API Privacy: A Look at G Suite Marketplace Permissions and Policies

Irwin Reyes
Two Six Labs
Arlington, VA, USA
irwin.reyes@twosixlabs.com

Michael Lack
Two Six Labs
Arlington, VA, USA
michael.lack@twosixlabs.com

***Abstract*—Software developers routinely use application programming interfaces (APIs) to leverage existing data and functionality offered by external services. Online services such as Facebook and Google offer their own APIs for that purpose, and allow developers to access private user information like messages, files, and calendars if given proper user authorization. This has, however, produced serious privacy breaches, most notably Cambridge Analytica's unexpectedly broad collection of user data through the Facebook API. In light of this, we examined a corpus of 987 Google API apps on the G Suite Marketplace. We found that nearly half of those apps are able to communicate with outside services, whose identities aren't reliably disclosed to users. Additionally, our data suggests that app auditing measures meant to protect users from potential API misuse may fall short: a new user limit placed on potentially risky unverified apps is not rigidly enforced, and thousands of users will nonetheless authorize risky apps if allowed. We offer potential directions for improvement of this ecosystem and hope to spur further investigations of online APIs as a whole.**

***Index Terms*—privacy, APIs, disclosure, measurement**

I. Introduction

Numerous online services expose application programming interfaces (APIs) that allow third-party software developers to take advantage of those services' existing capabilities [1]. Some online APIs merely expose data offered by the service. These allow programmatic access to large amounts of information in a consistent machine-parseable format, instead of arbitrarily structured text commonly found in human-readable websites. For example, US government agencies offer data for public use through APIs [2] [3] [4]. Other APIs also expose functionality that third-party products can use to process data or automate interactions with the online service. For example, websites and mobile apps commonly use the Google Maps API [5] for navigation and visualization. And Microsoft offers a tool that uses APIs offered by cloud storage providers (*e.g.,* Dropbox, Amazon S3, and Google Drive) to automate the migration of user files into Office 365 [6].

Online services often impose varying degrees of access control on their APIs [7]. Depending on the service's own business requirements and the sensitivity of what's exposed by the API, online services might require developers to obtain proper authorization in order to use the API at all. In this case, developers would need to include a valid API key—typically generated and tracked by the online service—in their software in order to use the API. Access control measures help ensure that the online service's resources are fairly allocated (*i.e.,* preventing one third-party developer from hogging all the service's resources and denying access to others) and that the online service knows who's using what API functionality.

Online APIs may also allow third-party software to obtain, modify, or otherwise interact with sensitive data that users have provided to the service. For instance, the aforementioned Microsoft file migration tool needs to read user files from a given cloud storage provider in order to move them to Office 365. The cloud storage APIs that enable this functionality not only require the software to obtain authorization from the provider, but individual users must also authorize the software to read their personal data. Online services may require third-party software to notify users of what sensitive data and operations they intend to access via API, then prompt the user for consent in order to proceed [8] [9].

Software developers routinely employ this notion of "notice and consent" when requesting access to sensitive user data. Prior investigations into this practice, however, has shown that users often consent to the requested terms merely out of habit instead of actual comprehension [10]. Indeed, this has resulted in grave breaches of consumer privacy. This happened most notably in 2016 when the political consulting firm Cambridge Analytica collected and exploited data from 87 million Facebook users without their full understanding [11]. Cambridge Analytica obtained this data through the Facebook web app "thisisyourdigitallife," initially developed as a personality quiz for academic purposes. Users authorized this app to access various parts of their Facebook data, such as their public profile, city, and page likes, as well as that of their friends. This sparked widespread backlash against Facebook, due in part to Cambridge Analytica's role in the highly contentious 2016 United States presidential election [12].

In response to the subsequent outcry from lawmakers [13] and the public at large [14], Facebook implemented stricter limits on the personal data third-party apps may access through the Facebook API, as well as limiting how long apps have access to consumer data without user interaction [15]. These measures, however, came about following sustained negative press coverage and intense scrutiny from regulators, and only after initial resistance from Facebook in light of the Cambridge Analytica revelations [16]. Although Facebook is a massive online service with a user base measuring in the billions [17],

it is not unique in its scale, scope of data collection, or offering third-party apps access to consumer data via API.

