Google

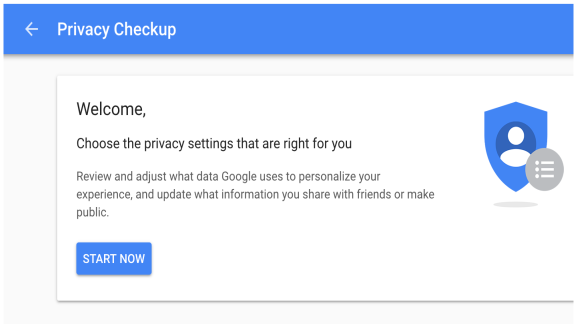
The Honorable Charles E. Grassley
Chairman
Committee on the Judiciary
226 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Mr. Chairman,

Thank you for your letter. I am responding on behalf of our Chief Executive Officer, Sundar Pichai.

Google works hard to provide choice, transparency, control, and security for user data. We appreciate the opportunity to tell you about how we protect our billions of users around the world.   Users themselves can find similar information across our sites, or by just typing <Google privacy> into their search engine of choice.

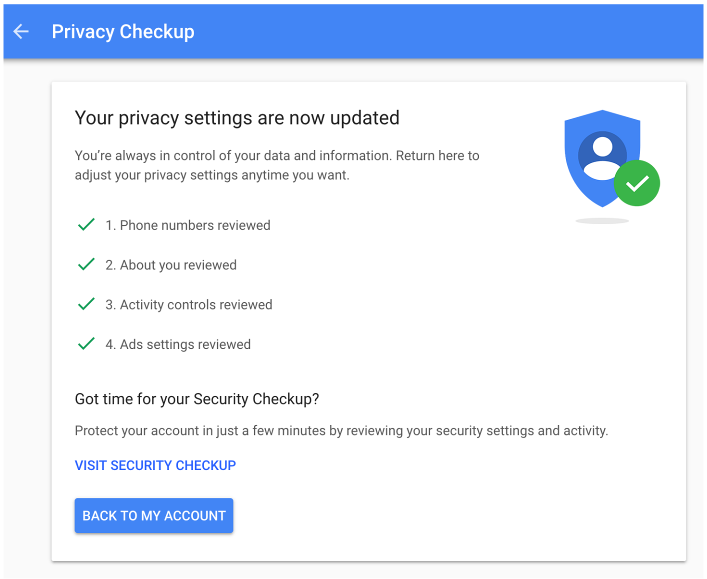
We were one of the first companies to offer a centralized data portal when we launched MyAccount in 2015 (https://myaccount.google.com/). MyAccount provides easy-to-use tools to help manage privacy and security. That includes our Privacy Checkup tool (https://myaccount.google.com/Privacycheckup) that lets our users review and change their privacy settings:



Welcome,

Choose the privacy settings that are right for you

Review and adjust what data Google uses to personalize your experience, and update what information you share with friends or make public.



Your privacy settings are now updated

You're always in control of your data and information. Return here to adjust your privacy settings anytime you want.

✓ 1. Phone numbers reviewed

✓ 2. About you reviewed

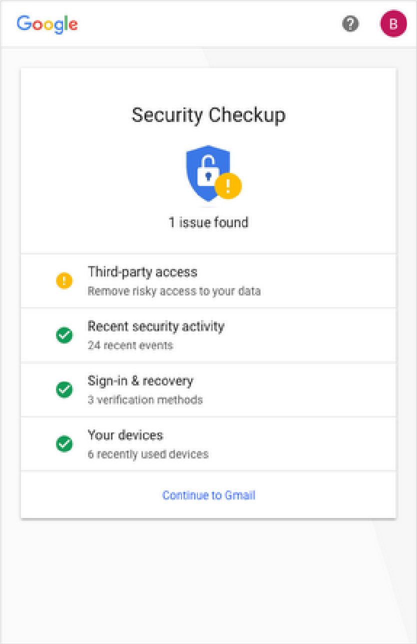
✓ 3. Activity controls reviewed

✓ 4. Ads settings reviewed

Got time for your Security Checkup?

Protect your account in just a few minutes by reviewing your security settings and activity.

