Homework 1

Christopher Brennan
cbrennan34@gatech.edu

1 QUESTION 1

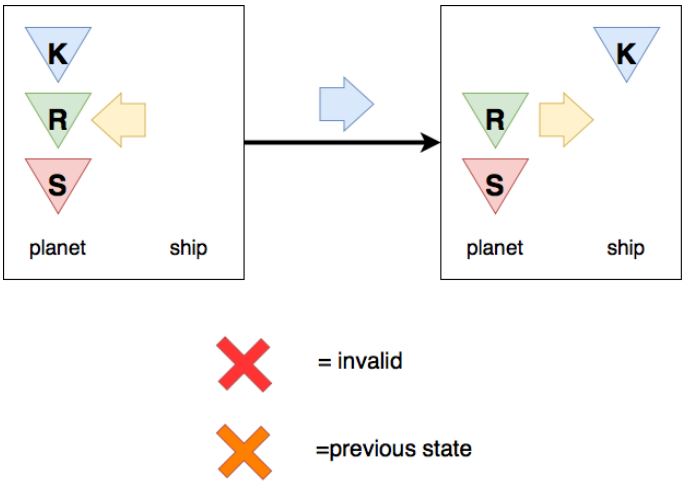

Figure 1—Semantic Network Rules - Colour implies character being moved (yellow means no-one)

