

Research Article

The Clash between the Right to Privacy and the First Amendment to the U.S. Constitution during American Presidential Campaigns

Tomasz Idzikowski*

Faculty of Economics and Management, Lazarski University, Świeradowska 43, 02-662 Warsaw, Poland.

* Correspondence: tomasz.idzikowski@lazarski.edu.pl

Abstract: Big Data analysis has fundamentally reshaped American presidential campaigns. At the heart of this shift is electoral microtargeting, which involves the meticulous profiling of citizens for highly customized political communications. Current study explores the complexities produced by such practices. The friction between First Amendment which protects the political expression and the right to everyone's personal privacy. Although American courts consistently uphold broad safeguards for political discourse, the large-scale aggregating of sensitive psychographic information by campaign organizations and private data brokers operates largely outside the current disjointed and highly fragmented U.S. data privacy regime. Current research aims to highlight legal deficiencies and evaluate the degree to which the prevailing First Amendment paradigm might counterintuitively impair democratic processes trapping voters in asymmetric information bubbles. The findings underscore a pressing need for comprehensive federal statutory reforms that would reconcile the freedom to campaign with mandates for transparency and stronger data security.

Keywords: political microtargeting; First Amendment; right to privacy; US presidential campaigns; personal data protection; freedom of speech; US presidential elections

1. Introduction

For over a decade, the United States elections have been a testing ground for innovative approaches to develop political communication strategies. Today in the age of digitization and internet penetration, traditional campaign practices have been overtaken by more sophisticated data-driven and hyper-targeted voter outreach practices. The 2012 and 2016 presidential campaigns were landmark events that signalled the paradigm change – showing that winning now depends not on how much one spends on mainstream media but rather on individualized cross-platform digital engagement (Zuiderveen Borgesius et al. 2018).

This change is accelerated by electoral microtargeting. It harnesses the power of aggregation and analysis of large citizens' datasets, often including thousands of variables ranging from their socio-demographic details and purchase histories to social-media behaviours. The ultimate purpose is to build comprehensive psychographic profiles (Hersh 2015, 22–25). Once available, these allow campaign operatives to predict individual voters' preferences with a high degree of accuracy and subsequently deliver hyper-personalized political messages to them (Chester and Montgomery 2017). The demonstrated efficacy of this tool has made it a staple practice in every US presidential race.

This phenomenon, however, gives rise to a fundamental constitutional dilemma, consisting in the clash of two values deeply rooted in the American legal order. On the one hand, the American legal system relies on almost absolute protection of freedom of speech, guaranteed by the First Amendment to the United States Constitution. The jurisprudence of the Supreme Court of the United States consistently treats political speech as a form of expression deserving the highest level of protection, subject to so-called strict scrutiny (Hasen 2016, 45–47). From this perspective, microtargeting is perceived as a modern, optimized form of campaigning and candidate outreach to the voter. On the other hand, the unprecedented scale and intrusiveness of the data collection methods pose a serious threat to the citizens' right to privacy (Bennett and Lyon 2019). The United States lacks a single, comprehensive federal law regulating personal data protection, such as the

Citation: Tomasz Idzikowski. 2026. The Clash between the Right to Privacy and the First Amendment to the U.S. Constitution during American Presidential Campaigns. *Legal Research & Analysis* 4(3), 28–33.

<https://doi.org/10.69971/lra.4.3.2026.204>



Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license <https://creativecommons.org/licenses/by/4.0/>.

European GDPR¹, and existing sectoral regulations rarely extend to the activities of political entities (Electronic Frontier Foundation 2020). Compounding this is the lack of transparency regarding algorithms and the operations of so-called data brokers, meaning that voters are often completely unaware of what information is being collected about them and how it shapes the messaging that ultimately reaches them (Barocas and Nissenbaum 2014, 55–58).

Current study critical analyses the tension between the First Amendment and privacy rights in the context of microtargeting practices in presidential elections. The key research question is whether the US legal system is capable of protecting citizens' informational privacy in this sphere without violating their freedom of political speech. To answer this, relevant legislative provisions and judicial precedents shaping the discourse around regulating electioneering practices will be examined.

