CS7637: Homework 1

Frank Huang
fhuang64@gatech.edu

***Abstract*—** In this assignment, we walk through a simplified river crossing-like problem using semantic networks and the generate and test method in the first half. In the second half, we evaluate an example of a device, company, or industry that is deeply intertwined with personalization and how they need to be adapted in order to conform to 2016's GDPR legislation by the EU.

1 QUESTION 1

In this section, we solve the question posed by the assignment instructions and use a semantic network representation to map out the solution to getting Rey, Snoke, and Kylo onto Leia's ship.

1.1 Semantic network

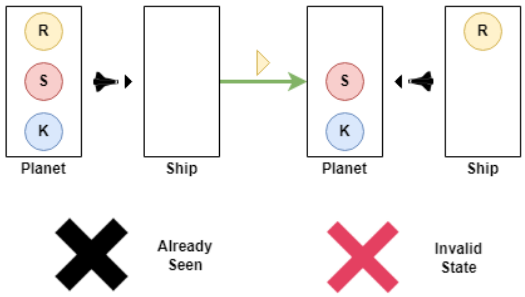


***Figure 1*—**Semantic representation of the problem feature two states and a transition

To solve this problem, state representations in the above figure will be utilized. Circles representing Rey, Snoke, and Kylo are created with their first initial and color-coded. Two regions (boxes) are set up to represent the planet and Leia's ship and the orientation of the shuttle is indicated by the shuttle icon and arrow.

A transition between two states is indicated by the green arrow along with a colored triangle indicating the direction and person that was moved by the shuttle to reach the next state. If no person is moved there will be a blank triangle (white). A red X will be used to indicate an invalid state and a black X will be used to indicate a state that was already seen and is discounted.

