Enterprise Cyber Security Group Report – Group I

Collusion Concerns – Paul McHard

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.[8]” The assumption is made that all of the client’s employees who use personal clouds will be using services provided by the set of most popular cloud providers. CloudRail reports that the top 4 cloud storage service providers are Dropbox, Google Drive, Microsoft OneDrive and Box. CloudRail does not support all cloud services, and so this report also investigates Apple iCloud and Mega [9] .

Powers and privileges given to cloud providers upon acceptance of the terms of service by a user (an employee of the firm) expose a risk to the firm. Terms are hidden in plain sight, the majority4 of users do not read these terms, leaving them unaware of the access they allow to their stored information and content. The critical issue observed in the terms of service of all six major 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. For example, Mega reserves the right to “deny you access to your data but keep it for evidential purposes”. This evidently is cause for concern as the handover of control of information and the disclosure of corporate content stored by employees, 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.

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. 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, the FBI demanded that Apple create software to allow the agency to bypass the locking and encryption methods in place on the phone, an effective government backdoor to data encrypted on iPhones.[12] While this specific case is in regards to local data stored on a device, its high profile nature and the very public display by Apple to resist creation of encryption bypassing mechanisms for the US government has clear and resounding implications for the level to which these companies value the privacy of their users and the integrity of their data, which extends to cloud stored data in similar circumstances. Thus the conclusion can be drawn that providers see too much risk with consequences that are too damaging to their public image to engage in such practices, thus the risk of collusion by the cloud service provider is determinably low.

However, the risk of legal cooperation without consent of the client 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.

*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> [Accessed 18/10/17]

6 - <https://www.microsoft.com/en-gb/servicesagreement/> [Accessed 18/10/17]

7 - <https://www.box.com/en-gb/legal/termsofservice> [Accessed 18/10/17]

8 - <https://www.apple.com/ca/legal/internet-services/icloud/en/terms.html> [Accessed 18/10/17]

9 - <https://mega.nz/terms> [Accessed 18/10/17]

10 - <https://www.google.com/intl/en/policies/terms/> [Accessed 18/10/17]

11 - <https://www.dropbox.com/transparency> [Accessed 18/10/17]

12 - https://www.theguardian.com/technology/2016/mar/28/apple-fbi-case-dropped-san-bernardino-iphone [Accessed 22/11/17]