Homework 1:
CS7637

Aravind Muralidharan Chilukoor
acm35@gatech.edu

1 QUESTION 1

The goal of the problem is to move Rey, Snoke and Kylo from planet Quesh to the orbiting ship using a shuttle which can move a maximum of one person at a time. (it can move without any passenger too)

1.1 Semantic Network to represent the problem

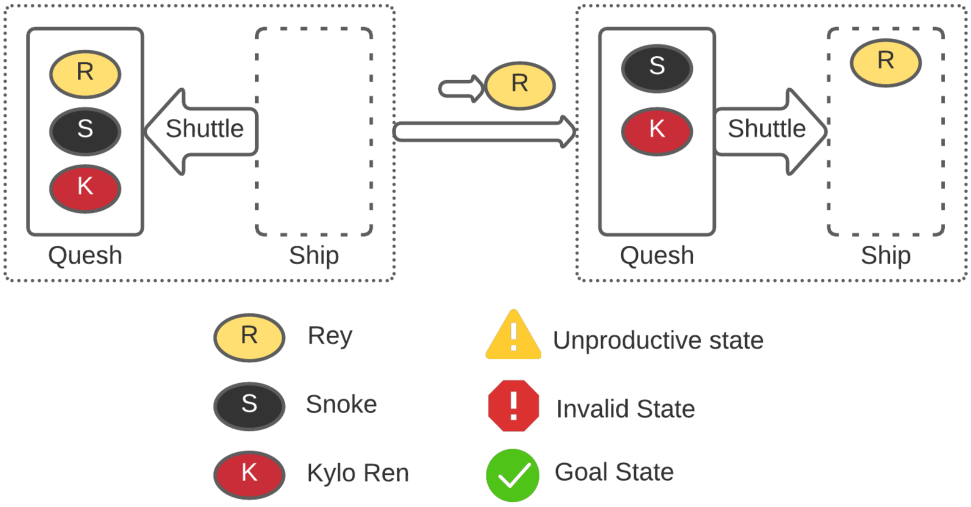

Figure 1— Semantic Network that showcases a transition between 2 states for Question 1 and the legend labeling the components

A semantic network to represent Question 1 is shown in Figure 1. A state is invalid if:

- Rey and Snoke or on the same side with the shuttle on the opposite side
- Rey and Kylo or on the same side with the shuttle on the opposite side

A state is unproductive if:

- It has already been generated and visited before.

1.2 Applying Generate and Test to solve the problem

The result of the generate and test is shown in Figure 2. Please note that the states have been simplified visually (removing the outline for the planet and the ship from Figure 1) in order to accommodate the image in one page.

