Security Privacy Policy Report – Alex Flynn

As I had mentioned in my bootstrapped budget, I plan to allocate $150 of monthly budgeting to IT Systems that were not originally analyzed in my system selection for ReFresh Kicks. This excess in budgeting was meant to satisfy payments to implement a cloud service, such as Dropbox, to ensure that all files and data remain "safe" and on the cloud. I was not inclined to include cloud storage systems in my system selection report for two reasons: I wanted to explore new types of systems that I had never considered, and I just assumed (like many people do) that I would just use Dropbox. It's the largest, most well-known cloud service, so why not?

This common misconception that large, renowned companies are "safe bets" when putting sensitive company-data on the cloud ignores important security concerns that consumers and business-owners should consider. This report will seek to understand the shortcomings of Dropbox, analyze it against two other prominently used cloud service systems, and offer a cloud system solution that, while lesser known, may be superior depending on one's priorities.

Dropbox

Dropbox stores half a billion users' files on its cloud storage for B2B and B2C service providing. Other storage companies like Box, for example, market their services primarily for B2B value propositions, however Dropbox primarily stores customer data with a less robust focus on B2B servicing. Regardless of what type of user one intends to be, s/he should be made aware of the security issues evident when storing files on Dropbox.

The company publishes its stance on customers' data security by noting, "at Dropbox, the security of your data is our highest priority." (Dropbox) Despite this, Dropbox generates the majority of its revenue on customers who value convenience over security. The company combats naysayers by highlighting its multi-pronged security approach involving 256-bit Advanced Encryption, Standard and Secure Sockets Layer (SSL)/Transport Layer Security to protect data in transit, and customers' ability to enable Two-Step Verification on logins. While these data safety precautions are widely considered adequate in protecting data from hackers (even though other systems offer even more security on that front), consumers are often less aware of Dropbox's ability and right to access their data and do with it what they please. Hackers are what scare consumers, but little do they know they should be more scared of Dropbox itself.

A handful of Dropbox employees have access to decrypt any users file at any time they please. While distributing this information would be illegal for an employee, the possibility that a cybercriminal from overseas hacks into your data is far less likely. Moreover, if legally "required" by subpoena, Dropbox will not just deliver your data to the law agency requesting it, but also decrypt it for them. Further, even if one deletes his/her own account in an attempt to expunge it from the cloud, Dropbox retains access to it and will decrypt it after the fact to comply with legal obligations, resolve disputes, or enforce agreements. Finally, if ownership changed, Dropbox would hand over your data to the acquiring party, diminishing the notion that you have exclusive right to your intellectual property.

These issues, and more, are present because you (the consumer) ignored the fine-print before signing Dropbox's non-negotiable terms and conditions. Scarier yet, Dropbox has the ability to use geolocation to track your whereabouts at all times. However, it realizes how egregious such a privacy breach would be, so it simply uses data embedded in the files you upload combined with your IP address to generate a rough estimate of your location.

These issues are extrapolated due to the fact that Dropbox has unrestricted access to 500 million users' sensitive data, nevertheless most users choose convenience over combing through service contracts and term sheets. For that reason, how do other widely-relied upon cloud service systems' security policies stack up?

iCloud

Like Dropbox, iCloud is many people's cloud system by default; they hardly notice how much personal data iCloud has access to and are simply amused when the photo they took yesterday popped up on their MacBook's iPhoto today. Similar to Dropbox's, iCloud's security policy grants them access to disseminate its users' files in the event of a lawful subpoena. Unlike Dropbox, iCloud's security policy also grants them access "at all times to determine whether content is appropriate… and may pre-screen, move, modify and/or remove content at any time, without prior notice and its sole discretion." (Patel)

iCloud customers have essentially given up ownership of their data to the "sole discretion" of Apple, which has played to several customers' disadvantage. For instance, in the second half of 2015, Apple surrendered personal data and device content in as many as 80% of U.S. law enforcement requests (not even subpoenas). Further, Apple's ambiguous verbiage not only grants them complete access to customer information, but essentially grants them complete ownership over it:

By submitting such content on areas of the service that are accessible by the public or other users with whom you consent to share such content, you grant Apple a worldwide, royalty-free, non-exclusive license to use, distribute, reproduce, modify, adapt, publish, translate, publicly perform and publicly display such content on the service… without any compensation or obligation to you. (Patel)

To make matters even worse, unlike Dropbox, Apple has access to all of customers' most personal data from their iPhones, MacBook's, and Apple Watches; with iCloud being a primarily B2C service, this should worry business's less than a customer who has their entire life stored on Apple products. However, given Apple's monolithic size, the risk of an acquisition is low, but they would likely hand these rights over given their previous record.