This work is a preliminary investigation into analogous risks to consumer data posed by Google's API and the various disclosure mechanisms surrounding it. Like Facebook, Google has an active user base in the billions [18], competes with Facebook in the social media and advertising space [19], and allows third-party apps to integrate with Google functionality and user data via an API [20]. Unlike Facebook, Google has not been subjected to the same level of criticism prompted by the Cambridge Analytica scandal. This work intends to motivate further examinations into how online services as a whole give third-party apps programmatic access to user data, as well as how consumers are informed of those privileges.

II. Related Work

A. API Privacy and Security

Risks posed by online APIs to user data privacy and security have seen renewed interest in the wake of the Cambridge Analytica scandal. Russell, et al. [21] characterized the general uses of APIs: content-focused APIs that provide data; feature APIs that allow other services to integrate existing software functionality from elsewhere; unofficial APIs that attempt to expose internal interfaces for external use; and analytics APIs that give developers information about users and visitors. This work points out that at the height of the Cambridge Analytica scandal, Facebook revoked access to thousands of apps that failed to submit to audit. Our analysis of Google API apps primarily covers content-focused APIs and feature APIs (*e.g.,* programmatic access to Gmail data and functionality), which may require apps to be verified depending on the sensitivity of the API functions involved.

Additionally, Google has taken actions themselves following the Cambridge Analytica backlash. As part of their own response, they started rolling out finer-grained app permissions [22]; rather than approving all or no permissions, users would be able to approve or deny app access to each service (*e.g.,* Gmail, Drive, Calendar, etc.). Our work, however, found that nearly all Google API apps in in the G Suite Marketplace use the old model, and we scraped that data accordingly.

B. Analysis of Web Apps

Prior work on the analysis of web apps focused heavily on the various third-party apps that users can authorize on their Facebook accounts. Huber, et al. [23] developed a method to analyze privacy leaks in Facebook apps at scale. Taking advantage of the fact that Facebook apps run in embedded iframes, Huber installed apps on test Facebook accounts and loaded the apps on browsers instrumented to capture network traffic. This approach focused on identifier leakage in the HTTP traffic with those iframes rather than the API permissions held by the app. We do, however, follow their method of analyzing apps listed in the API provider's central app repository.

Felt, et al. [24] in 2008 manually examined the permissions and runtime behaviors of 150 Facebook apps. By searching for the appearance of profile or social graph data in the app UI, this research found that 90% of the examined apps have unnecessary access to private user data. This was primarily due to the nature of Facebook app authorizations at the time: all apps required the user to install or log into the application, which automatically granted access to private data.

Our work most closely follows the methods and results by Wang, et. al [25], which in part analyzed the permissions requested by Facebook API apps at install time. This work presents a distribution of the most commonly requested API functionalities. We do the same, but we also tie those permissions into Google's policies regarding usage and review: Google API apps that request access to user data may be subject to review and have restrictions placed on them while pending verification [26].

III. Methodology

We investigate third-party uses of the Google API [20] to identify potential risks to consumer data, as well as how third-party developers and Google themselves communicate those risks. We chose to examine Google for a number of reasons. Google has a very large user base, with approximately 1.5 billion active Gmail users as of 2018 [18]. Everyday consumers and enterprises alike entrust Google services with highly sensitive data; this includes email [27], files [28], calendars [29], and contact lists [30], all accessible via API with the proper authorizations. And Google has not had a scandal of the same magnitude as Facebook did with the Cambridge Analytica incident [11].

A. G Suite Marketplace Apps

In order to shed light into how third-party developers actually use the Google API in the wild, we assembled a corpus of publicly available Google API apps and examined what sensitive API functionality they disclose to users at the time of authorization.

The G Suite Marketplace [31] is a catalog of web apps that individual users and G Suite administrators can give access to their Google account data. Despite the name, apps in the Marketplace do not necessarily require G Suite accounts; most are compatible with regular free Google accounts. Marketplace apps focus primarily on productivity, as indicated by the platform's top-level categories: "Business Tools," "Productivity," "Education," "Communication," and "Utilities." Popular apps include the bibliography manager EasyBib [32], the diagramming utility draw.io [33], and the 3D modeling tool SketchUp [34], all listed with over 10 million users each.

