

School of Computer Science

Data Management in Fulfilment of

DATA9911

Maksymilian Drzezdzon

C15311966

Degree: TU060/1

Module Coordinator: Emma Murphy

Declaration of Ownership: I declare that the attached work is entirely my own and that all sources have been acknowledged: 🗹

**Date: 2020/11/09**

**Introduction**

The product/service picked is apples MacOS and its wider app store ecosystem. This is more so to point at the legal concerns that Apple addresses on its devices that are introduced through third party apps. Google’s play store takes three-seven [1] days to review apps meanwhile Apple takes one-two [2], this is in order to review whether apps are compliant with their respected user guidelines. There is a significant difference in time investment considering that Apple is viewed as a pioneer in data privacy, this is a good learning opportunity to see potential inconsistencies in practice meanwhile review industry standards.

Companies like Facebook have gone unchallenged with unethical use of data and data manipulation in the form of psychological experiments on users. Apple’s update [3] to their operating system will notify users about their data being collected. This will push the conversation to the forefront of people’s day to day, before it didn’t seem like a popular talking point amongst the public.

**Data life cycle**

Apples MacOS is an operating system that supports Apples other products, which in turn collect user data. How and what data is collected is illustrated on apples privacy page, the kind of data collected and used is dependent on what services one uses and how they interact with the product.[4]

**Data creation**

Most data created is manually entered by the user, such as billing information, account details, age. Automated data collection only kicks in when a user decides to use some of apples other products and decides to opt in their financial planning apps, in that case they must provide consent before use etc. [4]

**Data storage**

Apple uses administrative, technical and physical safeguards to protect personal information. [6][7]

**Data Usage**  
 Similar can be said about health tracking apps [5] it not only collects info you’ve entered but also your medical history information, sensor information such as heart rate, technical data that “does not permit direct association with any specific individual” according to the policy. The info is used to support the studies, develop health related products or reports with anonymized data. Alternately if data is used for other studies the end user will be asked for permission.

**Data Archival**

I sent out an email to Apple asking about this process, I heard back as I was submitting my first attempt for this assignment. I got clarity on the retention of iCloud access logs, password changes etc. Along with indirect confirmation that services such as Siri, maps among other products collect data under an anonymized system.[13] The full email can be viewed in Figure 1 at the bottom of the report in the appendix. (Zooming in 50-70% makes it more legible)

I haven’t been able to find how Apple archives data or what their process is. I was able to find libraries for IOS applications or ‘archive’ options for users via iCloud but that doesn’t really portray their data life cycle, there is mention of data compression but it’s nothing of substance.[12]

**Data Disposal**

Apple retains personal data only for as long as needed to fulfil the purpose it was collected for.[8] The method or process isn’t necessarily specified.

**Publicly available data governance**

Apple states that they use “industry-leading” consent mechanisms, I assume they refer to the use of machine learning systems for this as later referenced in their document. Which gives users a choice whether they want to share data such as their location, reminders, health and the list goes on. This automated system would explain their faster turnaround time in reviewing apps and how they use data etc.

Apple then explains how many teams are involved in protecting customer and employee data, such as a senior director that directly reports to Apple’s general counsel along with legal and engineering teams overseeing how data is used and when used that it’s for its intended legal purpose.[9] Assuming that this approach is followed as strictly as its expressed then it’s a solid process.

Following that data undergoes review periods that ranger from one to two years depending on the potential risk involved.[9]

**Conduct first principal ethical test**

Does it preserve or enhance human dignity?

What is good is the section on transparency and communication where Apple cites their transparency report among others along with their commitment to human rights.[11]

Does it preserve the autonomy of the human?

Apple definitely does try to put what they have at the forefront of their privacy governance page with a link to their human rights policy which outlines company procedures.[10] Having said that they would have to uphold these values regardless.

Is the processing necessary and proportionate?   
There isn’t a way to completely validate this since this would be internal information, from their online documents consent is asked for user data and if it’s needed for research etc the end user is then notified and asked for consent again.

Does it uphold the common good?  
Publicly Apples has adequate procedures dealing with users requesting or reporting privacy complaints.[9] Apple also has a statement that they do not provide user information to any third parties. Apple deidentifies all data [9] meaning all personal elements, IP address must be removed.

Does the outcome violate any of these four points? If yes how could you

**N/A**

Mitigate any ethical risk?

