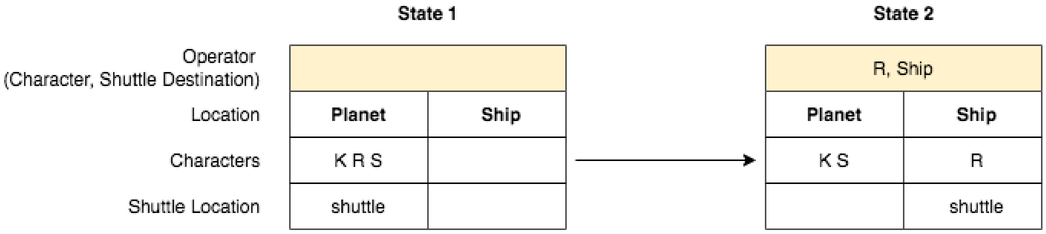
Homework 1

Taichi Nakatani
tnakatani3@gatech.edu

1 QUESTION 1: SPACESHIP GAME

1.1 Semantic Network

Figure 1 shows a semantic network of the spaceship game between two states. The top row represents the operation done to reach the state. The operation consist of two attributes: the character being moved and the destination of the shuttle. Note that state 1's operator is empty since it is the initial state of the game. The second row represents the location of entities (planet or ship), and applies to entities represented in row 3 and 4. The third row represents each character, abbreviated by the character's first letter (Kylo = K, Rey = R, Snoke = S). The fourth row represents the shuttle's current location (planet or spaceship).



	State 1			State 2	
Operator (Character, Shuttle Destination)				R, Ship	
Location	Planet	Ship		Planet	Ship
Characters	K R S		→	K S	R
Shuttle Location	shuttle				shuttle

Figure 1—Semantic network between two states.

1.2 Generate and Test

The entire semantic network of the spaceship game is shown in Figure 2. The initial state is shown on the far left and the target state is shown on the right with green circles. Invalid states are indicated by a red X. Invalid states are defined as either Kylo and Rey or Rey and Snoke being in the same location without a shuttle. Previously visited states are indicated by a gray X. For this implementation the tester was responsible for both validating states and checking previously visited states. In the end there were two sets of operations that legally reached the target state.

2 QUESTION 2: GDPR

The General Data Protection Regulation (GDPR) was implemented by the European Union in 2018 to protect the personal data of citizens from the European

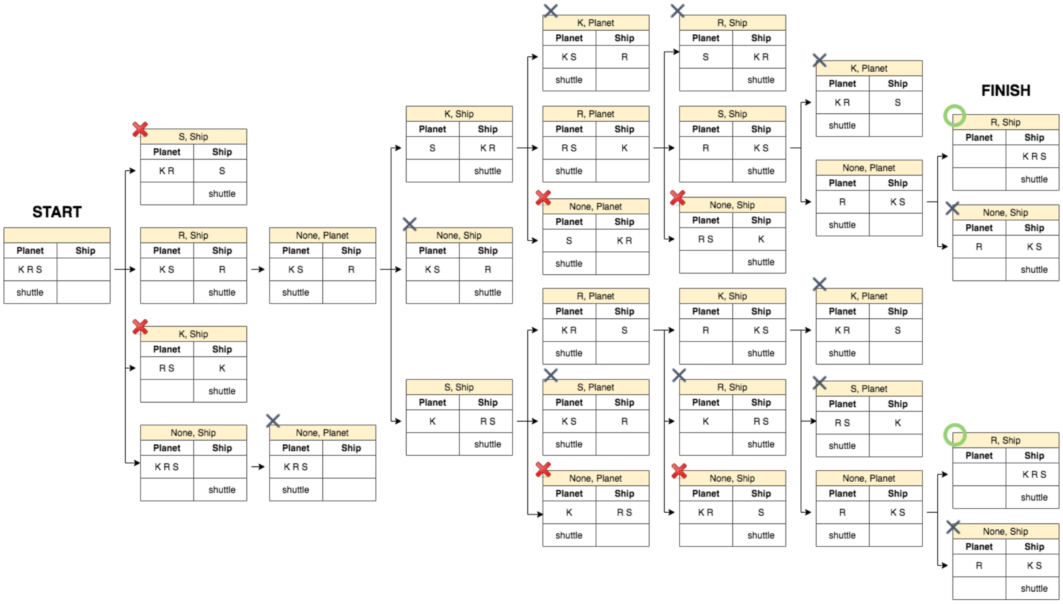


Figure 2—Entire semantic network of the spaceship game.