We manually visited each G Suite Marketplace category, subcategory (*e.g.,* "Marketing & Analytics"), and service collection (*e.g.,* "Works with Gmail") to find web apps that users can authorize on their Google accounts. This yielded 1,392 unique web apps. We then used a Selenium script to scrape each app's listed metadata(*e.g.,* user count, developer), requested privileges (Fig. 1), Google verification status, and any error messages thrown during the authorization process. We ran this Selenium script under a Firefox profile already signed into a regular free Google account (*i.e.,* a "@gmail.com" user).

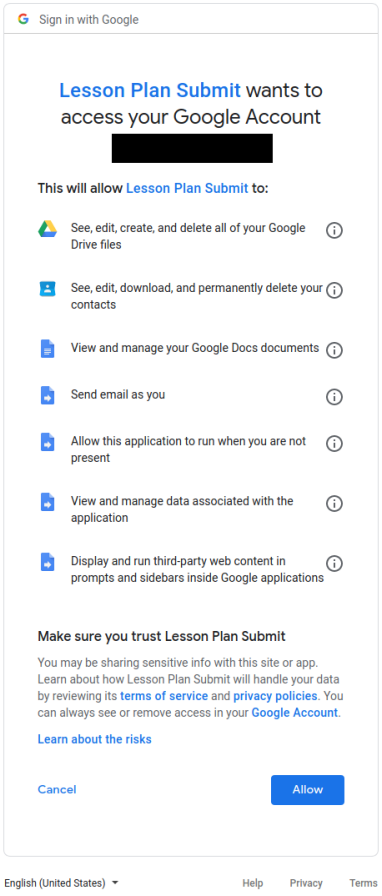

Fig. 1. Apps prompt the user for authorization to their Google data

This resulted in 987 apps that were successfully authorized to this account: 889 that requested API authorizations, and 89 that requested none (*i.e.,* those used the Google account only for authentication). Among the ones that failed to install, 237 apps were not compatible with regular Google accounts, as they require a G Suite administrator to perform the installation domain-wide. 133 apps could not be installed because they produced an error "Sign in with Google temporarily disabled for this app." And the remaining 35 apps threw various other errors. We collected this data on January 2, 2020.[1]

B. Limitations

Google does not provide a comprehensive listing of *all* products that integrate with its API. Our analysis of app authorizations and disclosures relied exclusively on the G Suite Marketplace. While the G Suite Marketplace yielded data for nearly 1,000 apps for this research, it is unlikely that this sample is representative of all software that integrate with the Google API. The G Suite Marketplace only lists web apps; no mobile apps or standalone desktop software. There are 3 million Android apps on the Play Store as of December 2019 [35] and 4 million iOS apps (which are able to use the Google API) on the Apple App Store as of July 2019 [36]. If even a small fraction of mobile apps use the Google API, those would likely dominate the results. We acknowledge that generalizable conclusions require broader investigation into how other classes of software use Google API functionality.

Further, Google does not appear to offer a definitive listing of all API authorizations and which ones Google considers "sensitive" enough to require verification under their API policy [37]. The policy defines "sensitive" API authorizations as those that "allow access to Google User Data" but fail to actually list them. This has led to confusion [38] and frustration [39] among app developers. For our research, this limits our ability to rigorously analyze which disclosed API functions pose potentially greater risks to user privacy than others. Any judgments to that effect in this analysis are ours alone. Those may be open to debate and interpretation until Google releases authoritative documentation of the relative sensitivity levels of all API functions.

Finally, we also acknowledge that although this work aims to investigate consumer data privacy and disclosure regarding online services' APIs, this research examined only Google specifically. There are many other major online services that offer APIs that third-party apps may use to access consumers' private data. These include Twitter [40], GitHub [41], Office 365 [42], and Slack [43], among countless others. Although some general observations and recommendations might be relevant to other APIs, this research only presents findings that are specific to Google's API.

IV. Results

We scraped the G Suite Marketplace and identified 987 web apps that we successfully authorized on a regular free "@gmail.com" account. We draw our findings from this corpus. We were unable to authorize an additional 405 apps listed on the Marketplace. Our analysis omits these apps because their authorizations prompts (Fig. 1) were unreachable. Refer to the *Methodology* section for further details.

