CS7637 Homework 1

Caleb Wagner
cwagner@gatech.edu

***Abstract*—This paper presents a solution to Homework 1. The first section contains the implementation of a semantic network for a Star Wars problem space. The second section describes the General Data Protection Regulation and its impacts to artificial intelligence.**

1 STAR WARS SEMANTIC NETWORK PROBLEM

1.1 Semantic network representation

A semantic network to represent the Star Wars problem space is shown in Figure 1. The two possible states are Quesh (the planet) shown on the left, and the ship, shown on the right. The states are made of three components, namely Rey, Kylo, and Snoke. The operator for this problem is the shuttle, which can take one or none of the components across states. The side the shuttle is on/the direction the shuttle is facing shows the direction of travel the shuttle just made. For example, in the Start state, the shuttle just came from the right (ship) to the left (Quesh). The transitions between states are labeled at the top of the new state, such as Move(Rey), which describes that Rey was moved on the shuttle to the right (ship) to generate the new state, where Kylo and Snoke are still on Quesh and Rey is on the ship.

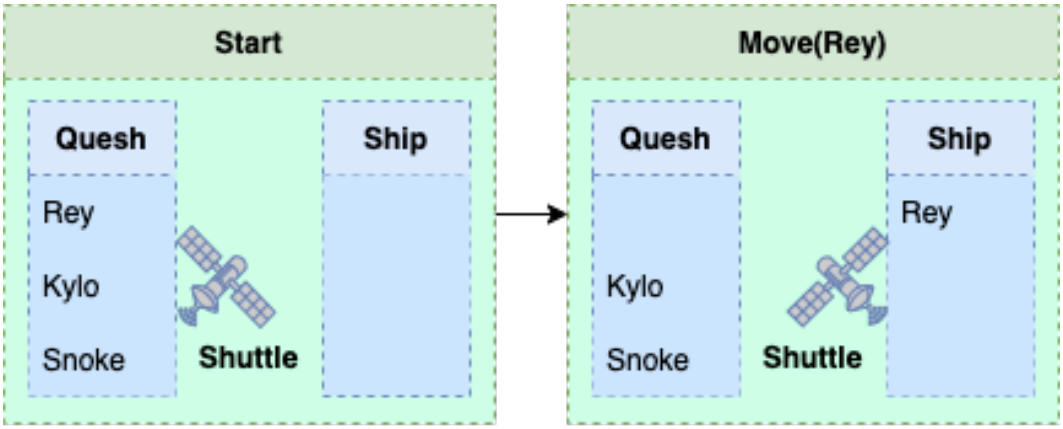

***Figure 1*—A semantic network representation for the Star Wars problem.**

1.2 Generate and test solution

Figure 2 depicts a legend that shows the quality of a given state. A state can be valid (green), invalid (red), duplicated (grey), or the goal state (orange). A state is invalid if Rey and Snoke are left alone together or if Rey and Kylo Ren are left alone together on either side. A state is duplicated if it has already been visited earlier during generation. The goal state is the desired state of the problem.

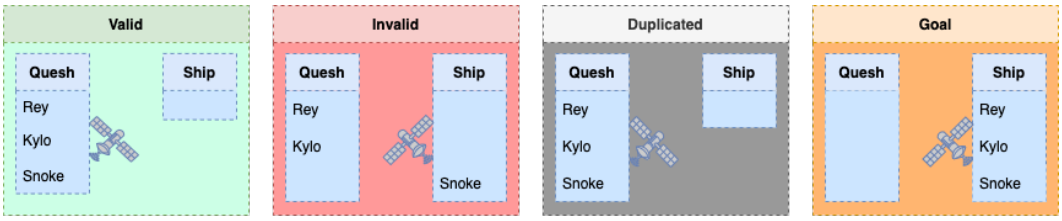

Figure 2—A legend depicting the various states of the search for the Star Wars problem.

Figure 3 shows the full expansion of the state space using generate and test. The 26 states (not including the initial state) are generated, 10 of which are valid. States 3, 17, and 18 were marked as invalid because Rey and Kylo were left alone together. States 5, 13, and 21 were marked as invalid because Rey and Snoke were left alone together. States 6, 8, 11, 12, 16, 19, 22, 23, 25, and 26 were invalidated as they were duplicates of previously generated states. In total, two valid solutions were found.

2 GENERAL DATA PROTECTION REGULATION

Personal data in the General Data Protection Regulation (GDPR) is defined as any information that relates to an individual, regardless of whether that individual can be directly identified or indirectly identified (*General Data Protection Regulation*, 2016). The GDPR seeks to control which parties (both the individual and third parties that control the data known as controllers) manage personal data as well as how the data is used by the different parties. In other words it seeks to give the control of an individual's data to the individual. It does this by establishing set of guidelines as well as penalties for violating the guidelines. The guidelines list the various rights that the GDPR affords to individuals. One of the first major guidelines concerns consent. Controllers must provide easy to understand terms and conditions statements, instead of terms that are ambiguous or full of legal jargon (Chapter 2, Article 7). It must be easy to also withdraw

Figure 3—A generate and test search graph for the Star Wars problem.

consent or revoke the access of the controller. Furthermore, controllers must ask for consent again anytime the data is used for a new purpose (Chapter 3, Article 15). Another guideline concerns the right to access data such as what data being collected and how it is used (Chapter 3, Article 12). This guideline is tightly coupled with the right to be forgotten, where individuals can ask that all of their individual data be deleted and no longer shared with other controllers (Chapter 3, Article 17). Other guidelines include the right to be notified of security breaches concerning individual data (Chapter 4, Article 34), controllers following privacy by design guidelines to design software to keep data safe (Chapter 4, Article 25), as well as establishing data protection offers for large companies (Chapter 4, Article 37).