Union (EU) and European Economic Areas (EEA). These regulations establish the rules in which third parties can collect and process an individual's personal data, and defines what rights citizens have with regards to the use of their personal data. These regulations impact how artificial intelligence can be used to create personalized experiences and consequently have business implications on devices, companies and industries where personalized user experience is either a deeply embedded or an essential part of their business.

2.1 Implication on Personalized User Experiences

Chapter 1, Article 4 of GDPR defines personalized data as any information that can either directly or indirectly identify an individual, and encapsulates a wide variety of data ranging from explicit personal information (e.g. drivers license ID) to less explicit (e.g. work logs of an employee) (European Parliament and Council of the European Union, 2016). With regards to providing personalized user experiences, several regulations on such personal data have a large impact: Requiring an individual's consent of its use, the individual's right to have their personal data deleted, prohibiting certain categories of personal data, and limits on automated individual decision-making.

GDPR's fundamental component is providing individuals the right to consent whether or not their personal data can be collected and stored. Chapter 2, Article

6 and 7 states that individuals must give consent to the collection and use of their personal data (with some exceptions) and can revoke that consent at any time. (European Parliament and Council of the European Union, 2016). Furthermore, Chapter 3 Article 17 gives individuals the "right to be forgotten", meaning individuals can order their collected personal data to be deleted (European Parliament and Council of the European Union, 2016). These regulations have strong implications as to whether services can make use of an individual's personal data to provide a personalized experience. At any time, an individual may revoke their consent or order their personal data to be removed which may effectively disable a personalized experience.

GDPR also prohibits certain categories of personal data to be collected under most circumstances. Chapter 2, Article 9 lists prohibited categories such as racial or ethnic origin, political opinions, genetic data, biometric data and more (European Parliament and Council of the European Union, 2016). There are, however, exceptions to this rule such as the individual providing consent, the individual publicly sharing this data, or when collecting said data is necessary for the field of employment and more. Hence, if a company is reliant on one or more of these types of data to deliver a personalized product, the onus is on them to meet one of these exceptions.

Finally, Chapter 3 Article 22 gives individuals the right to object being subject to a decision made solely by an automated system (European Parliament and Council of the European Union, 2016). Examples of such automated decisions that use personal data include credit card services that approves or deny an application or employment services that automates the decision to move forward with a potential employee. Both services are personalized services that in recent years has employed artificial intelligence to automate its processes. There are, however, exceptions to this rule. The same article lists exceptions such as when individual provides explicit consent to this automated service, if this process is necessary for the individual and the service to enter a contract (European Parliament and Council of the European Union, 2016).

2.2 Case Studies: Online Advertising and Biometric Security

Online advertisement is a canonical example of an industry that is highly reliant on personalization. Targeted ads are a common tool for advertisers, and business have expanded their reach in collecting personal data to increase their ROI. For example, Shoshanna Zuboff states that Google created a highly personalized dataset called "user profile information" (UPI), which aggregates a user's search patterns, location, and other behavior signals to provide the most relevant ad to the user (Zuboff, 2019). These businesses were able to collect such data because users, prior to GDPR, were not required to give explicit consent to providing such data.

Biometric security, such as fingerprinting and facial recognition systems, is an industry where collection of personal data is necessary in order to exist. An example business is Clearview AI, which provides a facial recognition service using a large database of facial images it has collected. According to GDPR, individuals that comprise this database must now provide consent to their likeness being stored in their database. Recently, the Commission nationale de l'informatique et des libertés, a French regulatory body, has demanded that the company cease its processing of images as it breaches GDPR articles (Commission nationale de l'informatique et des libertés, 2021).