A. App Authorizations

Of the 987 web apps in our corpus, 90% listed at least one Google API authorization. The remaining 10% only used the user's Google account for single sign-on. After successful authorization, however, all these apps gain access to the user's basic account information: name, email address, and profile picture [44]. From the apps that did list API privileges, our corpus yielded 130 unique strings describing the various API functionality the apps use. Table I summarizes the 10 most frequently requested authorizations.

The request to "Connect to an external service" is notable, as it indicates apps can communicate with other online APIs that neither Google nor the app developer might not control. 481 of the G Suite Marketplace apps we examined—nearly half—disclosed this capability. We note that the app authorization prompt only discloses if an app can connect to external services; it provides no details about what those external services are, or for what purpose a given app is using those APIs. While some developers do elaborate on this in their apps'

[1]https://irwinreyes.com/assets/files/2020-conpro/scrape-20200102.json

Authorization	% apps
Display and run third-party web content in prompts— and sidebars inside Google applications.	50%
Connect to an external service.	49%
See, edit, create, and delete your spreadsheets in Google Drive.	27%
Allow this application to run when you are not present.	25%
See, edit, create, and delete all of your Google Drive files.	21%
View and manage your Google Docs documents.	13%
Run as a Gmail add-on.	11%
View and manage data associated with the application.	11%
Send email as you.	10%
View users on your domain.	9.0%

TABLE I
10 MOST COMMON AUTHORIZATIONS, N = 987 APPS

Marketplace listings [45] or external privacy policies [46], a cursory spot check on a selection of these 481 apps shows this is not always the case [47] [48].

Within the 481 apps that can connect to external APIs, some that also indicate their ability to access highly sensitive user data. Among the most potentially risky are 103 (21% of this subset) that "See, edit, create, and delete all of your Google Drive files;" 81 (17%) that "View your email messages when the add-on is running;" and 15 (3.0%) that "See, edit, download, and permanently delete your contacts." Beyond Marketplace descriptions or privacy policies that developers voluntarily provide, users have little insight into the possibility that other services receive private user through external APIs.

B. *Unverified Apps*

In order to curb potential abuse of users' private data, Google's policy requires app developers to submit their products for review if they call API functions that "allow access to Google User Data" [37]. This review takes 3 to 5 days for apps that use "sensitive" API calls, or 4 to 8 weeks for apps that use the subset of "restricted" API calls specifically concerning Gmail or Google Drive data. Given long turnaround times, Google allows unverified apps to be made available without review [26], but subject to restrictions: only 100 new users may link a given unverified app to their accounts (with discretion to make adjustments "based on the app history, developer reputation, and riskiness"), and the app authorization dialog displays a warning discouraging users from doing so (Fig. 2).

Our scrape of the Marketplace produced 277 unverified apps. Of these, 133 threw an error "Sign in with Google temporarily disabled for this app," indicating that it had exceeded the new user limit imposed on unverified apps. We were unable to obtain API authorization data for these. We did, however, successfully link 144 apps to our Google account.

Table II shows the most frequently seen authorizations among the unverified apps in our corpus. While this list of declared privileges are generally similar in scope and function to those in the corpus as a whole (Table I), we observed a higher incidence of unverified apps' ability to access user' Google Calendar (23% among unverified apps vs. 7.1% for all corpus apps) and contacts (15% vs. 6.6%).

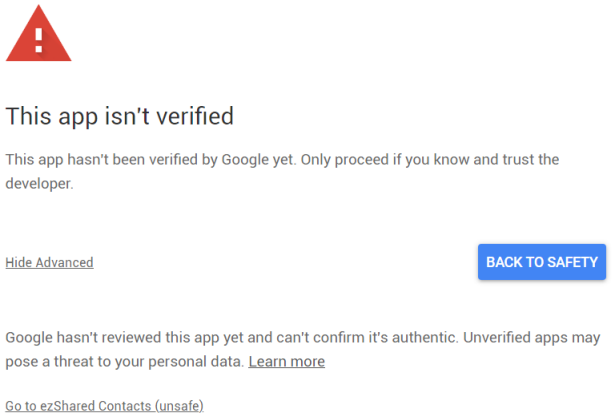

Fig. 2. The unverified app warning prior to the authorization prompt

Authorization	% apps
Display and run third-party web content in— prompts and sidebars inside Google applications.	53%
Connect to an external service.	40%
See, edit, create, and delete your spreadsheets in Google Drive.	30%
See, edit, share, and permanently delete all the— calendars you can access using Google Calendar.	23%
Allow this application to run when you are not present.	23%
See, edit, create, and delete all of your Google Drive files.	20%
View users on your domain.	17%
See, edit, download, and permanently delete your contacts.	15%
View and manage documents that this application has— been installed in.	13%
View and manage your Google Docs documents.	11%

