Privacy Issues in 2020 U.S. Campaigns' Apps & Websites: An IDAC Investigation & Recommended Best Practices

November 23, 2020

By Quentin Palfrey, Nathan Good, Will Monge, Ginny Kozemczak, and Lena Ghamrawi

Executive Summary

Collecting and analyzing voters' personal information plays an increasingly important role in modern elections. Campaigns take great pride in their ability to create data-rich profiles of potential voters, which can be used to fundraise, persuade, and encourage voters to turn out and vote. One of the ways that campaigns amass these data profiles is through their interactions with users of mobile phone applications and websites. In this largely unregulated space, users should be able to understand, and exercise control over, their personal information. Too often, users are not fully aware of what data is collected, shared with third parties, and subsequently used by campaigns and their third-party partners.

This report underscores the need for best privacy practices around campaign apps and websites; further education of developers, platforms, regulators, and users about data use and sharing by campaign apps; and stronger accountability measures to ensure that best practices are followed.

The International Digital Accountability Council (IDAC) conducted an investigation in September and October 2020 to provide greater insight into the practices of U.S. election apps.[1] Our investigative team ran a series of technical tests on the iOS and Android versions of the apps offered by the two major party candidates, President Donald Trump's Official 2020 Trump App ("Trump App") and former Vice President Joe Biden's Vote Joe App ("Biden App"), as well as 15 other election news apps (22 when accounting for Android and iOS versions). Additionally, we analyzed 132 campaign websites, including gubernatorial, United States Senate, and United States House of Representatives campaign websites to better assess and understand the political election digital ecosystem.

Launched in April 2020, IDAC is led by an experienced team of lawyers, technologists, and privacy experts with a shared goal of improving digital accountability through investigation, education, and collaboration. As a nonprofit watchdog, IDAC investigates misconduct in the digital ecosystem and works with developers and platforms to remediate privacy risks and restore consumer trust.

[1] IDAC would like to thank its partners at Good Research, AppCensus, and the Future of Privacy Forum for their support with this report. IDAC also thanks Daniel Weitzner, Bobby Richter, Joel Reardon, and Willie Boag for their input.

Based on the findings in the report, we have five recommended best practices for ways that campaigns can improve their privacy practices to promote the health of the information ecosystem around elections.

1. **Campaign apps should be explicit and forthcoming in their privacy policies** so that users have clear information about which third parties, if any, may get access to their data. In addition to identifying third parties, campaigns should explain what those third parties do with user data. For example, our report shows the Trump App sharing geolocation data and persistent identifiers with a third party called Phunware.[2] In our view, this kind of data-sharing should be disclosed explicitly if it is occurring.

2. **Campaign apps should not engage in "ID bridging."[3]** Our research suggests that the current version of the Trump App transmits a resettable advertising identifier and a persistent identifier simultaneously, raising concerns about possible circumvention of privacy protocols and platform terms and conditions. Our research also showed that an earlier version of the Biden App previously may have engaged in this practice as well.

3. **Campaign apps should refrain from requesting permissions characterized in the relevant terms of service as "dangerous," or should do so in ways that have rigorous privacy protections.** In particular, apps' requests for access to a user's phone's address book generally should be avoided, particularly in light of previous concerns about "contact-mapping" that emerged in recent elections.

4. **Campaign apps should not collect geolocation data and persistent identifiers beyond what is absolutely necessary for user functionality.** The Trump App seems to be collecting more geolocation data and persistent identifiers than is necessary to accomplish the purposes articulated in their privacy policy, which states that user location is collected "in order to provide certain location-based services, such as DJTFP promotional offers, merchandise offers, or event information or other DJTFP-related content that may be of interest to you."

5. The overall number of third parties to which user data is sent should be kept to a minimum in the spirit of privacy by design and data minimization. For example, our research shows that Lindsey Graham's official campaign website shares user data with 64 third parties, a much higher number than peer websites (more than double the number of third parties receiving data from the Biden and Trump websites, for instance).

Introduction

In recent campaign cycles around the world, the data practices of campaigns have come under increasing scrutiny. Notoriously, the British consulting firm Cambridge Analytica gained unauthorized access to the data of up to 87 million Facebook users for the purposes of political advertising in connection with a number of campaigns, including the Brexit vote and the 2016 campaigns of President Donald Trump and Senator Ted Cruz, among others.[4] Since 2016, there has been intense scrutiny of the facts underlying the Cambridge Analytica scandal, including legislation, law enforcement actions, scholarship, documentaries, and extensive

[2] Phunware has been the focus of several investigative reports for suspicious behavior. *See* Graham Kates, "The Trump campaign app is tapping a 'gold mine' of data about Americans," *CBS News* (Jul. 18, 2020), https://www.cbsnews.com/news/trump-campaign-app-data-americans-gold-mine-phunware/.

[3] ID bridging, explained in greater length in Section I, circumvents user privacy controls.

[4] Issie Lapowsky, "Facebook Exposed 87 Million Users to Cambridge Analytica," *Wired Magazine* (Apr. 4, 2018) https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/.

commentary.[5] A number of measures have been put in place by governments, court orders, and companies themselves to try to prevent external data misuse.[6]

At the same time, disinformation around elections has continued to distort and destabilize democracies around the world. There is good evidence that the Russian Federation, for example, has been engaged in online disinformation efforts and hacking with the goal of destabilizing U.S. elections.[7] False information about candidates' health, COVID-19, and voter fraud[8] have been widespread on the Internet in the run-up to the 2020 U.S. elections. Micro-targeted disinformation and voter suppression has also created risks to a free and fair election.[9]

Media reports have suggested that some of the data practices that distorted online discourse in the 2016 election have resurfaced in different forms in the 2020 election.[10] In particular, journalists, scholars, and civil society groups have raised concerns about the possible effects of campaign practices that seek to collect geolocation information, persistent identifiers, the contact information of users' social networks,[11] and other identifying data that users do not know is being shared.[12]

Methodology

Our goal was to identify apps and websites that an informed citizen would use to keep track of campaigns and upcoming elections. To do so, we tested apps created by the Trump campaign and Biden campaign, as well as a series of election apps that appeared as the most relevant apps when searching for terms regarding the election on both Google's Play Store and Apple's App Store.

In addition to the official campaign apps, we also surveyed the websites of both the Trump and Biden campaigns. In order to assess these websites, we surveyed a "baseline population" consisting of 130 other campaign websites ranging across political parties: six gubernatorial websites, 23 Senate websites and 101 House websites.

