Homework 1

Ali El-Khatib
aelkhatib6@gatech.edu

1 QUESTION 1

2 QUESTION 2

2.1 General Data Protection Regulation & You

The General Data Protection Regulation (GDPR) –adopted on April 27, 2016– is a regulation regarding the protection of personal data and privacy. In effect, it allows users within Europe to have increased control of all personal data (e.g., website cookies, email addresses, phone number). This means that users control the activation of cookies and trackers–methods which collect personal data–on websites they visit. In addition to data control, it enforces a number of other rights for users:

- Right of an individual to be free of inaccurate personal data (Article 16)
- Right to be erasure (or forgotten); ability to have data deleted upon request (Article 17)
- Right to have data provided in portable, standardized formats (e.g., .csv, .xlsx) (Article 20)
- Right to refuse their data being used in certain processes (Article 18, Article 21)
- Right to not have decisions based solely on automated processes (Article 22)

The GDPR applies in both European Union (EU) member states and the European Economic Area (EEA), both of which are illustrated in Figure 1. The EEA extends the single-market of the EU to other member states within the European Free Trade Association (i.e., Iceland, Liechtenstein, and Norway) , .

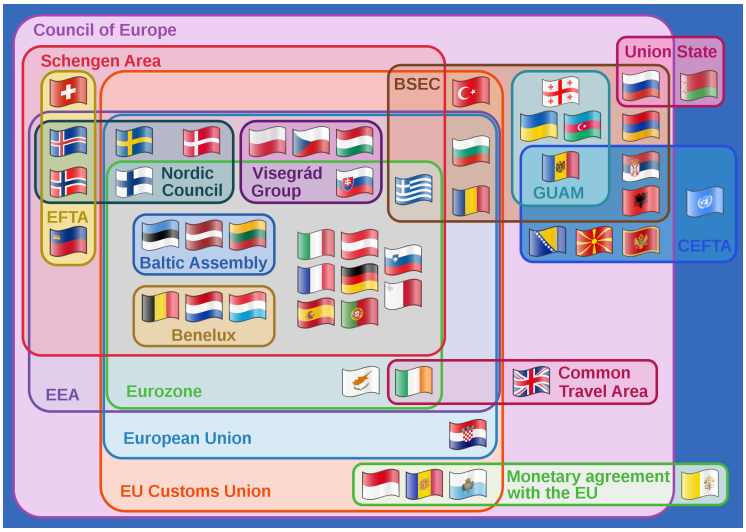

Figure 1—Euler Diagram illustrating the various multinational European organizations and agreements. European Union is shown in light blue; EEA is in purple. Source: Wikipedia

2.2 The Case of Google Advertising

An easily accessible example of the impact of GDPR is Google's Ad personalization, which provides a major revenue source for many websites as well as Google itself. As a result of the GDPR, Google now allows individuals to view the data that is being used to target ads specifically to them. At this moment, anyone with a Google account can go to Google Ad Settings and view the process behind Google's ad personalization, shown in 2. Additionally, it allows the selective removal of an individual's personal info as well as toggling off Ad personalization. Without the usage of AI algorithms in its infancy, Google's established reputation as a leader in web-indexing and advertising would have been overtaken by another innovative company.

To comply with GDPR–to the best of my knowledge–, Google has completed the following:

- Modifying or correcting personal data (Article 16),
- Complete deletion of personal data and accounts (Article 17)
- Allowed toggling off ad personalization (Article 18, Article 21, Article 22)

As a result of the GDPR, targeted advertising is still completed possible with only the consent of the users. Without being able to target potential markets, I

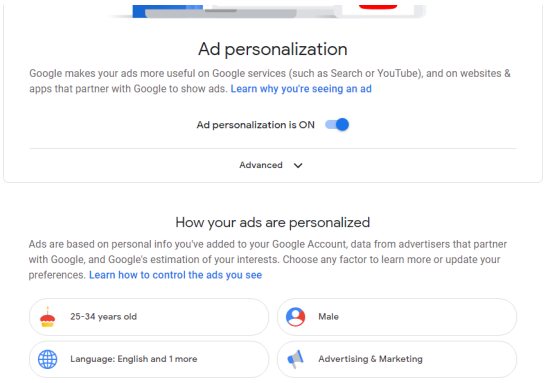

Figure 2—Example of data Google uses to target ads towards myself (the author)

would suspect that advertising would follow a more random approach, or more reasonably use third-party data such as a website's intended or suspected audience to control the ads shown. Though, this could lead to pervasive techniques such as virtual or physical geofencing marketing.

2.3 No GDPR, No Service

Clearview AI is a private American company specializing in facial recognition software, and caters to businesses, governmental agencies, and individuals, although explicitly mentioning only law enforcement agencies CDC Gaming,. Clearview AI's questionable practices involved scraping social media sites for user images and subsequently using those images in their AI software Hill, 2020. This is in massive violation of the GDPR regulations mentioned above, and this has resulted in numerous government mandates for the company to delete its facial recognition data within Europe Brandom, 2021, as well as Australia,. The company does not seem to be tenable, at least within Europe and even Australia. Their main product would require millions of individuals to waive their GDPR rights in order to be useful. In absence of these waivers, their facial recognition software would most likely not be of use due to lack of training data.

REFERENCES

[1] Brandom, Russell (Dec. 2021). *French regulator tells Clearview AI to delete its facial recognition data*. en. URL: https://www.theverge.com/2021/12/16/

22840179/france-cnil-clearview-ai-facial-recognition-privacy-gdpr (visited on 02/02/2022).

[2] CDC Gaming, Mark Gruetze (2022). *G2E: New generation of facial recognition enhances security, raises questions*. en-US. URL: https://www.cdcgamingreports.com/g2e-new-generation-of-facial-recognition-enhances-security-raises-questions/ (visited on 02/02/2022).

[3] *Clearview AI Forced to Cease Data Scraping Operations in Australia* (2022). en-us. URL: https://gizmodo.com/clearview-ai-forced-to-cease-data-scraping-operations-i-1847991895 (visited on 02/02/2022).

[4] Hill, Kashmir (Jan. 2020). "The Secretive Company That Might End Privacy as We Know It". en-US. In: *The New York Times*. ISSN: 0362-4331. URL: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (visited on 02/02/2022).

[5] *The Basic Features of the EEA Agreement | European Free Trade Association* (2022). URL: https://www.efta.int/eea/eea-agreement/eea-basic-features#1 (visited on 02/02/2022).