Homework 1

Pranav Srinivas Dutta Sriraj
pranavsrinivasdutta@gatech.edu

***Abstract*—**In the first section of this paper we are going to use Semantic Networks and the "Generate and Test" technique to imitate an AI agent to solve the given homework problem. In the second section we are going to look at what the *General Data Protection Regulation* (GDPR) law says about the usage of personal data to personalize individual user experiences online and understand it's jurisdictions. To elucidate this regulation, we will look at Google Ads to cite sections from GDPR which are relevant to this example.

1 SEMANTIC NETWORKS AND GENERATE AND TEST

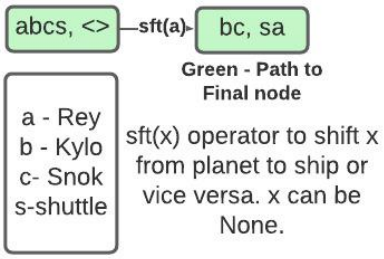

***Figure 1*—**Illustrates the Semantic Network Representation

This problem involves three fictitious people who reside on planet Quesh. Based on some constraints the three people need to be shifted from planet Quesh to the spaceship using a shuttle. The constraint disallowed Rey to be alone with Snoke or Kylo in the absence of the space shuttle. The shuttle enables movement between the planet and quarantine in the spaceship. The shuttle can move even without anyone in it.

Figure 1 Illustrates the nicknames for the characters used in the Semantic Network. The shuttle is represented by (s). In *figure 1,* the green box indicates a state. In a state, the left of " , " is Quesh and the right of it is the spaceship. If "s" is present on the left of " , " then the shuttle is on Quesh, otherwise it is on the spaceship. The shuttle can perform a shift (sft(x)) operation that enables the movement of people between the planet and Quarantine in the ship using the

shuttle. The shuttle can move from the planet to the spaceship without anyone in it. It can carry at most one passenger along. Figure 3 Represents the complete Semantic Network for this problem.

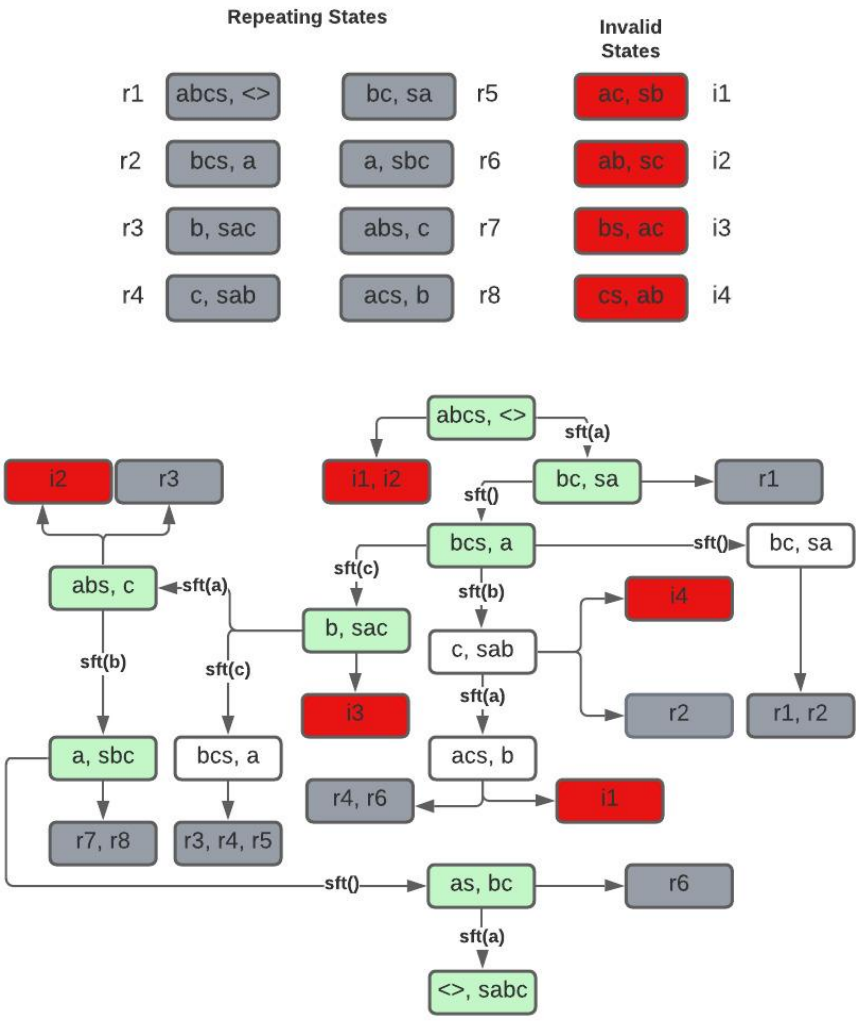

Figure 2 – Knowledge representation using semantic networks

Nodes colored red are illegal states since they don't comply with the rules of the puzzle. (Either Rey must be with Kylo without the shuttle or Rey must be with Snoke without the shuttle.) Repeating nodes are colored in Gray. In this semantic network, references to these nodes are mentioned instead of directly mentioning the repeating nodes. This is to optimize the space consumed by the semantic network. Certain gray nodes in this knowledge representation have multiple

references. This means the node represents more than one valid state that has already been generated.

