

C A M P A I G N F O R

ACCOUNTABILITY

June 26, 2019

By Email: press@google.com

&

First Class Mail

Jamie Rosenberg
VP, Business & Operations
Android & Google Play

Purnima Kochikar
Director
Google Play, Apps & Games
Google LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043

Re: Removal of Political Social Media LLC's Apps from Google Play

Dear Mr. Rosenberg and Ms. Kochikar:

Campaign for Accountability (“CfA”), a nonprofit watchdog organization, respectfully requests that Google remove all apps developed by Political Social Media LLC from Google Play. Political Social Media operates the brands, uCampaign, LLC and Jarbik, LLC, among others, which operate approximately 12 nearly identical apps that appear to be violating the Google Play Developer Distribution Agreement and Google’s Developer Program Policies.

Background

Political Social Media LLC was incorporated in Delaware on January 31, 2014.¹ The company employs several brand names including uCampaign and Jarbik.² Through these brands, the company operates several apps available for download in Google Play.³ The company appears to be violating the Google Play Developer Distribution Agreement and Google’s Developer Program Policies by failing to provide adequate privacy policies, misusing users’ personal

¹ Political Social Media LLC, Entity Details, Delaware Department of State, Division of Corporations, *accessed at* <https://icis.corp.delaware.gov/Ecorp/EntitySearch/NameSearch.aspx>.

² Laura Silver, *The Apps For Ireland's Anti-Abortion Campaigns Allow User Data To Be Shared With The NRA*, *BuzzFeed*, May 22, 2018, available at <https://www.buzzfeed.com/laurasilver/ireland-anti-abortion-campaigns-apps-privacy-nra>.

³ <https://play.google.com/store/apps/developer?id=Jarbik>;
<https://play.google.com/store/apps/developer?id=uCampaign>.

information, and building template apps and submitting them to Google Play on behalf its client organizations.⁴

The apps operated by Political Social Media target political conservatives.⁵ For instance, through the uCampaign brand, the company runs the official app for the pro-gun organization, the National Rifle Association (“NRA”), and the anti-abortion groups, Susan B. Anthony List (“SBA List”) and Family Research Council (“FRC”).⁶ The company also operates the official app for President Trump’s campaign committee and the app for the Great America PAC, a super PAC that supports President Trump.⁷ Additionally, uCampaign runs an app the Conservative Party of Canada and the Australian Christian Lobby.⁸

Jarbik runs an app for the Generation Atomic, an advocacy organization that supports nuclear energy, and has managed apps for several international political movements, including a nationalist party in Malta and an anti-abortion group in Ireland.⁹

Political Social Media’s apps for each of these organizations are virtually identical.¹⁰ The company sets up a boilerplate social media platform that is branded for each of its client organizations.¹¹ The apps draw in supporters of those organizations who use them to chat with each other and post comments on in-app newsfeeds. The apps also offer games and challenges for users to play and receive rewards.¹² The app descriptions suggest users can use the apps to stay up to date on the latest news about each client organization or candidate.¹³

The apps generate value for sponsoring organizations by leveraging the contacts of their users.¹⁴ Political Social Media prods users to turn over their address books and other identifying information to the app developers upon signing up.¹⁵ The company then encourages users to send

⁴ https://play.google.com/intl/ALL_us/about/developer-distribution-agreement.html;
<https://play.google.com/about/developer-content-policy/>.

⁵ <https://play.google.com/store/apps/developer?id=uCampaign>.

⁶ <https://play.google.com/store/apps/details?id=com.ucampaignapp.nra>;

<https://play.google.com/store/apps/details?id=com.ucampaignapp.sba>;

<https://play.google.com/store/apps/details?id=com.ucampaignapp.frc>.

⁷ <https://play.google.com/store/apps/details?id=com.ucampaignapp.americafirst>;

<https://play.google.com/store/apps/details?id=com.ucampaignapp.gap>.

⁸ <https://play.google.com/store/apps/details?id=com.ucampaignapp.cpc>;

<https://play.google.com/store/apps/details?id=com.ucampaignapp.acl>.

⁹ <https://play.google.com/store/apps/details?id=com.ucampaignapp.gna>; Silver, *BuzzFeed*, May 22, 2018; <https://appadvice.com/game/app/pn-malta/1232401367>.

¹⁰ Emma Hinchliffe, *A Four-person Company is Behind the Apps of Donald Trump, the NRA and Other Conservative Groups*, *Mashable*, October 7, 2016, available at <https://mashable.com/2016/10/07/ucampaign-conservative-apps/>.

