

Dominic R. Clark

Professor Nicol

PHIL355E


10/6/2023

A Deontological Analysis of User Data Privacy

The issue of protecting user data privacy in the digital age is critically important, as emphasized in Palmer's case study. Palmer highlights the vital need to safeguard user data, pointing out that people voluntarily provide personal information to online platforms under specific terms and conditions. According to Palmer, these platforms have a significant duty to ensure user data is utilized in an ethical, responsible manner. The situation draws attention to the unethical misconduct involved in the uncontrolled usage of data mining and exploitation without explicit, informed consent. Furthermore, given that user data includes private details, financial information, browsing patterns, and more, it underscores the potential for serious harm. The recent Cambridge Analytica scandal, where Facebook user data was improperly leveraged for political influence, provides a stark real-world example of the consequences of unrestrained data mining (Cooper and Coetzee 159-171). In this analysis, we will argue that the deontological ethical framework provides insightful principles demonstrating why the U.S. should adopt strict data protection regulations aligned with Europe. The fundamental importance of safeguarding individual rights and upholding ethical standards in data protection aligns with deontological ethics, which stresses adherence to moral duties and principles regardless of outcomes.

The concept of "informational privacy" is critical to Zimmer's work. At the core of

informational privacy is the protection of a person's personal information and their right to control the collection, use, and disclosure of that data (Allen, 2013). It essentially stresses that individuals should have agency over their own information and be able to choose how it is utilized. When considering Palmer's argument, this notion becomes extremely relevant. The loss of informational privacy appears as a major concern in the case Palmer highlights. Users willingly provide online platforms access to personal data with the expectation it will be used in accordance with mutually agreed upon terms and conditions. However, the case does show instances of user data being gathered and leveraged without explicit, informed consent. This blatant disregard for informational privacy violates users' trust in these platforms and infringes upon their fundamental right to control their own personal data.

When analyzing this issue through the lens of deontological ethics, it becomes evident the actions taken, which led to the breach of informational privacy, are morally questionable. Deontological ethics stresses the duty to uphold ethical responsibilities and principles regardless of consequences. It emphasizes the obligation to protect individuals' rights in this context, specifically their right to informational privacy. 

To comply with deontological ethics and remedy the situation, relevant parties including online platforms and data collectors should have made user consent and transparency top priorities. Standard practice should have included clear, informed consent procedures to fully inform users about how their data would be used and give them the choice to opt-in or opt-out. Additionally, ethically sound data minimization practices could have been used to limit data collection only to that which is necessary for clearly stated purposes, reducing the potential for overreach and misuse.

Furthermore, Zimmer's concept of informational privacy, when combined with the ethical

framework of deontological ethics, underscores the importance of maintaining moral standards and protecting individual rights in the realm of data protection. The failure to respect these standards in the scenario Palmer outlined resulted in a betrayal of trust and privacy violations. Strict data protection regulations, including rigorous consent processes and data minimization, should be instituted to address these moral dilemmas and ensure user data is handled with the highest care, respect, and ethical consideration. This approach is critical in developing a digitally just environment for all users and closely aligns with deontological ethics.

The notion of "property rights" is central to Buchanan's writing. Property rights refer to the legal right to own, use, and dispose of property—tangible or intangible—as one pleases, as long as doing so does not violate the rights of others (Cooper and Coetzee 159-171). Property rights are critical when examining Palmer's case because they are vital in establishing ownership. Property rights become salient in the context of user data and digital platforms when analyzing who owns and controls the data produced by users. Users frequently share private details with online platforms, generating valuable data in the process. Whether this data should be considered the users' property or viewed as belonging to platform operators or other entities is currently up for debate.

When Palmer's case is examined through the lens of property rights, the actions involving indiscriminate mining and use of user data without explicit, informed consent are clearly in violation of users' property rights. These activities infringe upon users' rights to manage and exert ownership over their personal data. Deontologically speaking, such violation of property rights is unethical because it contradicts core notions of individual liberty and autonomy.

To remedy this situation and align with the tenets of property rights and deontological ethics, the appropriate course would have been for online platforms and data collectors to respect

and uphold users' property rights. This necessitates instituting robust consent procedures that give users control over how their data is gathered and used. It also entails properly respecting users' property rights to their data and providing transparent information about data handling practices.

Together with the moral framework of deontological ethics, Buchanan's concept of property rights underscores the critical importance of respecting both individual and property rights when it comes to protecting user data. In the case Palmer cited, the failure to recognize and defend these property rights resulted in a betrayal of trust and infringements of personal freedom. Strict data protection laws, including robust consent processes and transparent data handling procedures, should be implemented to address these ethical concerns. This will help ensure user data is handled with the utmost care, respect, and ethical consideration.

In conclusion, Palmer's case serves as an excellent illustration of how the ethical analysis of data protection in the digital age spotlights the vital need to uphold people's rights and autonomy. The deontological ethical framework and concepts from authors like Zimmer and Buchanan provide insight into the moral duties that should govern the use of user data. By committing to ethical data practices, policymakers, companies, and individuals can work to support a digital ecosystem where individual rights are honored, privacy is safeguarded, and fairness prevails.

Works Cited

Allen, Anita. *An Ethical Duty to Protect One's Own Information Privacy? An Ethical Duty to Protect One's Own Information Privacy?* 2013.

Cooper, Antony K., and Serena Coetzee. "On the Ethics of Using Publicly Available Data." *Lecture Notes in Computer Science*, vol. 12067, 2020, pp. 159–171, https://doi.org/10.1007/978-3-030-45002-1_14.

Fletcher, Charlie. "Why the Ethical Use of Data and User Privacy Concerns Matter." *VentureBeat*, 26 Feb. 2022, venturebeat.com/datadecisionmakers/why-the-ethical-use-of-data-and-user-privacy-concerns-matter/.