MyAccount also includes our Security Checkup (available at https://myaccount.google.com/security-checkup), which helps people make informed decisions about security and privacy, including by identifying the apps that have access to their data and letting them revoke access to those apps:



Security Checkup

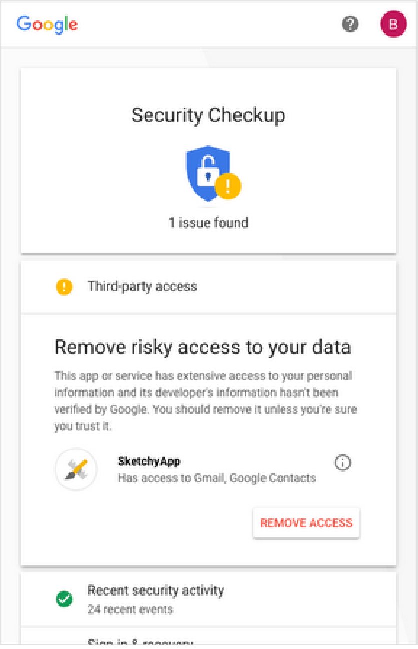
1 issue found

Third-party access
Remove risky access to your data

Recent security activity
24 recent events

Sign-in & recovery
3 verification methods

Your devices
6 recently used devices



Security Checkup

1 issue found

Third-party access

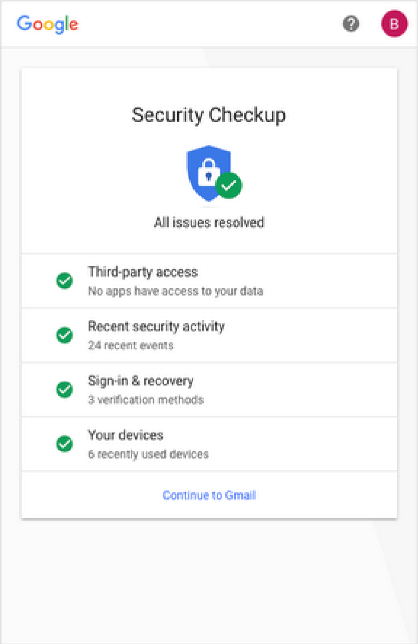
Remove risky access to your data

This app or service has extensive access to your personal information and its developer's information hasn't been verified by Google. You should remove it unless you're sure you trust it.

SketchyApp
Has access to Gmail, Google Contacts

Recent security activity
24 recent events

Sign-in & recovery



Security Checkup

All issues resolved

Third-party access
No apps have access to your data

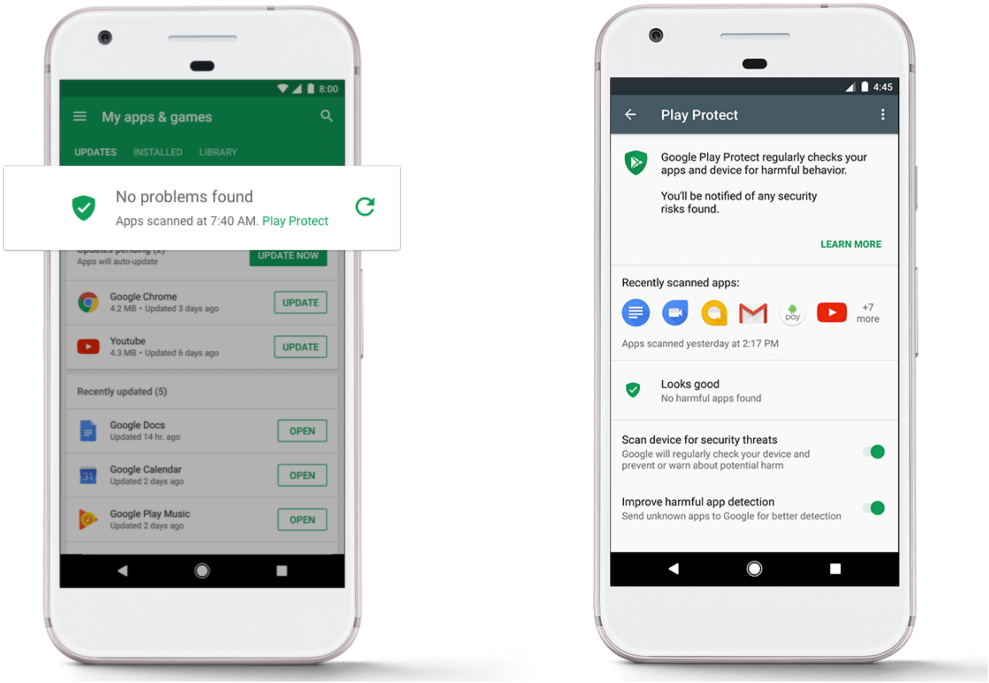
Recent security activity
24 recent events