---

[5] Voter Privacy Act of 2019, S.2398; *In the Matter of Cambridge Analytica*, FTC Administrative Complaint, https://www.ftc.gov/enforcement/cases-proceedings/182-3107/cambridge-analytica-llc-matter; *The Great Hack* (documentary film) Jan. 2019; JuanOrtiz Freuler, "The Cambridge Analytica scandal is a drop of water trickling down the visible top of an iceberg," *Berkman Klein Center Blog* (Mar. 20, 2018) https://cyber.harvard.edu/story/2018-03/cambridge-analytica-scandal-drop-water-trickling-down-visible-top-iceberg.

[6] Issie Lapowsky, "Data Firms Team up to Prevent the Next Cambridge Analytica Scandal," *Wired Magazine* (Sept. 17, 2019) https://www.wired.com/story/political-data-firms-prevent-next-cambridge-analytica/; Rae Hodge, "Feinstein's new bill seeks to prevent another Cambridge Analytica," *CNET* (Aug. 2, 2019) https://www.cnet.com/news/feinsteins-new-bill-seeks-to-prevent-another-cambridge-analytica/.

[7] Sheera Frenkel & Julian E. Barnes, "Russians Again Targeting Americans With Disinformation, Facebook and Twitter Say," *N.Y. Times* (Sept. 1, 2020) https://www.nytimes.com/2020/09/01/technology/facebook-russia-disinformation-election.html.

[8] Kevin Roose, "Tracking Viral Misinformation Ahead of the 2020 Election," *N.Y. Times* (Oct. 16, 2020) https://www.nytimes.com/live/2020/2020-election-misinformation-distortions. *See also* https://time.com/5887438/trump-mail-in-voting/.

[9] Ian Vandewalker, "Digital Disinformation and Vote Suppression," *Brennan Center Report* (Sept. 2, 2020) https://www.brennancenter.org/our-work/research-reports/digital-disinformation-and-vote-suppression.

[10] See, e.g., Sue Halperin, "How the Trump Campaign's Mobile App is Collecting Huge Amounts of Voter Data," *The New Yorker* (Sept. 13, 2020); Graham Kates, "The Trump campaign app is tapping a 'gold mine' of data about Americans," *CBS News* (Jul. 18, 2020).

[11] More specifically, we are referring to the sharing of users' list of contacts.

[12] Elizabeth Culliford, "How Political Campaigns Use Your Data," *Reuters* (Oct. 12, 2020), https://graphics.reuters.com/USA-ELECTION/DATA-VISUAL/yxmvjjgojvr/. *See also* Tate Ryan-Mosley, "Explainer: What do political databases know about you?" *MIT Technology Review* (Aug. 31, 2020), https://www.technologyreview.com/2020/08/31/1007734/political-databases-explainer-tracked-campaigns-election-2020/.

App Analysis

Our app analysis consisted of a combination of manual and automated interactions of the apps. In both cases, we ran a suite of dynamic and static tests. We performed manual testing on nine iOS apps, during which we downloaded the apps and interacted with them in the way a typical user would, trying to use as much of the app as possible to test all potential subsections and screens. Next, we ran our analysis on the network traffic. From these results, we were able to observe a variety of behaviors associated with the collection and transmission of personal information, including the types of personal data these apps collect, to whom the data is being sent, and other data transmissions.

In addition to the manual interactions, we also ran 17 Android apps through our automated testing bed. The automated testing consisted of static and automated dynamic tests. Here, we performed "app fuzzing" or "monkey testing", in which a script interacts with an app by sending a series of random actions. Our testing device pretends to be a user who "plays around" with an app, tapping and swiping randomly. The automated test is performed on each app for five minutes.[13]

Website Analysis

We tested the websites through a partner platform, Netograph,[14] which crawls and analyzes websites. We performed U.S.-based captures of each website and performed analysis focusing on what information is being collected by the website, the third parties present within the site, and what each third party is sending and receiving. In particular, we looked at the links present within the site (e.g., linked images, hyperlinked text, embedded content, etc.), the cookies the site is using (who created them, what they contain, how long are they stored for), and the flows of information from the website to other domains.

[13] These automated tests are not as thorough and complete as our manual tests, but the patterns that arise from these tests help illustrate some privacy practices at a larger scale.
[14] https://netograph.io/.

Table of Contents

I. Campaign and Election Mobile Apps

We analyzed a total of 20 unique apps on iOS and Android to better understand the data collection and transmissions of election apps to provide a baseline for creating best practices.

A. Official Trump 2020 App

With 1.4 million installs,[15] the Official Trump 2020 App ("Trump App") is the most downloaded campaign app we investigated. The Trump App allows users to register for and check in at political rallies, obtain the latest news about President Trump, register to vote, volunteer for the campaign, earn rewards for merchandise, and more.[16]

IDAC tested the Trump App to further investigate its data transmissions. On September 24th, we tested the Android 2.4.2 version and Apple iOS 2.5.0 version. The latter was performed on an iPhone device running iOS12.[17] On October 27th, we tested a newer version of the Trump app on iOS, version 2.6.0.[18] We later confirmed these behaviors being present on the most current version of the app (2.7.0) after the election: we ran an additional test November 5th on an iPhone 11, running iOS 14.1.

The chart below highlights our areas of concern.

Behavior	iOS or Android?	Potential Risk	Disclosed?
Sends geolocation to Phunware	Android	Location can be used to learn about users' position, habits, beliefs, contacts, and more.	Location collection and usage is disclosed in the Privacy Policy. However, sharing location with Phunware is not disclosed.
Sends Router SSID and Router BSSID to Phunware	Android and iOS	These are non-resettable identifiers that are well-known surrogates for location data. These identifiers allow the app to track users over long periods of time.	No

[15] Graham Kates, "The Trump campaign app...," *CBS News* (Jul. 18, 2020).
[16] Official Trump 2020 App, Google Play Store, https://play.google.com/store/apps/details?id=com.ucampaignapp.americafirst&hl=en_US.
[17] The iPhone device ran iOS 12.4.6.
[18] This test was performed on an iPhone device running a slightly more updated version of iOS12: 12.4.8.