2.3 European Economic Area (EEA)

The European Economic Area (EEA) is an agreement that effectively extends the free movement of goods, capital, services and persons beyond the European Union member states to other nations (European Free Trade Association, 2013). Specifically, three additional nations that are part of the European Free Trade Association (EFTA) are included in this agreement: Iceland, Norway and Liechtenstein. Article 3 ("Territorial Scope") of the GDPR states that its regulation applies to any processing of personal data of citizens in the Union (meaning EU and EEA), regardless of whether the data itself is processed in the territory (European Parliament and Council of the European Union, 2016). This means that even if personal data is collected and used outside of the Union, if this personal data is from a Union citizen these regulations apply.

Article 3 expands the territorial scope of the regulation beyond just within the Union. Article 3 section 2 states that these rules apply to activities where the monitoring of Union citizen's behavior occurs (within the Union territory) (European Parliament and Council of the European Union, 2016). With regards to the case studies mentioned, this means that these regulations even apply to companies outside of the Union territory if they are collecting and using personal data from citizens in the Union. For example, Clearview AI may be a US corporation but if it is collecting facial data from EU citizens for its facial recognition AI system, GDPR regulations will apply to them.

2.4 How Case Studies Subjects May Adapt to GDPR

2.4.1 *Online Advertisement and GDPR Adaptation*

After GDPR was implemented, Google has updated their EU user consent policy which requires any Google product to require the explicit consent of a user to have their personal data to be collected (Google,). They have also added new services such as Google Dashboard which allows individuals to delete personal data the company has collected.

2.4.2 *Biometric Security and GDPR Adaptation*

One way a company like Clearview AI may adapt to these restrictions is to legally claim that it does not require explicit consent because it fulfills an exception to Chapter 2, Article 9 Section 2, specifically, "processing is necessary for reasons of substantial public interest" (European Parliament and Council of the European Union, 2016). According to Clearview AI, the use of its security service is only available to law enforcement (Clearview AI, 2021) and hence could be argued that it is performing a task for the benefit of public interest.

Both online advertisement and biometric security have challenges in complying with GDPR, but neither industry would be impossible to conduct their business without EU/EEA individuals waiving their GDPR rights. Fundamentally, both personal behavior data and biometric data can be collected as long as the user gives consent, despite it inducing significant business challenges. The other method is to argue that their collection of personal data meets other requirements or exceptions set by GDPR and thus does not require a user's explicit consent. In conclusion, there may be challenges set forth by the GDPR but companies may have ways to continue collecting personal data by compelling its users to consent or invoking the need of its service for the public good.

3 REFERENCES

[1] Clearview AI (2021). *Law Enforcement*. [Online; accessed 29-Jan-2022]. URL: https://www.clearview.ai/law-enforcement.

[2] Commission nationale de l'informatique et des libertés (2021). *Facial recognition: the CNIL orders CLEARVIEW AI to stop reusing photographs available*

on the Internet. [Online; accessed 29-Jan-2022]. URL: https://www.cnil.fr/en/facial-recognition-cnil-orders-clearview-ai-stop-reusing-photographs-available-internet.

[3] European Free Trade Association (2013). *SUBCOMMITTEE V ON LEGAL AND INSTITUTIONAL QUESTIONS - The Basic Features of the EEA Agreement*. [Online; accessed 29-Jan-2022]. URL: https://www.efta.int/sites/default/files/documents/eea/1112099_basic_features_of_the_EEA_Agreement.pdf.

[4] European Parliament and Council of the European Union (2016). *EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.* [Online; accessed 29-Jan-2022]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

[5] Google (n.d.). *EU user consent policy*. [Online; accessed 29-Jan-2022]. URL: https://www.google.com/about/company/user-consent-policy/.

[6] Zuboff, Shoshana (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books.