Generate and test technique is used to solve this problem. The *not so smart generator* uses a BFS approach to generate valid states. The generated states contain illegal states and already generated nodes. The smart tester needs to identify illegal nodes as well as already generated nodes. Let's assume that nodes which were visited earlier are stored in memory for the agent to access and make decisions to not go ahead with processed nodes.

2 GENERAL DATA PROTECTION REGULATION (GDPR)

The GDPR provides a judicial framework for businesses and companies which enables the free movement and processing of personal data with the focus on protecting the fundamental rights and freedom of individuals (*Article.1*). This regulation can be enacted for citizens of the members of the European Economic Area irrespective of where they are living. In other words, businesses or companies anywhere around the world handling the data of citizens of the EU or EEA must follow this regulation. This regulation defines a few important stakeholders who are responsible for securely processing the personal data of individual's for various purposes.

Table 1—Describes the stakeholders as defined by GDPR

Name	Description
Data Subject	An identified or identifiable *natural person* (an identifiable living individual), whos personal data is to be processed (*Article 4.1*)
Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (*Article 4.7*)
Processor	Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (*Article 4.8*)
Supervisor Authorities	Independent public authorities to be responsible for monitoring the application of this Regulation (*Article.51.1*)

Personalization plays a vital part in revolutionizing the user experience on the internet. It involves collecting and processing volumes of personal data. This regulation empowers the Data Subjects to manage personal details shared with the controllers in exchange for personalization or other services. People are allowed to download their data and have a choice to move their data from one controller to another. *Article 17* allows Data Subjects the Right to be Forgotten.

Data Subjects can ask controllers to modify, remove or completely delete their data in the controllers' possession. Controllers need to seek prior consent from the Data Subjects to acquire their data for specific purposes. *Article-7* vividly captures the conditions for consent which the controller should abide by while procuring someone's approval to use their data. The Controller needs to maintain proof of consent as long as they are allowed to process personal data for a specific purpose (*Recitals 42*). Controllers can identify a natural person based on a unique id provided by their devices to build profiles to identify them (*Recital 30*). (Example, Apple devices have the *advertising identifier IDFA* for this purpose.) The data collected should be maintained up to date. Inaccurate data needs to be rectified or securely deleted. Data must be deleted by the Controller and the Processor when its purpose is complete (*Recital 65*). *Article 6.4* affirms that controllers cannot use the collected data for purposes other than those already agreed by the Data Subject. Repurposing of the collected information needs additional permission from the Data Subject. *Article 7.3* empowers Data Subjects to withdraw their given consent at any time. This gives the flexibility to Data Subjects to withdraw from any service at any time. It also mandates controllers to make the consent withdrawal process as simple as the consent receiving process. *Article 22.1* states that Data Subjects should not be subject to purely automated decisions that impact them legally or significantly. For example, issuing credit cards solely based on automated personalization might land a data subject in legal issues or significant jeopardy. Supervisor Authorities assigned by states belonging to the EU and EEA must ensure controllers and processors follow this regulation to protect the interests of the Data Subjects. Violation of GDPR will attract heavy penalties (as per *Article 83*).

2.1 A Few Instances of GDPR Violation

A news report in August 2021 said, Amazon Inc was fined $887 million for burying the actual intent of processing consumer data for personalization in lengthy terms and conditions without mentioning them concisely. (violating *art 7.2*). (Holland, 2021)

In a 2022 news report, tech giants Google and Facebook were charged a total of €210 million for not enabling the users to withdraw consent (given to store personal data in cookies) as simple as accepting them. The fines were not issued based on GDPR guidelines but the companies violated *Article 7.3* of the GDPR. An online investigation on these websites found that, while they offer a button

allowing immediate acceptance of cookies, the sites do not implement an equivalent solution (button or other) enabling the user to refuse the deposit of cookies equally easily, the CNIL said (BÎZGĂ, 2022).

Another report states that WhatsApp violated the transparency policies mentioned in GDPR *Article 12, 13, and 14*. (Data Privacy Manager, 2021) According to this report the European Data Protection Board and the lead Supervisory Authority of WhatsApp Ireland, assessed the penalty to be €225 million (Data Privacy Manager, 2021).