TABLE II
10 MOST COMMON AUTHORIZATIONS, N = 144 UNVERIFIED APPS

We also investigated Google's enforcement of the new user limit for unverified apps: 100 new users for apps in the "unverified" state. Following our initial scrape of the Marketplace on January 2, 2020, we re-scraped the 144 unverified apps on January 18, 2020.[2] 124 of those apps reported as "unverified" again at the time of the second scrape. Perhaps more notably, 24 of the original 144 unverified apps had actually gained more than 100 new users in the intervening time. Table III shows the 10 still-unverified apps with the most raw user growth.

We acknowledge the possibility that some portion of these still-unverified apps were verified in the intervening period but had become unverified again (*i.e.,* the developer updated the app with new authorizations). We don't believe that is the case, though. For all 24 still-unverified apps whose user counts grew by at least 100, those apps requested the same API authorizations on both occasions we performed the scrape.

One of these still-unverified apps drew our attention in particular: ezShared Contacts.[3] This app gained over 1,000 users between the two times when we scraped the Marketplace. Among its disclosed authorizations are "Read, compose, send,

[2]https://irwinreyes.com/assets/files/2020-conpro/scrape-unverified-20200118.json

[3]https://gsuite.google.com/marketplace/app/ezshared_contacts/220045392708

App	Users_{jan02}	Users_{jan18}	Δ
Chemistry Question Generator	103,570	112,968	9,398
YouCanBook.me	2,055,316	2,062,474	7,158
Zoho Projects	784,631	789,763	5,132
siteMaestro	782,979	786,611	3,632
Classroom Share	55,521	58,475	2,954
Hippo Video	98,830	101,162	2,332
ProProfs Knowledgebase	341,036	343,085	2,049
ezShared Contacts	47,228	48,363	1,135
Lesson Plan Submit	305,813	306,859	1,046
Side Study for Teachers	53,041	54,008	967

TABLE III
MOST GROWTH IN USER COUNT FOR UNVERIFIED APPS, JAN. 2 - 18, 2020

and permanently delete all your email from Gmail," "See, edit, download, and permanently delete your contacts," and "Connect to an external service." Given this app's use of the "restricted" API scope to read Gmail data, it's likely that this is subject to the long security review that takes 4 to 8 weeks. However, we were surprised that users were still able to connect their accounts to such a sensitive app in its unverified state. And that the number of new users who did so had exceeded Google's stated limit by over a factor of 10.

V. DISCUSSION AND FUTURE WORK

A. Install-Time Permissions

Prior investigations on mobile platforms' permission models present trade-offs in asking for all permissions at install-time. While relatively easy to implement and applicable to any type of permission [49], asking for user consent this way can result in misunderstandings and undesirable privacy leaks [50]. Mobile platforms have since moved away from install-time permissions, opting instead to ask users for consent in context as apps exercise each declared privilege at run-time [51].

The G Suite Marketplace apps we examined—and more broadly, Google API apps with OAuth access to user data [52]—all employ the install-time model when requesting consent to access sensitive user information. Given the number of unique authorizations (130) we observed in our analysis of Marketplace apps, and the confusion [38] [39] among technically-oriented software developers about which corresponding API functions are indeed "sensitive," it's possible that the Google API's user authorization prompt has similar usability and privacy drawbacks as the install-time permissions now deprecated on mobile platforms. Although we acknowledge that web apps and mobile apps may be designed for vastly different levels of user interactivity, there could be opportunity for improvement by attempting to apply run-time contextual permission requests in web app use-cases.

B. Platform-Generated Disclosures

The Google API authorization screen notifies users when apps have the ability to use external APIs (*i.e.,* "Connect to an external service"). Unless an app developer voluntarily elaborates that information (which we observed to not always be the case), users receive no further details about which external APIs those may be.