Data undergoes review periods that ranger from one to two years depending on the potential risk involved [9] on top of periodic reviews and updates of their privacy policies.[10] Routine post-mortems are evoked when a data security incident occurs with dedicated teams assigned.[9] Personally this seems like a general process with any indecent employed at all companies of apples size.

**Recommendation on how the company can be improved**

There isn’t a way for me to validate if these processes are followed or not, Apple’s approach seems to be good they have an extensive data ethics board with engineers specializing in data privacy, other than potentially providing more technical details they seem to check all the boxes with minimizing how much user data they collect, asking users permission, manual data entry etc.

Apple has acknowledged that data is owned by the user not the company. Meanwhile trying to create a standard in the tech industry as there currently is none. The GDPR is a reactionary response rather than an industry wide standard.

A real concern is that there is a lot of pushing paper and date from one end of the company to the other, this has a cost associated with it so having an efficient process as to what data is or is not needed can reduce costs.

The CEO of Netflix claimed that it’s better to collect all data because you never know when its going to be useful, this seems like a huge commitment from a data privacy perspective, Apple seems to do the opposite by limiting the amount of data collected in turn reducing risk.

There is no mention how bias in their ML systems is handled, just a statement about their use of said ML systems.[9] This can be improved and some general information could be provided for the sake of transparency.

**Summary and reflections**

I’ve gained a better understanding of roles that exist within data governance and a glimpse of a data management department at Apple through reviewing Apple’s data workflow, engineering roles are responsibilities.

I’ve overviewed Apple’s data management plan outlined above, although a little more material could have been made public or perhaps more details for a more technically advanced audience. I assume with many of these processes it’s easier to not say anything rather than stating too much and opening themselves up to legal claims adding even more overhead to an already heavy workload.

Data isn’t collected automatically for most apps making it a plus unless a user chooses to participate and uses said applications with the ability to have their data removed upon request. An obvious criticism is whether a user must provide consent before being given access to said application.

Other than system diagnostics most data are manually entered by the user which arguably adds a layer of transparency as the user should be cognitive of what they are doing and what information they are providing. Which circles back to my earlier point at the beginning once the public has the idea of data privacy put in front of them via Apple forcing third party apps request user permission to access data from x or y, it will hopefully make users more cognitive of what they are providing in the future when manually typing something in. This can be seen as a positive since Apple by proxy can be seen as educating the public on such affairs.

There is an outline of how long data review periods last but no indicator of how this is done, which again lacks detail probably due to potential legal claims that could arise from making too much information public.

# References

[1], G. (2021, Feb 27). *play console help*. Retrieved from support.google.com: https://support.google.com/googleplay/android-developer/answer/9859751?hl=en#:~:text=Note%3A%20For%20certain%20developer%20accounts,how%20long%20this%20should%20take

[10]Apple. (2021, March 6). *Our Commitment to*. Retrieved from apple.com: https://s2.q4cdn.com/470004039/files/doc\_downloads/gov\_docs/2020/Apple-Human-Rights-Policy.pdf

[11]Apple. (2021, March 6). *Transparency Report*. Retrieved from apple.com: https://www.apple.com/legal/transparency/

[12]. (2021, march 11). *Archive or make copies of the information you store in iCloud*. Retrieved from apple.com: https://support.apple.com/en-us/HT204055

[2] inc., A. (2021, Feb 27). *Preparing apps for review*. Retrieved from developer.apple.com: https://developer.apple.com/app-store/review/#:~:text=On%20average%2C%2050%25%20of%20apps,and%20you%20will%20be%20notified

[3] Hern, A. (2020, Nov 20). *Apple accuses Facebook of 'disregard for user privacy'*. Retrieved from theguardian.com: https://www.theguardian.com/technology/2020/nov/20/apple-accuses-facebook-of-disregard-for-user-privacy

[4] inc, A. (2020, Dec 14). *Apple Privacy Policy, Personal Data Apple Collects from You*. Retrieved from apple.com: https://www.apple.com/legal/privacy/en-ww/

[5] inc, A. (2020, Nov 20). *Apple Health Study Apps Privacy Policy*. Retrieved from apple.com: https://www.apple.com/legal/privacy/apple-health-studies/en-ww/

[6]Apple. (2020, March 1). *Apple Platform Security*. Retrieved from support.aple.com: https://support.apple.com/en-ie/guide/security/welcome/web

[7]Apple. (2021, Feb 27). *Apple Privacy Policy, Protection of Personal Data at Apple*. Retrieved from apple.com: https://www.apple.com/legal/privacy/en-ww/