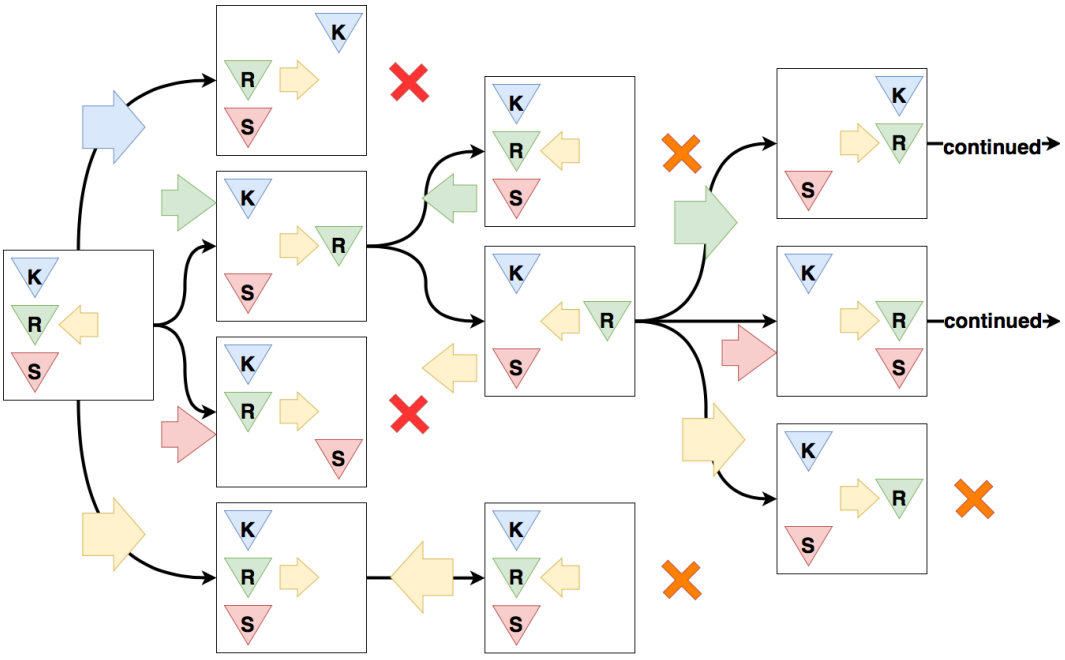

Figure 2—Start

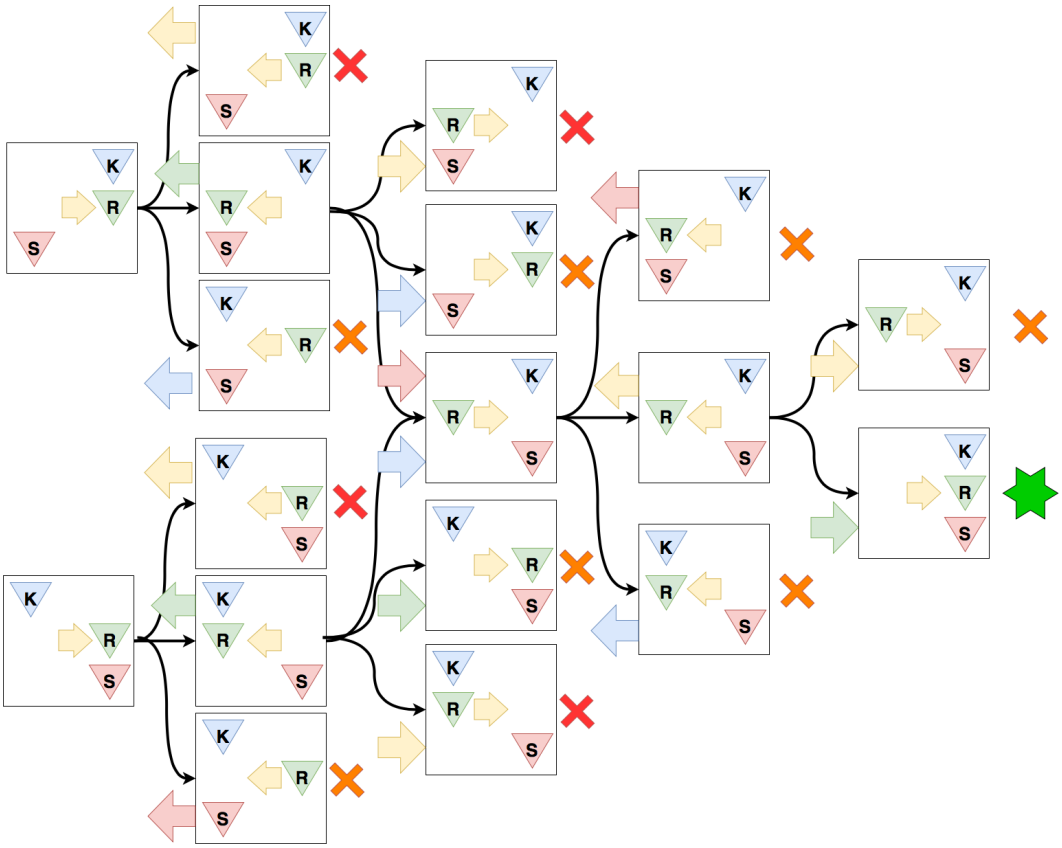

Figure 3—End

2 QUESTION 2

2.1 2016 General Data Protection Regulation from the European Union

The 2016 General Data Protection Regulation (GDPR) passed by the European Union (EU) is an EU law focused on data protection and privacy. GDPR applies if the data controller (organisation that collects the data), the data processor (organisation that processes data on behalf of the data controller) or data subject reside within the EU/European Economic Area.

GDPR **Article 6** establishes data may only be processed if and only if at least one lawful basis for processing applies.

2.2 GDPR and Personalising Individual Online Experiences

Personalising individual online experiences remains possible in a GDPR compliant environment, however it does become significantly more challenging.

2.2.1 *Lawful Basis*

A data controller must ensure at least one part of **Article 6** is satisfied in order to capture and process the data necessary for personalisation.

2.2.2 *Persistent Online Identifiers*

Online identifiers such as IP addresses and cookies are mentioned once in GDPR text (**Item 30 at the beginning**). They are therefore subject to GDPR and considered personal data. Data subject consent must be obtained for the collection of this data, except for strictly necessary cookies. Without online identifiers, the data related to an individual can be extremely limited, making personalisation challenging.

2.2.3 *Opt-In*

According to **Article 7**, a data controller must prove that the data subject has consented to the process of data; that is to say the data subject must opt-in. Consent for specific purposes, such as personalisation, must be clearly distinguishable, and can be withdrawn at any time.

2.2.4 *Data Minimisation*

Article 5 discusses the principle of data minimisation; collecting only necessary data. Personalisation requires data. Limiting what can be collected can inhibit true personalisation.

2.2.5 *Right To Be Forgotten*

Article 17 states that a data subject is allowed to have personal data removed by the data controller with immediate effect. If an individual chooses to 'opt-out', or have their data removed completely at any point, their data cannot be processed and personalisation isn't possible.

2.2.6 *Access to Data*

Article 15 allows the data subject the ability to request access to any and all personal data stored and processed by the data controller. While this does not necessarily prevent personalisation, it does add an additional requirement to performing it in ensuring all data is stored correctly and accurately.

2.3 Artificial Intelligence and Personalisation

All of the challenges listed in **Section 2.2** apply directly to the use of AI for personalisation also (lawful basis, opt-in consent, usage of online identifiers, data minimisation, right to be forgotten, access to data) and inhibit the impact it may have. However there is some additional challenges and parts of GDPR that apply specifically to AI.

