Critical Thinking Module 6:

The Ethics of Behavioral Analytics and Political Microtargeting

Alexander Ricciardi

Colorado State University Global

CSC502: Ethical Leadership in Software Development

Professor: Dr. Steven Evans

February 22, 2026

Critical Thinking Module 6:

The Ethics of Behavioral Analytics and Political Microtargeting

Modern political campaigning is vastly different from the early 2000s. It has evolved from using yard signs, debates, and television ads to using predictive models, such as machine learning models, to analyze population data to determine what to say, to whom, and where, by combining voter files, consumer data, and social media trends. These analytical and predictive methods allow campaigns to target and tailor political messaging with precision. In practice, this translates to optimizing voting turnout efforts by targeting specific neighborhoods' demographics and tailoring political messages to specific population segments based on a population's traits or vulnerabilities. Ultimately, the primary goal of campaigns is to predict what motivates a voter, or what triggers a voter's disengagement, to craft messages that maximize turnout, donations, and vote choice. However, from an ethics standpoint, these data analytic methods are not just benign marketing tools; they are powerful instruments that have the capacity to influence individuals' decision-making by analyzing and predicting individual behavior. Moreover, when behavioral science is fused with big data at a large scale, the resulting systems can become a form of large-scale persuasion and political manipulation directly affecting individuals' well-being, opportunities, and autonomy. While their impacts are sometimes aligned with democratic goals, such as informing voters and increasing participation, they can also be nefarious, exploiting populations' vulnerabilities, spreading targeted disinformation, or suppressing voter turnout among specific demographics. Within the context of data-driven systems and software engineering, this paper addresses two primary questions: what ethical considerations must guide the behavioral analytics that help political candidates tailor campaign messages, and what do professional ethics demand of the software engineers who build and deploy these systems?

Behavioral Analytics and Political Microtargeting

Behavioral analytics is a process that involves the analysis of large datasets consisting of behavioral data with the goal of extracting behavioral insights (Martinez, 2022). The process extracts preferences, traits, and likely actions from patterns in data, typically by combining statistical or machine-learning prediction with segmentation, such as grouping individuals into behaviorally similar groups, and experimentation, such as randomized A/B tests. Political campaigns hire organizations that use these methods to estimate support scores for a candidate or an issue, voter turnout likelihood, and the relative persuasiveness of groups of individuals or populations, by analyzing aggregated community- and population-level patterns such as turnout history, party registration ratios, and local issues of these precincts and communities. This microtargeting approach allows political campaigns to identify the individual voters who are most likely to be convinced and match and tailor their political message to the specific interests and vulnerabilities of these voters (Zuiderveen Borgesius et al., 2025). When implemented online across social media and ads, political microtargeting collects information about users' online behavior to target specific individuals with tailored political messaging based on these individuals' distinct interests and vulnerabilities. While microtargeting may be useful for political campaigns as it can help reach potential voters and increase their participation by providing information relevant to them, it can also be misleading by presenting inconsistent messaging in the form of distinct advertisements crafted for specific audiences, and raises privacy concerns as it requires extensive data collection. Additionally, campaigns often use the results from behavioral analytics to frame messages based on triggers such as fear vs. hope and norm cues such as cultural and religious values, leveraging identity-based appeals to influence political views.

Furthermore, when these tactics are used in combination with large-scale population analytics, they can cross from just being a persuasion tool into manipulation tactics, especially when the individuals in these populations are unaware that they are being psychologically targeted.

Autonomy, Privacy, and Consent

The ethical question that can arise from these microtargeting practices and marketing in general is whether the collected data used to identify and target voters was obtained with consent from the voters themselves and has usage limitations based on a legitimate purpose. For their analytics, political campaigns often rely on organizations that repurpose data originally gathered for other reasons, such as commercial transactions, browsing behavior, and app interactions. Although the data may be legally acquired, it could create an ethical legitimacy deficit if the individuals affected did not expect to be politically profiled or if their consent was bundled, coerced, or obscured behind small print and dense privacy policies. Additionally, regulators and legislators argue that political data analytics of personal information for political influence is an issue that does not respect countries' borders, requiring strong transparency and enforcement. An investigation by the Information Commissioner's Office (2018) into political campaign data analytics supports this assertion. It found that political data analytics of personal information is a global problem requiring updated data protection laws, as self-regulation by major technology platforms fails to adequately protect individual rights. From a software engineering perspective, protecting user privacy is not only about preventing security breaches. It is also about controlling the processing of personal information by limiting its usage to legitimate purposes and reducing downstream effects on people’s autonomy, that is, by controlling the way data is handled today to reduce the impacts on a person's free will tomorrow.

Furthermore, as Artificial Intelligence (AI) is increasingly integrated into data-driven software, these algorithms can assess users' personal traits, influencing making decisions that shape lives, which can "significantly undermine people's autonomy, affecting their content consumption, behavior, and self-regulation" (Wang & Pea, 2024, p.1). Engineers must mitigate these risks by implementing ethical privacy principles as software requirements throughout the life cycles of software and through risk management. Ultimately, as an ethical requirement to protect individual autonomy, political campaigns and the organizations they use for behavioral analytics should apply data minimization (collecting only the data strictly necessary for the task), purpose limitation, provenance tracking, opt-out mechanisms (allowing users to easily withdraw consent or disable tracking), and privacy risk assessment, not just as regulations and legal compliance, but as design constraints.