¹¹ Silver, *BuzzFeed*, May 22, 2018.

¹² <https://play.google.com/store/apps/developer?id=uCampaign>.

¹³ *Id.*

¹⁴ James Vincent, *Ted Cruz's app turns handing over your friends' contact info into a game*, *The Verge*, November 11, 2015, available at <https://www.theverge.com/2015/11/11/9711364/ted-cruz-campaign-app-gamification>.

¹⁵ The NRA app, for instance, asks users to share their location when they register.

messages to everyone in their address books, which benefits the sponsors.¹⁶ Even if users do not turn over their address books when they register, the apps regularly incentivize users to share their contacts. The NRA app, for instance, requires users to obtain 250 action points in order to post a comment on the platform. Users can obtain points by sharing the app with their friends or allowing the app to track their location, among other methods. *BuzzFeed* reported in May 2018 that some of the Political Social Media's apps previously required users to turn over their contact information in order access the apps' main features.¹⁷

Political Social Media founder Thomas Peters explained the app's method in a blog post discussing how his company helped Sen. Ted Cruz (R-TX) win the 2016 Iowa caucuses:

As a phone app it has authorized access to a supporter's phone address book contacts. That allows it to match those contacts to Cruz's voter universes and prompt *existing* supporters to reach out personally to *identified potential* supporters. To date the feature has matched over **a third of a million potential supporters** who are contacts of one or more of the app's current supporters.

The second source of data are self, individual friend and neighborhood surveys. App supporters have completed over 20,000 political ID surveys about themselves, their friends and their neighbors, generating valuable cross-section data on the supporters' political views, activism affinities and personal network, essential information for a modern, data-driven campaign.¹⁸ (emphasis in original)

Political Social Media uses this information to send political messages to the friends and family of an app's users.¹⁹ uCampaign boasted about the success of this model in a description of its apps on the *NationBuilder* website:

We follow the 80/20 rule - take your top 20% of supporters who will perform 80% of the actions and give them a smartphone app that allows them to do 10X more than what they would do on a website, while creating valuable data which is automatically synced to your Nation. Our platform allows you to manage your app once we have collaborated to build and launch it. **We offer advanced features such as matching your supporters' phone address book contacts to voter files** and big data as well as crowdsourcing grassroots activities like text messaging and fundraising to your supporters. Match your supporters to their state and federal elected officials using geolocation to make lobbying seamless. Our clients include

¹⁶ Natasha Singer and Nicholas Confessore, Republicans Find a Facebook Workaround: Their Own Apps, *The New York Times*, October 20, 2018, available at <https://www.nytimes.com/2018/10/20/technology/politics-apps-conservative-republican.html>.

¹⁷ Older versions of the Android operating system required apps to seek these permissions from users when they downloaded the app. The most recent version of Android allows apps to obtain users' permission after installing the app. See <https://developer.android.com/guide/topics/permissions/overview?hl=en>; Silver, *BuzzFeed*, May 22, 2018.

¹⁸ Thomas Peters, We Are the Stealth Startup that Helped Ted Cruz Win Iowa, *Medium*, February 4, 2016, available at <https://medium.com/@uCampaignCEO/meet-the-stealth-startup-that-helped-ted-cruz-win-iowa-fea6745b8a6d>.

¹⁹ Singer and Confessore, *The New York Times*, Oct. 20, 2018.

local, state, federal, presidential, international, advocacy and referendums.²⁰
(emphasis added)

The *Nationbuilder* description also reveals the scale of the privacy problem: for every person that downloads the app, the app can identify 34 possible supporters of an organization.²¹

Misusing Personal Information

While Political Social Media has received glowing media profiles for ingeniously leveraging users' contact data, the company's political activities have been scrutinized by government investigators.²² For instance, in 2016 uCampaign developed an app for the Vote Leave campaign, which advocated for Great Britain to leave the European Union.²³ A parliamentary committee tasked with investigating the campaign specifically cited the "data privacy concerns raised" by uCampaign's app.²⁴

Additionally, Political Social Media drew widespread criticism for misusing its users' data during the 2016 presidential election. For instance, *NBC News* reported:

Immediately after installation, the app requests access to users' address books; app creator Thomas Peters, CEO of uCampaign, said this is to help users share the app with their friends. But the app's privacy policy says the campaign can use that data — the names, emails, home addresses and more stored in a user's address book — however they'd like.

