Homework 1

Andrew Bushnell
abushnell3@gatech.edu

1 QUESTION 1: STAR WARS SEMANTIC NETWORK

The Star Wars problem consists of a transportation issue describing Rey needing to transport a captured Kylo Ren and Snoke with an automated one person shuttle. To make the problem more complex, Rey cannot be left alone with either Kylo Ren or Snoke without the Shuttle. Figure 1 depicts the Semantic Network representation of this problem, definitions for the lexicon symbols within each node, and definitions for the state values as they are generated. The arrow between the two states represents the operator between nodes and the appropriately colored and rotated triangles represent what transition movement has occurred in that operator.

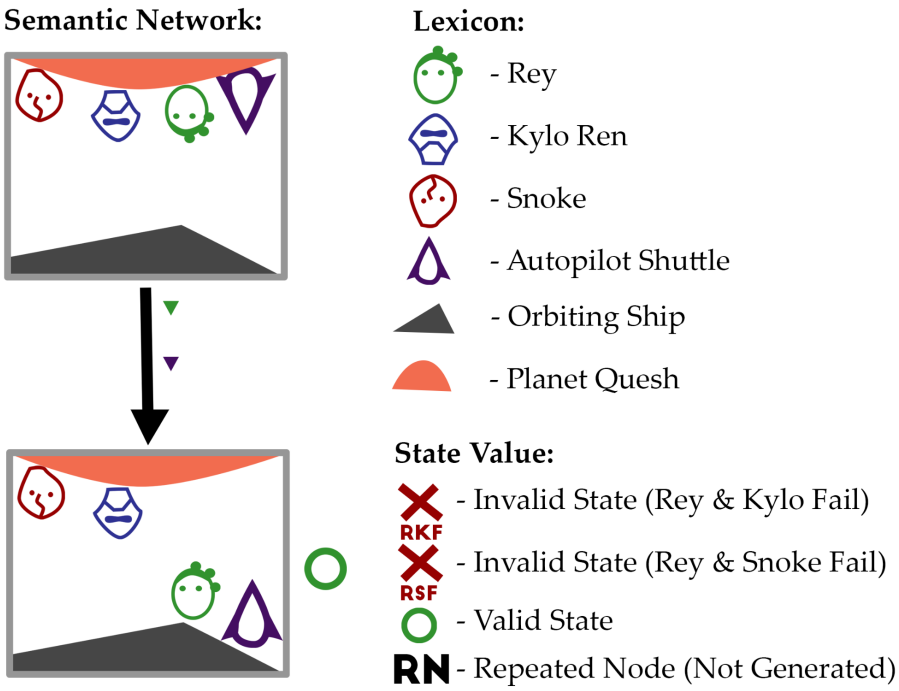

Figure 1—Semantic Network Representation of the Star Wars problem

Semantic Network Problem Space:

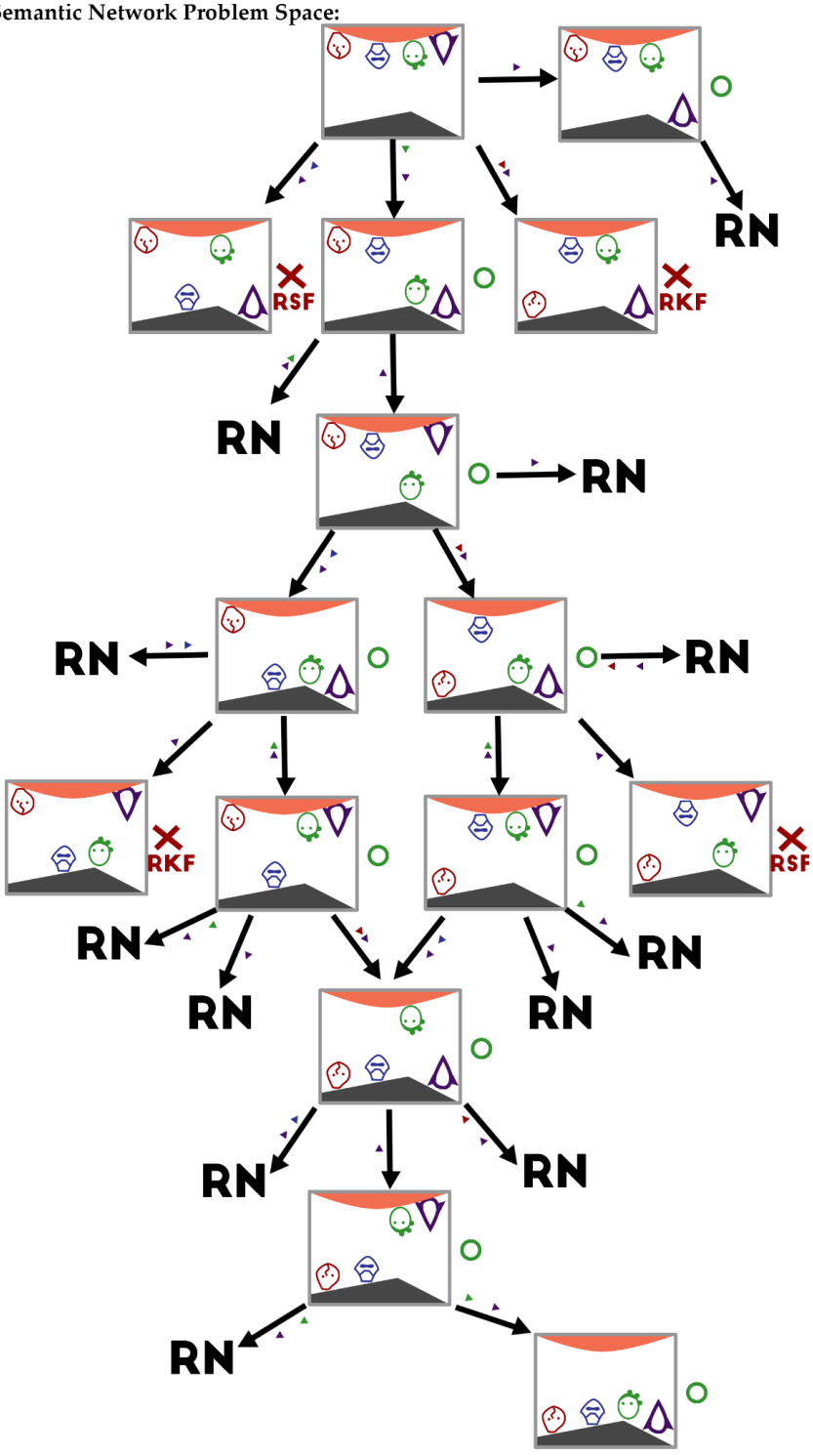

Figure 2—The Semantic Network of the entire Star Wars Problem Space when ran through a Smart Generator and Smart Tester

Figure 2 represents the entire problem space when run through a hypothetical smart generator and tester. The generator in this problem space generates all valid or invalid states as long as they haven't been seen before. The generator will store memory of all generated states and stop itself from generating any repeated nodes (RN). The smart tester will check for valid or invalid states to see if the generated node has failed either the Rey and Kylo rule (RKF) or the Rey and Snoke rule (RSF).

2 QUESTION 2: GDPR, TIKTOK, & FITBIT

Back in 2011, the European Union (EU) had an issue. The internet and social media had evolved at an alarming rate and its laws on user data protection were greatly outdated. The last EU law on data protection was made in 1995 when the internet was at its early stage (Lee & Webber, 2016), but now that corporate giants like Facebook and Google had transformed the digital landscape, the laws needed to transform as well. The EU commission soon put in proposals for a new law, the "General Data Protection Regulation" (GDPR), which would help European digital users regain control of how their data is recorded, stored, and used. While the law initially leaked to a major backlash from corporations (Lee & Webber, 2016), once it was released in 2018 a lot of the public saw it as a chance for the biggest companies to regain their trust and avoid scandals like the 2016 election incident with Cambridge Analytica (Lee & Webber, 2016a; Channel 4, 2018b).