The primary research method applied in this work is doctrinal legal analysis, encompassing a review of federal and state normative acts, selected jurisprudence of the US Supreme Court (including precedent-setting judgments concerning freedom of speech, such as *Citizens United v. Federal Election Commission*²), and relevant literature. This will allow for outlining a comprehensive picture of the legal challenges and formulating recommendations for optimizing American electoral law and data protection.

2. Political Microtargeting as a Campaign Tool

American electoral contests have long relied on studying voter behaviour based on a few basic categories of demographics and past voting trends. Due to modern digital platforms, the current campaign framework can target extremely specific groups of individuals online based on a user's information retrieved from their search history, social network activity, and extrapolated inclinations (Sernani et al. 2025). This practice known as political microtargeting, underwent a significant transformation in recent years due to the advancements in data science and artificial intelligence field. Currently, AI is used both for encouraging voters to engage in the political process by reaching out to them in a personalized manner and analysing massive amounts of data regarding the most relevant socioeconomic issues (Rehagen 2024). Within this framework, campaign organizations are believed to have a comprehensive overview of the digital habits and personal inclinations of citizens (Voinea 2024). This allows them to identify the most effective appeal that would encourage an individual to support a particular candidate or prevent them from endorsing their rival.

A key element of the infrastructure enabling microtargeting is the so-called data brokers. In the modern economy, data is as an invisible currency that drives not only innovation and commercial advertising but also direct political influence (Catalan 2026). In 2024, the global data brokerage industry was valued at over 389 billion dollars. Because the United States lacks a comprehensive federal privacy law, data brokers can freely aggregate and sell massive datasets of information to political campaign teams (Catalan 2026). Armed with such resources, political campaigns utilize highly granular ad targeting options on social media platforms (Bahi 2024). The message can be tailored based on specific location, age, gender, interests, or party affiliation, and this is just the tip of the iceberg, as the possibilities are nearly limitless. It is also possible to direct completely different messages to specific demographic groups. For example, promoting policies regarding climate change and student loans among young voters in California, and unrestricted access to firearms among voters in Texas, while simultaneously emphasizing healthcare issues in communication with the older electorate across the entire US (Bahi 2024).

The consequences of the widespread use of microtargeting for the democratic process remain highly ambivalent. On the one hand, these techniques strengthen the ability of politicians to effectively communicate their views. Microtargeted ads are characterized by significantly greater thematic diversity than traditional mass messages, precisely addressing niche social problems (López Ortega 2022). On the other hand, however, these strategies create a space for far-reaching manipulation. The goals of political microtargeting are diverse and often include not only mobilizing citizens but also causing disorientation, fear, and the deliberate demobilization of competitors' voters (Repp 2026).

The architecture of modern social media only amplifies these risks. Platforms such as YouTube, TikTok, or Instagram currently function as powerful political intermediaries, and their algorithms inherently favor and promote engaging, highly polarizing content with an extreme emotional charge (Bahi 2024). Such precise profiling is opening the door to the possibility of sending contradictory declarations to different segments of society and instrumentally exploiting the prejudices of recipients without confronting them with opposing viewpoints, and this leads to trapping voters in information bubbles (Voinea 2024). This limits not only the autonomy of the recipient themselves, but indirectly violates the right of citizens who were not subjected to microtargeting to access information regarding the political stances actually represented by a given candidate.

In conjunction with the advancing technological and technical capabilities related to disinformation (such as AI-generated deepfakes), microtargeting creates a real danger of fabricating alternative and artificial political and social realities within election campaigns. Trapping citizens in personalized information bubbles and disseminating disinformation weakens informed public debate, resulting in profound polarization of the electorate and the erosion of trust in democratic institutions in the United States (López Ortega 2022).

3. Case Study 1: The Cambridge Analytica Scandal and the 2016 Presidential Election

The event that permanently defined the public and academic debate on political microtargeting was the activity of the British consulting firm Cambridge Analytica during the United States presidential election in 2016. This is an almost textbook example of a loophole in the American data protection system and the impotence of regulatory bodies in the face of innovative political campaigns operating under the protective umbrella of the First Amendment to the US Constitution (Isaak and Hanna 2018).