Sending Android ID + Router BSSID + Router SSID to Flurry, Branch.io, and Crashlytics, raising concerns about possible "ID bridging"	Android and iOS	ID bridging violates Google's and Apple's Developer Policies because it circumvents privacy controls put in place by Google and Apple to give users more control over the extent to which they are tracked across devices, apps, and time. When companies perform ID bridging, it negates attempts by users to use these mechanisms to compartmentalize or reset what information is connected to their devices.	No
Requests "dangerous permissions" including: location, read contacts, access microphone, read content of USB storage	Android and iOS	Google describes some permissions as "dangerous," which govern an app's access to sensitive data and features by requiring explicit consent from the user.[19] In general, best practices dictate that dangerous permissions should be invoked only when necessary to deliver a core app feature. Leveraging these permissions, the app – as well as recipient third parties that supply its APIs and SDKs – can theoretically compile information about users' contacts and make inferences (or contact them). The specific details of what is accessible with some permissions is opaque to the user and therefore may permit data collection beyond what users consented to.	The permissions for Android App are listed in Google Play Store. The app also displays a pop-up screen requesting permissions upon installation and opening. The permission push notifications that are used to obtain user consent vaguely disclose permissions usage.

1. Trump App Shares Location Data with Third Party Phunware

We observed the Android Trump App collecting and sharing users' geolocation data with a third-party called Phunware when the location permission was granted. This data-sharing is not explicitly disclosed in the Trump App's privacy policy, which states that the Trump App "may rely on this location information in order to provide certain location-based services, such as DJTFP promotional offers, merchandise offers, or event information or other DJTFP-related content that may be of interest to you."[20] The privacy policy also informs the user that location data may be used in order to "improve the functionality of the DJTFP Apps and our other applications and services."[21]

[19] "Dangerous permissions cover areas where the app wants data or resources that involve the user's private information, or could potentially affect the user's stored data or the operation of other apps. For example, the ability to read the user's contacts is a dangerous permission." *See* Android Developers, "Permissions on Android," https://developer.android.com/guide/topics/permissions/overview#dangerous_permissions.
The following steps for developers are recommended: "If an app declares that it needs a dangerous permission, the user has to explicitly grant the permission to the app. Until the user approves the permission, your app cannot provide functionality that depends on that permission. To use a dangerous permission, your app must prompt the user to grant permission at runtime."

[20] Privacy Policy, Donald J. Trump for President, https://www.donaldjtrump.com/privacy-policy/.

[21] *Id.*

Location data is very sensitive because it can reveal an enormous amount about users, including their hobbies, lifestyle choices, and preferences. Collecting location data and sharing it with third parties comes with privacy risks.

In our view, if apps are going to share location data with third parties, they should be more explicit about it than the Trump App is here.

2. Trump App Shares Router BSSID and Router SSID with Phunware

We observed the Android and iOS Trump App collecting and sharing the device's Router SSID and Router BSSID with Phunware when the user's location permission is enabled. The Router BSSID and Router SSID are "location revealing" identifiers, since they are tied to a user's WiFi router and can be used to infer where users live.

Lastly, the collection and sharing of the Router SSID and Router BSSID is not disclosed in the app's Privacy Policy and neither is the fact that Phunware receives this information.

3. The Trump App Simultaneously Transmits Resettable & Nonresettable IDs, Creating the Potential For "ID Bridging"

The troubling practice of "ID bridging" appeared to be potentially taking place in the iOS and Android Trump Apps. ID bridging occurs when an ephemeral identifier (such as the Android Advertising ID or the iOS Identifier for Advertising) is sent simultaneously with a non resettable identifier (such as the Android ID). By allowing apps to collect resettable identifiers with non resettable identifiers together, the app is potentially able to "bridge" the old resettable identifier with the new non resettable one.

We should note that what we observed is the simultaneous transmission of the two identifiers, not any subsequent bridging of the two identifiers. This creates the potential for circumvention but we do not know if circumvention did, in fact, occur.

ID Bridging allows apps to circumvent users' choice by making the use of an ephemeral identifier irrelevant. Ephemeral identifiers are designed to be changed at the user's discretion, effectively giving the user a means of controlling the degree to which an application can track a user over time. By bridging the identifiers, an app effectively establishes a permanent identifier that continues to track the user based on historical data.[22] IDAC has observed this practice occurring in many other apps, suggesting this behavior, while restricted by Google and Apple, is a widespread ecosystem issue that is not unique to the election apps we observed.

Here, we observed the Trump App sending the Android ID, Router BSSID, and Router SSID simultaneously to third parties, including Flurry, Branch.io, and Crashlytics.

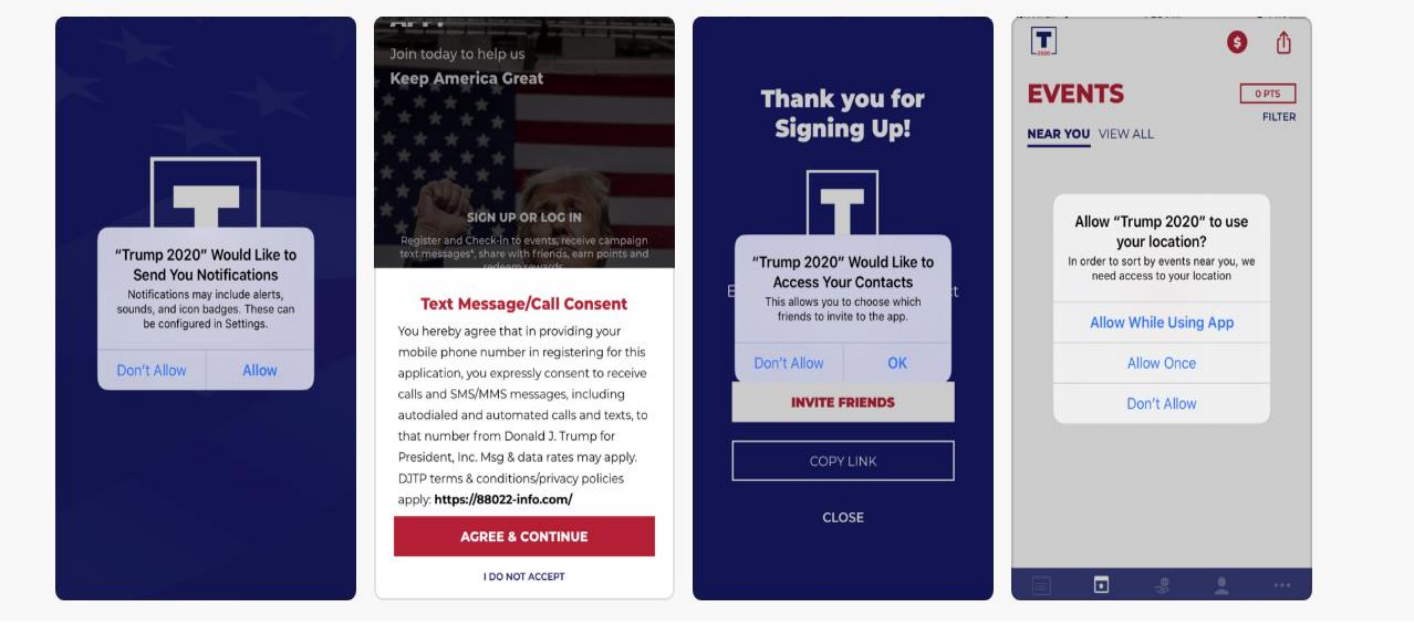
4. Trump App Permissions

[22] As a result, this practice negates any attempts by users to use these mechanisms to compartmentalize or reset what information is connected to their devices and control how they are tracked across devices, apps, and time.

