The General Data Protection Regulation (GDPR) is an EU directive that is innovative in the field of consumer data protection and privacy. It requires those who process and handle personal data to ensure a number of standards are followed in order to be in compliance. Requirements include reporting when a data breach occurs, building privacy by design, and ensuring consumers have greater control of their data than previously required in key, specific ways. This directive is a landscape change in the world of data protection and internet privacy, as any business that wants to operate within the EU in any capacity will also be subject to the directive in numerous ways. In this case analysis, I will argue that Ubuntu shows us that the United States should follow Europe's lead on this landmark directive because of its impact on the communities we all belong to and the negative impact a lack of direction can have.

In 2008, a group of researchers conducted a study that resulted in a dataset being collected and then published. Steps were taken by the researchers to protect the identities of the participants and anonymize or encode the dataset. Nevertheless, the steps taken seemed to be insufficient, and re-identification was possible. The incident brought to the forefront numerous ethical concerns and concepts in need of further analysis and discussion. One such concept is the public nature of certain pieces of data and the ethics surrounding their acquisition and use. Upon the data being used to re-identify participants, the researchers defended themselves from scrutiny by claiming that the data they used was already made public and should be viewed similarly to if a person-watcher in a public place gathered data on passersby. The researchers acquired intensely personal pieces of information (like email address, gender identity, political views, and college major, among others) that would likely not be easy to collect simply by watching people in a public square. Ubuntu, combined with Zimmer's analysis of the incident, can help us understand the folly of this line of thinking in an ethical way. Zimmer points out that the way researchers collect data is completely different from that of a person watcher. The ethical teaching of Ubuntu further helps us realize that the differences are such that they fundamentally change the act into a less personable, imprecise, and ultimately less ethical practice. Zimmer points out later on that just because data is available somewhere on a social media platform in some capacity does not mean it is simply fair game for all or any usage. Likely, each researcher would not prefer their data or the data of those they consider to be a part of their close community (friends, family, etc.) to be captured and used similarly. At the very least, notions of consent and communication channels would be emphasized in different ways. However, it does seem that the researchers failed in this aspect. The subjects were treated almost as if they were a part of a separate community, with their individuality severed, and thus little empathy was shown. This issue compounds as the nature of data, especially personal data, is more connected to the wider community than we often realize, as will be outlined later. Zimmer recommends, among the other lessons learned from the study, that both policymakers and researchers must be aware of the nature of conducting research on the internet and with social media and the complexities these challenges bring. Currently, without a similar framework to the GDPR in place, policy is lagging behind on this end. Tools like social media interact with research methods and companies to bypass consent, deanonymize people, and violate dignity through breaches of privacy. Ubuntu shows us how such results are deeply troubling and unethical. Without direction from policy, the community erodes, and as the community erodes, the individuality we gain from that participation in the community erodes as well. Individuals are made to be nothing more than a dataset, a dollar sign, or a plot on a graph. Without societal community-wide policy (and thus protection), how can any individual be protected? Further insight into this line of thinking is provided by Buchanan's insights.

Buchanan's work involves a tool that was developed that seemingly allows reliable results in identifying members of the Islamic State, only using an individual's social media presence. Per the article, the results, reliant on large scale data analysis through publicly available social media data, are both valid and reliable. Buchanan however, does acknowledge that there are a vast number of ethical concerns that have been brought forth relating to this tool. Firstly, it's pointed out that few would disagree with the tool's current usage of being employed against a universally reviled entity like the Islamic State. However, one could easily imagine the tool's methods could likely be turned to focus on a group only reviled by a select group of the population, such as Black Lives Matter or another activist group. Such a thing could have severe ethical implications and worries. Not only is the utility of the tool concerning, but Buchanan shines light on the ethical concerns of the very exercise of big data analysis itself. Once again, consent is sidelined, as its pointed out that researchers themselves consider it impractical to be able to get the consent of the 100,000+ participants in the dataset for the tool. Concerns are also raised about the idea of using data mining to make further inferences and judgments about a subject beyond what could be intuitively seen without deep analysis. These tools, after all, are determining which users who support the Islamic State merely through their social media presence, without any explicit calls to support. Buchanan shines light on how this is possible through his observations on datasets and individuals in the modern age. Buchanan clearly outlines this as he quotes benigni et al's insight that currently data analysis has become focused on analyzing networks to get information about certain individuals instead of the other way around. He follows this up by addressing a common concern he's had that big data research involves displacing researchers and subjects from each other in return, from a deeper contextualized meaning, with the subjects becoming ever more distant from those studying them. This anaylsis echoes the analysis above on Zimmer's work. These concerns and insights brought up by Buchanan, all seem to point to a deep connection between our modern plights and the ethics of Ubuntu. In fact, at points Buchanan seems to unintentionally suggest that big data analysis has all but proved Ubuntu's applicable ethics to our ethical concerns surrounding the topic. The big data analysis being conducted is using the networks, the communities as a whole, to gain insight into an individual. Taken along each data point is meaningless in defining any connection or broader analytical point. When taken together, within its communal and societal context, the data points gain meaning, just as an individual gains meaning through their place and participation in a community. While Ubuntu seems to be extremely applicable, and hold immense predictive power in explaining the relations, communities, and reasons for the ethical concerns brought up surrounding these studies and analyses, it also seems the lessons of Ubuntu on how to be ethical are not being consulted. This brings us to the shortcomings of U.S. policy surrounding privacy and personal data. As stated before, the community and our participation in it, is what gives us identity and defines us as a group. It seems however, that researchers utilizing big data, social media companies, and numerous other groups are distancing themselves from other individuals within their community. Subjects and customers, despite deriving identity from the community, are being treated as less than individuals, instead as data points or dollar signs. If we are to correct these wrongs, we should come together as a wider, full community and decide on how best to ensure empathy, consent, and solidarity are ensured and protected. To me, this sounds exactly like what a government is meant to be. The unit from which a society makes decisions on how to direct and govern itself. As Buchanan details, there has been little activity to update our privacy and internet laws to reflect the modern day. This is a severe mistake.

In conclusion, modern-day internet research and big data analysis pose a number of severe ethical concerns in our society. The GDPR is one such step in the right direction, as it provides some updates to privacy and data laws that bring us closer to reality than in the past. Zimmer and Buchanan help us clarify what this reality entails and entrench in us the fact that numerous insights from Ubuntu seem to apply precisely to that reality. However, while the effects of this reality on our communities and individuality are made clear, the ethical teachings on how to live and develop ethically are seemingly all but ignored by lawmakers, as the U.S. seems to push forward with little to no development occurring in bringing the laws of the past to meet the world of today. The implications of this rift are dire, as we are either looking to sluggishly keep up with other directives or deny reality and face the real-world ethical consequences of our defiance.