"Trump's [app] is at a whole other level," explained the American Civil Liberties' Nicole Ozer. "It's not just to pay with your privacy, but to sell out your friends and colleagues who are in your contact list."²⁵

Indeed, *Business Insider* reported in November 2016:

If users download the app and agree to share their address books, including phone numbers and emails, the app then shoots the data [sic] a third-party vendor, which looks for matches to existing voter file information that could give clues as to what may motivate that specific voter. Thomas Peters, whose company uCampaign created Trump's app, said the app is "going absolutely granular," and will — with

²⁰ <https://nationbuilder.com/ucampaignupdate>.

²¹ *Id.*

²² Hinchliffe, *Mashable*, Oct. 7, 2016.

²³ Mark Scott, [Politicians Follow in Facebook's Footsteps on Mass Data Collection](https://www.politico.eu/article/facebook-cambridge-analytica-data-protection-privacy-brexit-trump-vote-leave-ucampaign/), *Politico*, April 8, 2018, available at <https://www.politico.eu/article/facebook-cambridge-analytica-data-protection-privacy-brexit-trump-vote-leave-ucampaign/>.

²⁴ [Disinformation and 'Fake News': Interim Report](https://publications.parliament.uk/pa/cm201719/cmselect/cmcomeds/363/36306.htm), *Digital, Culture, Media, and Sport Committee, United Kingdom House of Commons*, July 29, 2018, Chapter 3, available at <https://publications.parliament.uk/pa/cm201719/cmselect/cmcomeds/363/36306.htm>.

²⁵ Jane C. Timm, [Trump's New App Wants You — And Your Data](https://www.nbcnews.com/politics/2016-election/trump-s-new-app-wants-you-your-data-n640236), *NBC News*, August 31, 2016, available at <https://www.nbcnews.com/politics/2016-election/trump-s-new-app-wants-you-your-data-n640236>.

permission — send different, A/B tested messages to users' contacts based on existing information.²⁶

Alarming, though, a 2018 version of the company's privacy policy stated that the company "may share your personal information with other organizations, groups, causes, campaigns, political organizations, and our clients that we believe have similar viewpoints, principles or objectives as us."²⁷ As *BuzzFeed* reported:

This means data can be shared...with previous clients such as the NRA, the Trump presidential campaign, the Republican National Committee, and the Susan B. Anthony List, a major US anti-abortion group. In the UK, the network includes the Conservative Party and main pro-Brexit campaign, Vote Leave.²⁸

Political Social Media's Privacy Policies

Political Social Media's apps can access users' precise location, camera, calendars, and contacts if users give them permission.²⁹ Of the 12 apps currently available for download from Political Social Media, 10 of them, including the apps for the NRA, the SBA List, and FRC, have identical privacy policies. Notably, the privacy policies listed in the app are not found on the websites of the sponsoring organizations themselves. Instead, using Google Play, all of these apps link to privacy policies on websites operated by Jarbik, uCampaign, or RumbleUp, another brand that belongs to Political Social Media.³⁰ The policy – common to all Political Social Media brands – provides:

As noted above, we share your Personal Information with the uCampaign client that administers the Client Application that you use. Except as otherwise set forth in this Privacy Policy, we do not share your information with other third parties, nor do we share information between uCampaign clients.³¹

This policy gives the company wide latitude to share personal information of its users:

We may, with your permission, collect third party contact information (including, without limitation, names, telephone numbers, emails and social media handles, if available) from your mobile address book.

²⁶ Maxwell Tani, [Donald Trump's Campaign is Using the Same App the 'Leave' Campaign Used During Brexit to Spur Voter Turnout](https://www.businessinsider.com/donald-trumps-phone-app-brexit-2016-11), *Business Insider*, November 7, 2016, available at <https://www.businessinsider.com/donald-trumps-phone-app-brexit-2016-11>.

²⁷ Silver, *BuzzFeed*, May 22, 2018.

²⁸ *Id.*

²⁹ <https://reports.exodus-privacy.eu.org/en/reports/29364/>.

³⁰ The following apps provide their own privacy policies: Atomic Action, Australian Christian Lobby, Australian Conservatives, Diabetes Patient Advocacy Coalition, and the Great America PAC.

³¹ <http://letsw.in/privacy.html>.

We may receive Personal Information about you from other users of the Platform. This may happen if they connect their address books to our services, or if they invite you to use our services via the Platform. Additionally, we may also receive Personal Information about you from the uCampaign client administering the Client Application. **If you have received a text message through our services, your information was uploaded to the Platform through the uCampaign client that contacted you.** We will treat all such Personal Information in accordance with this privacy policy.