2.2 GDPR and Artificial Intelligence

AI requires personal data to be processed to produce personalized results. GDPR as a framework allows companies and businesses to acquire personal data in a streamlined manner. The acquired data can be processed based on the intent specified to the data subject while getting consent. The computerized processing of personal data to gauge personal behavior, attributes or traits is called "Profiling" (*Article 4.4*). Personalization needs profiling. Profiling cannot be performed on personal data of children. This regulation gives the rights to the Data Subjects to data portability (*Article 20*), object (*Article 21*), halt (*Article 19*), and right to be forgotten (*Article 17*). This regulation builds a rigid framework that allows companies to profile personal data obtained with due consent without compromising on an individual's privacy.

2.3 What is the European Economic Area (EEA)?

The EEA is an international agreement which enables the extension of the European Union's single market to member states of the European Free Trade Association (Wikipedia, 2022). This is a commercial agreement that allows free movement of people, money, goods, products and services within the European single market. The European Single Market is a conglomeration of member states of the European Union as well as a few other countries mentioned in the EEA agreement (Switzerland, Iceland, Liechtenstein, and Norway). GDPR applies to all member states of the EEA.

2.4 Google Ads

Google collects personal data based on consent (according to *Recital 30*) to customize the Ads that are shown to the Data Subject (if personalization settings is turned on). Data Subjects can revoke their consent as per Article *7.3* to opt out

of personalization. Google must be able to provide proof of consent as per *Article 7.1*. Data subjects are given the right to object to the processing of their personal data (*Article 21.3*). Google uses browser's cookies to store and process personal data to personalize ads (*Sections related to processing 6.1, 6.4, 9.1, 9.2, 9.3*). Ads have no relevance if there is no personalization. Therefore google ads uses cookies to store information on a browser. There are three types of cookies that they use. NID, ANID and IDE. The contents of the NID cookies are used to personalize ads on google service for signed out users. The contents of ANID and IDE cookies are used to personalize ads on non google sites (Google Ads, 2022). These cookies host a wide range of personal data as provided by the user including browsing history, youtube history, precise location of the data subject, user profile information like name, age, etc. based on the privacy settings of the user. In case google violates this regulation, it will be subject to fines and penalties (*Article 83, 84*). Google must make sure the rights of the Data Subject be safeguarded as mentioned in chapter 3 of the GDPR. (*Article 15, 16, 17, 18, 20, 21*) Standard contract mechanisms can be used to move personal data outside the jurisdiction of GDPR.

People belonging to member states of the EEA should be able to use services provided by Google Ads without waiving their GDPR rights. Member states appoint lead Supervisor Authorities for businesses and companies who constantly monitor the application for compliance of this regulation. As mentioned in *section 2.1 of this paper* sufficient actions are taken by authorities to check implementation of this regulation. Any violation of this regulation will attract heavy penalties and fines as mentioned in this regulation. Google Ads need not comply with these regulations for citizens who don't belong to the members of EU, Simple Market or EEA. Since Google has personalized ad experience around the globe, Google's compliance with GDPR will benefit the entire world (even when Google does not need to comply with this regulation in other parts of the world). The absence of a supervisor authority for states outside of the EEA will be a deficit. Introduction of GDPR has acted as a catalyst for many nations across the globe to start thinking about the privacy and security of its citizens on the internet.

3 REFERENCES

1. Holland, M. (2021, August 6). Amazon GDPR Fine. *TechTarget*. https://www.techtarget.com/searchcio/news/252504997/Amazon-GDPR-fine-signals-expansion-of-regulatory-focus
2. BÎZGĂ, A. (2022, January 11). French Privacy Regulator Fines Facebook and Google a Combined €210 Million for Breaching EU Cookie Law. *Bitdefender*. https://www.bitdefender.com/blog/hotforsecurity/french-privacy-regulator-fines-facebook-and-google-a-combined-eu210-million-for-breaching-eu-cookie-law/
3. Data Privacy Manager. (2021, September 8). GDPR fine: WhatsApp faces €225 million for transparency violation – Data Privacy Manager. *Data Privacy Manager*. https://dataprivacymanager.net/gdpr-fine-whatsapp-faces-e225-million-for-transparency-violation/
4. Wikipedia. (2022, February 3). *European Economic Area*. Wikipedia. Retrieved February 6, 2022, from https://en.wikipedia.org/wiki/European_Economic_Area
5. Google. (2022, February 6). *Advertising – Privacy & Terms – Google*. Google Policies. Retrieved February 6, 2022, from https://policies.google.com/technologies/ads?hl=en-US
6. Google Ads. (2022, February 6). *How Google uses cookies – Privacy & Terms – Google*. Google Policies. Retrieved February 6, 2022, from https://policies.google.com/technologies/cookies?hl=en-US
7. GDPR. (2016). *GDPR Articles and Recitals*. General Data Protection Regulation (GDPR) – Official Legal Text. Retrieved February 6, 2022, from https://gdpr-info.eu/