Google Drive

On trend with the previous two services, Google Drive and its Cloud Services are often selected automatically by consumers for B2C transactions. Very similar to iCloud, users are granted free cloud storage by having Google accounts, enticing millions of consumers to utilize its cloud system. Google's cloud policy includes features that egregiously build upon the shortcoming in Dropbox's and I Clouds; Google not only retains access to users' files, but it automatically scans

each file uploaded, including emails. Google uses the information it steals from you, to customize your search results and ad experiences.

I chose to analyze these three services, as they are readily accessible and available to all entrepreneurs at a low price and use their scale to offer seamless integration into other aspects of consumers lives. This analysis specifically peaked my interest about: why don't or can't these major companies establish true cloud security and privacy? I understand that the benefits outweigh the costs, and that their respective monopolistic market dominance allows them to do so, but the question is: is it legally plausible, or even ethical, for a data storage provider to refuse disseminating data within its possession if the government imposes a court-ordered subpoena?

Regardless of one's ethical opinion on the matter, the answer is: yes, if cloud-provider cannot even access the information themselves. If the cloud providing system is physically incapable of decrypting the data, then that data is completely secure. This high-level security is only available in smaller cloud servicing systems such as pCloud.

pCloud

pCloud offers all of Dropbox's security measures and more. The likelihood of a hacker penetrating pCloud's more advanced security encryption procedure is even less than it would be at Dropbox. However, the defining difference between pCloud, and similar security-focused cloud systems, is a concept called Zero Knowledge Encryption.

Zero-Knowledge Encryption means that the cloud providers have no knowledge, or even emergency access, to the data the user stores on their services. This involves several encryption processes, one of which happens within your own device before its sent to the servers and again once it comes back, therefore the stored data is encrypted without the cloud provider having the key. This is truly the most secure way to store data, so long as the cloud provider has a robust procedure protecting against third-party hackers, which pCloud does. The only drawback to this encryption is that if the user forgets a password, pCloud does not have the ability to retrieve it. However, unlike Dropbox, iCloud, and Google Drive, if the President of the United States ordered pCloud to release personal or content data from its cloud, it wouldn't because it couldn't.

apf58

Appendix:

- “9 Ways to Make Dropbox More Secure and Safer to Use.” Comparitech, 14 May 2018, www.comparitech.com/blog/cloud-online-backup/make-dropbox-more-secure/
- “Is Dropbox Safe to Use?” Dropbox, www.dropbox.com/help/security/safe-to-use.
- Ivanova, Vanina. “Dropbox Alternatives: Top 5 Best Cloud Storage Services 2018.” Medium.com, Medium, 28 Apr. 2017, medium.com/@Vanina/dropbox-alternatives-top-5best-cloud-storage-services-2017-a703af7d7796.
- Mika, Bobby. “Is Dropbox Safe to Use? How Dropbox Works to Secure Your Files Online.” TipTopSecurity, tiptopsecurity.com/is-dropbox-safe-to-use-how-dropbox-works-to-secure-your-files-online/.
- Patel, Nilay. “Is Google Drive Worse for Privacy than ICloud, Skydrive, and Dropbox?” The Verge, The Verge, 25 Apr. 2012, www.theverge.com/2012/4/25/2973849/google-drive-terms-privacy-data-skydrive-dropbox-icloud.
- “Top 5 Worst Privacy Policies You've Probably Agreed To.” Sync, www.sync.com/blog/top-5-worst-privacy-policies-youve-probably-agreed-to/.
- Winder, Davey. “Cloud Storage: How Secure Are Dropbox, OneDrive, Google Drive and ICloud?” Alphr, Alphr, www.alphr.com/apple/1000326/cloud-storage-how-secure-are-dropbox-onedrive-google-drive-and-icloud.