**PWD- CW 1**

**Position A: You are a founder of HM with ethics responsibilities**

1. To what extent do you have a positive duty proactively to explore areas where the combination of user data with other data could lead to problems?

As a founder of HM, I would argue that there is a degree of social corporate responsibility HM needs to take on. For example, HM need to protect users with reference to where and to whom their data is sold on to. Although re-sold data is anonymised, there is still a need to make sure that users cannot be identified as a result of our resale of their data. Precautions should be taken to make sure our users cannot be identified through a combination of the data we sell and other forms of data from other organisations and/ or publicly available data.

Conversely, there is a limit to how much influence we have on the global data industry. As long as we make sure we are upholding our promise to users to only resell their anonymised data, it is impossible for us to monitor what external organisations do with this data. If users are identifiable due to a combination of their data from a variety of different sources, we cannot be held responsible for this. In this regard, responsibility shifts from us to the user to make sure that they are not easily identifiable due to their online activity.

1. To what extent and in what circumstances should you inform the users when you consider that there are new possible risks arising from the use of their data?

Although users have opted-in to use HM (as is required under GDPR legislation), and have been made aware of how we use their data, it is nevertheless important for us to keep users informed of our activities. This could be done through an e-newsletter. If new possible risks were identified, it would be our duty to keep users informed. It is better to be transparent at all times, than to later be guilty of the misuse of user data and mistrust which could be significantly detrimental to HM.

Nevertheless, it may not always be necessary to inform users of potential new risks, as an element of risk always exists. We would not want to inundate our users with new information telling them of every potential risk arising from the use of their data. Furthermore, we would not want to deter our users from using our services in the future. The only time it would be absolutely necessary to tell users of a potential risk, would be when we deem this risk to be exceptionally high, and when we would need to communicate with the user for further action.

1. To what extent should you differentiate between the interests in confidentiality of different categories of users?

User categories could be defined as the user’s membership type when subscribing to HM, or indeed the different categories users could fall in to as a result of their personality analysis results. Nevertheless, the confidentiality of our users should be uniform across all categories of users. Our users have all signed a confidentiality agreement when subscribing to use our services, and we should adhere very strictly to this confidentiality agreement which is a requirement of law. It would be unfair, illegal and inappropriate for us to differentiate between users based on which category of user they fall in to, and we would have no moral or legal grounds in which to do so.

Nevertheless, depending on what the consequences of not disclosing confidential information could be, it may be necessary to break confidentiality and disclose information for the public interest. For example, if we were to come across data from a user which indicated dangerous behaviour, or giving evidence of a serious health condition with potentially dangerous implications, it may be deemed necessary to disclose this information to the relevant authorities in the interest of public safety and/ or safety of the individual in question.

1. If you discover that a given user fits into a pattern associated with other users who encounter a particular medical problem, should you proactively inform the user of this risk?

It would be inappropriate for us to contact a user based on them fitting into a pattern associated with other users who encounter a particular medical problem. Machines and algorithms tend to find many patterns; however, this does not always guarantee that these results are significant. Our machine algorithm would never be able to replace the expertise and experience of a medical professional. Furthermore, we cannot be sure that the information which the user has provided is accurate and correct, and therefore we would not want to cause undue worry by speculating. Our users have not consented to receive such information, and therefore we would not endeavour to provide such a service.

Nevertheless, if users consented to this service, we would be able to provide them with the results which our algorithm has identified, with the caveat that such results are not founded by any medical domain knowledge and that their significance is unknown. Without the users’ consent, it would be inappropriate to contact users proactively to inform them of medical risk as our findings cannot be justified. Instead, it is more appropriate for us to stick to our intended purpose of providing a personality analysis service.

1. Would you feel it appropriate to use data provided by the users in support of a political or other cause of which you strongly approve?

It would under no circumstance be appropriate to use data provided to us by users to support a political or other cause which I personally strongly approve of. The data we collect is to offer personality analysis services to our users, and we would never make their deanonymised information available to third party organisations for political use or other means. It is inevitable that users will support a range of different political parties/ other causes and it would be highly risky and very detrimental to HM if it was ever found to be guilty of such data abuse.