¹ General Data Protection Regulation (GDPR), <https://eur-lex.europa.eu/PL/legal-content/summary/general-data-protection-regulation-gdpr.html>

² Supreme Court of the United States, judgment of January 21, 2010, case no. 558 U.S. 310, *Citizens United v. Federal Election Commission*, pp. 339-340.

The Cambridge Analytica's operation relied on acquiring the data of nearly 87 million Facebook platform users via a seemingly innocent research application (a personality quiz) named "ThisIsYourDigitalLife". A key aspect of this procedure was the exploitation of Facebook's application programming interface (API) at the time, which allowed the collection of information not only about the individuals directly installing the app but also about their entire extensive network of friends. This process took place without their explicit knowledge and consent (Cadwalladr and Graham-Harrison 2018). Millions of data points collected in this manner were used by data engineers to create advanced psychometric models based on the Big Five psychological model - OCEAN: openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism (Susser, Roessler, and Nissenbaum 2019).

This precisely profiled database, enabled campaign teams to direct highly personalized messages to specific psychological types. For example, to voters characterized by a high level of neuroticism and susceptibility to fear, algorithms served political ads highlighting the threats associated with immigration or crime. Conversely, individuals with high levels of agreeableness and conscientiousness received messages emphasizing the defence of community, family, and traditional values (Susser, Roessler, and Nissenbaum 2019). Such deep, algorithmic interference in the cognitive autonomy and vulnerabilities of voters went far beyond traditionally understood, open political campaigning.

From a legal and constitutional perspective, it exposed the paralysis of American legislation. While the Facebook (Meta) platform itself was ultimately penalized by the Federal Trade Commission (FTC) with a record settlement and a 5 billion dollar fine for a flagrant violation of consumer privacy, the political actors utilizing this data remained largely beyond the reach of legal sanctions (Federal Trade Commission 2019). The lack of rigorous federal regulations regarding political microtargeting and data trading meant that the actions of the campaign teams were a form of expression protected by the First Amendment to the US Constitution. It was de facto recognized that algorithmic message optimization was merely a technological tool serving the realization of the candidates' constitutional right to free communication with the electorate. This scandal clearly demonstrated that the lack of regulation at the intersection of data trading and electoral law allows for the unprecedented commercialization and instrumentalization of psychological data, creating a direct threat to the integrity of the democratic process and the citizens' right to privacy (Persily 2017).

4. Case Study 2: The Role of TikTok's Algorithms in the 2024 Presidential Campaign

The 2024 presidential election was an unprecedented evidence of the power of behavioural microtargeting, and the social media platform TikTok became the main arena for these activities. Although the application officially banned paid political advertisements in its terms of service, campaign teams efficiently circumvented these restrictions by utilizing the phenomenon of so-called proxy microtargeting. This consisted of establishing cooperation with a vast network of influential internet creators, who organically smuggled political messages to strictly selected target groups.

TikTok's architecture, centralized around the algorithmically generated "For You" page (For You Page – FYP), is the most advanced form of informational targeting. Unlike older platforms, which were based primarily on the social graph (connections between friends), TikTok's recommendation algorithm relies on the interest graph and the exceptionally intrusive analysis of behavioural micro-signals. The platform's engine continuously measures metrics such as the dwell time on a specific video frame, the screen scrolling speed, or the frequency of interactions with specific audio tracks.

During the 2024 campaign, campaign teams aggregated their own datasets and information from external data brokers, and subsequently, via contracted creators, tailored messages to the behavioural profiles of the platform's users. This allowed generating content tailored to very narrow niches, e.g., undecided Generation Z voters living in the suburbs of so-called swing states, based solely on their digital habits. This phenomenon created exceptionally hermetic information bubbles. The voter, absorbed in a seamless stream of short videos, received a personalized political message that gave the impression of being fully grassroots, while in reality, it was an element of a precisely orchestrated informational campaign.

The case of TikTok in 2024 is a perfect illustration of the titular legal clash. Efforts to sell or block the platform due to massive threats to citizens' data privacy met with immense legal resistance. Civil liberties organizations and technology lawyers unanimously argued that the state cannot cut citizens off from their preferred channel of political expression, as this violates the rigorous standards of the First Amendment to the US Constitution. The right to protect sensitive behavioural data was broadly understood freedom of speech, creating an ecosystem in which the commercialization of voter attention encounters almost no constitutional barriers.

