AppCensus

www.appcensus.io

sales@appcensus.io

Do you know whether your privacy policy correctly describes your mobile app's behavior?

Do you know if your app engages in behaviors that might violate various privacy laws, such as GDPR, COPPA, CalOPPA, and CCPA?

AppCensus knows.

In the past year, data from AppCensus has been cited in a half a dozen state and federal privacy lawsuits.

AppCensus allows:

- Enterprises to monitor and regulate the privacy behaviors of mobile apps on their networks
- App developers to detect app privacy issues before releasing those apps and becoming liable for them
- Regulators to detect bad actors and gather evidence against them
- Compliance organizations to confirm that app behaviors comply with disclosures and applicable regulations
- Consumers to learn about the privacy practices of the apps that they use

The Team:

AppCensus was founded by thought leaders in the privacy, security and networking domains, including **SERGE EGELMAN**, **NATHAN GOOD** and **NARSEO VALLINA-RODRIGUEZ** of the International Computer Science Institute and the University of California at Berkeley, **JOEL REARDON** of the University of Calgary, and team members from Amazon, Pinterest and Smyte (now Twitter). We're based in San Francisco and provide privacy protection products, as well as privacy-analysis-as-a-service, at scale.

The AppCensus Difference

AppCensus is the only system that can handle the scale of evaluating hundreds of thousands of apps for privacy leaks automatically and with high accuracy

AppCensus is already being used by regulators to detect violations of various privacy regulations, including COPPA, GDPR, and CalOPPA

AppCensus has been used to detect and report privacy and security violations in thousands of existing apps, for which it has received bug bounties from Google and Facebook

Our team includes a unique mix of leading experts in Privacy, Security, User Experience and Networking

Our team has deep experience detecting and countering the methods app developers use to hide privacy violations

AppCensus has already evaluated a large percentage of apps in the Google Play Store, and we are glad to do custom evaluations of new apps or apps of special concern

www.appcensus.io

sales@appcensus.io

This is an extraordinary time for privacy.

The popular media is awash with accounts of large-scale violations and unsavory business practices by mobile apps and platforms. Regulators and plaintiffs' attorneys have responded by filing lawsuits against app developers and third-party services. Meanwhile, consumers are left confused and upset about widespread abuses of their personal information.

And why wouldn't they be?

Prior to AppCensus, usable tools to provide actionable insights into app privacy behaviors simply did not exist.

To address this, AppCensus has built a scalable system to do automatic static and dynamic analysis consisting of:

- on-demand app testing via API or through the web-based dashboard, allowing developers to identify privacy issues in their apps prior to releasing those apps
- an instrumented version of Android to monitor precisely when apps attempt to access sensitive user data and with whom they share it
- a searchable database of the privacy behaviors of hundreds of thousands of apps, allowing enterprise customers to gain insights into the privacy risks faced by their employees and consumers
- custom network-monitoring tools that allow for the detection of exfiltrated user data
- APIs to allow Mobile Device Managers (MDMs) to query the data they need to apply policies

How It Works

1 Examine App Binaries

AppCensus performs static analysis of what sensitive data an app's code might access, and then goes beyond existing tools by observing whether it actually does so in practice.

2 OS Instrumentation

AppCensus performs dynamic analysis to monitor what apps actually do, including accessing personal data through unofficial non-API mechanisms like the filesystem, the use of Java reflection, or native code and libraries.

3 Human Automated Testing

AppCensus operates the app to observe its real behaviors. Humans can make sure specific complex interactions are tested, while automation lets us test app behaviors at scale.

4 Deep Packet Inspection

AppCensus examines all inbound/outbound dataflows to detect the presence of sensitive data. Our analysis results are being used by regulators and platforms to identify bad actors.

5 We Provide Results

AppCensus provides results via our dashboard, in bulk through our API, or custom reports.

Whether you're a regulator, an app marketplace, an app developer, a privacy or compliance consultancy, a privacy-aware consumer, or an enterprise with a fleet of mobile devices, you'll find unique insights and value in AppCensus's data and products.

AppCensus