Sign-in & recovery
3 verification methods

Your devices
6 recently used devices

Similarly, our goal is to make Android the safest computing platform in the world. That's why we invest in technologies and services that strengthen the security of Android devices, apps, and the global ecosystem. And why we demand that app developers protect the privacy of users. Apps on Google Play, for example, are required to link to a comprehensive and accurate privacy policy that describes the data they collect, what they do with it, and with whom they share it.

Those requirements are backed by the security of Google. Our advanced security tools protect our users when they interact with apps. Google Play Protect, for example, comes pre-installed on all Google-licensed Android devices and continuously monitors users' phones, along with apps in Play and across the Android ecosystem, for potentially malicious apps. It scans more than 50 billion apps every day and warns users to remove apps we identify as malicious:



No problems found

Apps scanned at 7:40 AM. Play Protect

Apps will auto-update

Google Chrome
4.2 MB • Updated 3 days ago

Youtube
4.3 MB • Updated 6 days ago

Google Docs
Updated 14 hr. ago

Google Calendar
Updated 2 days ago

Google Play Music
Updated 2 days ago

Google Play Protect regularly checks your apps and device for harmful behavior.

You'll be notified of any security risks found.

Apps scanned yesterday at 2:17 PM

Looks good
No harmful apps found

Scan device for security threats
Google will regularly check your device and prevent or warn about potential harm

Improve harmful app detection
Send unknown apps to Google for better detection

Play Protect uses a variety of different technologies to keep users and their data safe, but the impact of machine learning is already quite significant: 60.3% of all Potentially Harmful Apps were detected via machine learning in 2017. More information about Google Play Protect is available at https://www.android.com/play-protect/.

1. **What are your current policies and procedures with respect to the sharing of data with third party developers, including how you notify users of such sharing and/or request their consent?**

    a. **How have these policies and procedures evolved/changed since 2010?**

    b. **Do you intend to make any changes in light of recent events?**

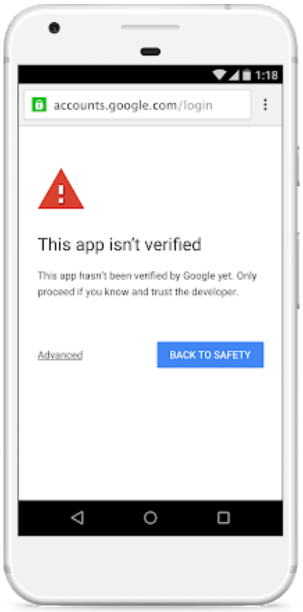
Google has a longstanding commitment to ensuring both that our users share their data only with developers they can trust, and that they understand how developers will use that data.

For example, our Google APIs terms of service, which govern how developers can access user data, were introduced in 2011 (https://developers.google.com/terms/).

Since their inception, our terms have required that developers provide and adhere to a privacy policy that clearly and accurately describes what user information they collect and how they use and share that information with others.

Since 2016, those terms have been supplemented by a user data policy found at https://developers.google.com/terms/api-services-user-data-policy. That policy prohibits developers from exposing a user's non-public content to other users or to third parties without explicit opt-in consent and also prohibits scraping, building databases, or otherwise creating permanent copies of users' data.

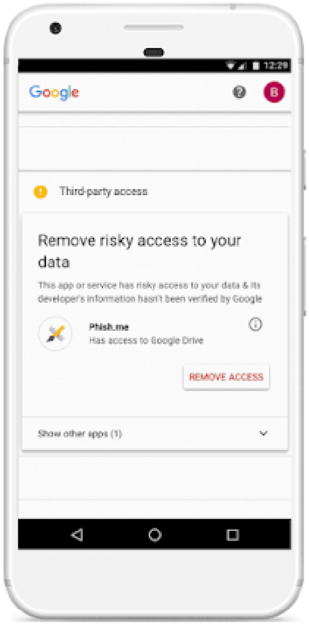
We support our policies with verification, monitoring, and enforcement. We require web apps that request access to sensitive data to complete a verification process, described at https://developers.google.com/apps-script/guides/client-verification. That process involves a review of the app's privacy policy to ensure that it adequately describes the types of data it wants to access and a review of the suitability of permissions the app is requesting. If an app is not verified by Google, we display a prominent warning to users that they are using an "unverified app" and strongly discourage them from proceeding. Those apps would also be flagged to users by our Security Checkup tool:



accounts.google.com/login

This app isn't verified

This app hasn't been verified by Google yet. Only proceed if you know and trust the developer.



