Enterprise Cyber Security Group Report – Group I

Collusion Concerns – Paul McHard

A prevalent issue that has been raised by the client is the concern over collusion between personal cloud providers and competing firms, states or parties involved with on-going cases. The following shall discuss the root cause for the client’s concern, identify what legal power and rights are wielded by the client and provider respectively in this regard and assess the risk associated, in terms of both the damage that might ensue and the likelihood of collusion occurring.

In a strictly legal sense, collusion is defined as two parties entering “a deceitful agreement, usually secret, to defraud and/or gain an unfair advantage over a third party, competitors, consumers or those with whom they are negotiating”1. For the purposes of this report the term shall be considered both on this strict description as well as in reference to any cooperation between a cloud service provider and any third party embroiled in a legal case with the client, be that a state, competitor or otherwise, without necessitating permission by the client or their respective employee responsible for the personal cloud in which the relevant data is contatined. For this consideration, the assumption is made that all of the client’s employees using personal clouds will be using services provided by the set of most popular cloud providers. Cloud service providers do not appear to publicly broadcast their monthly, annual or total user statistics, however a report2 by CloudRail, a company which provides a cross-platform API integration service for most cloud services reports that the top 4 cloud storage service providers are Dropbox with 47.3% of users, Google Drive with 26.9%, Microsoft OneDrive with 15.3% and Box with the remaining 10.5%. Important to note that CloudRail does not support all cloud services, and for this reason this report also investigates Apple iCloud and Mega3.

To identify the risk of collusion, the powers and privileges given to the cloud provider by the user, here the employee, must be determined. These are outlined in the Terms of Service or Terms & Conditions which the user must agree to in order to use the service. This legal hand over of power is in itself a risk, as the information entailed in a terms of service agreement for in individual user scenario are best described as hidden in plain sight, as the vast majority4 of users do not read these terms, leaving users unaware of the access to their information that providers have.

The critical issue which can be observed in the terms of service of all six of the aforementioned providers is that they each individually reserve the right5,6,7,8,9,10 to maintain user uploaded content and provide it to any government or otherwise involved organisation, such as is necessary for the legal case in question. Note that Google Drive and Microsoft OneDrive terms of service are both contained within larger documents pertaining to multiple products by each company. In particular, Mega reserves the right to “deny you access to your data but keep it for evidential purposes”9. This evidently is cause for concern in a large multinational corporation who potentially has a significant portion of their workforce storing potentially sensitive or secret information in cloud storage services provided by any one of these providers. The concern comes from the effective handover of control of information which occurs under these terms, and the fact that disclosure of corporate content, while strictly defined as being under legal direction only, is no longer the sole responsibility of the client, but also of the cloud service provider. Shortly, the risk posed by this issue will be discussed; firstly, however, the other key collusion risk must be identified.

This second risk manifests in the access that third parties and malicious employees have to user information and stored content. Dropbox, Google and Microsoft make clear statements that user information is shared with third parties approved by the companies, detailing that this is specifically for the purposes of their own outsourced work, such as Customer Support. There is indication that only user information and not user content is shared with these third parties. However, as will be discussed in the risk assessment portion of this report, there is potential for compromise of data integrity and theft by malicious employees, both internally at the provider and from the third party outsourced businesses.

Returning to the earlier description of the collusion, there are two scenarios posited in regard to collusion between the provider as an entity and any third parties. In the strict sense of collusion as a deceitful, secret and potentially unlawful practice, it is highly unlikely that the large companies which control the lion’s share of personal clouds would risk the reputations of their businesses or the trust of the public in their services to participate in such deals. This has in recent times been an issue involving a number of these companies and the United States. Dropbox makes a statement to this end in their transparency declaration11, describing their resistance to overly broad government data requests and their rejection of the idea of government ‘backdoor access’. Famously over the issue of the San Bernardino shooting, Apple was involved in a legal case with the FBI regarding the agency’s demand for Apple to create software allowing the agency to bypass the locking and encryption methods employed on the phone, an effective government backdoor to data encrypted on iPhones.[Source] While this specific case is in regards to local data stored on a device, its high profile nature and the very public resistance displayed by Apple to resist creation of encryption bypassing mechanisms for the government has clear and resounding implications for the integrity of cloud stored data in similar circumstances. Thus it can be surmised that risk to the provider of public trust being undermined is so great that risk of provider collusion with third parties, states or otherwise is determinately low. However, in consideration of collusion in the sense of cooperation without consent of the client, risk is substantial. The major cloud providers all clearly detail in their respective terms of service that they retain the right to disclose private user information and content in suitable legal or emergency circumstances. This is a risk to the client as a corporation if employees store sensitive company data on personal clouds, as the client would be concerned over losing their sole privilege and responsibility in regards to disclosure of information.

In regards to concerns over malicious employees of providers or associated third parties gaining access to user data, the case of [SOURCE] is relevant to discuss.

FIND SOMETHING, TALK ABOUT ITS RELEVANCE, DISCUSS RISK.

*References:*

1 - http://dictionary.law.com/Default.aspx?selected=232 [Accessed 18/10/17]

2 - https://blog.cloudrail.com/cloud-storage-report-2017/ [Accessed 18/10/17]

3 - http://www.techradar.com/news/top-10-best-cloud-storage-services-of-2017 [Accessed 18/10/17]

4 - <https://www.theguardian.com/money/2011/may/11/terms-conditions-small-print-big-problems> [Accessed 18/10/17]

5 - <https://www.dropbox.com/en_GB/privacy>

6 - <https://www.microsoft.com/en-gb/servicesagreement/>

7 - <https://www.box.com/en-gb/legal/termsofservice>

8 - <https://www.apple.com/ca/legal/internet-services/icloud/en/terms.html>

9 - <https://mega.nz/terms>

10 - <https://www.google.com/intl/en/policies/terms/>

11 - <https://www.dropbox.com/transparency>