Best practices for mobile apps should take into account the amount, type, and kind of permissions being requested. Permissions are the means by which an app requests access to some kind of information or action on the mobile phone. For example, if an app would like to access the phones contacts and location, then the app has to ask for permission to use the contacts and the location in order for the app to be able to use the contacts and permissions.

The Trump Android App requests many permissions, some of which may not be necessary for the app to provide its services. When users download a new app, the app asks for certain permissions to function. These permissions indicate the means through which the app is trying to obtain data—directly or through inference—from a user's device.

Some permissions have been designated as "dangerous" by Google because they provide access to sensitive data.[23] To acquire these permissions, apps must explicitly ask users for consent at the time the permission is first used. Permissions such as "access microphone," "obtain location," "read content of USB storage," and "read contacts" have the potential to be sensitive.



Trump App iOS Permission Request Screenshots

In our view, a best practice would be for campaign apps to refrain from requesting permissions characterized by Google as "dangerous," or should do so in ways that have rigorous privacy protections and keep users informed.

Requests for access to a user's address book generally should be avoided in light of previous concerns about "contact-mapping" that emerged in recent elections.

B. Vote Joe App

[23] Permissions Overview, Android Developers, https://developer.android.com/guide/topics/permissions/overview.

With 64,000 installs,[24] the Biden App reaches far fewer users than the Trump App. We ran the same technical tests on the iOS and Android versions of Joe Biden's official campaign app, Vote Joe.

The chart below highlights our area of concern.

Behavior	iOS or Android?	Potential Risk/Harm	Disclosed
Previously sent Android ID + AAID to Branch.io (in a previous version of the app), raising concerns about possible "ID bridging"	Android	ID bridging violates Google's Policies because it can allow circumvention of privacy controls put in place ID bridging subverts privacy preserving controls set by Google to give users more control over the extent to which they are tracked across devices, apps, and time. When companies perform ID bridging, it negates any attempts by users to use these mechanisms to compartmentalize or reset what device information is tracked over time.	No
Requests potentially sensitive permissions including: read contacts, read USB storage and files	Android	With contacts information, the app can compile information about users' contacts and make inferences (or contact them). It is against best practice and potentially harmful to request permissions that do not have a corresponding feature or necessity. Some permissions open the door for data collection beyond what users consented to or may expect.	The permissions for Android App are listed in Google Play Store. The "ask-on-first-use" prompt[25] is used to obtain user consent and disclose which permissions are requested. The Privacy Policy states that the users' contacts may be matched with voter registration files.

1. An Earlier Version of the Biden App Simultaneously Transmitted Resettable & Nonresettable IDs, Creating the Potential For ID Bridging

We observed a previous version of the Android Biden App sending the Android ID and the Android Advertising ID simultaneously to Branch, an analytics company. During our September 24, 2020 test, we found that version 2.3.0 potentially engaged in ID bridging, a behavior that violates Google and Apple's Developer Policies because

[24] Graham Kates, "The Trump campaign app...," *CBS News* (Jul. 18, 2020). *See also* "Vote Joe," Google Play Store, https://play.google.com/store/apps/details?id=com.joebiden.teamapp.real.

[25] An "ask on first use" prompt is when the user is prompted to allow or deny access to a sensitive resource the first time an app attempts to use it.

it allows the app to circumvent user-based privacy controls.[26] We should note that what we observed is the simultaneous transmission of the two IDs, not any subsequent bridging of the two IDs. This creates the potential for circumvention but we do not know if circumvention did in fact occur.

However, as of October 26, 2020, we found that version 2.5.1 does not appear to connect to Branch servers at all. Traces of the Branch SDK appear to have been removed.[27] Therefore, it does not appear that the Biden App is currently engaging in ID bridging.[28] Our final test, performed on the latest version iOS (2.5.0) after the election, on November 5th, on an iPhone 11 running iOS 14.1, also did not find any more transmissions to Branch.

2. Biden App Requests Potentially Invasive Permissions

The Biden Android App requests many permissions, some of which are classified as dangerous by Google and could be invasive if used improperly. As discussed in section A4, it goes against best practices for an app to request permissions that do not have a direct corresponding necessity. Here, similar to what we observed in the Trump App, the "read contacts" permission is potentially problematic. The Biden App's Privacy Policy discloses that the purpose for this request is for "providing you functionality that allows you to share messages with your contacts."[29]

C. Third Party Data Sharing

Another trend we observed was the large number of third parties that receive app users' data on both the Biden App and Trump App. In addition to recognizing the number of third parties, it is also important to consider the ways in which third parties can use personal data. As one technologist explains, "The danger in sending even small bits of information is that analytics and tracking companies are able to combine these bits together to form a unique picture of the user's device."[30] The amalgamation of data as a whole may create "a fingerprint that follows the user as they interact with other apps and use their device."[31] With that in mind, IDAC is concerned with both the *amount* of personal data and the *manner* in which it is combined.

D. Election News and Polling Apps

In addition to the Trump App and Biden App, we analyzed 15 other unique apps (22 when accounting for the Android and iOS versions) that we categorized as election news apps because they provide information on elections, offer countdowns, map electoral college votes, provide polling results, and provide other related news. A full list of apps we tested can be found in **Appendix A**. Below are the following observations that arose from observing these election apps.