Third-party access

Remove risky access to your data

This app or service has risky access to your data & its developer's information hasn't been verified by Google

Phish.me
Has access to Google Drive

Similarly, developers who distribute apps through Google Play, our Android app store, must agree to comply with a robust set of developer policies regarding the access of personal or sensitive information. Those policies can be found at https://play.google.com/about/developer-content-policy/. Since 2016, our Google

Play policies have required developers to provide and adhere to a privacy policy if they collect certain types of personal data, including personally identifiable information, financial and payment information, authentication information, phonebook or contact data, microphone and camera sensor data, and sensitive device data.

We are always reassessing our policies and procedures to ensure the protection of our users. If we find that our policies can be improved, we will make those changes.

2. **How do you ensure that user data shared with third party developers is not improperly transferred or used?**

As discussed above, to protect our users, web apps that request access to sensitive data must go through a verification process. We use machine learning to monitor apps once they have been given access. If we detect significant changes in the behavior of the app, we manually review the app. If that review determines that the app is violating our terms, the "Unverified App" screen is displayed to users and we restrict the app's ability to use our service.

Apps on Google Play are also subject to automated and, in some cases, manual review for security and policy compliance. We also use automated scanners to protect millions of users each day from malware, phishing scams, fraud, and spam, including through Google Play Protect, which continuously scans all Google-licenced Android devices for potentially malicious apps and protects two billion Android users daily.

Lastly, Google acts promptly on user reports about privacy and security issues. We reward researchers and developers who flag privacy and security issues, and we engage in research and community outreach on privacy and security issues to make the internet safer.

3. **Do you limit the ability of third party developers to collect data beyond the scope of their application? If so, how do you ensure that third party developer agreements are limited in scope?**

We are committed to protecting our users' data and prohibit developers from requesting access to information they do not need. Our developer guidelines for web apps and Google Play are clear: requests for access to users' data should make sense to users, and should be limited to the critical information necessary to implement the app. Developers may only request access to Android device data or Google user data that is necessary to implement existing features or services in their app. Developers are not allowed to request access to information for services or features that have not yet been implemented. You can find those Google Play developer policies at https://play.google.com/about/privacy-security-deception/permissions/, and our web developer policies at https://developers.google.com/terms/api-services-user-data-policy#request-relevant-permissions.

Web apps and apps on Google Play requesting sensitive data are required to link to a comprehensive, accurate, and easy to read privacy policy, describing what user data they collect, what they do with it, and with whom they share it. We require developers to limit their use of data to the practices explicitly disclosed in that policy. If they want to change their app to use data in a manner that is inconsistent with their existing privacy policy, they must prompt users to consent to an updated privacy policy. As discussed above, if apps do not include an explicit and accurate privacy policy or otherwise violate our terms, our automated and manual reviews are designed to identify and either remove them or warn users that they are accessing an unverified app.

4. **What remedies do you have against a third party developer who exceeds the scope of their access?**

Our terms of service explicitly give us the authority to review and analyze apps and to ensure compliance with our policies. We reserve the right to terminate developers' access to our system and we reserve all rights and remedies we have against developers under contract, tort, or any other law or regulation.

5. **Do you have protocols built into your third party developer platform to monitor data usage or access?**

Yes. As discussed above, we require web apps to go through a verification process when they request access to Google users' sensitive data. To address the possibility that apps change their behavior after the verification process, we use machine learning to continually evaluate apps to identify anomalous behavior. If anomalous behavior is detected, the app is flagged for manual review. For apps on Android, Google Play Protect works daily to protect the data of more than two billion Android users by scanning all of the apps on Google-licensed Android devices to identify and recommend to users that they remove apps engaged in malicious behavior.

