

Tatum Grambow, Aditya Sharma, Trevor Buchanan, Xilin Chen, Sheryas Reddy, Kevin Yuan  
Group Project, Group 3

04/29/2025

LIS 461

### Case Assignment: Case 1 Variation A

Word Count: 1073

Our objective is to form a profitable company to track and evaluate the driving patterns of taxi drivers using state-of-the-art vehicle tracking technology, and generate safety ratings which are purely based on driving patterns. By taking in various factors such as speed, breaking habits, etc., we would aim to provide an unbiased assessment of a driver's skill and safety level on the road. This rating would be sold to rideshare companies, like Uber and Lyft, to help them better match drivers to customers. Our goal is to create a system that benefits drivers, driving companies, and society by encouraging safer driving habits while maintaining transparency, fairness, and respect for privacy.

One of the most pressing ethical concerns in the deployment of our vehicle monitoring device by a private company is the issue of informed consent. According to Kleinig's *The Nature of Consent*, for consent to be ethically valid, the policy must be informed, voluntary, and given by an individual that is able to consent (Kleinig, 2010). In practice, while many users may claim to agree with the data policy, they could agree due to coercion or a lack of understanding of the terms and conditions that they are agreeing to. This is important because consent is a reflection of respect for individual autonomy. Consent must involve disclosing important information and the individual being able to understand the data policy without coercion. A company that prioritizes profitability might downplay or bury such disclosures in legal jargon. This could

undermine the moral legitimacy of any data collection practices and could damage the company's reputation in the long term.

This in-vehicle monitoring device raises potential privacy risks. Although the system collects driving behavior to generate safety scores, detailed data such as location, time, and steering patterns can reveal sensitive personal information. As Lundberg et al. (Lundberg et al., 2019) show in the *Fragile Families Challenge* case study, even de-identified data can be reidentified through linkage with external datasets, exposing individuals to surveillance, discrimination, or reputational harm (Lundberg et al., 2019). Helen Nissenbaum's theory of Contextual Integrity (Nissenbaum, 2004) highlights that privacy depends on maintaining appropriate information flows. Drivers reasonably expect that driving data will be used only for internal safety assessments, not shared with advertisers, insurance firms, or others without consent. Unauthorized flows would violate these expectations and harm driver trust. Thus, protecting data privacy is essential not only to respect drivers' autonomy but also to uphold the company's reputation and support the ethical, sustainable use of monitoring technology.

A third ethical issue we must address is the possibility of undermining user autonomy by presuming consent through an opt-out privacy policy. An opt-out privacy policy is one where users of the tracking device are automatically enrolled into opting in to any and all tracking features, often with minimal disclosure and intentionally difficult paths to opt-out. While this strategy can help the business profit, this strategy is not ethical according to James William's *The Ethical Dimensions of Persuasive Technologies*. William states that ethical technologies must respect the freedom of users to make informed decisions. Presuming consent and making the large barriers to withdraw consent disregard this and fail to meet the ethical standards for voluntary agreement (Williams, 2021). Therefore, we must strive to make this tracking device

feature opt-in policies that enhance user autonomy and actually attempt to garner users' consent instead of presuming it.

Our last ethical issue we want to address is balancing collecting data for profit and respect for individual rights. We can monetize data collection through a multitude of ways; selling performance analytics, enhancing driver incentives to purchase our tracker, and more. However, as Cathy O'Neill states in her talk *Weapons of Math Destruction*, profit driven algorithms can unintentionally harm vulnerable groups. Certain drivers could become exploited or unfairly penalized based on an algorithm not taking social aspects into context (O'Neill, 2017). This issue can be further exacerbated by the fact that drivers may not fully understand what is being collected and how this data could harm them when consenting to be tracked. Carissa Veliz discusses in *The Surveillance Delusion* that mass data collection without meaningful consent can lead to reputational risks (Veliz, 2023). To protect drivers and trust in our business, we should pursue clear and upfront communication about any data collection practices. It would also be beneficial to give drivers access to their basic data summaries to maintain fairness in what data is being sent to companies like Uber and Lyft. Developing a data profit model that can still maintain a profit while keeping drivers in mind will help decrease this ethical concern.

