The General Data Protection Regulation (GDPR) is a regulation of the European Union (EU) that took effect on May 25, 2018. After four years of debating and preparation, the European Parliament approved the GDPR in April 2016 and it was published in all the official languages of the EU in May 2016. The purpose of the regulation is to strengthen and build onto the European Union current data protection framework. The GDPR replaced the 1995 Data Protection Directive. The GDPR is considered the core of Europe’s digital privacy legislation and ensures that many people will have more control over their personal data. Organizations that collect and handle data are obligated to make sure that it is protected from being misused or exploited. This will mean that almost every major corporation should consider adopting a privacy law regulation similar to GDPR in order for people to gain trust into organizations handling their personal data. In this Case Analysis I will argue that the ethics of care shows us that the United States should follow Europe’s lead because it will help innovate the country’s rights to privacy, help the country expand globally in data protection, and encourage the development of a strong data protection agency.

When trying to adopt privacy laws similar to Europe’s, the United States should consider identifying personal information first. When identifying personal information, the United States will know what type of data they will need to protect. The United States could do research by identifying what data is being used on company and organization websites, shopping websites, or social media platforms. For instance, in Michael Zimmer's “*But the data is already public”: On the ethics of research in Facebook*”, Zimmer explained about a research project called Tastes, Ties, and Time (T3). The Tastes, Ties, and Times project began as a dataset when a group of researchers publicly released data from Facebook accounts of college students. Even though the collecting and releasing the data may cause privacy concerns, the T3 researchers took multiple steps to protect identities of the profiles being used. The Tastes, Ties, and Times project went from 2006 to 2009. As a result, the Tastes, Ties, Times project was perceived as a failure because the researchers did not adhere to the ethical standards due to the college students not giving consent. The United States can use the Tastes, Ties, and Times research project as a blueprint to try to make sure that the privacy of individuals will be protected from deductive disclosure.

For the United States to have a privacy law similar to the GDPR, the country must come up with ways to innovate the rights to privacy. Innovation is an effective way to have more structured privacy laws and protection from data breaches. The United States can use these new innovations as solutions to many privacy issues in the past such as the Tastes, Ties, and Time research project. The United States can use the Tastes, Ties, and Time research project as a lesson to make sure that companies and organizations are given consent by the citizens to protect or release certain data. If the United States considers these innovations and looks to the GDPR as an inspiration, then the country will have privacy laws that will be regional, but also global. By adopting the same privacy laws as Europe, the United States can use the new privacy regulations as an opportunity to be in the lead of data privacy and become a model to inspire other countries similar to theirs which will cause economic growth and increase in data privacy. These are reasons why considering these new innovations will likely improve and recover the United States from the Tastes, Ties, and Time research project failure which can lead to the country to expand their privacy laws globally.

When adopting similar privacy laws to Europe, the United States has many major issues with protecting data such as handling it. The GDPR has two different types of data handlers that it applies to which are controllers and processors. Controllers are a person, public authority, or agency that determines the purposes and what it means to process data. Processors will process the personal data on the behalf of the controller. The ethics of care is relatable to this concept because in order to control or process personal data. By using the ethics of care, the United States can have privacy laws that carefully process and control the personal data of the people and gain some sort of trust.

The biggest issue that the United States has when it comes to data protection and privacy is not having a federal privacy agency. To begin a federal privacy agency, the United States will have to identify or detect threats that may put networks and organizations in jeopardy. For instance, in Elizabeth Buchanan’s “*Considering the ethics of big data research: A case of Twitter and ISIS/ISIL*”, the article explains about an Iterative Vertex Clustering and Classification (IVCC) model which was used to identify ISIS/ISIL supporters among Twitter users. The main purpose of the Iterative Vertex Clustering and Classification model was to approach OEC detection within networks from an analysis standpoint and provided a case study of an online community which consisted of more than 22,000 Twitter users that supported ISIS. The IVCC was used to get an insight on how the online community was created on Twitter and how they interacted with each other. As researchers went more in depth in their research, they learned that the IVCC model offered a promise to make detecting online extremism on social media a practical reality. As a result, researchers hope that one day they will be able to have a model like IVCC to counteract the influence of groups like ISIS. By looking at the IVCC model as an inspiration, the United States can make a structured federal privacy agency to counteract the influence of online extremism on social media platforms to keep data protected from outside sources reach.

Another element that the United States should take in consideration when establishing a federal privacy agency that adheres to the adopted privacy laws similar to Europe’s would be planning out who the regulations will comply to. Everything should always be planned out before putting things in place. For the United States to adopt a privacy law similar to Europe’s, they will have to come up with a plan like theirs which means they should take the GDPR five step plan as an inspiration. First, they should appoint a leader within marketing that is familiar with GDPR and review the data- handling procedures which will include documenting data collecting, reviewing mailing lists, and communicating with the marketing team about GDPR. Second, they should take action when collecting personal data by providing clear consent wording, making a cookie consent notice, and creating an age verification. Third, they will have to manage any existing contacts and leads within a database by sending reverification emails or creating a preference center for people to have control over their subscriptions for services they pay for. Fourth, they will have to update their privacy policy on the regular and notify the public about it. Fifth, they should come up with a data breach plan to detect breaches in a quick manner and notify the public to make sure they are working on fixing it. This is the five step GDPR plan the United States can follow when establishing their privacy laws and creating a structured federal privacy agency. By planning out the privacy law, the United States can repair where the IVCC model lacked when detecting online extremism on websites.

The ethics of care can be relatable for the United States establishing a structured federal privacy agency because they will have to carefully plan out on how to adhere to the new privacy laws and make them successful. The ethics of care is an ethical tool that the United States should use to give the people what they deserve when it comes to data privacy and protection. There are a lot of privacy concerns that Congress will still have to consider to make data protection strong in the United States. The main purpose for them to use the ethics of care is to care for online safety, people, and the country. By using the ethics of care, the United States will give the citizens a federal data agency that cares about the people and their safety online.

There are many aspects to turn to when adopting privacy laws for the United States to successfully protect the people’s personal data. The GDPR is a great inspiration to consider in order to have effective privacy laws and secured protection. There are many issues that have not been solved, so the United States should revisit those problems and use them as a blueprint for creating privacy laws. The IVCC model and the Tastes, Ties, and Times (T3) project were not too successful because they did not have proper planning which caused them to fail from minor mistakes. The ethics of care would have been an effective ethical tool for both of these research projects because they would learn how to carefully put in place their research and trace their mistakes as they go. Overall, I believe that the United States should adopt similar privacy laws to Europe’s because using the code of ethics with having the knowledge of the GDPR, as a country they can innovate the rights to privacy, expand globally to inspire other countries’ privacy laws, and develop a structured federal privacy agency.