PROFESSIONAL RESEARCH PRACTICE ASSIGNMENT 1:

Group 10.2

Part 1: Data analytics: opportunities & constraints:

Part-1(a) Opportunities:

In this information driven world, data is a prime component in many sectors, one where it's extensively utilized is the data analytics field. Data analysis is defined as "the process of examining information, especially using a computer, in order to find something out, or to help make decisions" (Cambridge Dictionary, n.d.). It's also related to the accumulation of highly complex and voluminous unstructured data (Garg, et. al., 2020).

Advertisements are directly targeted at the user, by gathering data from the digital footprint that the consumer leaves behind whenever they do something as simple as visiting a website, typing something into a search engine, or scrolling through social media. This data collection can prove to be very useful to consumers as well as advertisers, as it enables websites to generate ads that appeal to the user (Goldfarb et. al., 2020). This allows the user to receive adverts that are more relevant to their interests and likely purchase the products, generating revenue for the advertiser.

The automated targeting feature that's displayed on Instagram's business page explicitly states the categories they use to target ads are location and demographics. (Instagram, n.d.) Data analysis in this context can help businesses immensely, as it can help with building a customer base, and is a more resourceful way of advertising because of such tools, as you can gain information about your target audience and adjust your marketing strategy accordingly in order for it to be effective.

Part-1(b) Constraints:

One major concern about data analytics is preserving sensitive information, therefore information security is an increasing concern (Acharjya, 2016). Many users unknowingly agree to share their data to third parties and some might not consent to their data being gathered (ProQuest, 2018). Some companies may be sharing their users' data without their consent and used for various reasons, such as political advertising.

Cambridge Analytica alongside Aggregate IQ, two data analytics firms, made headlines in the news due to their involvement in the Brexit campaign. They used data available from Facebook to micro-target adverts to users who would be most prone to be swayed by such content (Cadwalladr, 2017), breaking data protection laws set out by the GDPR. Besides, consumers tend to negatively react to such imbalance of privacy practice (Kelly et.al., 2017).

As a result, Facebook has changed some policies for EU users, by allowing greater transparency about how their data is collected and used (Uzialko, 2018) via the 'Access Your Information' tool that gives more control to users to manage the information they've previously shared. It is always advised to check their privacy and advertisement settings (ico.org.uk, n.d.). The company has emphasized privacy as being of utmost importance to them via regular articles (Facebook, n.d.), where updates about new features are posted ensuring users more privacy and greater control over their data, and news about the legal action they are taking on companies who abuse the platform (Romero J. 2020).

Reference List:

1. Cambridge Dictionary (n.d.), Data Analysis [Online]
   Available at: https://dictionary.cambridge.org/dictionary/english/data-analysis
   Accessed on: 4th October 2020

2. Garg, T. and Khullar, S. (2020) 'Big Data Analytics: Applications, Challenges & Future Directions', *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2020 8th International Conference on*, pp. 923–928. doi: 10.1109/ICRITO48877.2020.9197797.

3. Goldfarb, A. and Tucker, C. (2020) Privacy Regulation and Online Advertising | Management Science [Online]
   Available At: https://pubsonline.informs.org/doi/abs/10.1287/mnsc.1100.1246
   Accessed On: 5 October 2020

4. Instagram (n.d.) Build Your Business on Instagram [Online]
   Available At: https://business.instagram.com/advertising/
   Accessed On: 7th October 2020

5. Acharjya, Debi & P, Kauser. (2016). A Survey on Big Data Analytics: Challenges, Open Research Issues and Tools. *International Journal of Advanced Computer Science and Applications*. 7. 511-518. 10.14569/IJACSA.2016.070267.

6. ProQuest (2018) Facebook Scandal Raises Data Privacy Concerns [Online]

   Available at: https://search.proquest.com/openview/1fb525cb130501583b3bf76fc4c98c8f/1?pq-origsite=gscholar&cbl=47271

   Accessed On: 9th October 2020

7. Cadwalladr, A. (2017) 'The great British Brexit robbery: how our democracy was hijacked', *The Guardian* [Online]

   Available At: https://www.theguardian.com/technology/2017/may/07/the-great-british- b
   rexit-robbery-hijacked-democracy

Accessed On: 8th October 2020

8. Kelly D.M. & Patrick E.M. (2016). The Role of Data Privacy in Marketing. *Journal of the Academy of Marketing Science*. 10.1007/s11747-016-0495-4.

9. Uzialko A. (2018). 'How Facebook's GDPR policy shift does (and doesn't) impact advertisers'. *Business News Daily*

   Available at: https://www.businessnewsdaily.com/10702-facebook-privacy-settings-gdpr-changes.html

   Accessed On: 11th October 2020

10. Ico.org.uk (n.d.) 'Social media privacy settings' *Information Commissioner's Office* [Online]

    Available at: https://ico.org.uk/your-data-matters/be-data-aware/social-media-privacy-settings/

    Accessed on: 13th October 2020

11. Facebook (n.d.) Privacy Matters [Online]

    Available at: https://about.fb.com/news/tag/privacy-matters/

    Accessed On: 12th October 2020

Part 2: Mass Civilian Surveillance through Facial Recognition System:

The God's-Eye Incorporated was a company which specialized in facial recognition systems implementing next-generation technologies, which could be utilized in modern surveillance cameras. The government of a country had inducted this company to assist in their capitalistic legislation.

They had implemented an advanced surveillance system, allowing the government to monitor almost everything the citizens do in their daily life, including their day-to-day activities. They had also introduced a points-based system for the citizens, where doing positive work will increase and illegal work decrease the score. The regional top and bottom 50 were publicly announced regularly. And this data was stored in a poorly maintained unsecured database. Hackers took advantage of this vulnerability and leaked important personal information about citizens to other organizations.

This technology made an adverse impact on people's lives and depreciated their privacy and independence. Collecting information and monitoring citizens like this allowed some people to take advantage of the system to gain popularity while others just carried on with their lives.

As the technology became more publicly known, media attention was gradually turned towards it and reports criticising the government's actions began to flood papers internationally. Other governments were in agreement with the media, as the technology from God's-Eye was seen to be slowly removing individual autonomy. Eventually, as more pressure was put on from around the world, the project was shut down and all devices and technology were removed from the public.

Analysis:

The way facial recognition technology was implemented in the scenario straightforwardly violated the Principle 1.6 of the ACM Code of Ethics by violating the privacy of the citizens, and not safeguarding the data from unauthorized access. Besides, this purposefully infused a sense of insecurity among the citizens and created an invisible barrier between them and their freedom. Besides, the public disclosure of the points on a regular basis also violated the Principle 1.7 which is about honouring the confidentiality of the client's data. Since every citizen becomes a client of this technology, it becomes a duty to avoid publicizing their information (Points in this regard), which is abominably violated.

The overall outcome of that technology contradicted the Principle 1.1 and 1.2 since everyone's actions are not expected to be the same and different people have different personalities. Hence, this violated the code of respecting diversity (included in Principle 1.1) while also affecting the social life of the inhabitants (Principle 1.2). Not all of the citizens have the same capabilities to contribute to the society, while a part of them even need the assistance to survive. But this technology can only be fully utilized by the individuals who are physically and mentally capable, which violated the inclusiveness of the Principle 1.4. Ultimately, Principle 3.1 is breached by abusing the people's right to privacy. Therefore, the technology did not comply with the ACM community's standard and failed to prove as a sustainable technological implementation.