6. **What audit procedures do you have to ensure compliance with third party developer agreements?**
    a. **How often have these audits been carried out?**
    b. **How compliant have third party developers been?**

We conduct periodic audits of web apps and apps on Google Play to ensure compliance with our policies. For example, we recently conducted an audit of privacy policies of apps on Google Play to confirm that developers' uses of privileges were reasonable. We not only use these audits for enforcement purposes but also to enhance our policies and processes. These types of manual reviews are conducted in addition to our continuous automated methods of detecting malicious behavior by app developers, such as Google Play Protect. Last year, Google Play Protect led to the identification and removal of 39 million potentially harmful apps from Android devices. We remain committed to ensuring the protection of our users' data and plan to continue both our periodic manual audits and automated monitoring of apps in the future.

7. **Have third party developers breached your terms/agreements in the past, and what remedies have you taken?**

We have taken a wide-range of enforcement efforts, including warning users about apps that we have been unable to verify and removing apps from our Play Store when they violate our policies. When we suspect an app is engaged in malicious behavior on an Android device, we take action, including notifying users and recommending that they remove apps from their device. When a developer engages in repeated or serious violations of our policies (such as malware, fraud, and apps that may cause user or device harm), we terminate their accounts.

8. **What are your current policies and procedures with respect to notifying users of a data breach?**
    a. **How have these policies and procedures evolved/changed since 2010?**
    b. **Do you intend to make any changes in light of recent events?**

As we described above, Google is committed to protecting the data of its users and to transparency. We have internal policies that require employees to report any suspected security or privacy incidents to our dedicated 24x7x365 worldwide incident response teams, so that we can respond, including securing and protecting users' data and handling user notifications. This is in addition to the warnings we provide our users when we suspect any malicious activity by developers or when they are interacting with apps we have been unable to verify. As discussed above, if a web app is not verified by Google, we display a prominent warning to users that they are using an "unverified app" and strongly discourage them from proceeding. And on Google-licensed Android devices, Google Play Protect scans for suspicious activity. When we suspect an app is engaged in malicious behavior on an Android device, we take action, including notifying users of the malicious behavior and recommending that the user remove the app.

We continue to review our policies to ensure they are protecting our users' interests and will revise them when we believe we can make improvements.

9. **What are your current policies and procedures with respect to notifying users of an improper transfer of their data?**

    a. **How have these policies and procedures evolved/changed since 2010?**

    b. **Do you intend to make any changes in light of recent events?**

We're are always looking at ways we can improve our policies around the protection and notification of the improper transfer of users' data and will continue to do so in light of recent events. We've had a long-established commitment to transparency for our users. As described above, we automatically flag any suspicious or unverified web apps for our users. We also protect 2 billion Android users through Google Play Protect, which uses automated scanners to identify malicious behavior and notifying users of the malicious behavior. This is in addition to the work we do to educate our users about who is who is accessing their data to prevent the improper use or transfer of data by malicious apps. In 2009, we launched Google Dashboard, which shows people the products they are using and the data associated with each. In 2015, we initiated MyAccount, which lets users make informed choices about their data through easy-to-use tools designed to help manage their privacy and security.

10. **Do you restrict the ability of third party developers to access data for a political purpose?**

As reflected in our various user tools, we believe that users should have the opportunity to make informed decisions. That is why we require that <u>all</u> developers be transparent about the data they are collecting, and what they are using that data for. Web apps and apps accessing sensitive data on Google Play, for example, are required to link to a comprehensive, accurate, and easy-to-read privacy policy, describing what user data they collect, what they do with it, and with whom they share it. We warn users when web apps have not been verified and we prohibit developers from engaging in impersonation, deception, malicious behavior, and facilitating the use or distribution of restricted content. You can find our policies regarding impersonation at https://play.google.com/about/ip- impersonation/, and our policies regarding deception and malicious behavior at https://play.google.com/about/privacy-security-deception/.

We are also committed to transparency on our ads platform, where we'll soon be rolling out the commitments around Election ads that we announced in Fall 2017, including a transparency report and a publicly accessible repository of Election Ads from across our Ads products.

11. **What engagement do you have with political campaigns and do you have policies and procedures governing these engagements?**
    a. **How have these policies and procedures evolved/changed since 2010?**
    b. **Do you intend to make any changes in light of recent events?**

Google is fully committed to ensuring the integrity of democratic elections, and we have invested in tools to ensure election security. We established an Elections Security Team to advise campaigns on security in the run-up to elections, including campaign trainings and workshops on email and campaign website security.