---

[26] While this behavior does not confirm with best practices, it is not unique to the Biden App.
[27] All tests were conducted on a custom build of Android 9.
[28] Nevertheless, the older version of the Team Joe app (2.3.0) still performs ID bridging.
[29] Privacy Policy, Joe Biden for President, https://joebiden.com/privacy-policy/
[30] Bill Budington, "Ring Doorbell App Packed with Third-Party Trackers," *Deeplinks (Electronic Frontier Foundation)* (Jan. 27, 2020), https://www.eff.org/deeplinks/2020/01/ring-doorbell-app-packed-third-party-trackers. See also Peter Eckersley, "A Primer on Information Theory and Privacy," *Deeplinks (Electronic Frontier Foundation)* (Jan. 26, 2010) https://www.eff.org/deeplinks/2010/01/primer-information-theory-and-privacy.
[31] *Id.*

- **Privacy Policies:** Generally, these apps were transparent about the type of personal information collection and how it is used. However, many apps fell short of best practices with respect to transparency because they did not disclose the third parties with which they shared user data. Lastly, the *Joe Prez* and *US Election 2020 Countdown* apps did not have accessible privacy policies, in violation of Google and Apple's policies.

- **ID Bridging:** We observed six Android Apps and one iOS app potentially engaging in ID bridging *(see Section A3 for more information on ID bridging)*.

- **Personal Data Collected:** We observed iOS apps collecting users' names, phone numbers, emails, zip codes, mailing address, and year of birth. We also observed a multitude of third parties collecting this data, such as Amplitude, Google Analytics, Facebook, Solarwinds, and Appsverse.

- **Software Development Kits (SDKs):** SDKs are pieces of code that developers embed in an app to provide a specific functionality. SDKs are commonly used in the development of apps. The presence of SDK, without more, is not problematic. However, best practices are for coders to use SDKs with care because SDKs have the ability to collect and share data beyond what the app developers or users expect. Here, we observed the presence of social network SDKs (Facebook and Twitter), Google's Advertising SDK, and Crashlytics' Analytics SDK in a small handful of Android apps.

II. Campaign Websites

In addition to the apps we tested, we analyzed 132 campaign websites to create a baseline that we can use to compare the Biden and Trump campaign websites against. By analyzing the universe of available US 2020 campaign websites, we were better able to understand the website ecosystem better and observe trends. We investigated the two major party presidential campaign websites, six gubernatorial campaign websites, 23 United States Senate campaign websites and 101 House of Representatives campaign websites. A full list of the websites we tested can be found in **Appendix B.**

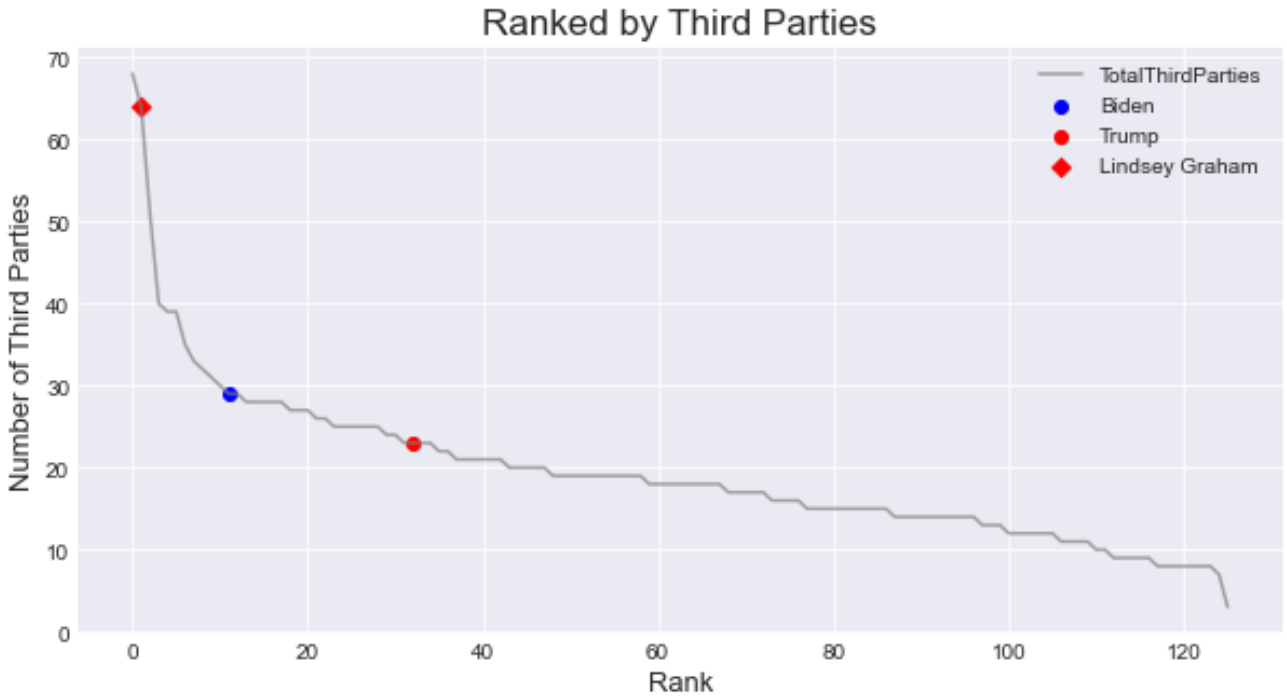
1. Use of Third Parties

After running our analysis on the 132 campaign websites, it became clear that these websites use a significant amount of third parties for various purposes, including for analytics, marketing and advertising. We surveyed both major party presidential candidates and close U.S. senatorial race websites. During our analysis, we found that South Carolina Senator Lindsey Graham's official campaign website to be an outlier, having a greater amount of third party data recipients.

- On average, a campaign website uses 20 third parties.[32]
- Trump's official campaign website (www.donaldjtrump.com) ("Trump's Website") was observed using 23 third parties, three of which were ad networks.
- Biden's official campaign website (www.joebiden.com) ("Biden's Website") was observed using 29 third parties, five of which were ad networks.

[32] As explained earlier, we analyzed what information is being collected by the website, the third parties present within the site, and what each third party is sending and receiving. In particular we looked at the links present within the site (e.g., linked images, hyperlinked text, embedded content, etc.), the cookies the site is using (who created them, what they contain, how long are they stored for), and the flows of information from the website to other domains.

