IV. STUDENTS’ THOUGHTS AND REMARKS

The GDPR came into in effect on May 25, 2018. Though it’s an EU law, what does this mean for other countries and businesses? GDPR applies to all businesses that deal with the personal data of EU citizens in all parts of the world. <https://www.blakesbusinessclass.com/what-the-gdpr-means-for-canadian-businesses/> Given that EU citizens live in all parts of the world, this means that Facebook will be violation of GDPR for tagging EU citizens in any part of the world. Facebook head of public policy, Kevin Chua faced questions about FB past practices of allowing third parties to gain access users personal data, therefore violated the Canadian law. <https://www.thestar.com/news/canada/2018/04/19/facebook-admits-it-may-have-violated-canadian-law.html> . We installed the FDVT extension, and classified some EU citizens account that currently live in Canada. We discovered that these users have been tagged some sensitive ad preferences before and after their arrival in Canada. It can be seen that FB also labels Canadian residents with potentially sensitive ad preferences for advertisement purposes.

Is the data collected from FDVT users safe in the hands of the authors? We know during the installation process users have to agree that their data collected will be used for research purposes. The question is, Will user’s data be sold to the third party, now or in the future? We believe FB would do a better job at keeping our data safe because they have been around for a longer time and cannot be easily persuaded by third party agencies to sell our personal data as compared to a smaller company. It’s a case of who watches the watchman (FDVT) and who we could trust with our personal data?

And lastly, we ran the FDVT classifier across various accounts. We noticed a certain trend, some of the potentially sensitive ad preferences assigned to users were not accurate. Given the serious implications and privacy risks an ad preference can pose a user, it’s even worse that users may have to suffer due to wrongfully assigned ad preferences. For instance, a user may be tagged with “Drinking in the Night (Wrongfully)”, “Driving”,“Cinemas”; If this user goes to the cinema every Friday night, it could be concluded that the user drinks and drives as well. If there is an accident during this period and the police has access to this information, the user could potentially become a suspect of a murder.

Many online companies use our personal data for online advertising in exchange of giving us free services to use their platform. We use most of these online services for our day to day life. How can we not have to change our daily routine while keeping our personal data secured? Who can we trust with our personal data?