When the GDPR was created in 2016, it was a lengthy regulation that spanned 11 chapters and 99 articles. These regulations helped establish data rights for users and set in a variety of security rules for corporations to strictly follow. Companies would now have to gain unambiguous consent to record users' data, they'd have to hash identifiable data while storing it to make it "pseudonymous" if it was breached (Lee & Webber, 2016), and would have to tell users in a timely manner if the data was breached (Channel 4, 2018). European users would also gain new rights to access their own personal data from companies recording it and allow for data deletion if they wanted their records forgotten (Channel 4, 2018). Penalties for companies who broke these regulations were massive at 4% of a companies annual turnover or 10 million euros (whichever is more) (Channel 4, 2018). Although these regulations were only passed in the European Union, their effect was felt globally as it applied to any company that offered goods or services to Europeans, worked in the EU, or monitored the behavior of EU

residents (Lee & Webber, 2016) This meant companies without a presence in the EU would need to comply and a lot of technology-based companies had to drastically adapt how they offered services.

The implementation of GDPR is impacted companies that rely on or work within artificial intelligence and personal data. Article 22 of the regulation creates restrictions on automated individual decision-making or profiling and requiring human review of AI-powered decisions (Alford, 2021). This law could impact AI companies and limit some automated activities such as personalized shopping, personalized media content, or automated customer loans. Manual review of all AI decisions would defeat the purpose of setting up an intelligent system in the first place and slow down processes that use to be fast for both the company and the user. This personalized data was also used by companies like Facebook and Google to generate precisely targeted ads that would generate a good chunk of their revenue. Now with the GDPR allowing users the right to control their data, these targeted ads could potentially be opted out and easily lose the precision that garnered them a lot of attention from retail companies. On the other hand, others argue that these new regulations and control over AI and personalized data within the GDPR could also help foster trust between users and automated systems that has grown weary over scandals like Facebook's "Cambridge Analytica" issue (Channel 4, 2018). Regardless, any company that utilizes personalized data from users has had to drastically adapt how they use and store data to fit this new regulation.

One such company is Fitbit, a business that creates wireless wearable fitness tech to allow users to easily track and view their biometric data. In order for its business to work, Fitbit has to use the personal data of every user and collect identifiers, demographic information, biometric information, geolocation data, and more (Mareaotoole, 2021). Without personalized data, Fitbit cannot work as a company or service. When GDPR became law in 2018, Fitbit had to alter the way it utilized its data as it did business and had an office within 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). The EEA's 30 countries now fell under the GDPR and so Fitbit had to adapt for any user from Norway to Italy. As the data that Fitbit collects contains a wide variety of identifiers of its users it must allow users free access (General Data Protection Regulation Article 12 & Article 15, 2018) and control of this data (General Data Protection

Regulation Article 18, 2018). Since this data is identifiable, the data needs to be protected by measures like pseudonymization (General Data Protection Regulation Article 25, 2018) and tell users of any potential breaches in a timely manner (General Data Protection Regulation Article 33, 2018).

In order to continue running, Fitbit will have had to adapt to the GDPR restrictions. First, Fitbit will have to hash its identification data to protect the users in the EEA area from the possibility of data leaks. Also, before collecting any fitness data, the app will have to gain explicit consent to collect data and explicit consent if it wants to share that data with business customers (these consents should also be able to be revoked at any time). This consent could be collected by a clear form at the beginning of the app that clarifies what data is collected. To prevent losing users that are more privacy focus, FitBit could also allow users to choose what data is recorded at this form as well. Certain users could opt-out on location data use but allow for heart rate data to be collected. Fitbit could also allow customers to use the app with an "anonymous" account so they don't have to include any extremely personable information if needed.

Fitbit has explicitly stated how it has gone through a number of steps to adjust its business with the new regulations of the GDPR (Fitbit Health Solutions, 2021), so its fitness devices should still be accessible to residents of the EEA without waiving their rights. First, it has included a section within its privacy policy on "How to exercise your legal rights"(Mareaotoole, 2021) to instruct users on how to access and control their data. It also has an email for allowing users to reach out if they have confusion or questions on data protection (protection-office@fitbit.com)(Mareaotoole, 2021). Fitbit was also acquired by Google and so the European Commission forced a few adjustments by ensuring that the fitness data is stored separately from any other data used for Google ads and marketing (Schechner, 2020). I think these changes show the changes Fitbit has gone through in order to provide adjustments to GDPR regulation with EEA users. But, at the end of the day, users will have still have to provide data to use Fitbit ad the company is centered around collecting and depicting fitness data.

