Bailey Berry

Professor Posner

Systems and Infrastructures

Write Up #4

There are several privacy issues that have been raised related to cloud storage and computing. These problems mostly arise from trusting a third party to securely store records and personal information, often at remote locations that are obscure to the user. Other privacy issues related to using any third-party internet service relate to the fact that they collect and store information on each user, often without notifying the user first. The ITU-T report on Privacy in Cloud Computing defines privacy as "the right to self-determination, that is, the right of individuals to 'know what is known about them', be aware of stored information about them, control how that information is communicated and prevent its abuse".[1] ITU-T goes on to indicate that in the Software as a Service model, which Dropbox falls into, the user has "little or no influence how input data is processed". It lists several relevant questions to consider when using a cloud service, as laid out in the Madrid Resolution:

• Who are the stakeholders involved in the operation?

• What are their roles and responsibilities?

• Where is the data kept?

• How is the data replicated?

• What are the relevant legal rules for data processing?

• How will the service provider meet the expected level of security and privacy?

In a report that investigated Cloud Service Contracts, Jessica Bushey et al. raised several issues to look for in keeping records in the cloud. Written for the Canadian Journal of Information and Library Science, the report was more concerned with how organizations could be sure that their records remain authentic and reliable while stored in the cloud. They identify these risks: unauthorized access to information and records, privacy breaches, loss of access to and management of information and records, alteration of information in the cloud, lack of transparency regarding account management, server locations, data destruction and recovery.[2] They further bring up the point that while records may clearly belong to users of the cloud, metadata produced by the user may technically belong to the cloud service provider.

Dropbox does attempt to be transparent, especially in relation to its technology, by maintaining a blog, which details how data is stored and retrieved at every level of operation. They further attempt to address these concerns in their Privacy Policy. Dropbox admits that it collects information regarding

---

[1] Guilloteau, Stephane and Venkatesen Mauree. "Privacy in Cloud Computing". *ITU-T Technology Watch Report*. ITU: March, 2012. https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf, Accessed February 15, 2020.

[2] Bushey, Jessica et al. "Cloud Service Contracts: An Issue of Trust". *Canadian Journal of Information and Library Science*. University of Toronto Press: June, 2015. Vol. 39:2, pp. 128-153.

your account (name, email address, phone number, payment info, etc.); "Your Stuff"- the records and files you store in Dropbox along with "Related information" regarding your profile and "the size of the file, the time it was uploaded, collaborators, and usage activity"; Contacts; Usage Information- actions you take in your account; and Device Information (IP addresses, type of browser and device you use, webpage you visited before Dropbox and your location).[3] Dropbox also mentions that it uses Cookies and pixel tags and targets marketing towards its users and towards others associated with its users. The reasons it claims to collect this information mostly relate to "provide, improve and promote our Services". Dropbox also claims to use personal data for "legitimate business needs". These needs mostly relate to tracking how you use services to target new ones for you, to understand how their services are functioning and to improve them and to track any unusual activity for security reasons. Dropbox claims that it will ask for user consent before processing personal data for other purposes.[4]

In its Privacy Policy, Dropbox also mentions that it shares your information with "Trusted third parties": Dropbox, Inc., Amazon Web Services, Inc. (Infrastructure), Teleperformance A.E. (an international customer experience management company), Salesforce.com (a partnered business management company), Serenova, LLC (cloud contact center), Google LLC (Customer Support), Zendesk, Inc. (customer support tool), Oracle America, Inc (Billing and Customer Support). Dropbox assures that these companies will only access your data "only..to perform tasks on Drobox's behalf" (FAQ). In terms of identifying who the stakeholders in all of this are, the picture becomes more complicated with the wide range of different companies associated with Dropbox who can each have access to your personal information. Added to this is the concern that various governments can technically access both your personal information and any files you've stored through a cloud service. This is especially a concern in the United States where the Patriot Act allows the government to access any data stored in a provider's jurisdiction.

According to Dropbox, you can request that they stop, limit use of or delete personal data- but only if "we have no lawful basis to keep using your data".[5] However, Dropbox defines its legal basis for using your data as: "to provide to Dropbox Services to you pursuant to our contract with you; in furtherance of its legitimate interests in operating our services and businesses" it also mentions that this should all happen "with your consent".[6] Its recommendations for correcting or deleting your personal data are either changing your account information or deleting your Dropbox. It also provides the email address privacy@dropbox.com, where you can complain about use of personal data or request the deletion of it. This same email address is provided for any requests for Data Access. In "your account", a user can opt out of notifications from Dropbox, but otherwise there is no simple way to block access to personal information.

If you do decide to delete your account on Dropbox, it claims that it will delete all of your data within 30 days. This is referring to the files that you store on Dropbox, but does not address all of the personal data and information Dropbox and its affiliates have collected about you. Further, Dropbox does not make it clear in its Terms of Service whether metadata created on its site belongs to its users

---

[3] "Dropbox Privacy Policy". *Dropbox.com.* Dropbox: December 17, 2019. https://www.dropbox.com/terms#privacy, Accessed February 15, 2020.
[4] ibid
[5] "The Dropbox Privacy Policy: Frequently asked questions." *Dropbox.com.* Dropbox. https://help.dropbox.com/accounts-billing/security/privacy-policy-faq, Accessed February 15, 2020.
[6] ibid

or to Dropbox, something that Bushey et al. define as essential in determining the privacy standards of cloud storage. Dropbox does release a report for the amount of times the government has accessed user data including information. It includes what types of requests they've been, what states the requests have been made in, the amount of requests. Dropbox claims that it lets its users know when requests have been made for their information, but their own report shows that they've only been legally allowed to do so in about 40% of the cases.[7]

There have been several data breaches at Dropbox, including in 2016 when 68 million Dropbox Account email addresses and passwords were published online.[8] Dropbox offers encryption services incorporated into its blockchain technology to protect files during transfer. It also tests its infrastructure by using third-party services, such as "Hacker One", which invites internet users to find vulnerabilities and offers a bounty for any found and reported to Dropbox.[9]

There are many concerns related to privacy and security with Dropbox. While Dropbox is fairly transparent about the data that it collects, how it uses that data and who it shares it with, Dropbox gives no indication of how or where that data is stored. Users are fairly powerless to prevent Dropbox and its affiliates from collecting that data unless they simply decide to delete their Dropbox accounts altogether. Once those accounts are deleted, Dropbox does not clarify whether the data it has collected is also deleted or can continue to be used by Dropbox et al. Finally, the level of data security and protection vary slightly depending on how much users are willing to pay for their plans. For example, certain Dropbox Business owners are able to store data in Europe, making it eligible for the EU-U.S. and Swiss-U.S. Privacy Shields Framework laws. This means data is protected by European law, even if Dropbox is a country associated with the United States. These are all very real and relevant concerns for anyone considering using Dropbox as a cloud storage service.

---

[7] "Transparency at Dropbox". *Dropbox.* June, 2019. https://www.dropbox.com/transparency/reports, Accessed February 15, 2020.

[8] Mendelsohn, Tom. "Dropbox hackers stole e-mail addresses, hashed passwords from 68M accounts". *Ars Technica*. Condé Nast: August 31, 2016.

[9] "Security". *Dropbox.* Accessed February 15, 2020.