Autonomy and Psychological Targeting

In addition to privacy and consent concerns, behavioral analytics systems can be leveraged to exploit individuals' cognitive biases or vulnerabilities to steer their choices subconsciously, undermining their autonomy. When utilized for that purpose, behavioral analytics transitions from targeted communication to psychological manipulation. In practice, it can be used to influence a specific group of individuals or entire populations by profiling and targeting to influence and shape their behavior in ways that are difficult to detect, contest, or resist, effectively manipulating decision-making without informed awareness (Susser et al., 2019). In large-scale online field experiments by Matz et al. (2017), researchers demonstrated that matching persuasive appeals to individuals' specific psychological characteristics significantly influences and changes their behavior, such as increasing clicks and purchases on social media and e-commerce platforms.

In the context of political campaigning, psychological targeting is highly effective and can work on a large scale. It can be used to craft tailored messaging that can shift voting behavior and alter election outcomes, ultimately affecting millions of individuals. Ideally, political campaigns should ensure that political persuasion respects voter autonomy and use psychological targeting to empower voters rather than exploiting them. From a software engineering standpoint, data-driven software systems used for political behavioral analytics should be designed with strict ethical guardrails to avoid exploiting vulnerabilities such as anxiety, loneliness, or addiction-like scrolling or engagement loops, especially when the voters cannot recognize that they are being targeted for manipulation.

Ethical Requirements for Political Analytics Software

In practice, when used in the context of precincts (the smallest geographic unit in which voting can take place), political message tailoring based on behavioral analytics can address local concerns such as jobs, schools, and infrastructure. However, it can be ethically problematic if it is leveraged to target a precinct population trait such as race, religion, or ethnicity, as it can be used not to disseminate information but rather to deliberately exclude the specific groups from receiving key information, often intending to suppress votes either directly or indirectly. In the context of data analytics, even neutral models often introduce inequities due to historical data bias. In software engineering, developers should design software systems that integrate fairness, not as an afterthought, but as a requirement throughout the software development lifecycle. Ethically, political campaigns and the organizations they use for behavioral analytics should not use targeting strategies that suppress voting, rely on proxies, or create unequal informational access.

In addition to introducing fairness as a requirement, transparency, explainability, ownership, and accountability should also be introduced as requirements throughout the software development lifecycle. These principles matter as political persuasion is not a commercial transaction; rather, they influence elections, shape public goods, and can legitimate or delegitimate the democratic process, depending on citizens being able to understand, evaluate, and contest political claims. Moreover, when these principles are not applied while using microtargeting, so that only the targeted voter can see a message, it weakens public accountability, allowing campaigns to deploy inconsistent, misleading, or emotionally manipulative messages without scrutiny (Zuiderveen Borgesius et al., 2025). In software engineering practice, not applying these principals translate to building opaque systems that lack oversight and accountability. Therefore, the algorithms and software that allow political campaigns to target precincts and individuals should be designed not only for performance (clicks, conversions, turnout) but also for transparency, explainability, ownership, and accountability.

Conclusion

The integration of big data and behavioral science into political campaigning has transformed the political campaign processes. Microtargeting and predictive analytics have improved political campaigns' capabilities to promote civic engagement and tailored messaging; however, they also have introduced ethical risks, more specifically behavioral analytics, ranging from the erosion of personal privacy to psychological manipulation and targeted voter suppression. These risks must be addressed by implementing ethical frameworks within microtargeting and behavioral analytic processes, ensuring voter autonomy by requiring consent from individuals, purpose limitation of collected data, and by rejecting psychological targeting that exploits groups or individual vulnerabilities.

More importantly, implementing ethical data-driven systems does not rest exclusively on political campaign managers; it is, moreover, a responsibility of the software engineers who build and deploy them. Professional ethics demand that software developers stop viewing behavior analytic software systems as neutral, performance-driven marketing tools. As these analytics systems have the potential to shape public goods and legitimize or delegitimate electoral outcomes, software engineers have an ethical responsibility to embed ethical constraints directly into the software development lifecycle. These demands, integrating fairness, transparency, explainability, ownership, and accountability principles into the development life cycle of analytic software applications as requirements rather than treating them as afterthoughts. Ultimately, preserving democratic election principles requires that political campaigns and software developers commit to ethical standards prioritizing voter consent and public transparency over the pursuit of behavior metrics and behavioral manipulation.

References

Information Commissioner's Office. (2018, November 6). *Investigation into the use of data analytics in political campaigns: A report to Parliament*. UK Information Commissioner’s Office. https://ico.org.uk/media2/migrated/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf

Martinez, L. S. (2022). Behavioral analytics. In L. A. Schintler & C. L. McNeely (Eds.), *Encyclopedia of big data* (pp. 69–72). Springer. https://doi.org/10.1007/978-3-319-32010-6_18

Matz, S. C., Kosinski, M., Nave, G., & Stillwell, D. J. (2017). Psychological targeting as an effective approach to digital mass persuasion. *Proceedings of the National Academy of Sciences of the United States of America, 114*(48), 12714–12719. https://doi.org/10.1073/pnas.1710966114

Susser, D., Roessler, B., & Nissenbaum, H. (2019). Online manipulation: Hidden influences in a digital world. *Georgetown Law Technology Review, 4*(1), 1–45. https://pure.uva.nl/ws/files/45242068/Susser_Roessler_Nissenbaum_Online_Manipulation_.pdf

Wang, G., & Pea, R. (2024). *Algorithmic autonomy in data-driven AI* (arXiv:2411.05210v1) [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2411.05210

Zuiderveen Borgesius, F. J., Möller, J., Kruikemeier, S., Ó Fathaigh, R., Irion, K., Dobber, T., Bodó, B., & de Vreese, C. (2025). *Online political microtargeting: Promises and threats for democracy*. arXiv. https://doi.org/10.48550/arXiv.2510.17712