We offer Project Shield (https://projectshield.withgoogle.com/public/), which provides campaigns with the ability to secure their websites from attack, at no cost. And last year we launched our Advanced Protection Program (https://landing.google.com/advanced protection/) which integrates physical security keys to protect those at greatest risk of attack, like journalists, business leaders, and politicians.

As threats evolve, we will continue to adapt to understand and prevent new attempts to misuse our platforms and will continue to expand our use of cutting-edge technology to protect our users and campaigns. You can learn more about our work with campaigns here: https://protectyourelection.withgoogle.com/intl/en/.

Interactions with campaigns by our Sales Teams are governed by policies established by our dedicated political law compliance specialist.   In 2010, we had only one sales team member working with the small number of campaigns that sought to advertise online. As our team who works with political clients has grown, our policies and procedures have evolved. For example, we have a strict "firewall" between the team that works with campaigns seeking to advertise on Google platforms and the team that works with independent expenditure only committees seeking to advertise on Google platforms.

Lastly, we continuously review our policies with respect to elections and political campaigns with an eye to improving them. This year, we are implementing the commitments we announced in Fall 2017 with respect to Election ads, including verifying that advertisers running Election Ads are US-based; disclosing who paid for each Election Ad; publishing our first ever transparency report, detailing who is buying Election-related ads on our platforms and how much money is being spent, and introducing a publicly accessible repository of Election Ads from across our Ads products .

12. **How do you monitor the ability of foreign entities to access user data? What restrictions are in place to limit such access?**

Developers, wherever they are located, must fully comply with our terms of service and developer policies, which protect our users and their data from misuse and require transparency about who is accessing their data and how they'll use it.   Additionally, since 2012, if we suspect that one of our users is being targeted by a government-backed attacker, we show them prominent warnings in Gmail and guide them through steps to secure their information. More information about those warnings are available at https://security.googleblog.com/2012/06/security-warnings-for-suspected-state.html.

13. **How do you monitor the ability of foreign entities to influence and interfere with U.S. elections?**

Google is very concerned about attempts to undermine democratic elections and deeply committed to addressing this issue. We have a global team of thousands of policy experts, reviewers, product managers, and data scientists focused on creating, maintaining, and enforcing our policies against abuse. They work closely with machine learning tools and our algorithms to ensure our platforms are protected. Through a combination of sophisticated algorithms, other technologies, and human review, we detect violations and respond to complaints. We also partner with NGOs through our trusted flagger programs, programs like the Trust Project, and our partnership with the Belfer Center for Science and International Affairs on its Defending Digital Democracy Project. And we continue our long-established policy of routinely sharing threat information with our peers, working with them to better protect the collective digital ecosystem. We also welcome input from law enforcement and Congress.

14. Are you aware of any foreign entities seeking to influence or interfere with U.S . elections through your platforms?

Protecting our platforms from state-sponsored interference is a challenge we have been tackling as a company for many years. We face motivated and resourceful attackers, and we are continually evolving our tools to stay ahead of ever-changing threats. We've built industry-leading security systems and we've put these tools into our consumer products. Back in 2007, we launched the first version of our Safe Browsing tool, which helps protect users from phishing, malware, and other attack vectors. Today, Safe Browsing is used on more than three billion devices worldwide. If we suspect that users are subject to government-sponsored attacks we warn them. And we recently launched our Advanced Protection Program, which integrates physical security keys to protect those at greatest risk of attack, like journalists, business leaders, and politicians.

As outlined in our 2017 Congressional testimony, we identified very limited activity on our platforms prior to the 2016 election, but the threat is evolving and our investigation and monitoring efforts to prevent and detect misuse are ongoing. We will continue to develop tools and processes to combat evolving threats — we understand the importance of maintaining and enhancing our controls as we go into the 2018 election season. We are committed to working with Congress, law enforcement, others in our industry, and the NGO community to strengthen protections around elections, ensure the security of users, and help combat disinformation campaigns.

Thank you again for the opportunity to tell you about our efforts. Please do not hesitate to contact me if you have further questions.

Best,

Sue Molinari

Susan Molinari, Vice President, Public Policy and Government Affairs, Americas