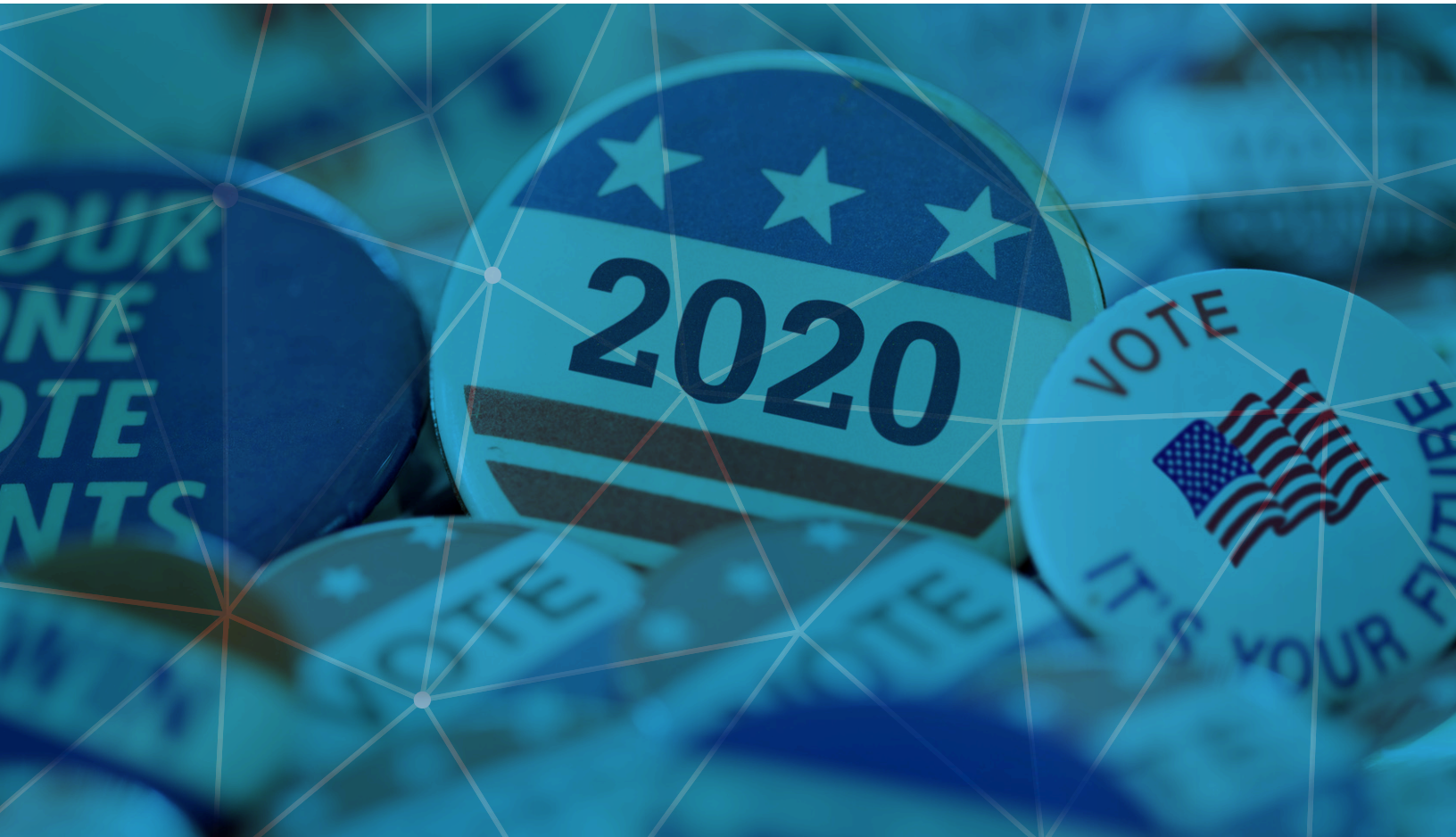
RISKIQ®

2020 Election Mobile App Landscape Report

An Analysis of Infringing and Official State Election Apps



Today's elections are almost entirely digitized. Many voters can register to vote, research candidates and issues, update their information, and even cast their ballots without ever touching a piece of paper. The Help America Vote Act and measures to counter the dangers of COVID-19 significantly accelerated the adoption of new election technology.