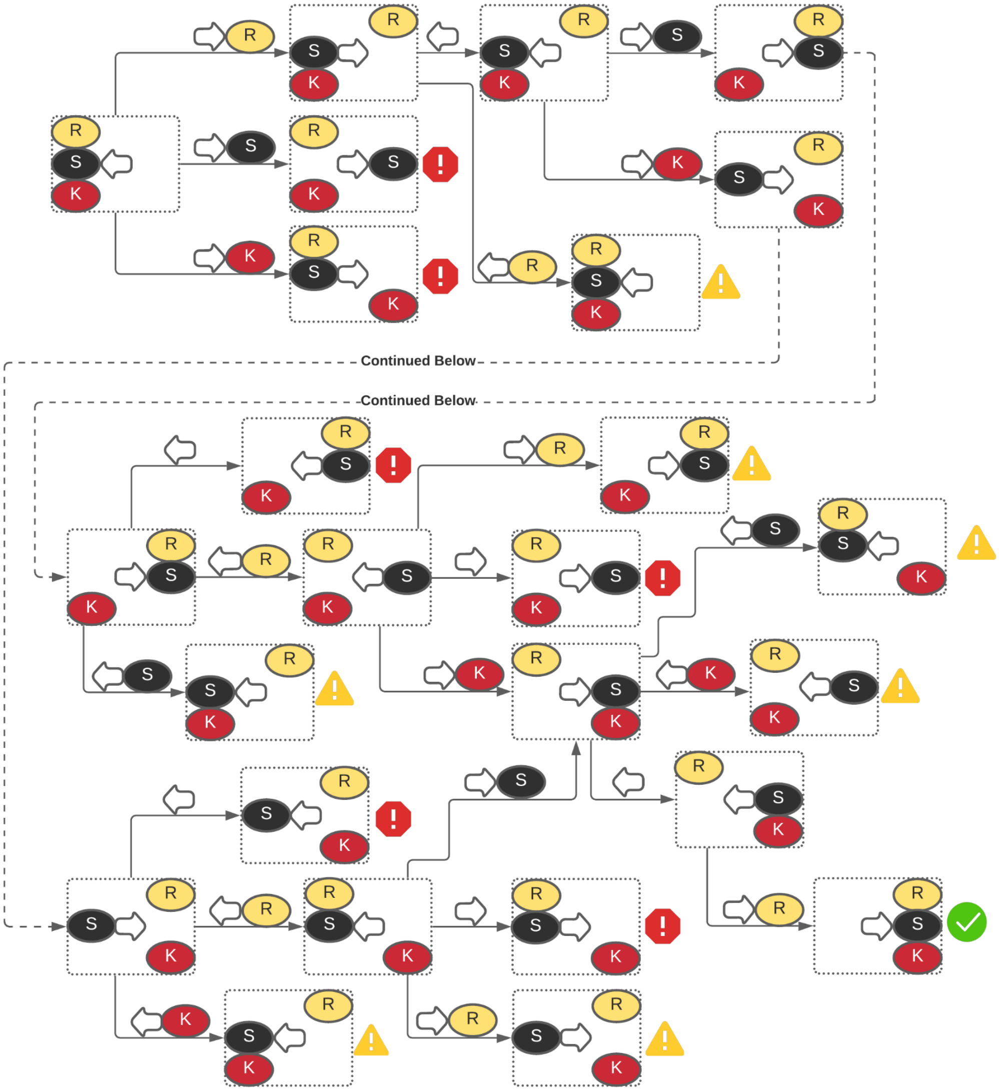

Figure 2 — Applying Generate and Test to the Semantic Network

2 QUESTION 2

The General Data Protection Regulation (EU) 2016/679 is a regulation that requires the protection of personal data and privacy that have been collected by businesses in the European Union (EU) and the European Economic Area (EEA) that consists of the Member States of the European Union and three countries of the European Free Trade Association (EFTA) (Iceland, Liechtenstein and Norway)

Most of the points relevant to personal data processing are captured in Chapter 2 (GDPR, 2016, Articles 5 through 11) of the regulation. To summarize, personal data should be:

- Processed in a lawful and transparent manner.
- Collected only for explicit and legitimate purposes and not be further used for in a manner that is incompatible with the initial purpose
- As accurate as possible. Inaccurate personal data should either be erased or rectified
- Processed in a manner that ensures the security of the data.

2.1 Possible impacts of the regulation on the use of AI to create personalized experiences

With Artificial Intelligence and Machine Learning algorithms coming to the fore in the recent past, a lot of tools that we use on a day to day basis tend to integrate some type of AI and learning techniques in order to provide us with a more personalized experience. A really good example of this is targeted advertisements. There are a lot of scenarios where an online platform uses the existing data it possesses on us and generates advertisements with products that may cater to our needs. How is this possible one might ask. Well, a lot of these businesses might have sophisticated AI algorithms running their decision making based on it's learnings from our personal data. The main challenge of the regulation is to make sure that consumers are protected from possible adverse effects of AI using our personal data without slowing down the development of AI technology.

