Data Privacy and Data Regulations as a Function of Hegemonic Power

As data regulations continue to evolve, in the U.S. political concerns over data privacy, specifically, how state actors that the U.S. considers hostile handles citizens data is increasing. Proposals by politicians to force ByteDance, the parent company of TikTok, to localize data for U.S citizens to only be contained in the U.S. is an example of state actors using data regulations as to shift the balance of power or maintain the balance of power in the international system. The new policies in the EU and California show a shift in state actors priorities. Using IR theories it is possible to analyze these regulations to think about how data is used in international relations and what objectives state actors have when forming regulations.

At the start of the project the question that I was attempting to answer was "How is big data used in international relations?" The scope of this question was too large to research in the time frame that was given. I was guided by my professor to look into the General Data Privacy Regulations (GDPR) in the EU and the California Consumer Privacy Act (CCPA). After looking into the history of how data regulations were initially proposed and what recommendations were given by International Governing Organizations such as the UN it was clear that concerns about data regulations were salient at the formation of the internet.

Academic sources that I found included discussions about the implications of the GDPR and CCPA. Multi-national actors that are forced to comply with different regulations are faced with growing fines in areas that regulations are more strict such as the EU. The GDPR stemmed from leaks of classified information from whistleblower Edward Snowden. This made it clear that the United States priority was national security and it was willing to mislead its allies and other state actors to believe it was following privacy regulations. Edward Snowden's book, and intelligence committee reports about Edward Snowden's leaks were useful in leading to additional sources about the subject. A conversation with a cashier at a retail shop who happened to be a former army intelligence officer led to a recommendation to look into SP00-18, the policy that was implemented after the Snowden leaks to outline how the data of US persons will be protected.

Eventually my focus shifted from looking for sources in library databases to using government websites such as the Office of the Director of National Intelligence as well as news stories related to recent developments in data regulations. Evaluating news sources and ODNI information proved to be difficult. It was not always clear to what extent US governments sources were being transparent, and to what extent international state actors were being transparent. An example of this is that while the U.S. was found to be violating the privacy of citizens in its collection of data, intelligence partnerships such as Five Eyes and Nine Eyes would possibly have given officials in the EU knowledge of what kind of intelligence was being collected by the U.S. It was necessary to consider perspectives from all state actors and international governing organizations as possibly having a bias.

Ultimately what is clear is that research into these topics continues. Sources that contribute to these discussions are from reputable publications such as the Stanford Journal of Law, but include contributions from individuals that have connections to multi-national corporations such as Amazon. Finding sources that can speak to these issues remains difficult. Evaluating what data is collected, and to what extent state actors follow data regulations is subject to the extent that actors are transparent about what data they collect. Until violations to data regulations are revealed by whistleblowers, there is no evidence that state actors have any incentive to reveal when their intelligence operations violate data regulations.