- Graham's official campaign website (www.lindseygraham.com) ("Graham's Website") served as an outlier and was observed using 64 third parties.[33]



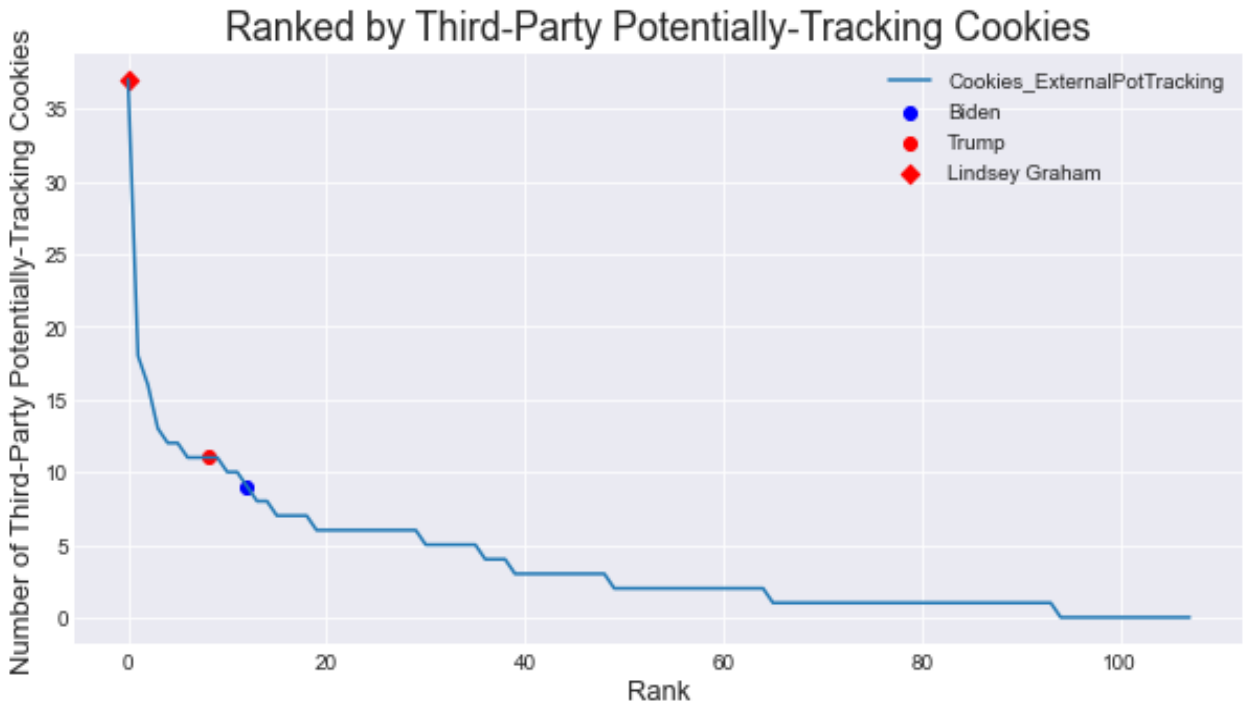
2. Third Party Cookies

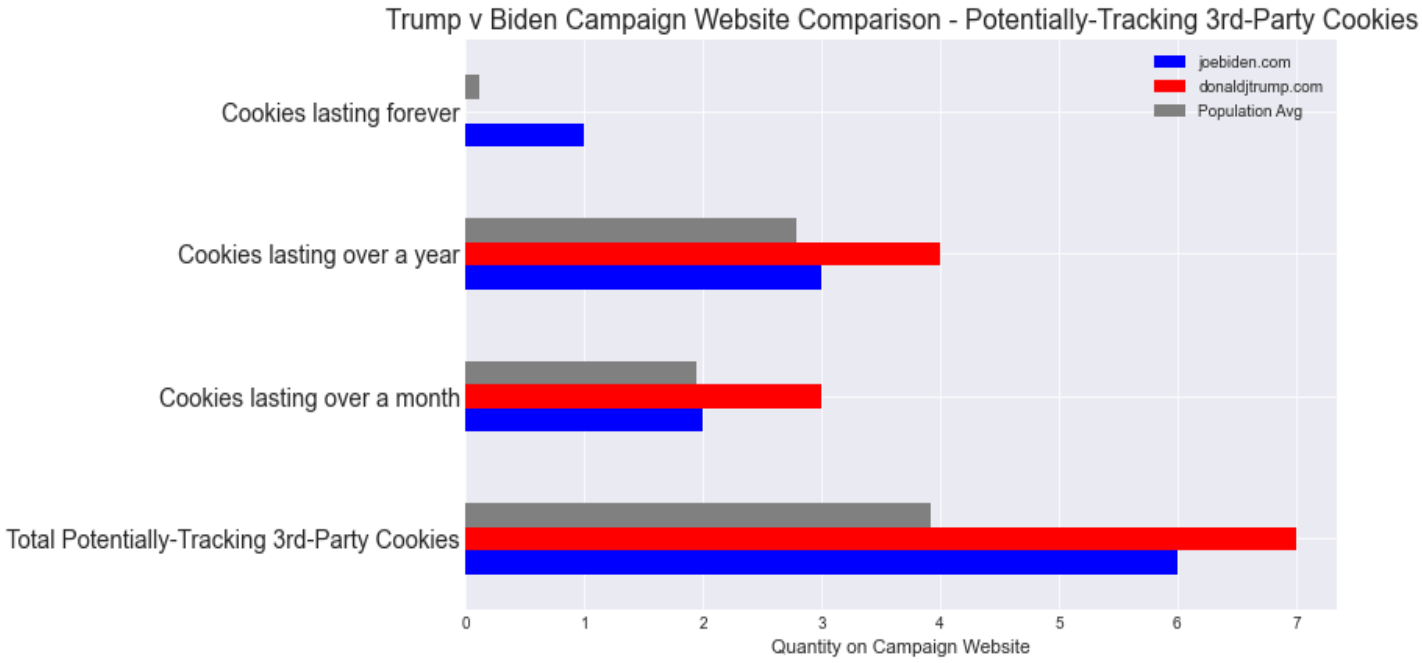
Third party cookies are small pieces of data placed on a users' browser by a third party. Third party cookies are used to identify users when they visit that website or other websites that contain cookies from the same third-party. The most common third party entities that place these cookies are advertisers, marketers, analytics companies and social media platforms. Additionally, it is common for third party cookies to be used in combination with other advertising tracking technologies to help enhance unique user profiles and/or to monetize this information.

With respect to campaign websites, it is not clear how third parties are utilizing cookie data, but it is clear, given the number of third party cookies, that cookies are being used to track and analyze what websites the user visits to better understand their preferences and interests.

- On average, a campaign website had five third party cookies placed on it.
- Trump's Website had 11 third party cookies.
- Biden's Website had nine third party cookies.
- Graham's Website was an outlier, with 39 third party cookies.

[33] 46 out of the 64 (78%) could be classified as ad networks or trackers.