We may share your Personal Information with other entities affiliated with us for internal reasons, primarily for business and operational purposes. uCampaign, or any of its assets, including the Platform, may be sold, or other transactions may occur in which your Personal Information is one of the business assets of the transaction. In such case, your Personal Information may be transferred.³² (emphasis added)

The privacy policy for Political Social Media's apps allows the developer to collect the personal information of individuals who received text messages from an app's users, *even if the recipient did not download one of the company's apps*. Political Social Media does not provide message recipients with an opportunity to consent to this data collection.³³

While the company has removed the alarming language that *BuzzFeed* highlighted, the current policy still allows the company to share users' information with anyone "affiliated with us." Presumably, the company can rely on this policy to share users' data with any of the clients that use its apps. The policy further states:

Information about your use of the Platform as an end-user will also be available to the uCampaign client that is administering the Client Application. For more information about this uCampaign client's privacy practices, please refer to the client's privacy policy.³⁴

The instruction to refer to "the client's privacy policy" is futile. Ten of Political Social Media's apps, including those of FRC and SBA List, do not, in fact, provide a link to the client's privacy policy. Beyond the app, the SBA List's own website does not even include a link to its privacy policy.³⁵ The only way to find the SBA List's organizational privacy policy is through an outside search engine. And even then, the available policy applies only to the organization's website; there is no reference to the Political Social Media app.³⁶ Similarly, FRC's privacy policy does not provide any information about its app.³⁷

³² *Id.*

³³ As noted below, this is a violation of Google's Developer Program Policies which states that Google doesn't allow "unsolicited promotion via SMS services." See <https://play.google.com/about/storelisting-promotional/>.

³⁴ <https://ucampaignapp.com/privacy.html>.

³⁵ <https://www.sba-list.org/about-susan-b-anthony-list>.

³⁶ <https://www.sba-list.org/privacy-policy>.

³⁷ <https://www.frc.org/privacy-policy>.

Google Play Developer Distribution Agreement

Privacy

Google provides developers with a wealth of information regarding how to build apps for Android and Google Play. Repeatedly, Google emphasizes the requirement that app developers protect users' privacy. For instance, the Google Play Developer Distribution Agreement states:

You agree that if You make Your Products available through Google Play, You will protect the privacy and legal rights of users. If the users provide You with, or Your Product accesses or uses, usernames, passwords, or other login information or personal information, You agree to make the users aware that the information will be available to Your Product, and **You agree to provide legally adequate privacy notice and protection for those users.** Further, Your Product may only use that information for the limited purposes for which the user has given You permission to do so.³⁸ (emphasis added)

Despite the agreement, Political Social Media does not provide an “adequate privacy notice” for its users. For 10 of the 12 apps offered by Political Social Media, the only privacy policy included is that for Political Social Media's companies.

Moreover, Political Social Media's privacy policy states:

You have the right to access your Personal Information held by us and, if necessary, have it amended or deleted. You can also request not to receive email communications and/or other marketing information from us.³⁹

For most of the apps, though, the only contact information listed is for uCampaign or Jarbik.⁴⁰ There is no contact information for the client organizations benefitting from the apps and, presumably, storing users' information. As a result, users cannot have confidence that their data will be deleted by all of the parties that obtain their personal information.

Personal Information

Beyond the privacy policy, the Google Play Developer Distribution Agreement explains that developers must not misuse the personal information of their users. The Privacy, Security, and Deception section of Google's Developer Program Policies states:

You must be transparent in how you handle user data (e.g., information collected from or about a user, including device information). That means disclosing the collection, use, and sharing of the data, and limiting the use of the data to the purposes disclosed, and the consent provided by the user. In addition, if your app

³⁸ https://play.google.com/intl/ALL_us/about/developer-distribution-agreement.html.

³⁹ <https://ucampaignapp.com/privacy.html>.