1.2 Solving with generate and test

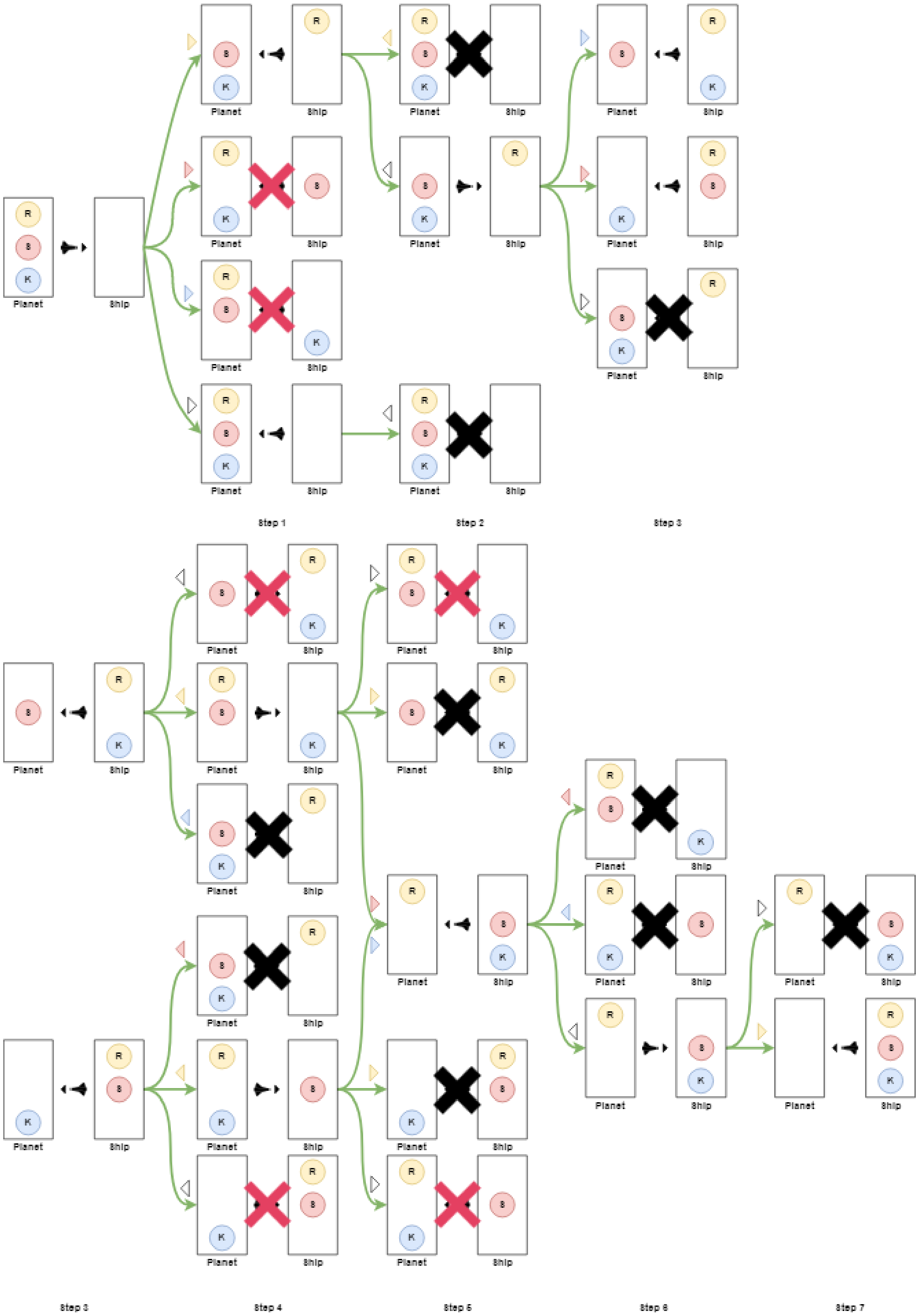


Figure 2—Solving problem with generate and test (larger form in Appendices)

In the above solution, the tester implements "smart" decision making by disqualifying invalid states (where Rey is alone with Snoke or Kylo) and states that have already been seen (meaning it would be unproductive).

2 QUESTION 2

2.1 GDPR background

The General Data Protection Regulation lays down a set of rules regarding the protection of personal data (both in data processing as well as movement of data). It lays out a series of fundamental rights that a person has (Articles 12-23) as well as lays down rules for which data controllers and processors need to follow in order to ensure that the data rights of individuals have been protected (Articles 24-43) ("General Data Protection Regulation", n.d.). These fundamental rights include the right of access, right of rectification, right to erasure (also known as the right to be forgotten), right to object, and right to opt out of purely-automated decision making or profiling, among others ("General Data Protection Regulation", n.d.).

Data controllers and processors who use the data provided by individuals are also subject to restrictions and responsibilities that dictate data storage limitations and data protection provisions. Personal information must only be used for specific processes that dictate the need for such information and processing activities must be thoroughly documented ("General Data Protection Regulation", n.d.). This is in addition to making available the necessary tools and processes to allow individuals to access their fundamental data rights as well as requirements for informed consent when collecting data ("General Data Protection Regulation", n.d.).

The GDPR also lays down additional restrictions for processing "special categories" of personal data in Article 9. This kind of data pertains to any data that relates to race, political affiliation, religion, genetic or biometric information, as well as health or sexual orientation ("General Data Protection Regulation", n.d.).

2.2 GDPR and AI usage for personalized experiences

Clearly, the GDPR lays down a wide-reaching set of rules that directly impact the usage of artificial intelligence in personalized experiences. In order to train AI models, information needs to be collected from individuals. GDPR lays out requirements that impact any data processing or warehousing to be compliant with data privacy and protection laws. The implication of a person’s right to be forgotten involves making sure that any trace of their data is scrubbed from the system, which may impact the usage of a model trained with data that needs to be removed.

The right to view data is also tied to how data stewardship and lineage is maintained in a given data ecosystem. Datasets that are continuously transformed may still have data pertaining to a given person, and it is the responsibility of the data controllers and processors to be able to track that lineage. To help address this, the GDPR also lays out the concept of pseudonymisation in its list of definitions in Article 4.

> “‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;” (“General Data Protection Regulation”, n.d.)

What is potentially quite tricky and would warrant a separate paper altogether is the insinuation of a “right to explanation.” This would entail understanding why a particular decision occurred as the result of an automated assessment. This isn’t captured in the main body of the GDPR regulation but in the recitals, particularly Recital 71 (“General Data Protection Regulation”, n.d.).

> “... such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. ” (“General Data Protection Regulation”, n.d.)

Why the GDPR does not include an explicit right to explanation in Chapter 3 (rights of the data subject) is curious, but Recital 71 does imply that part of the intent of the GDPR is to allow individuals to fully understand the reasoning behind any impact the processing of their data had. This makes AI systems more difficult to implement, as it is quite easy to imagine that complex models have tons of potential features and weights that make it hard to derive an explanation for a particular outcome.