However, we do have to remain aware that regulation lags behind technology. Once we have re-sold anonymised data, we are no longer able to control who has access to it further down the chain, and it could well become available to such organisations. Nevertheless, as long as we have upheld our duty to anonymise data before selling it on, we cannot be held accountable for any ethical or moral wrongdoing.

**Position B: You are a user of HM.**

1. Would you be happy for your data to be used for strictly medical research?

As a user of HM I would consent to my data being used for strictly medical research, as long as my data remained anonymous. I am happy for my data to be used for this purpose, as my data will be used as a force for good. Furthermore, it means that in return, I am able to use HM services for free. Moreover, I would add that I am not very concerned about my data being used, as long as the purpose is justifiable and my data remained anonymised. For example, I would not consent for my data to be used were it to be de-anonymised, and used by predatory organisations for commercial purposes.

Nevertheless, I would question why my data would be needed for medical research, and why it is useful. I would assume that more complex and detailed data is available from medical trials and that there is a high volume of such data available. Ultimately, I would like to know exactly how my data will be used to support medical research, and what its function is.

1. Would you be happy for your data to be used for more general social research?

As mentioned above, I would consent to my data being used for general social research if my data remained anonymous. Social research is alike medical research, a justifiable and good use of my data and therefore I would consent to my anonymised data being used for such purposes.

However, I would again question why my data is useful for this purpose. I would question what this general social research specifically entails and what exactly is being studied. I would argue that by being transparent, HM is more likely to get my buy-in as I am more likely to trust and value them as an ethical organisation if they make their activities public knowledge. Conversely, I do understand that there always an element of risk of identification, and this is why I remain adamant that whatever data of mine is re-sold is first anonymised.

1. Would you be happy for your data to be used for commercial purposes, which might lead to your receiving advertisements/offers for products/services tailored to your predicted preferences?

I personally would not consent to this, as I find this kind of advertisement very persistent, predatory and a nuisance. Furthermore, if my data is truly anonymised before resale, it should be impossible for my data to be used for this purpose without my consent. For example, I would expect my email, phone number and other sensitive pieces of information to be removed before the re-sale of my data.

As mentioned previously, I am aware that an element of risk of identification due to the re-sale of my data by HM does exist, and that I have agreed to accept this risk by signing-up to use their services. Nevertheless, I would expect the company to take on the responsibility of making sure that predatory organisations are not able to identify me, or access my personal and sensitive information. Were this to happen, I would seriously reconsider using HM and would feel as though my data and trust of the company have been abused.

1. Would you be happy for your data to be used for charitable purposes in line with your perceived sympathies?

The two important principles to be aware of here would be whether my data remains anonymised or not, and what exact purpose the charity would like to use my data for.

Once again, I would argue that if my data was to be used as a force for good and remain anonymised, I would consent to this. I do believe that charitable purposes are on the whole a cause for good, however fundraising campaigns tend to be highly commercialised and some charities do operate similarly to commercial businesses. For example, after donating to a particular charity, I might later be inundated with further advertisements from the same or other charities. Nevertheless, were my data to remain anonymised the risk for this would be low.

On the other hand, were my data to be de-anonymised without my consent, I would question the purpose behind this. For example, why are the results of my personality analysis questionnaire required for charitable purposes? What’s more, were these charitable purposes to become more akin to commercial purposes and carry out activities such as cold calling for donations, I would view this as an abuse of my data and good will.

1. Would you be happy for your data to be used in the interest of political parties which you support?

To some extent, I would not object to my data being used by the political party which I support, be it either anonymised or de-anonymised. This is mostly due to myself not being particularly concerned about the political party I support accessing my data, as I am likely to give it to them myself when becoming a member of their party or signing up to their campaigns. Nevertheless, I would expect HM to anonymise my data even if selling it on to the political party which I support, as this is what they have stated they will do.

Moreover, I understand that there is still a risk that other political parties which I do not support may get a hold of my anonymised data, and that they might be able to identify me from this data. Again, this is the risk which I have taken and as long as HM make sure my data is anonymised before it is sold on, I would not hold them accountable if another political party was able to identify me. I would however question the effectiveness of anonymising my data, and re-think when signing up to other services which operate similarly to HM.