Any use of personal data for a specific purpose requires the consent of the data subject according to the regulation. Even if an individual offers consent for the usage of his data in a business' personalization program, they should be able to opt out at any time. Let's say an individual had initially given his consent to using his data for a particular company's product that is heavily reliant on personalized experiences. Now he decides to opt out. The AI agent which has already been operating on a knowledge base that involves the user's data and has possibly learnt from this data now has to potentially "unlearn" all of this. It might be easy to delete a user's data from a database, but making a sophisticated AI agent that learns from its decisions is extremely complicated and maybe even impossible. The fact that the AI agent can make future decisions based on learnings from the data collected from a user who has decided to opt out will go against the GDPR regulations.

The transparency in how personal data is being processed that is demanded by the GDPR regulations might cause another possible impact to businesses that rely heavily on a proprietary AI and learning algorithm. With more transparency, these businesses will have to tend to use methods that are less effective.

2.2 Example of an industry in which personalization is deeply embedded but not essential

The industry that I'm going to talk about in this section is the digital fitness industry. An example of a company in this industry is UnderArmour and one of its main products, MyFitnessPal.

MyFitnessPal is one of the many digital fitness services that are offered that follow the Freemium model. This kind of business model involves providing an end user with the service for free and then charging a premium for additional, exclusive services. Most of the companies that have products that follow the freemium model mostly have personalization deeply embedded in the premium section of the product. However, end users could still use the product effectively without signing up for it and giving up any data as the core services offered, for example calorie tracking and exercise recommendations are still available for free without requiring any user data.

However, since the products still collect data from its premium users, they are still required to be GDPR compliant.

2.3 Example of an industry in which personalization is deeply embedded and is essential

The industry that I'm going to talk about in this section is the facial recognition industry. Without user biometrics, there is no service offered. This industry covers multiple companies and products which use facial recognition in order to offer services to either the government or private firms. All biometrics collected by companies that fall under this industry are subject to GDPR regulations.

The GDPR defines biometric data as “personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data” (GDPR, 2016, Article 4, Definition 14)

The GDPR clearly states that the processing of biometric data for uniquely identifying a person or data concerning their health is strictly prohibited (GDPR, 2016, Article 9, Paragraph 1) unless

- Explicit consent has been given by the data subject (GDPR, 2016, Article 9, Paragraph 2).
- Processing is necessary for reasons of public interest (GDPR, 2016, Article 9, Paragraph 2).

One of the companies that falls under this industry is Clearview AI. The selling point of the company is that it’s the largest intelligence platform that is trusted by law enforcement.

However, it was learnt that Clearview AI had amassed a database of some 10 billion images by scraping selfies off of the internet. France’s CNIL found 2 breaches of the GDPR:

- Collecting and using biometric data without a legal basis (GDPR, 2016, Article 6)
- Variety of data access rights (GDPR, 2016, Articles 12, 15 and 17)

According to CNIL, the company neither had consent nor could they rely on it falling under alternate exceptions (especially public interest ones) due to it’s intrusive nature and hence provided a formal notice to Clearview AI to stop the unlawful processing of personal data.

Though the order that was passed by the CNIL is applicable only to data the company holds on people from French territories, more such orders were expected from other countries from the EU member states and EEA countries where GDPR was a part of national law (around 30 countries). The company was also ruled in breach of privacy rules in Canada, Australia and the UK (which wasn't in the EU post Brexit but still retained the GDPR in national law).

The very intrusive nature of these kinds of companies within the industry means that it's extremely difficult for them to be GDPR compliant. They could adapt by doing the following:

- Be 100% transparent as to whether your data is stored in their databases and allow users who have provided consent to retrieve their data whenever they want.
- Offer a method to opt-out, i.e delete your data from their databases

Unless such adaptations are made, it is impossible for people to use such services in the European Union and in the EEA unless they completely waive their GDPR rights.

3 REFERENCES

1. General Data Protection Regulation - Wikipedia. Retrieved Feb 1st, 2022, from https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
2. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016. Retrieved Feb 1st, 2022 from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
3. Clearview GDPR breaches France. Retrieved Feb 1st, 2022 from https://techcrunch.com/2021/12/16/clearview-gdpr-breaches-france/