

## 2.4 Case Analysis on User Data

Mackenzie Coleman

Cybersecurity Ethics

October 2, 2022

When a company or an organization makes the decision to collect user data, they need to be held accountable for what happens to that data whilst in their possession. User data is not only, usernames or emails, but it is also social security numbers, private addresses, banking information, and so much more that is vital to an individual's life. In the article, Palmer talks about GDPR, General Data Protection Regulation, which is a regulation of the European Union, EU, that is designed to ensure that European citizens are given more control over what happens with their personal data on websites. GDPR is a huge step for the EU and the citizens. This regulation also is a great example of how the EU emphasized the citizens' rights, their human rights, to control over their information. However, while giving the EU citizens more control over their personal data, this new privacy law still gives organizations and businesses the right to collect data, but now for it to be legal they must have consent from users. In this case analysis, I will argue that ubuntu ethics shows us that the United States, U.S, should follow Europe's lead because there are millions of people's sensitive information at risk of being stolen or misused due to insufficient data protection and there needs to be steps taken to protect the privacy rights of U.S citizens.

In the article, "But the data is already public": On the ethics of research in Facebook", by Michael Zimmer, he writes about the Taste, Ties and Time (T3) Project. This was a project done in 2008, when a group of researchers collected Facebook profile data including detailed personal information, from a U.S. University's Freshman class. While trying, and ultimately failing, to hide the identities of the Facebook users, the T3 researchers released this study to the public. Zimmer mentions a few user data protection issues following this research project and Facebook but one concept that stood out to me was when he mentioned the harm-based theory and the dignity-based theory. Dignity-based theory is a moral theory that focuses on a duty-based sense

of morality. Zimmer used this theory to describe how some saw this breach of privacy. This theory suggests that when these user-data profiles were released to the public, this invasion of privacy could have been seen as harming someone's sense of dignity and gave them lack control over their personal information. This dignity-based theory can also be tied in with ubuntu ethics because of the concentration on the empathy that we as people should feel towards respecting other people's privacy.

Ubuntu ethics, in summary, is the feeling of moral goodness in becoming realizing your humanity. That empathetical feeling of care and compassion towards another is an example of ubuntu ethics. Zimmer explains what the researcher's data collected included and it not only included self-reported information like gender and ethnicity but also included information such as their home state, sexual preference, political views, and more highly personal information. The collection and release of this data, without the subject's consent or awareness, raised many questions to Facebook's morals on protecting their user's data. When the EU put their new privacy laws in place, that gave their people more control of their user data and personal information, this showed that the EU noticed a concern for people in the community with their human rights and tried to give their people back control. The new EU privacy law also states that if a company or organization who collects user data misuses or compromises the information, they will be held accountable and fined.

In the past, when Facebook has been called out for lack of user data protection, the usual response is that they are not liable for what happens to a user's data, primarily due to the terms and conditions page the user agrees to at the beginning of creating the account. The U.S. should follow the EU with their ethical view to try to put in perspective, what is best for the community and what improvements need to be made to our laws to ensure the protection of our citizens. This

includes, holding companies and organizations, who chose to collect user data, accountable for the misuse of user data and violations of user privacy. Zimmer also talks about, if the U.S were to follow Europe's lead, this would give the U.S citizens more power over what happens to their personal information and will show that privacy rights as well as basic human rights are valued as a part of this community. Sense of community is also valued in ubuntu ethics saying that community and sense of being a part of something is important in finding who you are as an individual and in your humanity. This is another reason that our right to privacy should be extended to the collection of user data and the presence of oneself online.

One of the main problems addressed by researchers of user data privacy is that this private information is so easily accessible via the internet, as well as this information is being provided voluntarily by the user. Privacy has become more and more challenging to protect. Elizabeth Buchanan addresses this issue of user data privacy in: "Considering the ethics of big data research: A case of Twitter and ISIS/ISIL" where she discusses an innovation that presented the idea of an Iterative Vertex Clustering and Classification (IVCC) model to identify ISIS/ISIL supporters on the social media platform, Twitter. The intent behind this IVCC model would be able to detect specific individuals and groups, in large data sets, being able to identify ISIS/ISIL supporters through user following, mention, and hashtag ties within their profile (Buchanan, E (2017)).

In this article, Buchanan says that with data mining "...across social media and the Internet has presented ethical dilemmas surrounding privacy, rights and autonomy, and such social justice issues as discrimination." (Buchanan, E (2017)). Big data research has often led to the collection of mass user data information for a specific research purpose. If the U.S were to put a more effective privacy law in place that prevented the collection of this data without the

consent of the users, like the EU, this will help user data protection and privacy. Normally, In a research study conducted with human subjects, there is a moral and ethical process that must be followed. Buchanan raised the question, are we seen as data subjects or as human subjects when it comes down to the information gathered in this research? Ubuntu ethics can be tied into what Buchanan says here when she asks where the line is drawn between data subjects and human subjects by ensuring that we are treating each other and our private information with respect. Respecting our basic human right to privacy needs to be recognized when considering this big data research and what information these researchers are making available to the public.

Ubuntu ethics can be tied together with a familiar standard that is taught to us at a young age; Do to others as you would have them do to you or, in other words, “treat others how you want to be treated”. If big data researchers saw their information being used, without consent, I bet they have a different perspective of how invasive this research has the potential to be. Buchanan can also be tied back to when Zimmer mentions the dignity-based theory of morality, that this invasion of privacy can be seen as stripping someone of their dignity due of the content of the information that is readily available on the Internet. Buchanan strongly focuses on why ethics need to be the number one rule of research when humans are involved, digitally and physically. This ethical guidance for the research should be in place by U.S government through updated laws for putting the control of user data back in the hands of the original user.

When the European Union placed the new data protection regulation, GDPR, they gave their citizens more control over their personal data, something that should have been in their control from the start. Consent for the use of a user’s data is required before a company or organization can use their information. This was a huge step in regulating data mining and misuse of user data collection. In the United States there is currently no privacy law or statute that

governs the use of database information. While there are privacy laws that pertain to technology and personal information, none specifically stop or prevent the misuse of user data. Ubuntu ethics shows us that a sense of community is important in finding oneself and that we should treat others with respect. This ethical viewpoint can be added to technology as well. We, as people, a community, should respect the privacy of user data information as we expect to be respected in our daily lives as people.

## References:

- Buchanan, E. (2017). Considering the ethics of Big Data Research: A case of twitter and Isis/ISIL. *PLOS ONE*, 12(12). <https://doi.org/10.1371/journal.pone.0187155>
- Zimmer, M. (2020). “but the data is already public”: On the Ethics of Research in Facebook. *The Ethics of Information Technologies*, 229–241. <https://doi.org/10.4324/9781003075011-17>