Ranked by Third-Party Potentially-Tracking Cookies
Number of Third-Party Potentially-Tracking Cookies
Rank
Cookies_ExternalPotTracking
Biden
Trump
Lindsey Graham
0
5
10
15
20
25
30
35
0
20
40
60
80
100


Trump v Biden Campaign Website Comparison - Potentially-Tracking 3rd-Party Cookies
joebiden.com
donaldjtrump.com
Population Avg
Cookies lasting forever
Cookies lasting over a year
Cookies lasting over a month
Total Potentially-Tracking 3rd-Party Cookies
0
1
2
3
4
5
6
7
Quantity on Campaign Website

Appendix A - List of Apps Analyzed

Platform	App Name	URL
Android	Electoral College Calculator	https://play.google.com/store/apps/details?id=com.aamirki.electoralcollegecalculation
Android	PresDatabase - US Presidential Election Database	https://play.google.com/store/apps/details?id=com.aamirki.presdatabase
Android	US Presidential Election Day 2020 Countdown	https://play.google.com/store/apps/details?id=com.ActuallyUsefulSoftware.edc
Android	PRESIDENT TRUMP NEWS	https://play.google.com/store/apps/details?id=com.andromo.dev231870.app482676
Android	Joe Prez - Daily News on Joe Biden's 2020 Campaign	https://play.google.com/store/apps/details?id=com.andromo.dev801484.app964690
Android	Election Tracker 2020 - US Presidential Election	https://play.google.com/store/apps/details?id=com.chinesepoweredlabs.democratic_primaries_2020
Android	2020 Electoral Map, Presidential	https://play.google.com/store/apps/details?id=com.elabs.election
Android	U.S. 270 Free	https://play.google.com/store/apps/details?id=com.flashmatch.us270free
Android	US Election 2020 Countdown	https://play.google.com/store/apps/details?id=com.greenmayo.uselectioncountdown
Android	Vote Joe	https://play.google.com/store/apps/details?id=com.joebiden.teamapp.real
Android	Election Countdown 2020 - widgets included	https://play.google.com/store/apps/details?id=com.klawton.electioncountdown
Android	2020 Election	https://play.google.com/store/apps/details?id=com.mobiletrendsrl.uselection2020
Android	US Presidential Election 2020	https://play.google.com/store/apps/details?id=com.mobixed.USPresidentialElection2020Edition
Android	US Election 2020 - Election Polls and Results	https://play.google.com/store/apps/details?id=com.starenkysoftware.usa_election_tracker
Android	PocketPolls	https://play.google.com/store/apps/details?id=com.tsh.pocketpolls
Android	Official Trump 2020 App	https://play.google.com/store/apps/details?id=com.ucampaignapp.americafirst
Android	Vote With Me	https://play.google.com/store/apps/details?id=org.newdataproject.votewithme
iOS	ActiVote	https://apps.apple.com/us/app/activote/id1457987563
iOS	Election Watch 2020	https://apps.apple.com/us/app/election-watch-2020/id1482004780
iOS	Election Tracker 2020 - US Presidential Election	https://apps.apple.com/gh/app/election-tracker-2020/id1477911200

iOS	Electoral College Calculator	https://apps.apple.com/us/app/electoral-college-calculator/id1382486963
iOS	Official Trump 2020 App	https://apps.apple.com/us/app/official-trump-2020-app/id1135325440
iOS	PocketPolls	https://apps.apple.com/us/app/pocketpolls/id1473498393
iOS	PresDatabase - US Presidential Election Database	https://apps.apple.com/us/app/presdatabase/id1515590795
iOS	Vote Joe	https://apps.apple.com/us/app/vote-joe/id1523760221
iOS	Vote With Me	https://apps.apple.com/us/app/votewithme/id1292398078

Appendix B - List of Campaign Websites Analyzed

2020 Presidential Race					
	Incumbent	**Inc. Party**	**Inc. Website**	**Challenger**	**Chall Website**
	Donald Trump	Rep.	https://www.donaldjtrump.com/	Joe Biden	https://joebiden.com/
2020 US Senate Races					
State	**Incumbent**	**Inc. Party**	**Inc. Website**	**Challenger**	**Chall Website**
CO	Gardner	Rep.	https://www.corygardnerforsenate.com/	Hickenlooper	https://hickenlooper.com/
GA	Perdue	Rep.	https://perduesenate.com/	Warnock	https://warnockforgeorgia.com/
IA	Ernst	Rep.	https://joniernst.com/	Greenfield	https://greenfieldforiowa.com/
ME	Collins	Rep.	https://www.susancollins.com/	Gideon	https://saragideon.com/
MT	Daines	Rep.	https://www.stevedaines.com/	Bullock	https://stevebullock.com/
NC	Tillis	Rep.	https://www.thomtillis.com/	Cunningham	https://www.calfornc.com/
AZ	McSally	Rep.	http://www.mcsallyforsenate.com/	Kelly	https://markkelly.com/
GA	Loeffler	Rep.	https://kellyforsenate.com/	n/a	
KS	Marshall	Rep.	https://kansansformarshall.com/	Bollier	https://bollierforkansas.com/
SC	Graham	Rep.	https://www.lindseygraham.com/	Harrison	https://jaimeharrison.com/
MI	Peters	Dem.	https://petersformichigan.com/	James	https://johnjamesforsenate.com/
AL	Jones	Dem.	https://dougjones.com/	Tuberville	https://tommyforsenate.com/
2020 Governor Races					
State	**Incumbent**	**Inc. Party**	**Inc. Website**	**Challenger**	**Chall Website**
MT	Cooney	Dem.	https://www.cooneyformontana.com/	Gianforte	https://gregformontana.com/
NC	Cooper	Dem.	https://roycooper.com/	Forest	https://danforest.com/
MO	Parson	Rep.	https://mikeparson.com/	Galloway	https://nicolegalloway.com/
2020 US House Races					
State	**Incumbent**	**Inc. Party**	**Inc. Website**	**Challenger**	**Chall Website**
AZ-01	Tom O'Halleran	Dem.	https://www.tomohalleran.com/	Tiffany Shedd	https://sheddforcongress.com/
CA-48	Harley Rouda	Dem.	https://harleyforcongress.com/	Michelle Steel	https://www.michellesteelca.com/