⁴⁰ *Id.*; <https://jarbik.com/privacy.html>.

handles personal or sensitive user data, please also refer to the additional requirements in the “Personal and Sensitive Information” section below.⁴¹

And:

Personal and sensitive user data includes, but isn't limited to, personally identifiable information, financial and payment information, authentication information, phonebook, contacts SMS and call related data, microphone and camera sensor data, and sensitive device or usage data. If your app handles sensitive user data, then you must:

- Limit your collection and use of this data to purposes directly related to providing and improving the features of the app (e.g. user anticipated functionality that is documented and promoted in the app's description).
- Post a privacy policy in both the designated field in the Play Console and within the app itself. The privacy policy must, together with any in-app disclosures, comprehensively disclose how your app collects, uses, and shares user data. Your privacy policy must disclose the type of parties to which any personal or sensitive user data is shared.
- Handle all personal or sensitive user data securely, including transmitting it using modern cryptography (for example, over HTTPS).⁴²

An example of a “common violation” is:

An app that accesses a user's phone or contact book data and doesn't treat this data as personal or sensitive data subject to the Privacy Policy, Secure Transmission, and Prominent Disclosure requirements.⁴³

The policy also provides that if an “app handles non-public phonebook or contact information,” Google does not “allow unauthorized publishing or disclosure of people's non-public contacts.”⁴⁴ Additionally, Google’s Unwanted Software Policy states:

We’ve found that most unwanted software displays one or more of the same basic characteristics: It collects or transmits private information without the user’s knowledge.⁴⁵

The Developer Program Policies also prohibit apps from using a person’s contacts to promote an app. The Store Listing and Promotion section states:

⁴¹ <https://play.google.com/about/privacy-security-deception/personal-sensitive/>.

⁴² *Id.*

⁴³ *Id.*

⁴⁴ *Id.*

⁴⁵ <https://www.google.com/about/unwanted-software-policy.html>.

We don't allow apps that directly or indirectly engage in or benefit from promotion practices that are deceptive or harmful to users or the developer ecosystem. This includes apps that engage in the following behavior:

Unsolicited promotion via SMS services.⁴⁶

Despite the clear prohibitions, Political Social Media appears to be flagrantly violating the Google Play Developer Distribution Agreement and Google's Developer Program Policies by failing to appropriately handle the personal information of its users. As Political Social Media has stated publicly, the purpose of its apps is to collect contact information from its users in order to deliver messages from its clients to their contacts at scale.⁴⁷ As Political Social Media acknowledged on *Nationbuilder*, its apps "Identify on average 34 individuals per supporter who downloads the app and generate up to 28 new ways to contact these individuals."⁴⁸

Permissions

Previously, Political Social Media required users to turn over their phonebook and location, among other things, in order to access most of an app's features.⁴⁹ Previous versions of the Android operating software required users to grant or deny permissions to an app before installing it.⁵⁰ The most recent version of Android, however, allows users to grant or deny permissions after installing an app, providing users with more control over their personal information.⁵¹ Still, Google makes clear that developers may not abuse permissions granted by users. For instance, the Google Play Developer Distribution Agreement states:

You are responsible for uploading Your Products to Google Play, providing required Product information and support to users, and accurately disclosing the permissions necessary for the Product to function on user Devices.⁵²

The permissions section of Google's Developer Program Policies states:

Permission requests should make sense to users. You may only request permissions that are necessary to implement critical current features or services in your application. You may not use permissions that give access to user or device data for undisclosed, unimplemented, or disallowed features or purposes.⁵³

And:

⁴⁶ <https://play.google.com/about/storelisting-promotional/>.

⁴⁷ <https://nationbuilder.com/ucampaignupdate>.

⁴⁸ *Id.*

⁴⁹ Silver, *BuzzFeed*, May 22, 2018.

⁵⁰ <https://developer.android.com/guide/topics/permissions/overview?hl=en>.

⁵¹ *Id.*

⁵² https://play.google.com/intl/ALL_us/about/developer-distribution-agreement.html.

⁵³ <https://play.google.com/about/privacy-security-deception/permissions/>.

Apps may only use the permission (and any data derived from the permission) to provide approved critical core app functionality (e.g. critical current features of the app that are documented and promoted in the app's description). You may never sell this data. The transfer, sharing, or licensed use of this data must only be for providing critical core features or services within the app, and its use may not be extended for any other purpose (e.g. improving other apps or services, advertising, or marketing purposes). You may not use alternative methods (including other permissions, APIs, or third-party sources) to derive data attributed to the above permissions.⁵⁴

The developer guide for Android states:

In some circumstances, you want to help the user understand why your app needs a permission. For example, if a user launches a photography app, the user probably won't be surprised that the app asks for permission to use the camera, but the user might not understand why the app wants access to the user's location or contacts. Before your app requests a permission, you should consider providing an explanation to the user.⁵⁵

The developer guide also states:

Only use the permissions necessary for your app to work. Depending on how you are using the permissions, there may be another way to do what you need (system intents, identifiers, backgrounding for phone calls) without relying on access to sensitive information.

And:

Be transparent. When you make a permissions request, be clear about what you're accessing, and why, so users can make informed decisions. Make this information available alongside the permission request including install, runtime, or update permission dialogues.

