Proposal to Google for Improved Third-Party Data Sharing Processes

Abstract

It makes sense why you (Google) have pursued the revenue model that you have chosen, which involves learning from user behavior to provide advertisements. Until now Google has been able to continue this revenue model, because users have been okay with getting useful and amazing services with advertising instead of paying. With this information in mind, it makes complete business sense to be hesitant to completely change your company's practices, even after privacy experts haven written papers explaining how what you are doing may be wrong. Unfortunately, this time it is not just privacy experts that are complaining, but actual users who are acting against this third-party data sharing. This proposal looks to fill the hole left by these professionals to provide you with constructive solutions to help you respond to this change in user demand, instead of just telling you that current third-party data sharing processes are not sufficient. Specifically, this proposal will present and defend data sharing guidelines for you to implement into Google's current processes and platform to make it better for its users.

Growing User Concerns

Until recently, many third-party data policies have been constructed as "a binary notice-and-choice, take-it-or-leave-it framework" [3]. Having an all or nothing response to how a user's data is used may have worked initially but obviously needs to change. With the variety of data that Google now contains about its users, it does not make sense to treat the sharing of all of this information the same, since each data point will have a different sensitivity level. It is great that the leadership at Google has started to realize these issues, but more can be done, especially since users are starting to ask for more. Unfortunately, publications on this problem have explained the issue without providing companies, like Google, with specific ways to improve and contribute to the solution. In this proposal, you will be provided with these guidelines that previous publications have been missing and shown how it will actually help Google if you implement them.

For example, when Cambridge Analytica was able to gain "access to users' friends' data through the Facebook Open API", it actually changed user behavior [1]. Specifically, the way that users and the public replied to this event was a glaring sign of what to expect from them in the future, and it became clear that this response will not be a passive one. A Pew Research Center study of US adults after the incident found that 54% of adults surveyed adjusted their privacy settings on Facebook, 42% took a break from checking Facebook, 26% deleted the app from their phone, and 74% performed at least one

of these activities [4]. The varied actions taken by these users show that they are beginning to reevaluate how they interact with Facebook and put thought into the best ways to mitigate the exposure of their data. In addition, the large percentage of people that responded is a clear message that this is a popular movement. Google should therefore take a proactive response to show that they care about this change in user expectations.

Therefore, since this data sharing issue is no longer just talk from privacy experts, but now involves changes in user behavior, it will cause two main issues for Google's main revenue model. One, the reduction of users using Google's services will decrease the value that Google can provide to their advertisers, which in turn leads to decreased revenue from advertisers. Second, less users also means less data available to Google, which will slow down data science developments at Google. Google has made some of the most important data science and machine learning advances in recent history, and these advances have become Google's main differentiator in the market, which means that these issues will hinder Google's main competitive advantage. Long term, both of these problems will weaken Google, which will further reduce its users and their engagement with the platform. This can certainly continue until many Google services become financially infeasible to keep up.

Fortunately, there is good news if you are proactive with improving your company's third-party data policies. There is legislation, like the General Data Protection Regulation in Europe, that already grant "individuals the right to access their data in a free, electronic format" [3]. The goal is to take these regulations a step further and allow users greater control over their data. Creating a platform and relationship with users where they feel like they are in control would have significant benefits now and well into to the future. Increasing user trust will not only open the way for more users to want to use Google products, but it will also make current users want to interact with the services more and in new ways. This growth in overall use will increase the value of Google and open the way for you to improve Google's services from the new influx in data.

Build the Foundation

The first step in creating a platform that fosters an environment where users can better control their data is to have a control center similar to Google's current "Activity Controls" page but that is more accessible and comprehensive. These factors are what will make customers really trust Google and believe that your company is being transparent. This is important because if users feel that this is not

the case, then this lack of trust will counteract the whole goal of the control center in the first place, which is to make the user feel safer while using Google services.

To begin, this updated control center needs to be extremely accessible, since it directly ties to a user's trust of the tool and platform. Hiding the menu under layers of button clicks or in an unclear location of the UI will throw a red flag to users in a couple of ways: either that the controls are not of importance to the platform, that the company wanted to hide it from the user, or both. A hidden control center would contribute to the trust and respect problem that it was trying to solve. To correct this, the link for a user to manage their data sharing should get a dedicated card in Google's account settings menu. In addition, accessibility also means making it so that all of the pages used to control data sharing are not spread out and difficult to access. This means that after the user gets into the control center they should not be funneled through multiple links and pages to make changes. All of these nested links and pages will make the user feel you are hiding something, similar to how hiding the first link to the control center would.

Moreover, the menu needs to be comprehensive in the data that is shown to the user, which should include information that involves two general entities: the data and the third-parties involved. In regards to data, the types of information that is shared and the way that data is used needs to be included. The major goal of this information is to be explicitly clear with the user about what the company knows and why it is sharing this knowledge. For example, Google knows the gender of many of its users. Two different third-parties may want to know this information in different ways. One could possibly want it as an aggregation of the percentage of males in that town, and the other may want it directly, so that it can be used for that user's experience in their Google extension. In this case, there should be an item in the control center saying that the user's gender could be shared and under that item, as a drop down or some kind of list, should be that it can be shared as part of an aggregation of a given minimum number of users and directly by itself. Then, next to each item in the list there should be an action item, such as a toggle, for the user to turn off the sharing if they would like. In addition, there should be a way to turn off the sharing of gender all at once with one click or action. In this way, the user will know specifically that their gender can be shared, that it can be shared as part of an aggregation or directly, and that they can take quick and effective action to change the sharing.