5. American Legal Framework Regarding Privacy

American privacy protection drastically differs from the European model based on the General Data Protection Regulation (GDPR 2016). In the United States, there is no single, comprehensive federal personal data protection law in effect, and the system is strictly sectoral and fragmented in nature (Solove and Schwartz 2020, 1102–5). Federal regulations protect only selected, relatively narrow categories of data, such as health information (the HIPAA Act³), financial information (the GLBA Act⁴), or the online data of children under 13 years of age (the COPPA Act⁵). Faced with the years-long legislative inaction of the United States Congress regarding universal privacy protection, individual states began to create their own legal frameworks, spearheaded by the pioneering Californian laws: the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), followed by initiatives in Virginia, Colorado, or Connecticut (Chander, Kaminski, and McGeveran 2021).

³ HIPAA Administrative Simplification, <https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf>

⁴ Gramm-Leach-Bliley Act GLBA, <https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act>

⁵ Children's Online Privacy Protection Rule ("COPPA"), <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>

However, from the perspective of election campaigns, both state and sectoral regulations exhibit a critical structural gap. American privacy law focuses almost entirely on consumer relations (business-to-consumer), predominantly excluding non-profit entities as well as political organizations and committees from its jurisdiction (Burkell and Regan 2021). Hence, the campaign teams of US presidential candidates operate in a legal vacuum, in which standard, contemporary principles concerning data minimization, the requirement to obtain explicit consent for its processing (the opt-in model), or the citizen's right to be forgotten do not apply to them. The Federal Trade Commission (FTC), which is the primary body enforcing regulations protecting American consumers, is incompetent to intervene in activities of a purely political nature (Richards 2021, 120–23). The actions of campaign teams also do not fall under the purview of the Federal Election Commission (FEC), because its competencies end with issues related to campaign financing, and not with data trading. Hence, campaign teams and the data brokers cooperating with them can completely legally carry out the mass aggregation and utilization of sensitive demographic, behavioural, and psychographic information, without fearing the spectre of administrative sanctions for violating citizens' privacy.

6. The First Amendment to the US Constitution and Freedom of Political Speech

The lack of rigorous federal regulations regarding political data is not merely due to lack of political consensus, but has deep roots in the American constitutional tradition. The First Amendment to the US Constitution, constituting the absolute foundation of the American system of civil liberties, grants political speech the highest possible level of protection (Chemerinsky 2023, 1150–53). The Supreme Court of the United States consistently rules that freedom of political speech is the very centre of the American democracy, and any attempts at interference or its restriction by the authorities are subject to the strictest standard of judicial review, so-called strict scrutiny. The legal foundation protecting operations on political data has been strengthened by the landmark Supreme Court judgments in the last decade. Although the 2010 judgment in *Citizens United v. Federal Election Commission* concerned the lifting of political spending limits for corporations, it solidified the principle that the state cannot restrict the voice of any entity in public debate, and that the financing of campaign tools is equivalent to speech itself. In turn, in the 2011 *Sorrell v. IMS Health Inc.* judgment, the Supreme Court explicitly recognized that the mere collection, aggregation, creation, and sale of data hold the status of protected speech under the First Amendment⁶.

This line of jurisprudence legitimizes the use of microtargeting. Algorithmic voter profiling is merely a modern tool, necessary for the effective formation and distribution of political speech to appropriate audiences (Post 2022). Accordingly, microtargeting is solely a technological evolution of direct door-knocking or sending direct mail to voters. Limiting campaign teams' ability to create their own precise databases is perceived by lawyers as a direct blow to effectively express their platforms and views, which would violate the First Amendment to the US Constitution. This framework means that any legislative initiative aiming to block or strictly regulate the transfer and processing of voter data would very likely be challenged as unconstitutional (Balkin 2020). Thus, a severe legal challenge arises, in which regulations intended to protect the right to privacy are completely subordinate to the right of unfettered political expression, which in the digital era is a glaring asymmetry of power between politicians and citizens, unaware of the manipulation of their own data.