Some developers on the G Suite Marketplace use Google Apps Script [53] (GAS) to implement and deploy their products. GAS apps run on Google's cloud infrastructure. Given that the API provider also controls the run-time infrastructure at least for this subset of Marketplace apps, it might be possible for the platform to monitor and disclose the external services that GAS apps communicate with. Users would receive greater insight into the what other remote services—besides Google and the GAS app itself—might also have indirect access to their sensitive Google account data. This additional transparency is especially valuable for unverified apps, as the cap (of 100 new users) imposed on unverified apps does not appear to be rigidly enforced, and that actual users—on the order of thousands over our 16-day scrape/re-scrape period— are indeed exposing themselves to risk by granting account access to unverified apps.

C. User Awareness and Controls

Our investigation only considered the Google API web app ecosystem from a strictly technical standpoint: what API functionality apps use, how the platform discloses that, and the measures the platform owner takes to regulate how developers use the API. However, we acknowledge that this narrow scope does not address how actual users interact with the disclosures and controls provided to them.

After Cambridge Analytica, Facebook restricted the data their platform API exposes to third-party apps, as well as implemented a timeout that revokes access to user data if 90 days have passed since the user has interacted with a given app [15]. The Google API does not appear to have a similar mechanism; indeed, their documentation instead instructs users to review app authorizations manually [44]. We envision further investigations measuring consumer awareness of these manual controls, and characterizing the degree to which consumers have granted apps access to their sensitive data (*i.e.,* for how long, with which authorizations, if users wish to revoke part or all of those authorizations). By examining the various apps that actual users in the wild have authorized to their accounts (rather than only analyzing apps listed in a non-comprehensive store, like the G Suite Marketplace web apps presented in this paper), we would also gain visibility into other classes of software that use the Google API, specifically mobile apps and standalone desktop software.

VI. CONCLUSION

The Google API allows properly-authorized third-party apps to access and interact with user data. This work examined a corpus of 987 web apps listed on the G Suite Marketplace that use this API and found that half of those are able to communicate with undisclosed external services, with a portion of those apps also holding permission to access users' Google Drive files, emails, or contacts. Additionally, while Google requires developers to submit apps for review if an app uses "sensitive" API functions, those products may still be listed on the Marketplace as "unverified." We found that the restriction on unverified apps gaining new users is not

rigidly enforced, and that unverified apps will continue to draw many new users—on the order of thousands in our 16-day observation period—despite warnings that attempt to persuade them otherwise. We believe that even after a major scandal stemming from the abuse of an API provided by a competitor, our results show that there is still ample risk in these systems, and recognize opportunities for improvement in how online services such as Google expose user data for programmatic use by third-parties.

REFERENCES

[1] D. Machado, "public-apis/public-apis: A collective list of free APIs for use in software and web development," https://github.com/public-apis/public-apis, last Accessed: January 13, 2020.

[2] U. S. Patent and T. Office, "United States Patent and Trademark Office - Open Data Portal," https://developer.uspto.gov/api-catalog, last Accessed: January 9, 2020.

[3] U. S. G. Survey, "APIs - Data and Tools," https://www.usgs.gov/products/data-and-tools/apis, last Accessed: January 9, 2020.

[4] F. T. Commission, "FTC for Developers — Federal Trade Commission," https://www.ftc.gov/developer, last Accessed: January 9, 2020.

[5] I. Google, "Google Maps Platform — Google Developers," https://developers.google.com/maps/documentation, last Accessed: January 9, 2020.

[6] Mover, "Fast Cloud Migrations - Mover," https://mover.io, last Accessed: January 9, 2020.

[7] P. J. Windley, "Api access control with oauth: Coordinating interactions with the internet of things." *IEEE Consumer Electronics Magazine*, vol. 4, no. 3, pp. 52–58, July 2015.

[8] I. Facebook, "Permissions - Facebook Login," https://developers.facebook.com/docs/facebook-login/permissions/overview/, last Accessed: January 17, 2020.

[9] I. Twitter, "App permissions – Twitter Developers," https://developer.twitter.com/en/docs/basics/apps/guides/app-permissions, last Accessed: January 17, 2020.

[10] R. Böhme and S. Köpsell, "Trained to accept?: a field experiment on consent dialogs," in *Proceedings of the 28th international conference on Human factors in computing systems*, ser. CHI '10. New York, NY, USA: ACM, 2010, pp. 2403–2406. [Online]. Available: http://doi.acm.org/10.1145/1753326.1753689

[11] I. Lapowsky, "Facebook Exposed 87 Million Users to Cambridge Analytica," https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/, last Accessed: January 13, 2020.