2.3 EEA, and GDPR scope on social media

For this section, I will use the example of social media, where personalization drives just about every aspect of its business model. First, I will contextualize this by defining the European Economic Area (EEA), which is all EU member states along with Iceland, Liechtenstein, and Norway, that the GDPR applies to ("EEA Agreement", n.d.). In Article 3, the GDPR also defines its territorial scope to encompass processing of any personal data belonging to subjects within the EEA, regardless of whether the data controller or processor (and thus the processing itself) is in the EEA or not ("General Data Protection Regulation", n.d.). In Article 2, the GDPR defines its material scope by saying that the regulation applies to processing of data that is wholly or partly automated ("General Data Protection Regulation", n.d.).

Due to this territorial and material scope, we see that the GDPR (along with the articles discussed in the previous section) are applicable to most major social media platforms that operate in the EEA (Facebook, YouTube, Twitter, etc). This includes rights of data subjects (Articles 12-23) and the rules controllers and processors need to follow (Articles 24-43). Social media also encompasses data that fall under the category of special data (Article 9), which calls for stringent safeguards ("General Data Protection Regulation", n.d.).

2.4 How social media can adapt to GDPR

For the kinds of data processing that social media tends to carry out, it falls under the requirement for consent as defined in Article 5 clause 1.1 ("General Data Protection Regulation", n.d.). Social media platforms can (and have) implemented updated terms and conditions that users must agree with in order to use said platforms.

Social media platforms can also implement many of the data controls and rights that are afforded to users, such as the right to be forgotten when they deactivate their accounts, as well as requesting to see all the data that is stored about them or shared with other data controllers and processors. Many platforms already implement such controls, such as Instagram, Facebook, and LinkedIn.

Of course, there will need to be infrastructure-level changes (as discussed earlier) to allow these sorts of changes. There is also a relatively gray area with the aforementioned right to explanation and the impact on AI systems used in social media. To this end, the provision in Article 35 of the GDPR allows for the use of a data protection impact assessment for new types of processing, which may be relevant to implementation of new social media algorithms or behaviors ("General Data Protection Regulation", n.d.).

2.5 Summary and further thoughts

In summary, I believe it **is** possible to allow users in the EEA to continue to use social media without waiving their GDPR rights. In fact, many social media platforms have implemented tools and features in order to be GDPR compliant. Compared to some privacy laws that I am personally familiar with due to my job (California's Consumer Privacy Act), the GDPR is much more thorough and strict with their data protection requirements. The general trend seems to lean towards more and more focus and adoption of personal data protection laws and affording data subjects the right to access or remove their data, especially with the rise of artificial intelligence and big data analytics. In late 2021, New York City passed a local law (to go into effect January 2023) which regulates the usage of automated hiring tools and required provisions for bias auditing of said systems (Kobetz & O'Keefe, 2021).

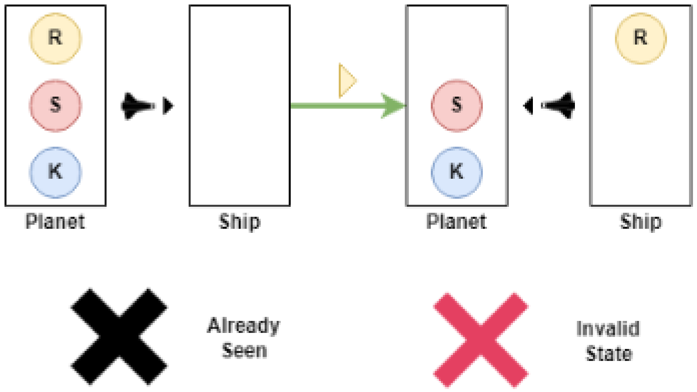
However, one thing I've noticed, from reading the GDPR to the content of the NYC law, is that there is typically an ambiguity to the requirements that require further definition ("Automated employment decision tools", n.d.). This includes standardized metrics for how and when to measure impact of data processing. What is the bar in which a data subject is considered impacted? How do we measure impact in deeply complex systems (tied to how data lineage is defined)? If we conduct bias audits, what are the standards and metrics for bias?