[8]Apple. (2021, Feb 27). *Protection of Personal Data at Apple*. Retrieved from apple.com: https://www.apple.com/legal/privacy/en-ww/

[9]Apple. (2021, Feb 27). *Privacy Governance*. Retrieved from apple.com: https://www.apple.com/legal/privacy/en-ww/governance/

[13]Privacy Response Team “Re:How” Message to Maks Drzezdzon March 15 2021. E-mail

**Appendix**

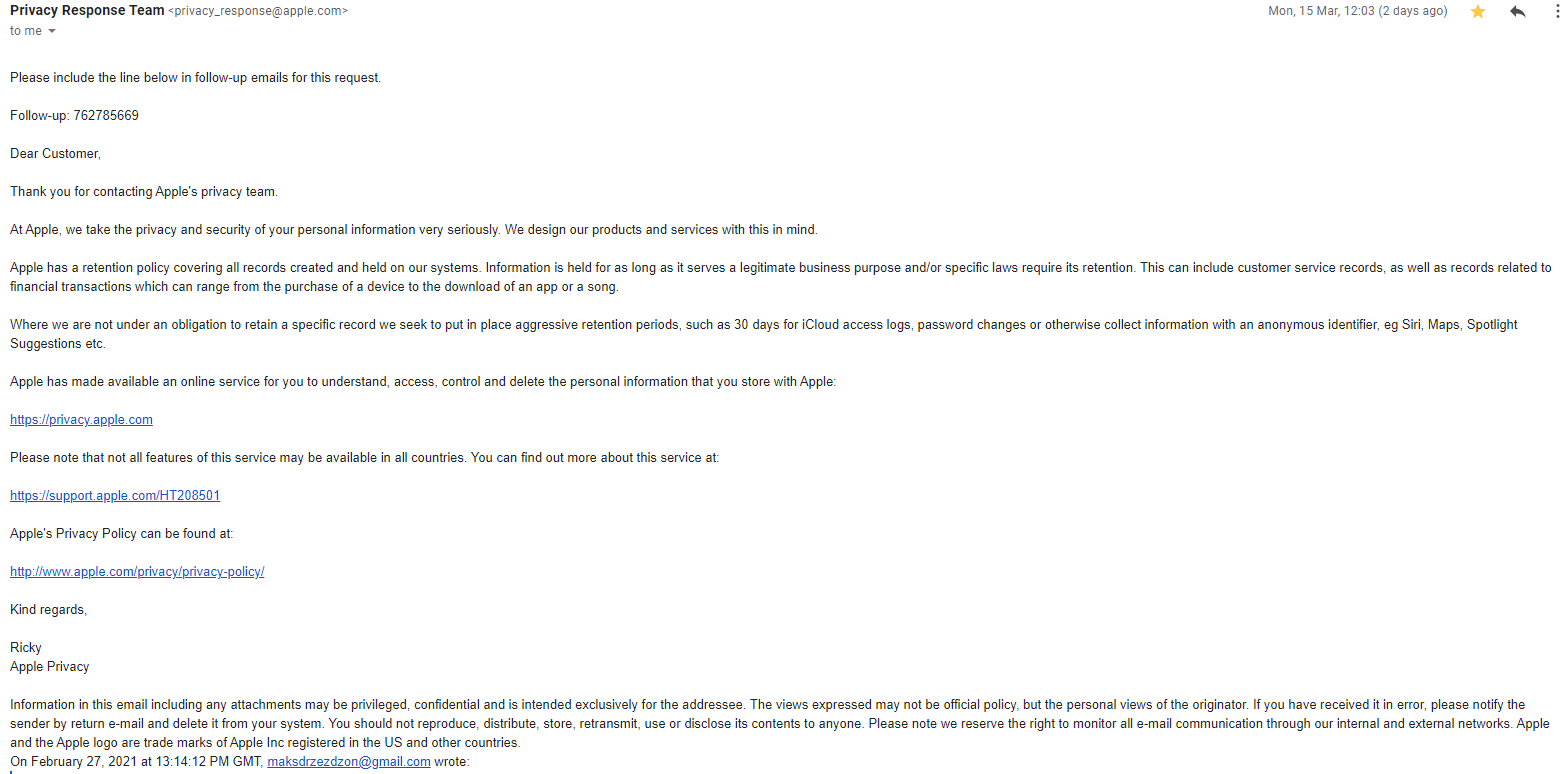


Figure 1 Copy of email response receive from Apples privacy response team