[12] S. Detrow, "What Did Cambridge Analytica Do During The 2016 Election?: NPR," https://www.npr.org/2018/03/20/595338116/what-did-cambridge-analytica-do-during-the-2016-election, last Accessed: January 17, 2020.

[13] U. S. Senate, "Testimony of Mark Zuckerberg, Chairman and Chief Execute Officer, Facebook," https://www.judiciary.senate.gov/imo/media/doc/04-10-18%20Zuckerberg%20Testimony.pdf, last Accessed: January 13, 2020.

[14] F. González, Y. Yu, A. Figueroa, C. López, and C. Aragon, "Global reactions to the cambridge analytica scandal: A cross-language social media study," in *Companion Proceedings of The 2019 World Wide Web Conference*. ACM, 2019, pp. 799–806.

[15] S. Perez, "Facebook begins blocking apps from accessing user data after 90 days of non-use — TechCrunch," https://techcrunch.com/2018/04/10/facebook-begins-blocking-apps-from-accessing-user-data-after-90-days-of-non-use/, last Accessed: January 10, 2020.

[16] J. C. Wong, "Document reveals how Facebook downplayed early Cambridge Analytica concerns — Technology — The Guardian," https://www.theguardian.com/technology/2019/aug/23/cambridge-analytica-facebook-response-internal-document, last Accessed: January 17, 2020.

[17] I. Facebook, "Company Info — About Facebook," https://about.fb.com/company-info/, last Accessed: January 17, 2020.

[18] Statista, "Number of Gmail active users 2018 — Statista," https://www.statista.com/statistics/432390/active-gmail-users/, last Accessed: January 10, 2020.

[19] T. Romm, "DOJ issues new warning to big tech: Data and privacy could be competition concerns - The Washington Post," https://www.washingtonpost.com/technology/2019/11/08/doj-issues-latest-warning-big-tech-data-privacy-could-be-competition-concerns/, last Accessed: January 17, 2020.

[20] I. Google, "Google Developers," https://developers.google.com/, last Accessed: January 10, 2020.

[21] A. M. W. S.-R. N. Cameron Russell, Florian Schaub, "Apis and your privacy."

[22] B. Smith, "Project Strobe: Protecting your data, improving our third-party APIs, and sunsetting consumer Google+," https://www.blog.google/technology/safety-security/project-strobe/, last Accessed: January 13, 2020.

[23] M. Huber, M. Mulazzani, S. Schrittwieser, and E. Weippl, "Appinspect: Large-scale evaluation of social networking apps," in *Proceedings of the First ACM Conference on Online Social Networks*, ser. COSN '13. New York, NY, USA: Association for Computing Machinery, 2013, p. 143–154. [Online]. Available: https://doi.org/10.1145/2512938.2512942

[24] F. Adrienne and E. David, "Privacy protection for social networking apis," in *The Web 2.0 Security and Privacy 2008 (in conjunction with 2008 IEEE Symposium on Security and Privacy)*, 2008.

[25] N. Wang, H. Xu, and J. Grossklags, "Third-party apps on facebook: privacy and the illusion of control," in *Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology*, ser. CHIMIT '11. New York, NY, USA: ACM, 2011, pp. 4:1–4:10. [Online]. Available: http://doi.acm.org/10.1145/2076444.2076448

[26] I. Google, "Unverified apps - Google Cloud Platform Console Help," https://support.google.com/cloud/answer/7454865?hl=enref_topic=3473162, last Accessed: January 21, 2020.

[27] ——, "Gmail API — Google Developers," https://developers.google.com/gmail/api/, last Accessed: January 14, 2020.

[28] ——, "Google Drive API — Google Developers," https://developers.google.com/drive/, last Accessed: January 14, 2020.

[29] ——, "Calendar API — Google Developers," https://developers.google.com/calendar/, last Accessed: January 21, 2020.

[30] ——, "Gmail Contacts API version 3.0 — Google Developers," https://developers.google.com/contacts/v3/, last Accessed: January 14, 2020.

[31] ——, "G Suite Marketplace," https://gsuite.google.com/marketplace, last Accessed: January 15, 2020.