Finally, the control center should encompass the information regarding the potential parties that could obtain access to any of the user's data in any way, which should include not only the parties but information about the parties and how they may use the data as well. It is important to stress that all parties must be included. The list of third-parties should contain organizations that may directly

interact with the user and others that may operate without explicitly interacting with the user. Notifying users of third-parties that they do not directly interact with is the main thing missing from Google's current setup. In an article by Pew Research, there is a quote by IT University of Copenhagen associate professor Irina Shklovski saying "as [online] entities create conditions that make online interactions the most effective way to achieve particular goals, more of such interactions will happen" [6]. Google needs to make sure that users feel like this new and updated control center meets all of their needs for controlling their data sharing, which means having all third-parties shown in the control center. In return, users will feel confident knowing that the control center is giving them all of the tools they need, and, in response, they will increase their use of the platform.

For example, suppose there are two third-parties that would like to know a user's age. For one of the third-parties the user is the one that initiated the request to have their age shared, and the other company is not directly known by the user but needs their age for a microservice that is a part of Google's GSuite service. Both of these third-parties would need to show up in the control center so that the user can have a unified place to learn about these companies and learn what the companies would like to use their data for. From that same screen, the user should then be able to quickly turn off the access to either company if need be. Since all of the companies will be shown, there may be some companies on the list that cannot be turned off, such as an auditor or other company that is contracted to verify the company's operations for policy or legal reasons. In these cases and only in these cases, the option to turn off the access can be greyed out to not allow the user to turn it off, but there must be an explicit explanation to the user detailing why they cannot.

Improve User Relationship

Lastly, with the creation of a proper data sharing control center, there should then be constant communication setup with the user to allow them to react to changes regarding their data. This should be done in two ways: through periodic general reminders and direct communications when changes occur. Google currently implements a basic form of the first with their Security Checkup, which on occasion, at login, will link the user to a page to verify "that the websites, apps, and devices connected to [their] account are ones [they] still use and trust" [5]. This can be taken one step further by having this link sent to them in a yearly email. In this way, the company will demonstrate to the user that they not only care but that they want to encourage the user to be active in the process. This will ultimately also increase trust, because the user will not feel in the dark and they will feel like they are being kept in the loop.

Moreover, specific and easy to understand emails, or some other form of communication, should be routinely sent to users with a summary of changes in the data or third-parties that are included in the sharing chain. For example, Google may need to hire a new contractor to verify the security of the data storage and process of a new service they want to launch. In this scenario, Google would then, in their next update email, inform their users of the addition of the contractor to their data control center. Included in this email or other form of communication should be a link to the user's control center and to an appropriate channel of contact in case the user wishes to ask questions about the change or voice their opposition. Finally, these responses must then be taken into account when considering the business's actions going forward. In addition, Google should respond to and answer users' issues with the changes and an action plan should be provided to remedy the issue if a majority of users do not agree with the change. This last part requires a significant amount of confidence in the company's internal processes, but also presents on of the most significant ways that your company can keep user trust. For users to feel like they are in control, they have to feel heard and this is the best way to do that for them.

Conclusion

Getting third-party sharing right is difficult and can get convoluted, but it is also critical in keeping a healthy relationship between Google and the consumers that interact with its services. In addition, it is important that experts from all domains contribute to and help develop the best solutions for this issue going forward. Up until now, publications have been warning about third-party sharing issues, but have not been contributing answers. This proposal's goal was to provide some of these answers by giving you guidelines to help you implement fixes to correct the problem of sharing third-party data within Google's services. You can follow these practices knowing that they will help Google's users and improve Google's services in the long run.

Works Cited

[1] J. Isaak and M. J. Hanna, “User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection,” Computer, vol. 51, no. 8, pp. 56–59, Aug. 2018.

[2] M. C. Meinert, “GDPR,” American Bankers Association. ABA Banking Journal, vol. 110, no. 3, pp. 30–33, 2018.

[3] “Three's a crowd: towards contextual integrity in third-party data sharing,” Harvard Journal of Law & Technology, vol. 28, no. 1, pp. 325–347, 2014.

[4] A. Perrin, “ Fact Tank - Our Lives in Numbers September 5, 2018 Americans are changing their relationship with Facebook,” *Pew Research Center*, 05-Sep-2018. [Online]. Available: http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/. [Accessed: 25-Oct-2018].

[5] “Google Privacy | Why data protection matters,” *Google*. [Online]. Available: https://privacy.google.com/take-control.html?categories_activeEl=sign-in. [Accessed: 26-Oct-2018].

[6] L. Rainie and J. Anderson, “Theme 2: The nature of trust will become more fluid as technology embeds itself into human and organizational relationships,” *Pew Research Center: Internet, Science & Tech*, 10-Aug-2017. [Online]. Available: http://www.pewinternet.org/2017/08/10/theme-2-the-nature-of-trust-will-become-more-fluid-as-technology-embeds-itself-into-human-and-organizational-relationships/. [Accessed: 04-Nov-2018].