2.1 Impact to AI

These guidelines will and already have impacted the use of artificial intelligence to create personalized experiences. Because individuals can revoke access to data at any time, this has and will limit what data is collected/shared. The requirement to remove data from datasets that was collected without consent will also limit the amount of data that is available to learn from. This greatly impacts tech-

niques involving statistical or probabilistic methods as they often require large datasets. Individuals limiting the access of data to controllers can also create issues of biased datasets, where certain groups of people restrict access to data but not others. The limitation that a controller must ask for consent each time something new is done with the data may also affect the way research is performed. For example, if a company wants to implement a new AI technique, they will need to ask for consent again which may or may not be given, especially in the quantities needed to implement the new technique. Research is also affected by the guideline to only collect what is needed. Controllers cannot just ask for a large amount of data about individuals so that they will have everything they could ever want for multiple different AI techniques.

2.2 Personalization example

An example of a company for which personizalization is deeply embedded in its functional purpose but it is not essential for it to be useful is YouTube. YouTube recommends content based off of personal interests and previously viewed content. However, YouTube is still a useful platform even if content recommendation is disabled, as users can still search for videos manually. An example of a company for which personalization is deeply embedded in its functional purpose and is essential for it to be useful is Fitbit. Fitbit is a fitness company that produces wireless-enabled wearables and activity trackers such as smartwatches, GPS, pedometers and monitors for heart rate, quality of sleep, and overall fitness metrics. Excluding some of the more generic products such as smartwatches, the fitness trackers must be tied directly to an individual's biometrics, therefore requiring a high degree of personalization.

2.3 Data regulation practices evaluation

Fitbit has already committed to GDPR compliance (*Fitbit GDPR*, 2021) so that it may sell to the European Economic Area (EEA). The EEA consists of all the European Union's (EU) countries as well as Iceland, Liechtenstein and Norway. This allows the EEA to be part of the EU's single market (*Countries in the EU and EEA*, 2015). Based on the guidelines above as well as the checklist provided by the GDPR (*GDPR Compliance Checklist*, 2021), the sections taken from the GDPR listed above are relevant to Fitbit as it sells to the EEA market. Related to the GDPR guideline on consent, in order to obtain consent regarding the collection of data, Fitbit has a Terms of Service and Privacy Policy that must be agreed to

before using their products. The GDPR guideline concerning the right to access data and see how it is used is also relevant to Fitbit as Fitbit maintains personal accounts that store data about individuals. The guideline concerning the right to be forgotten also applies. Fitbit currently provides ways to export data in a convenient format as specified by the GDPR (*Export Fitbit Data*, 2021), as well as ways to delete both a Fitbit account and all data associated with it (*Delete Fitbit Account*, 2021). Other guidelines that apply to Fitbit include notifying of security breaches and following privacy by design guidelines, something that Fitbit dealt with recently when a database containing personal information was found to be openly accessible and not password protected (McKeon, 2021).

I believe that there are ways Fitbit can change their devices and business models such that users do not have to waive their GDPR rights as Fitbit for the most part currently requires (*Common sense privacy standard privacy report for Fitbit*, 2021). A lot of the collected information such as height, weight, gender, sleep cycles, female health tracking, calories burned, credit card information, GPS signals, and IP address are used for certain features such as targeted advertisements (*Fitbit Privacy Policy*, 2021). Fitbit could allow users to opt out of this data collection. Data is also collected for the purpose of developing algorithms to accurately track biometrics such as heart disease. These algorithms do not need to be trained on central servers, but can instead be trained directly on the end device through techniques such as federated learning (Sozinov, Vlassov, and Girdzijauskas, 2018). Finally, users should be able to store more data locally, such as directly on the health tracker or on a phone. Metrics do not need to be shared to Fitbit's servers, but instead have a local database that keeps track of the personal data. The biggest limitation to these changes is that it requires the devices to process and store more information, which is something they may not be able to do at this time or will raise their current price.

3 REFERENCES

[1] *Common sense privacy standard privacy report for Fitbit* (2021). URL: https://privacy.commonsense.org/privacy-report/Fitbit.

[2] *Countries in the EU and EEA* (July 2015). URL: https://www.gov.uk/eu-eea.

[3] *Delete Fitbit Account* (2021). URL: https://help.fitbit.com/articles/en_US/Help_article/1285.htm.

[4] *Export Fitbit Data* (2021). URL: https://help.fitbit.com/articles/en_US/Help_article/1133.htm.

[5] Fitbit (Apr. 2021). *Fitbit GDPR*. URL: https://healthsolutions.fitbit.com/gdpr/.

[6] *Fitbit Privacy Policy* (2021). URL: https://www.fitbit.com/global/us/legal/privacy-policy#info-we-collect.

[7] *GDPR Compliance Checklist* (2021). URL: https://gdpr.eu/checklist.

[8] *General Data Protection Regulation* (2016). URL: https://gdpr.eu/tag/gdpr/.

[9] McKeon, Jill (Sept. 2021). *61M fitbit, Apple users had data exposed in Wearable Device Data Breach*. URL: https://healthitsecurity.com/news/61m-fitbit-apple-users-had-data-exposed-in-wearable-device-data-breach.

[10] Sozinov, Konstantin, Vlassov, Vladimir, and Girdzijauskas, Sarunas (2018). "Human Activity Recognition Using Federated Learning". In: *2018 IEEE Intl Conf on Parallel Distributed Processing with Applications, Ubiquitous Computing Communications, Big Data Cloud Computing, Social Computing Networking, Sustainable Computing Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom)*, pp. 1103–1111. DOI: 10.1109/BDCloud.2018.00164.