GA-06	Lucy McBath	Dem.	https://lucyforcongress.com/home/	Karen Handel	https://karenhandel.com/
GA-07	Open	Rep.		Carolyn Bourdeaux	https://www.carolyn4congress.com/
MI-08	Elissa Slotkin	Dem.	https://elissaforcongress.com/	Paul Junge	https://pauljunge.com/
MI-11	Haley Stevens	Dem.	https://www.haleystevensforcongress.com/	Eric Esshaki	https://vote.ericesshaki.com/
MN-02	Angie Craig	Dem.	https://www.angiecraig.com/	Tyler Kistner	https://www.tylerkistnerforcongress.com/
NJ-07	Tom Malinowski	Dem.	https://malinowskifornj.com/	Thomas Kean Jr.	http://www.njleg.state.nj.us/members/BIO.asp?Leg=220
NV-03	Susie Lee	Dem.	http://susieleeforcongress.com/	Daniel Rodimer	https://danrodimer.com/
NY-19	Antonio Delgado	Dem.	https://delgadoforcongress.com/	Kyle Van De Water	https://www.kyleforny19.com/
PA-07	Susan Wild	Dem.	https://wildforcongress.com/	Lisa Scheller	https://schellerforcongress.com/
PA-08	Matthew Cartwright	Dem.	http://www.cartwrightcongress.com/	Jim Bognet	https://bognetforcongress.com/
TX-07	Lizzie Pannill Fletcher	Dem.	https://www.lizziefletcher.com/	Wesley Hunt	https://wesleyfortexas.com/
TX-23	Open	Rep.		Gina Ortiz Jones	https://ginaortizjones.com/
CA-21	T.J. Cox	Dem.	https://tjcoxforcongress.com/	David Valadao	http://www.valadaoforcongress.com/
FL-26	Debbie Mucarsel-Powell	Dem.	https://debbie2018.com/	Carlos Gimenez	http://www.carlosgimenezforcongress.com/
IA-01	Abby Finkenauer	Dem.	https://www.abbyfinkenauer.com/	Ashley Hinson	https://ashleyhinson.com/
IA-02	Open	Dem.		Rita Hart	https://www.ritahart.com/
IA-03	Cindy Axne	Dem.	https://cindyaxneforcongress.com/	David Young	http://www.davidyoungforiowa.com/
ME-02	Jared Golden	Dem.	https://jaredgoldenforcongress.com/	Dale Crafts	https://dalecraftsforcongress.com/
MN-07	Collin Peterson	Dem.	https://www.petersonforcongress.com/	Michelle Fischbach	http://www.fischbachforcongress.com/
NJ-03	Andy Kim	Dem.	https://andykimforcongress.com/	David Richter	http://www.richter2020.com/
NM-02	Xochitl Torres Small	Dem.	http://www.xochforcongress.com/	Yvette Herrell	https://www.yvetteherrell.com/
NY-11	Max Rose	Dem.	http://www.maxroseforcongress.com/	Nicole Malliotakis	http://nicolemalliotakis.com/

NY-22	Anthony Brindisi	Dem.	http://brindisiforcongress.com/	Claudia Tenney	https://claudiaforcongress.com/
OK-05	Kendra Horn	Dem.	http://www.kendrahornforcongress.com/	Stephanie Bice	https://biceforcongress.com/
SC-01	Joe Cunningham	Dem.	https://www.joecunninghamforcongress.com/	Joe Cunningham	https://nancymace.org/
UT-04	Ben McAdams	Dem.	https://www.benmcadams.com/	Burgess Owens	https://www.burgess4utah.com/
VA-02	Elaine Luria	Dem.	https://elaineforcongress.com/	Scott Taylor	https://www.scotttaylor2020.com/
VA-07	Abigail Spanberger	Dem.	https://abigailspanberger.com/	Nick Freitas	https://www.nickforva.com/
AZ-06	David Schweikert	Rep.	https://davidschweikert.com/	Hiral Tipirneni	http://hiralforcongress.com/
CA-25	Mike Garcia	Rep.	https://www.electmikegarcia.com/	Christy Smith	https://www.christyforcongress.org/
IN-05	Open	Rep.		Victoria Spartz	https://www.spartzforcongress.com/
MO-02	Ann Wagner	Rep.	https://annwagner.com/	Jill Schupp	https://jillschupp.com/
NE-02	Don Bacon	Rep.	https://donjbacon.com/	Kara Eastman	http://eastmanforcongress.com/
NJ-02	Jeff Van Drew	Rep.	https://www.vandrewforcongress.com/	Amy Kennedy	https://amykennedyforcongress.com/
NY-02	Open	Rep.		Andrew Garbarino	https://www.garbarinoforny.com/
OH-01	Steve Chabot	Rep.	https://stevechabot.com/	Kate Schroder	https://kateforcongress.com/
PA-10	Scott Perry	Rep.	https://patriotsforperry.com/	Eugene DePasquale	https://eugeneforcongress.com/
TX-21	Chip Roy	Rep.	https://chiproy.com/	Wendy Davis	https://www.wendydavisforcongress.com/
TX-22	Open	Rep.		Troy Nehls	https://www.nehlsforcongress.com/
TX-24	Open	Rep.		Beth Van Duyne	https://www.bethfortexas.com/
AK-00	Don Young	Rep.	http://alaskansfordonyoung.com/	Alyse Galvin	https://www.alyse4alaska.com/
FL-15	Open	Rep.		Scott Franklin	https://www.votescottfranklin.com/
IL-13	Rodney Davis	Rep.	https://electrodney.com/	Betsy Londrigan	https://www.betsydirksenlondrigan.com/
MI-03	Open	Libertarian		Peter Meijer	https://www.votemeijer.com/

MI-06	Fred Upton	Rep.	http://fredupton.com/	Jon Hoadley	http://www.jonhoadley.com/
MN-01	Jim Hagedorn	Rep.	https://www.jimhagedorn.org/	Dan Feehan	https://www.danfeehan.com/
MT-00	Open	Rep.		Matt Rosendale	https://mattformontana.com/
NC-08	Richard Hudson	Rep.	https://richardhudson.org/	Patricia Timmons-Goodson	https://www.timmonsgoodsonforcongress.com/
NY-01	Lee Zeldin	Rep.	http://www.zeldinforcongress.com/	Nancy Goroff	https://www.goroffforcongress.com/
NY-24	John Katko	Rep.	http://www.johnkatkoforcongress.com/	Dana Balter	https://electdanabalter.com/
PA-01	Brian Fitzpatrick	Rep.	https://www.brianfitzpatrick.com/	Christina Finello	https://www.finelloforcongress.com/
TX-03	Van Taylor	Rep.	https://www.vantaylor.com/	Lulu Seikaly	https://lulufortexas.com/
TX-10	Michael McCaul	Rep.	http://www.michaelmccaul.com/	Mike Siegel	https://www.siegelfortexas.org/
VA-05	Open	Rep.		Bob Good	https://www.bobgoodforcongress.com/