2.3.1 *Profiling and Profiling Logic*

Articles 21 and 22 state a data subjects right to object, and the right not to be subject a decision based solely upon automated decision making or profiling. In this context, profiling is the automated processing of data to analyse or predict characteristics of a person, such as behaviour, personal preferences, or interests. AI for personalisation could certainly fall under this Article. It could be argued that **Article 22** doesn't apply for basic personalisation as there is possibly no legal or similarly significant impact on the data subject, as outlined in the Article. GDPR nevertheless imposes the additional challenge of ensuring this Article is not contravened.

Alongside **Article 22**, **Article 15** (Access to Data) also outlines that details of the logic involved (information on the algorithmic method), the significance and potential impact on the data subject of automated decision making must be available to the data subject in plain, understandable language. While not necessarily preventing the use of AI, it does create an additional burden and difficulty on the data controller in using AI for personalisation.

2.3.2 *Right To Be Forgotten*

The 'Right to Be Forgotten' can have a significant impact on the use of AI in general, including for use in personalisation. If data from a training set must be removed at the data subjects request, it adds further complications to the data controller, as well as potential cost/time implications in re-training models.

2.4 An Industry With Deeply Embedded AI - Medical AI Devices/Agents

Medical devices/agents are an example of devices/an industry that without the use of AI for personalisation, potentially would fail to function completely.

2.4.1 *European Economic Area*

The European Economic Area (EEA) consists of the member states of the European Union, as well as three countries from the European Free Trade Agreement (Iceland, Norway and Lichtenstein). It aims to strengthen trade and economic relations between the members. GDPR applies to all countries within the EEA.

2.4.2 *GDPR and Medical AI Devices/Agents*

Medical data is classified as 'special category' or sensitive data by GDPR. Not only is medical data subject to a lawful basis of general data processing in **Article 6**, it is also subject to seperate conditions of processing under **Article 9**. This would usually be satisfied in this context by **Article 9 Section 2 (h)**, around the provision of healthcare. This implies that for any data subject within the EEA, and data controller/processor within the EEA/ processing data from EEA citizens, GDPR applies and there must be a lawful basis, and a special categories lawful basis for processing the data.

Article 22 most certainly applies to Medical AI devices, as the automated decisions taken by AI in this context do have a legal or similarly significant impact on the data subject. Data subjects within the EEA have the right to object to profiling or automated decisions, and if this right is exercised for the case of medical AI devices, it may render devices useless for the data subject.

The legal requirement to provide details on any algorithmic methods, and their potential impacts to data subjects, as outlined by **Article 15** is a large challenge for medical AI devices. Often, neural networks are used for such complex tasks as healthcare, which are considered to be 'black-box techniques'. This possess and issue both in their complexity, and their explainability, especially in plain language to a data subject. Nevertheless, any data controller/processor working within the EEA, or with data subjects from the EEA must ensure that they satisfy this explainability criteria of the models within medical devices/agents.

The right to object (**Article 21**) and the right to be forgotten may also pose a significant challenge for data controllers working within the EEA/ working with data subjects from the EEA. The AI must be trained, and if data subjects within the training set (who previously consented) withdraw consent, there is potential implications of the AI in terms of needing to be re-trained. This risk is especially high for internally implanted devices.

2.4.3 *Adapting to GDPR - Can EEA Members Use These Devices*

Despite medical data being sensitive data, there is sufficient provisions within GDPR law that provided data subjects consent to the processing of data, there is a legal basis for medical AI devices/agents.

The transition to GDPR is not without adaptation however. The opt-in nature of consent in GDPR requires data processors and controllers to obtain explicit consent to not only data processing, but automated decision making also. The requirement of explainability is potentially something that would not have been considered pre-GDPR, and now must be explainable in plain language. The right to access data now requires data processors/controllers to keep a sufficient record of all data and the output of the processing, which again may not have occuring to the same extent pre-GDPR. Data minimisation may also require adaptation of AI models. If there is no legal basis for data points in a model, models must be changed to ensure GDPR is conformed to.

A data subjects right to object/right to be forgotten possibly poses the greatest challenge to whether EEA members can use medical AI devices. It is possibly counter-intuitive of a data subject to object to processing for medical AI devices/agents, given that the medical AI devices or agents may potentially be life-saving. On the otherhand, a data subjects right to be forgotten poses significant issues with trained AI models. As it stands, the only answer in the context of data subjects exercising this right, is to abandon and re-train models. While in theory this is possible, in reality the cost and time demand of this means it is almost impossible, especially for something as complex as healthcare. As data processors/controllers learn to live in a GDPR world, and continue to advance data privacy measures, maybe the fears of data subjects will be assuaged and GDPR will be opened slightly to definitively allow advances in areas such as healthcare. But as it stands, I see stumbling blocks that may prevent the use of these tools on EEA citizens, in particular the right to be forgotten.