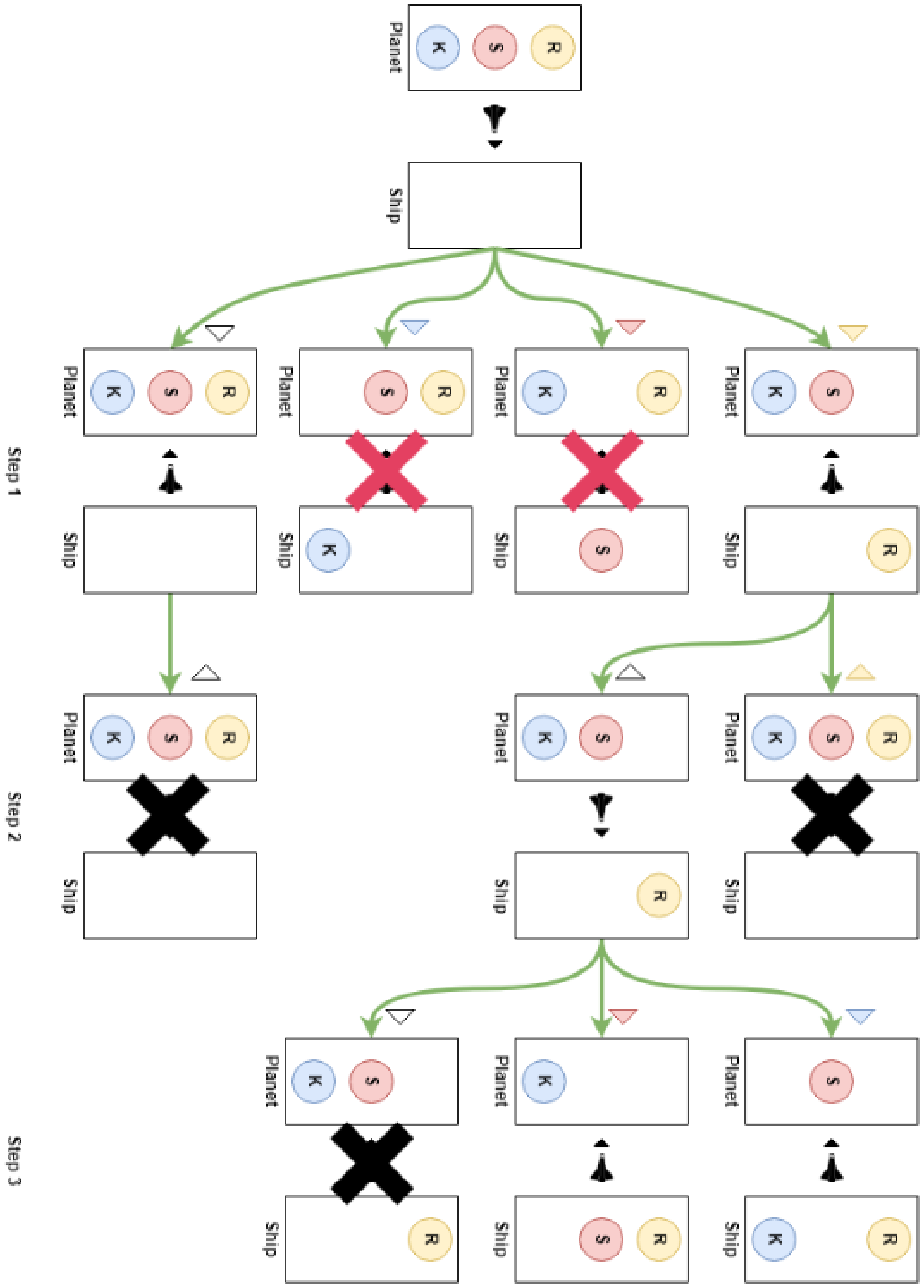
In my AI ethics class (CS6603), we discussed how there are many different bias mitigating techniques and metrics, with none of them being a "silver bullet" for minimizing bias or ensuring fairness. While we may have platforms doing data processing "legally", we may yet run into ethical concerns about how our data is being used even under consent such as when Facebook carried out experiments on user's newsfeeds (Meyer, 2014). Still, privacy laws such as GDPR and CCPA are certainly a step in the right direction from a consumer perspective.