The developer guide also states that apps will only be allowed on Android if:

The app requests only the absolute minimum permissions that it needs to support core functionality.

And:

⁵⁴ *Id.*

⁵⁵ <https://developer.android.com/training/permissions/requesting.html?hl=en>.

The app does not request permissions to access sensitive data (such as Contacts or the System Log) or services that can cost the user money (such as the Dialer or SMS), unless related to a core capability of the app.⁵⁶

Political Social Media's apps, however, do not abide by these standards. As the company has made abundantly clear throughout its marketing materials, the purpose of its apps is to convince users to turn over their contact information for the benefit of the sponsoring organizations. Political Social Media entices users to enjoy its platform and play the games in order to get access to the phonebooks of its users. Political Social Media's apps, therefore, are a prima facie violation of the Google Play Developer Distribution Agreement.

Template Apps

Google's Developer Program Policies also prohibit Political Social Media's template model. The guidelines regarding "repetitive content" state:

We don't allow apps that merely provide the same experience as other apps already on Google Play. Apps should provide value to users through creation of unique content or services.⁵⁷

Google offers examples of common violations:

Copying content from other apps without adding any original content or value.

Creating multiple apps with highly similar content and user experience. If these apps are each small in content volume, developers should consider creating a single app that aggregates all the content.

Apps that are created by an automated tool, wizard service, or based on templates and submitted to Google Play by the operator of that service on behalf of other persons are not allowed. Such apps are only permissible if they are published by an individually registered developer account belonging to the user of the automated tool, not the operator of the service.⁵⁸

Nevertheless, Political Social Media is publishing nearly identical template apps for each of its clients and submitting them to Google Play using its own developer account, instead of each client, including FRC and SBA List -- submitting its own app as Google requires.⁵⁹ As *TechCrunch* reported, Google's policy was rewritten to address this exact problem.⁶⁰

⁵⁶ <https://developer.android.com/docs/quality-guidelines/core-app-quality>.

⁵⁷ <https://play.google.com/about/spam-min-functionality/spam/repetitive-content/>.

⁵⁸ *Id.*

⁵⁹ Sarah Perez, *Google Follows in Apple's Footsteps by Cleaning Up Its Play Store*, *TechCrunch*, July 27, 2018, available at <https://techcrunch.com/2018/07/27/google-follows-in-apples-footsteps-by-cleaning-up-its-play-store/>.

⁶⁰ *Id.*

Unfortunately, Google has yet to remove Political Social Media's apps from Google Play despite the company's clear violation of this policy. The fact that the official apps for two controversial advocacy organizations, FRC and SBA List, are nearly identical and published by Political Social Media highlights the problem with failing to implement this rule.

Enforcement

The Google Play Developer Distribution Agreement states:

If Google becomes aware and determines in its sole discretion that a Product or any portion thereof (a) violates any applicable law; (b) violates this Agreement, applicable policies, or other terms of service, as may be updated by Google from time to time in its sole discretion; (c) violates terms of distribution agreement with device manufacturers and Authorized Providers; or (d) creates liability for or has an adverse impact on Google or Authorized Providers; then Google may reject, remove, suspend, or reclassify the Product from Google Play or from Devices. Google reserves the right, at its sole discretion, to suspend and/or bar any Product and/or Developer from Google Play or from Devices.⁶¹

Here, it is clear that Political Social Media's apps violate the Google Play Developer Distribution Agreement and should be removed from Google Play.

⁶¹ https://play.google.com/intl/ALL_us/about/developer-distribution-agreement.html.

Conclusion

Previously, Google has revoked access to apps that violate the company's rules. Yet here, Google has failed to act despite clear evidence that Political Social Media and, to a lesser extent, FRC and SBA List and others by failing to submit their own apps, are in violation of the Google Play Developer Distribution Agreement. Further, beyond simply violating the rules, Political Social Media's apps have been investigated by United Kingdom government regulators and criticized by privacy advocates. At a time when democracies are struggling to cope with and confront the ever-increasing onslaught of misleading information filtered through social media, Google should remove these apps from Google Play to ensure users have access to rule-abiding apps that share legitimate information.

Sincerely,

A handwritten signature in black ink, appearing to read "Dan E Stevens", with a long horizontal flourish extending to the right.

Daniel E. Stevens
Executive Director

A handwritten signature in blue ink, appearing to read "Alice C.C. Huling", with a stylized, flowing script.

Alice C.C. Huling
Counsel