One of the overarching results of this hastened departure from traditional polling mechanisms is the impact mobile applications now have on the election process. Official mobile apps developed by states and other informational apps enhance the voting process and make it easier for citizens to exercise this constitutional right. However, these apps also present an opportunity for threat actors to create fraudulent apps that fool voters to spread misinformation or steal data to impersonate a vote.

Official election mobile apps are typically published to official stores, such as the Apple App Store or Google Play Store, by state election officials and distributed to the constituency through various mediums on behalf of the state election authority. However, the mobile landscape is getting bigger, busier, and more complex by every measure, making it easier than ever to develop and hide malicious apps. RiskIQ cataloged 18% more apps in 2019 than in 2018.

RiskIQ analyzed[1] 128 app stores and 40 million mobile applications worldwide to uncover how widespread infringing election mobile apps are. Infringing apps often claim to be official and even mimic official state election apps but were likely not approved by the State or election authority.

State	Record Count
Louisiana	35
California	34
Tennessee	24
North Carolina	14
Ohio	14
Georgia	11
Alabama	11
New Jersey	8
Indiana	7
Conneticut	7
Montana	7
Pennsylvania	5
Rhode Island	4
South Dakota	2
Arizona	2
Wisconsin	1

Fig 1 - A complete list of election mobile apps analyzed by RiskIQ

Of the 186 total election apps, our systems surfaced 152 unauthorized applications comprising 16 state elections. Of these, at least 16 apps were noted for exhibiting malicious[2] activity, showing election applications are an attractive target for threat actors who may try to disrupt

[1] RiskIQ observes and categorizes the threat landscape as a user would see it, monitoring both the well-known stores like the Apple App Store and Google Play as well as more than 128 others around the world. RiskIQ also leverages daily scans of nearly two billion resources to look for mobile apps in the wild. Every app we encounter is downloaded, analyzed, and stored to record changes and new versions.

[2] Malicious apps are defined as having sufficient permissions, demonstrating activity, or linking to resources that could spy on users, harvest information, phish them, or install malware on the user's device.

and misinform American voters.

This report highlights the distribution of these infringing apps across stores, the types of stores that host them, and the countries in which these apps can be found. It also offers guidance on how voters can avoid them and ensure the apps they're using are legitimate leading up to election day.

Types of Election Mobile Apps

Official voting apps provide constituents with a convenient way to access election information. While no states offer the ability to vote through a mobile app—Colorado and West Virginia both ended these programs—voters can register to vote, update registration information, and track mail-in-ballots. However, almost all the election apps examined in this research provide critical information on voting processes, and if modified, could be a vector for disinformation and voter suppression.

These are the capabilities purported by the 186 apps across the election mobile app landscape:

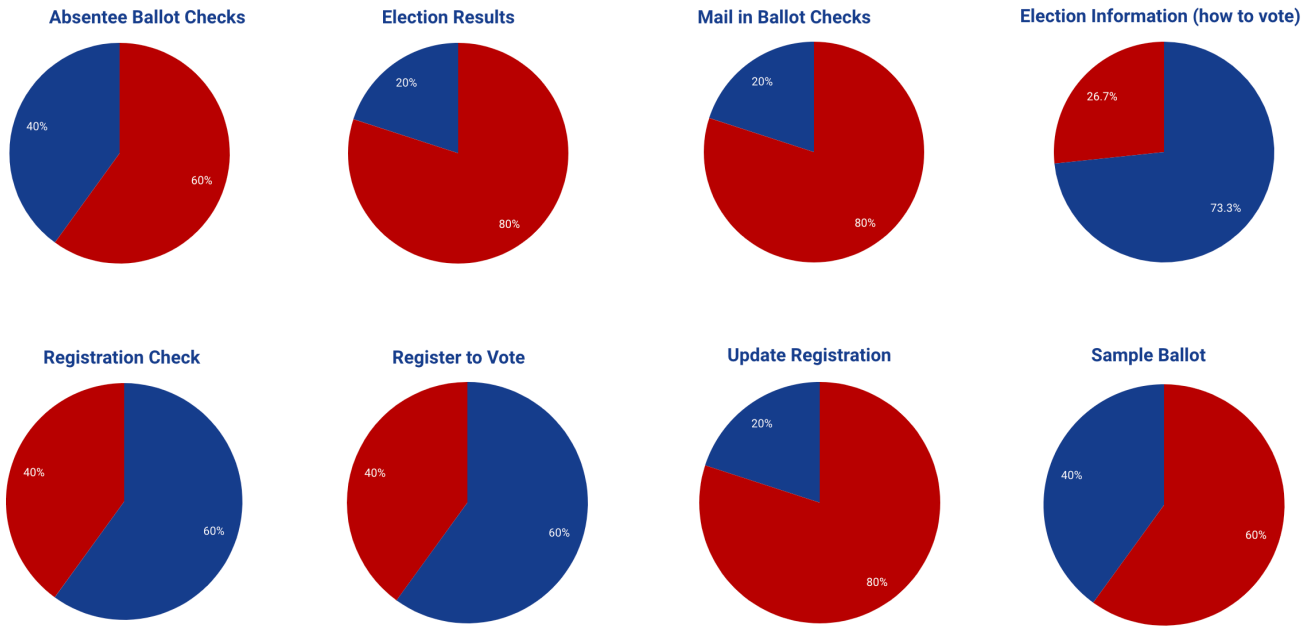


Fig 2 - Election apps by voting function. Blue indicates the functionality is provided by an app; red, indicates the functionality is not.

Mobile App Store Distribution

Mobile applications are dispersed across any number of different app stores without the state's explicit permission. There are four primary store types with varying implications for an app's legality - official, affiliate, hybrid, and secondary. Applications found in official stores such as the Apple App Store, the Google Play Store, and Samsung Galaxy Apps Store are almost

always official and legitimate. These stores present the lowest risk for malicious apps.

However, hybrid stores (stores built on several architectures) and secondary stores host apps operating in unofficial capacities and likely never receive versions directly from the original developer. Worse, these stores often do not monitor how a developer adds an app or whether the apps it hosts have been modified in malicious ways. The lack of monitoring and security controls make it the perfect place for threat actors to store their infringing apps.

Below are the distribution of the 186 election by type of store across the mobile app landscape:

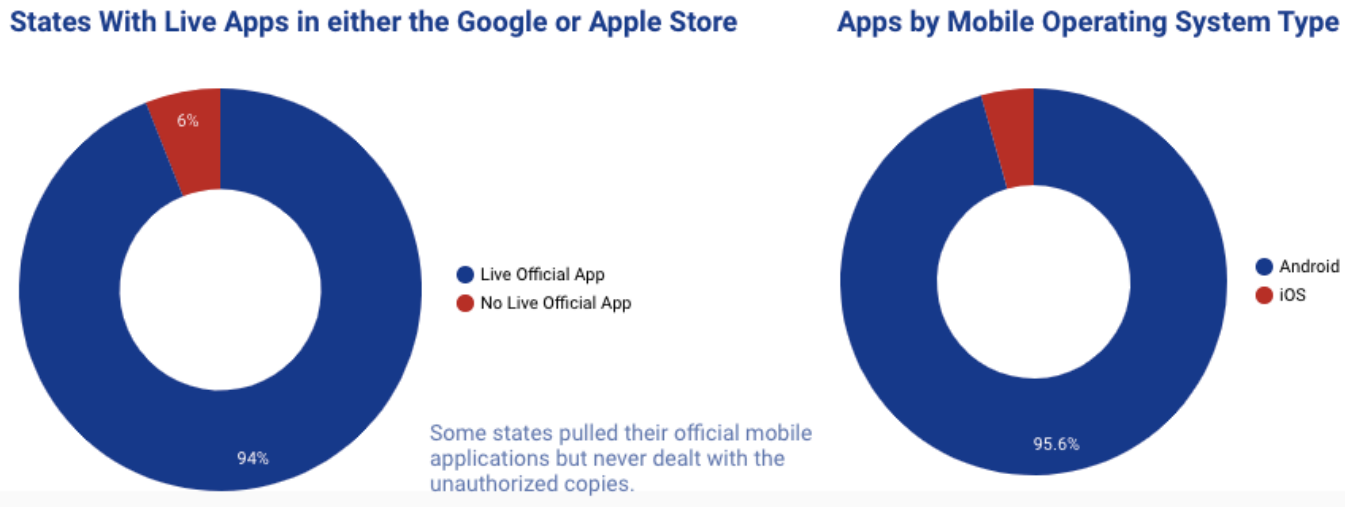


Fig-3 - Election by operating system

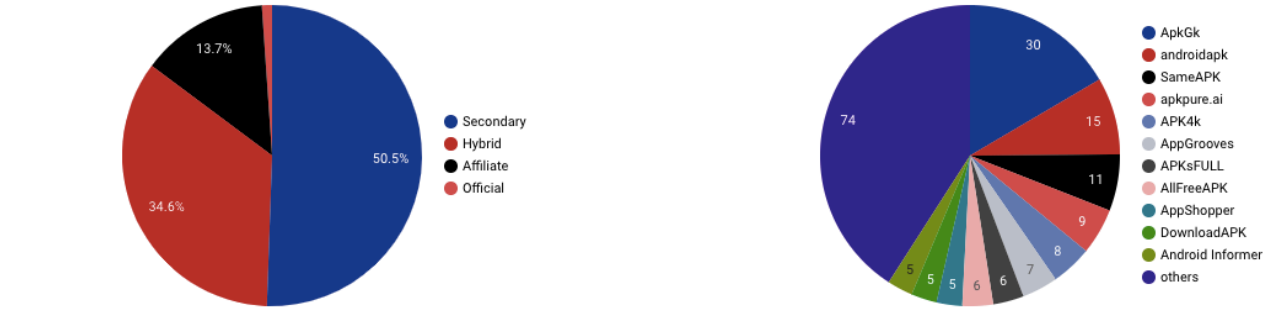


Fig-4 - Election apps by app store

Infringing Apps by Country of Origin

App stores are distributed across the world, subject to the country's laws and regulations in which they're hosted. As such, applications weaponized in foreign countries can prove more challenging to take down than in the United States.

The 152 infringing apps uncovered in this research spanned 12 different countries, including the United States, Hong Kong, Canada, Panama, China, Vietnam, the Netherlands, Denmark, United Arab Emirates, Portugal, and Spain. The 16 apps modified[3] from their original version and considered malicious came from app stores in Hong Kong (GA, NC), China (LA, IN, CT), Ethiopia (LA), Spain (LA), and Romania (LA).

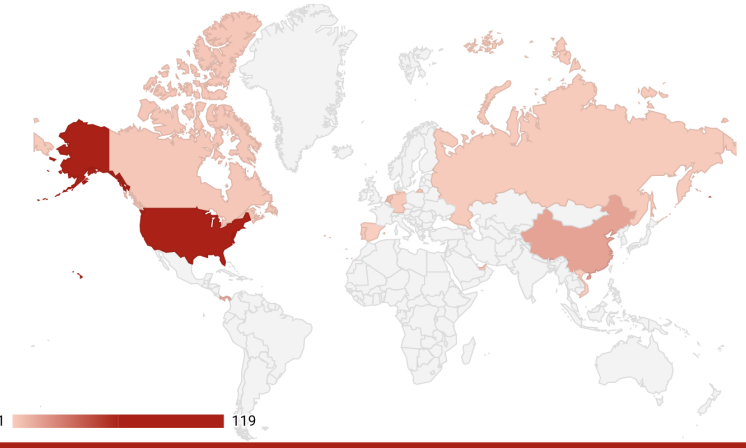
Below is where each infringing mobile app uncovered in our research is dispersed worldwide:

2020 Election Mobile Application Landscape

App stores are distributed across the world where they are subject to different laws and regulations. Applications weaponized in foreign countries can prove more difficult to take down than in the United States.

Apps by App Store County of Origin

US	87
HK	17
CN	14
PA	10
NL	5
AE	5
CA	3
PT	2
RU	2
DE	1
ES	1
VN	1



Malware Hits by County

HK	13
CN	3
AE	0
ES	0
PA	0
PT	0
VN	0
null	0
DE	0
RU	0
CA	0
NL	0

State / Record Count

Country	California	Louisiana	Tennessee	North Carol...	Ohio	Alabama	Georgia	New Jersey	Conneticut	Indiana	Montana
US	28	18	15	4	12	11	5	6	4	6	3
HK	-	5	-	7	-	-	4	1	-	-	-
CN	1	1	3	-	-	-	2	-	2	1	2
PA	-	4	1	3	1	-	-	-	-	-	-
NL	1	1	1	-	-	-	-	-	1	-	-
AE	1	1	1	-	1	-	-	-	-	-	1
CA	2	1	-	-	-	-	-	-	-	-	-
PT	1	-	-	-	-	-	-	1	-	-	-
RU	-	1	1	-	-	-	-	-	-	-	-
DE	-	-	1	-	-	-	-	-	-	-	1
ES	-	1	-	-	-	-	-	-	-	-	-
VN	-	-	1	-	-	-	-	-	-	-	-

Fig-5 - Infringing election mobile apps by geographic location

3 A portion of the total apps discovered were analyzed in depth and may not reflect the full scope of all modified applications.