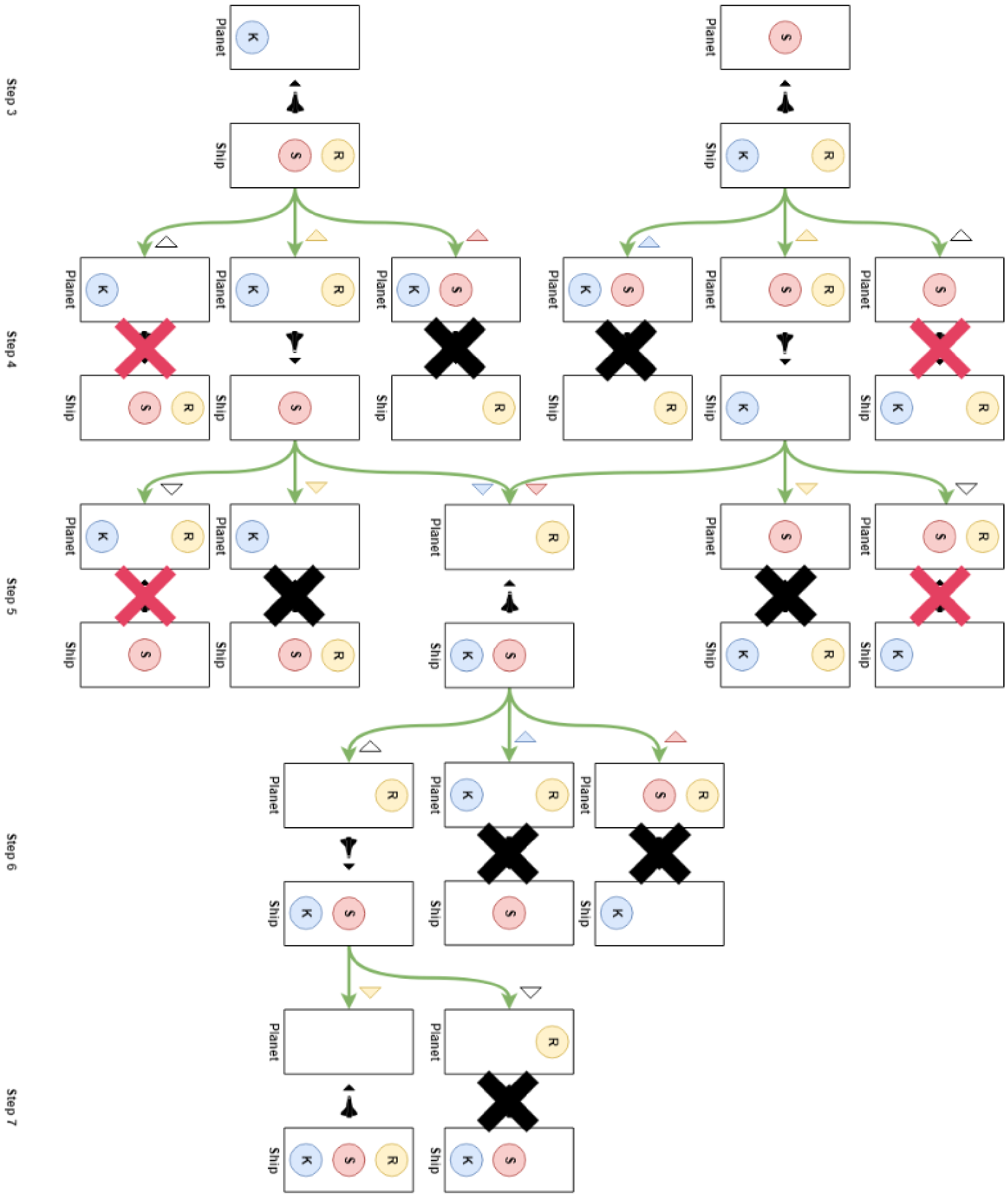
3 REFERENCES

1. Automated employment decision tools. (n.d.). The New York City Council. Retrieved February 6, 2022 from https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9
2. EEA Agreement. (n.d.). EFTA. Retrieved February 6, 2022 from https://www.efta.int/eea/eea-agreement
3. General Data Protection Regulation. (n.d.). Intersoft Consulting. Retrieved February 6, 2022 from https://gdpr-info.eu/
4. Kobetz, A. E. & O'Keefe, J. C. (2021, December 20). New York City Enacts Law to Regulate Use of Automated Hiring Tools. The National Law Review. https://www.natlawreview.com/article/new-york-city-enacts-law-to-regulate-use-automated-hiring-tools
5. Meyer, R. (2014, June 28). Everything We Know About Facebook's Secret Mood-Manipulation Experiment. The Atlantic. https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/

4 APPENDICES




Planet
K
S
R
Ship
Step 1
Step 2
Step 3


Step 3
Step 4
Step 5
Step 6
Step 7
Planet
Ship
K
S
R