Law Coursework

Group 14

June 13, 2018

1 Max Planck Institute For Meteorology Licence

Terms 1 and 2 serve mainly to define language, and do not restrict the four freedoms.

Term 3 violates freedom 0 because it disallows use of the software for commercial purposes, in a modified form or otherwise. It could be interpreted as violating freedom 2 and 3; however, it does not explicitly mention distribution for commercial purposes, so we do not believe it violates these.

Term 4 violates freedom 2 as it says you are "not allowed to sell this Software or any part of it.". It restricts how you may distribute the software. For example, it may be unfeasible to distribute without charging, so this term could potentially limit your ability to help others by sharing the software. It goes on to fully violate freedoms 2 and 3 by disallowing distribution of the software as a whole, original or modified. However, it does allow sharing among colleagues and limited distribution of modular modifications.

For term 5 we assume that the provided definition of a modification applies in term 4 (where personal modification is allowed). Hence, it violates freedom 1 as it limits how you may change the program, even for personal use. The requirements to add notices to your changes do not seem to breach the principle behind the freedoms. However, the Free Software Foundation believes you should not need to notify the creators when you make changes, so it violates freedom 3. The last paragraph of this term places limitations on distribution and usage of independent new components of the models, as it restricts them in the same way as the licence restricts the existing components. This does not directly violate the four freedoms but instead the principles that govern them. It also enforces that your code be free, restricting your freedom to distribute the code as you wish.

Term 6 does not explicitly violate the freedoms, as they refer to software rather than publications. However, one of the tenets of the four freedoms is that you may make modifications without notifying the original creators, so the requirement to notify the creators upon publishing results from the software may not be in the spirit of the freedoms.

Terms 7, 8, 9, 10, 11 and 12 do not appear to violate any of the four freedoms, as they do not explicitly restrict use or regard distribution beyond the other terms.

In term 13, we take the use of "shall" in "This license shall be governed by [...] Germany" to be integrating the export control regulations of the specified region as part of the licence. In the freedoms, it is intended that, although the licences are subject to the laws of their region, those laws are not included in the licence itself.

2 Cambridge Analytica / Facebook Story

2.a Relevant Data Protection Law Requirements

Cambridge Analytica, as a processor, are required to follow the terms of their contract with GSR (who Kogan worked for) through which the terms of the GSR-Facebook contract terms would have flowed, however CA were using data for profiling in order to influence elections which likely would not have been part of the contract, this would have been in breach of article 5(1)(b).

GSR (a processor) was providing a personality test app but was actually collecting data on Facebook users and their friends which was not necessary for the app, this is in breach of GDPR article 5(1)(c).

Facebook did not keep sufficient logs or monitor them frequently enough, evidenced by the time taken for them to realise GSR were collecting unessential data, this may have breached article 30.

Facebook should have notified the relevant authority within 72 hours of learning of the data breach, this would have breached article 33 of the GDPR.

Facebook should have performed a data protection impact assessment on the entire chain of data processing, with the help of GSR and CA, not doing so was been in breach of article 35.

2.b What Could Facebook Have Done Differently?

Report the data breach to a relevant authority within 72 hours, for example the ICO in the UK.

2.c Recommendations

Facebook could create a more restrictive API that limits the amount of data third parties can access, for example by not allowing access to friends' data, this will reduce the amount of data vulnerable to a data breach. Perhaps Facebook could only provide third-parties access to anonymised data. Facebook could also keep logs of their API usage and monitor them frequently in order to help track how third parties use the data, this would also help Facebook comply with their legal requirement to notify the relevant authorities within 72 hours in the event of a data breach.

Orginisational changes Facebook could implement include performing an impact assessment on the entire chain of data processing with the help of third parties, this will help Facebook comply with the DPIA section of the GDPR requirements and may also help them weed out third parties who are using personal data for malicious purposes. Facebook could also ensure that policy is in place for notifying the relevant authorities in the event of a data breach. They could also implement policy for regularly monitoring the personal data they hold and deleting it if it is no longer relevant.

Facebook could enforce the use of stricter contracts for third parties and ensure that the terms of the contract flow down to subprocessors. As the part of the contract Facebook could ensure that third parties only use the data for necessary purposes. Facebook could also ensure that third-parties regularly monitor and delete data if it is no longer relevent.