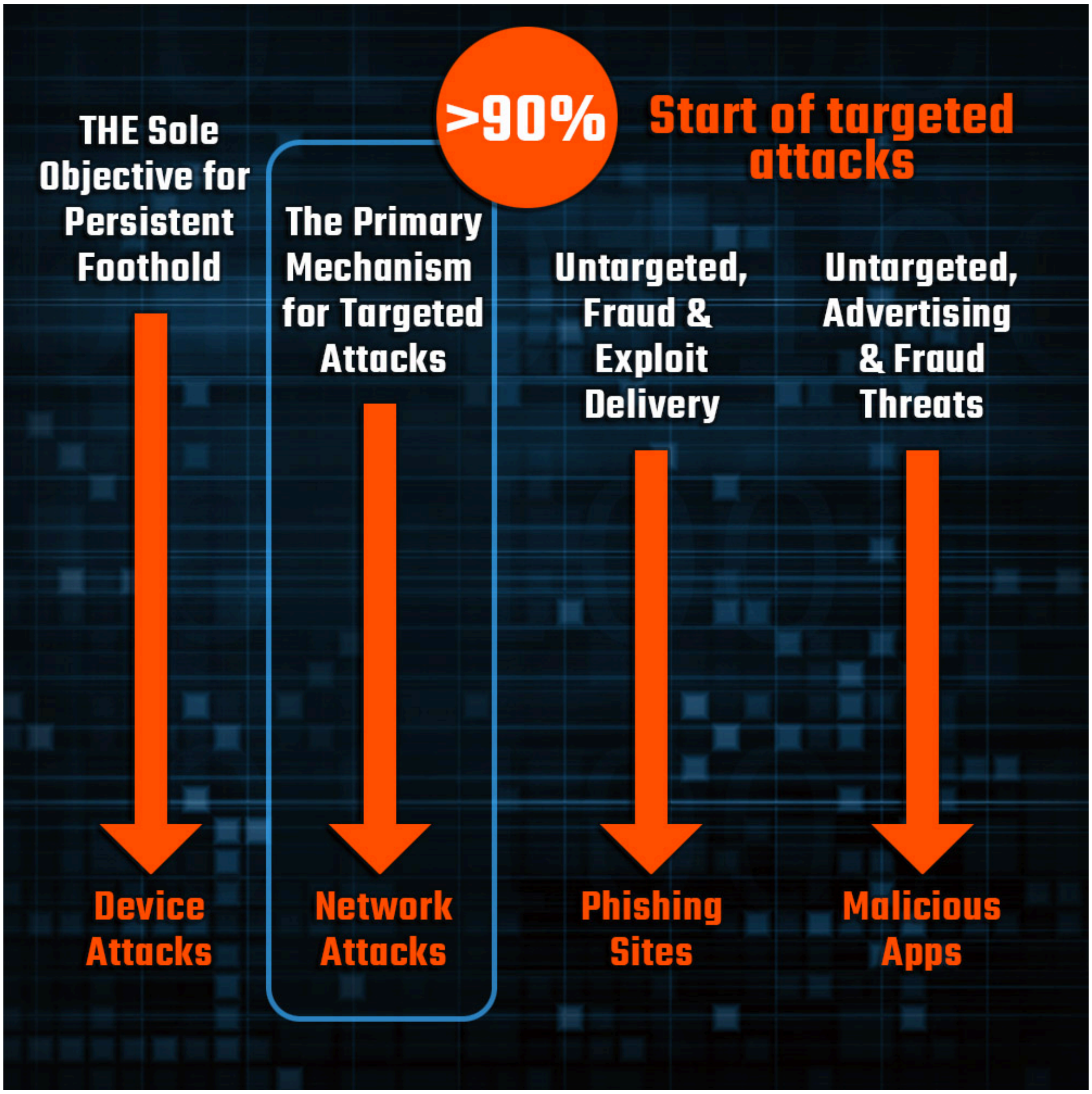
Mobile devices are now the de facto platform for productivity in business. That means that the traditional computing devices (e.g., servers, desktops and laptops) on which enterprises have focused their security and compliance efforts are only about 40% of their enterprise's endpoints.

The other 60% of devices that connect to enterprise networks—mobile devices—must be made CCPA-compliant as well. This is particularly difficult to monitor on mobile apps residing on mobile devices, since personal data gathered via mobile apps includes functions users do not monitor, such as geolocation data, audio, electronic, visual, thermal, olfactory, or similar information.



Fact #3: Mobile endpoints are under attack

One critical difference between mobile devices and other types of endpoints is the variety of attack vectors that mobile devices are exposed to. Ensuring the integrity of mobile devices requires protecting them against all of these forms of attack.


>90%
Start of targeted attacks
THE Sole Objective for Persistent Foothold
The Primary Mechanism for Targeted Attacks
Untargeted, Fraud & Exploit Delivery
Untargeted, Advertising & Fraud Threats
Device Attacks
Network Attacks
Phishing Sites
Malicious Apps

Fact #4: CCPA requirements apply to mobile

CCPA requirements apply to any mobile apps that hold or gather personally identifiable information (PII) on California users.

The danger of unauthorized exfiltration of PII from mobile apps is real and continuously evolving. No longer just an imaginary capability in popular spy movies and thrillers, there are documented cases today of mobile malware that can and does turn on the victim's cell phone camera and microphone without the user's knowledge.

Protecting PII is fundamental to CCPA compliance, and failing to do so may subject a business to a penalty of up to **$7,500 for each violation**.

Fact #5: Zimperium is the solution for CCPA mobile compliance

Zimperium provides an SDK that ensures that your enterprise's mobile applications remain safe from cyber attacks by providing immediate device risk assessments and threat alerts. Organizations can minimize exposure of any PII, and prevent their customers and partners' data from being jeopardized by malicious and fraudulent activity.

Mobile app developers can simply embed its engine within applications by using an easy-to-implement software development kit that works with common development platforms. This enables mobile app protection against cyber attacks. To safeguard PII, such as customer/partner transactions, developers can implement custom auto-response workflows with the intelligence injected into the application.

To date, the engine has detected 100 percent of zero-day device exploits found in the wild without requiring an update or suffering from the delays and limitations of cloud-based detection or legacy security architectures. This makes Zimperium uniquely capable of meeting CCPA mobile requirements.

When you are ready to ensure compliance with CCPA mobile requirements, please contact us for a custom evaluation.

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244

Fact #5: Zimperium is the solution for mobile HIPAA compliance

Zimperium leverages a patented, machine learning-based engine to detect mobile device, network, phishing and app attacks in real time. The engine runs efficiently on smartphones and tablets without violating user privacy. To date, it has detected 100 percent of zero-day device exploits without requiring an update or suffering from the delays and limitations of cloud-based detection or legacy security architectures, making Zimperium uniquely capable of meeting HIPAA mobile requirements.

Mobile apps containing and processing patient data must be secured against attacks as well, even on patient-owned devices. Zimperium has the solution.

Contact Zimperium for HIPAA mobile compliance

When you are ready to ensure compliance with HIPAA mobile requirements, please contact us for a custom evaluation.

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244