Voter Guidance

Here are five ways to avoid downloading these dangerous apps and be confident the app you're using is legitimate.

Use official election apps published in major app stores: While some third-party mobile apps are safe—and some even contain more information than the state's official app, the vast majority of malicious applications observed by RiskIQ are hosted on third-party app stores. If you choose to download apps published outside of official app stores, be sure to follow the guidance below.

Be wary of suspicious permissions: Excessive permissions like access to contacts, text messages, administrative features, stored passwords, the phone camera, or credit card info are strong indicators of threat activity. Be sure the permissions requested in the app you're using match its function.

Know who is making your apps: Conduct an in-depth look at each app and ensure the Secretary of State or the state's election authority is listed as the app's developer. Some states may leverage consultants for app development, always validate developer information in those instances. New developers, or developers that leverage free email services (e.g., @gmail) for their developer contact, can be big red flags—threat actors often use these services to produce mass amounts of malicious apps in a short period. Also, poor grammar in the description highlights the haste of development and the lack of marketing professionalism that are hallmarks of mobile malware campaigns.

App reviews are not always what they appear to be: Just because an app seems to have a good reputation doesn't make it so. Rave reviews can be forged, and a high amount of downloads can simply indicate a threat actor was successful in fooling many victims. If the developer is not the state election authority or has a strange appearance or spelling, think twice. You can even do a Google search on the developer for more clues about their reputation.

Use both active and passive protection: Both Android and iPhone users should be judicious when downloading any app to their phones. Android users should not trust apps from unknown sources (not validated by Google) for any election utility. Any text or email received encouraging the installation of applications from unofficial stores or applications should be reported to the app store. Users could also consider installing mobile antivirus software as an additional safeguard for their mobile devices. Although antivirus software cannot make up for preventative measures such as checking permissions, anti-malware products provide a layer of protection from malicious code.

Know Your Mobile Attack Surface

This hidden mobile threat landscape threatens voters and can hinder their ability to exercise their right to vote. Whether an election authority has an official mobile presence, has formerly published official apps, or has no app at all, state and local (county) election officials must be aware of the entire mobile app landscape. Monitoring primary stores like the Apple App Store and Google Play as well as having visibility into apps in lesser-known app stores across the world is paramount.

The data in this report is as of October 20. Find updated counts, as well as a full list of all infringing mobile apps here.

Responsible Disclosure: RiskIQ has notified the specific app stores and marketplaces identified as hosting the infringing apps suggesting that they remove the unauthorized copies. While RiskIQ cannot enforce the removal of the apps on behalf of the states, we hope the marketplaces hosting them will act to remove them. RiskIQ can and is willing to provide detailed reports and analysis to any affected party or organization.

DISCLAIMER: *The information provided in this report is "as-is." RiskIQ makes no representation or warranty, express or implied, as to the accuracy or completeness of the information. RiskIQ shall not have any liability resulting from use of this information.*

About RiskIQ

RiskIQ is the leader in digital threat management, providing the most comprehensive discovery, intelligence, and mitigation of threats associated with an organization's digital presence. With more than 75%of attacks originating outside the firewall, RiskIQ allows enterprises to gain unified insight and control over web, social and mobile exposures. Trusted by thousands of security analysts, security teams and CISO's, RiskIQ's platform combines advanced internet data reconnaissance and analytics to expedite investigations, understand digital attack surfaces, assess risk and take action to protect the business, brand, and customers. Based in San Francisco, the company is backed by Summit Partners, Battery Ventures, Georgian Partners and MassMutual Ventures.

Try RiskIQ Community Edition for free by visiting https://www.riskiq.com/community/. To learn more about RiskIQ, visit www.riskiq.com.

RISKIQ®

RiskIQ, Inc.
22 Battery Street, 10th Floor
San Francisco, CA. 94111

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com