[32] I. Chegg, "Easybib - G Suite Marketplace," https://gsuite.google.com/u/3/marketplace/app/easybib/960498119546, last Accessed: January 15, 2020.

[33] J. Ltd., "draw.io Diagrams - G Suite Marketplace," https://gsuite.google.com/u/3/marketplace/app/drawio_diagrams/671128082532, last Accessed: January 15, 2020.

[34] I. Trimble, "SketchUp for Schools - G Suite Marketplace," https://gsuite.google.com/u/3/marketplace/app/sketchup_for_schools/260457348581, last Accessed: January 15, 2020.

[35] Statista, "Number of available applications in the Google Play Store from December 2009 to December 2019 — Statista," https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/, last Accessed: January 14, 2020.

[36] ——, "Number of available apps in the Apple App Store from 2008 to 2019 — Statista," https://www.statista.com/statistics/268251/number-of-apps-in-the-itunes-app-store-since-2008/, last Accessed: January 14, 2020.

[37] I. Google, "OAuth API Verification FAQ - Google Cloud Platform Console Help," https://support.google.com/cloud/answer/9110914?hl=en, last Accessed: January 17, 2020.

[38] xaphod, "oath 2.0 - Where is the list of which Google OAuth2 scopes are considered "sensitive"? - Stack Overflow," https://stackoverflow.com/questions/54351702/where-is-the-list-of-which-google-oauth2-scopes-are-considered-sensitive, last Accessed: January 17, 2020.

[39] A. Goel, "Five annoying issues with Google's OAuth Scope Verification," https://www.gmass.co/blog/five-annoying-issues-google-oauth-scope-verification/, last Accessed: January 17, 2020.
[40] I. Twitter, "Developer," https://developer.twitter.com/, last Accessed: January 14, 2020.
[41] I. GitHub, "GitHub Developer — GitHub Developer Guide," https://developer.github.com/, last Accessed: January 14, 2020.
[42] M. Corporation, "Welcome to Office 365 APIs — Microsoft Docs," https://docs.microsoft.com/en-us/previous-versions/office/office-365-api/, last Accessed: January 14, 2020.
[43] I. Slack Technologies, "Slack API — Slack," https://api.slack.com/, last Accessed: January 14, 2020.
[44] I. Google, "Third-party sites & apps with access to your account - Google Account Help," https://support.google.com/accounts/answer/3466521?hl=en, last Accessed: January 17, 2020.
[45] S. Software, "TExt gBlaster (SMS Texting) - G Suite Marketplace," https://gsuite.google.com/marketplace/app/text_gblaster_sms_texting/360232482012, last Accessed: January 17, 2020.
[46] DigiShuffle, "Privacy Policy - DigiXport," https://www.digishuffle.com/digixport-privacy-policy/, last Accessed: January 17, 2020.
[47] A. Gapps, "Add reminders - g suite marketplace," https://gsuite.google.com/marketplace/app/add_reminders/404177452106, last Accessed: January 20, 2020.
[48] OpenAdvocate, "Writeclearly - g suite marketplace," https://gsuite.google.com/marketplace/app/writeclearly/28387801957, last Accessed: January 20, 2020.
[49] A. P. Felt, S. Egelman, M. Finifter, D. Akhawe, and D. Wagner, "How to ask for permission," in *Proceedings of the 7th USENIX conference on Hot Topics in Security*, ser. HotSec'12. Berkeley, CA, USA: USENIX Association, 2012, pp. 7–7. [Online]. Available: http://dl.acm.org/citation.cfm?id=2372387.2372394
[50] P. Wijesekera, A. Baokar, A. Hosseini, S. Egelman, D. Wagner, and K. Beznosov, "Android Permissions Remystified: A Field Study on Contextual Integrity," in *Proc. of USENIX Security*, 2015. [Online]. Available: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/wijesekera
[51] I. Google, "Request App Permissions — Android Developers," https://developer.android.com/training/permissions/requesting, last Accessed: January 21, 2020.
[52] ——, "Using OAuth 2.0 to Access Google APIs — Google Identity Platform," https://developers.google.com/identity/protocols/OAuth2, last Accessed: January 21, 2020.
[53] ——, "Apps Script — Google Developers," https://developers.google.com/apps-script/, last Accessed: January 21, 2020.