Another such company that has personalization deeply embedded into its business is TikTok. TikTok is a social media app popularized by Generation Z that provides users with a series of short-form video content created by its users. While TikTok has a simple premise, its success lies within its use of tracking users' personalized data to generate a feed of videos most likely to keep the user

watching. A Wall Street Journal report demonstrated that the automated system tracked more than just likes, comments, and hashtags to determine the video queue (WSJ Staff, 2021). The algorithm also kept track of how long users watched a video so it could keep a user towards videos that would keep them on the platform (Smith, 2021). Without this automated system built on personalized data, TikTok could still function as a video platform but it would not have the addictiveness that has made it so successful. As TikTok is available to EEA residents, it too falls under the jurisdiction of the GDPR and has to follow its regulations. In order to track and maintain users' information on how long they watch videos, TikTok has to gain unambiguous consent from users to track this data (General Data Protection Regulation Article 6, 2018). Users also should be able to opt-out of the data-driven algorithm and it provides a feed with automated individual decision-making (General Data Protection Regulation Article 22). Also, a lot of TikTok's users are under the age of 18 which puts its data at specific restriction under the GDPR (General Data Protection Regulation Article 8, 2018).

TikTok has recently got into hot water with privacy and data issue by the Irish Data Protection Commission (DPC) for possible violations of this article. The DPC was "looking into its processing of children's personal data and whether TikTok is in line with EU laws about transferring personal data to… China"(BBC, 2021). In order to comply, TikTok has made some alterations to its system to adapt to teh GDPR. "In January [2021], it made all under-16's accounts private by default"(BBC, 2021), and "in July [2021] [deleted] millions of accounts which it said belonged to under-13s" (BBC, 2021). I believe TikTok can expand on these adaptations to fit more cleanly within the GDPR by creating a separate non-automated, incognito video feed for EEA users who value their privacy. They also could be more transparent on how the automated system works so users can understand how their data is used and comply. With these adaptations and transparency, I think EEA residents could use TikTok without waiving their privacy rights.

3 REFERENCES

1. Alford, James, et al. "GDPR and Artificial Intelligence." *The Regulatory Review*, 6 Aug. 2021, https://www.theregreview.org/2020/05/09/saturday-seminar-gdpr-artificial-intelligence/.

2. "European Economic Area." *Wikipedia*, Wikimedia Foundation, 3 Feb. 2022, https://en.wikipedia.org/wiki/European_Economic_Area.
3. "GDPR Explained: How the New Data Protection Act Could Change Your Life." *YouTube*, Channel 4, 23 May 2018, https://www.youtube.com/watch?v=acijNEErf-c. Accessed 5 Feb. 2021.
4. "GDPR." *Fitbit Health Solutions*, Fitbit, 23 Apr. 2021, https://healthsolutions.fitbit.com/gdpr/.
5. General Data Protection Regulation (2018)
6. Lee, Phil, and Mark Webber. "GDPR 1.0 - The Top 10 Things You Need to Know." International Association of Privacy. International Association of Privacy, 31 Jan. 2016, Milpitas, California.
7. https://www.youtube.com/watch?v=NxgZ57BTkFQ
8. Mareaotoole. "You Ask: I Answer: The GDPR & Fitbit." *Rock-Privacy.com*, Rock Privacy Solutions, 23 Jan. 2021, https://www.rock-privacy.com/post/you-ask-i-answer.
9. Schechner, Sam. "Google Must Silo Fitbit Data, EU Says, Clearing $2.1 Billion Deal." *The Wall Street Journal*, 17 Dec. 2020, https://www.wsj.com/articles/google-must-silo-fitbit-data-eu-says-clearing-2-1-billion-deal-11608219201?page=1.
10. Smith, Ben. "How Tiktok Reads Your Mind." *The New York Times*, 6 Dec. 2021, https://www.nytimes.com/2021/12/05/business/media/tiktok-algorithm.html.
11. Staff, WSJ. "Inside TikTok's Algorithm: A WSJ Video Investigation." *The Wall Street Journal*, 21 July 2021, https://www.wsj.com/articles/tiktok-algorithm-video-investigation-11626877477.
12. "Tiktok Faces Privacy Investigations by EU Watchdog." *BBC News*, BBC, 15 Sept. 2021, https://www.bbc.com/news/technology-58573049#:~:text=TikTok%20is%20under%20investigation%20by,over%20two%20privacy%2Drelated%20issues.&text=TikTok%20said%20privacy%20was%20%22our,looking%20into%20GDPR%2Drelated%20issues.