## Policies

- To solve the ethical concerns presented, our company wants to pursue two types of policies, a front-end policy and a back-end policy.
  - In creating a front-end policy, we are taking inspiration from Privacy as the Default principle (Cavoukian, 2011), the vehicle monitoring application should

implement a default privacy mode policy under which all non-essential data collection is turned off by default.

- When a user downloads the application, data collection should be at a minimum level, sufficient enough to fuel the core functionality. This default setting ensures that privacy and informed consent is enforced even if users take no action.
- It helps solve the ethical concerns of privacy, informed consent, and the use of persuasive technologies through an opt-out policy.
- A back-end policy that helps solve privacy and ensures that the collection of data will not hurt drivers despite the need to profit would be federated data collection.
  - Instead of allowing the raw data to go to an overall server, we could have a policy in which the raw data stays local with the transmitter. The transmitter is then able to create models and provide analysis about one's driving. Then the analysis and model could be sent to the overall company server (Tian, Yuan et al., 2024). While models could still provide some details, the models are meant to help predict and test data against the model. It's not raw information. These models could also be shared with third party companies and provide a layer of privacy between third party companies and drivers. Drivers wouldn't be able to be targeted directly by third party companies. Adding more barriers between company and data helps promote drivers' privacy and attempts to limit harm that could come to drivers.

- It helps solve the ethical concerns of privacy and the possibility of harm to drivers while still profiting (collecting data for profit).

## References

- Cavoukian, Ann. *Privacy by Design the 7 Foundational Principles*,  
privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf. Accessed 27  
Apr. 2025.
- Kleinig, John. "The Nature of Consent." *The Ethics of Consent: Theory and Practice*, edited by  
Franklin G. Miller and Alan Wertheimer, 1st ed., Oxford University Press, 2010, pp.  
3–24. ResearchGate,  
[https://www.researchgate.net/publication/295106929\\_The\\_Nature\\_of\\_Consent](https://www.researchgate.net/publication/295106929_The_Nature_of_Consent). Accessed  
29 Apr. 2025.
- Lundberg, I., Narayanan, A., Levy, K., & Salganik, M. J. (2019). Privacy, Ethics, and Data  
Access: A Case Study of the Fragile Families Challenge. *Socius*, 5.  
<https://doi.org/10.1177/2378023118813023> (Original work published 2019)
- Nissenbaum, Helen. "Privacy as Contextual Integrity." *Washington Law Review*, vol. 79, no. 1,  
2004, pp. 119–157. *Digital Commons @ UW Law*,  
<https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10>. Accessed 29 Apr. 2025.
- O’Neil, Cathy. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens  
Democracy*. Penguin Books, 2017.
- Tian, Yuan et al. “Personalized Federated Learning Scheme for Autonomous Driving Based on  
Correlated Differential Privacy.” *Sensors (Basel, Switzerland)* vol. 25,1 178. 31 Dec.  
2024, doi:10.3390/s25010178

Véliz, Carissa, 'The Surveillance Delusion', in Carissa Véliz (ed.), *Oxford Handbook of Digital Ethics*, Oxford Handbooks (2023; online edn, Oxford Academic, 10 Nov. 2021), <https://doi-org.ezproxy.library.wisc.edu/10.1093/oxfordhb/9780198857815.013.30>, accessed 27 Apr. 2025.

Williams, James, 'Ethical Dimensions of Persuasive Technology', in Carissa Véliz (ed.), *Oxford Handbook of Digital Ethics*, Oxford Handbooks (2023; online edn, Oxford Academic, 10 Nov. 2021), <https://doi-org.ezproxy.library.wisc.edu/10.1093/oxfordhb/9780198857815.013.15>, accessed 27 Apr. 2025.