7. Clash of Values: Analysis of the Legal Conflict

The clash between the phenomenon of microtargeting and the First Amendment to the US Constitution is a fundamental paradox of today's American democracy. Historically, freedom of speech in the US relied on the concept of the "marketplace of ideas," formulated over a century ago by Justice Oliver Wendell Holmes (Sunstein 2021, 74–78). According to this theory, truth emerges through an open, public, and unfettered exchange of views, in which citizens can freely confront different stances. Political microtargeting completely deconstructs this model. This mechanism creates hundreds of thousands of atomized, private information bubbles in which the political message is invisible to the broader public, and thus not subject to societal and journalistic verification (Dobber, Ó Fathaigh, and Zuiderveen Borgesius 2021).

The legal conflict, therefore, does not merely boil down to a simple opposition between the right to privacy and the candidate's freedom of speech, but concerns the protection of the voter's cognitive autonomy itself. When political committees, fuelled by data from the information black market, exploit the psychological vulnerabilities of citizens to purposefully induce fear or apathy, the democratic process becomes corrupted. Paradoxically, then, the absolutization of the First Amendment in jurisprudence, which protects algorithmic data processing as a form of expression, destroys the foundations of informed civic participation that the very same First Amendment was originally intended to safeguard (Franks 2020, 112–15). US courts face the necessity of determining whether the acquisition of highly sensitive psychographic data without the user's consent falls within the permissible boundaries of political freedom, or whether it constitutes an autonomous harm violating the citizens' constitutional right to self-determination.

8. Legal and Political Challenges

The current legal system in the United States is unable to deal with the challenges of the automated campaign era, leading to a series of political and legislative barriers (Appelman and Ó Fathaigh 2022). The first and most important challenge is the drastic information asymmetry between campaign teams, technology platforms, and ordinary citizens. Candidates possess software capable of analysing millions of data points about every voter, while the voter themselves is rarely able to check why they saw a specific advertisement with a particular content.

Another challenge is the structural difficulty in defining the boundaries between the commercial and political use of data. While use of data in commerce may be subject to FTC regulations protecting consumers against unfair market practices, the inclusion of a political element in the message automatically activates the protective shield of the First Amendment. Lawmakers attempting to regulate the digital market fear introducing restrictions on politicians, aware of the risk of years-long and costly lawsuits to

⁶ Supreme Court of the United States, judgment of June 23, 2011, case no. 564 U.S. 552, *Sorrell v. IMS Health Inc.*, pp. 570–571.

declare such laws unconstitutional (Bhagwat 2022, 201–4). Technology corporations such as Meta (Facebook) or Alphabet (Google) exploit this ambiguity, manoeuvring between voluntary self-regulation and reaping massive profits from political advertising expenditures. Furthermore, the extraterritorial nature of data flow complicates law enforcement in cases where the data brokers' servers are located outside the jurisdiction of a given state or country.

9. Recommendations and Political Interventions

Resolving such a deep conflict requires a multidimensional intervention at the federal level that reconciles the First Amendment to the US Constitution with privacy protection. A key recommendation is the implementation of broad transparency requirements, the so-called compelled disclosure (Hasen 2022, 130–35). The jurisprudence of the Supreme Court (including the *Buckley v. Valeo* case) indicates that the disclosure obligation for campaign committees does not violate freedom of speech to the same extent as a prohibition on the speech itself. Consequently, Congress should enact legislation mandating the labelling of digital political advertisements with clear information not only about who funded the message but also based on exactly what algorithmic criteria (e.g., location, political views, gender) a given voter was targeted for it.

The second step should be an intervention in the data broker market. Federal legislation could ban or drastically restrict the ability of campaign teams to purchase citizen data from third parties, forcing political committees to rely exclusively on data collected directly from their supporters (so-called zero-party and first-party data) with their explicit consent (the opt-in model).

The third pillar of political intervention is the tightening of self-regulatory requirements for major technology platforms. Following the example of actions taken in some European countries, social media platforms in the US can limit the degree of granularity in political microtargeting, for example, by allowing ad targeting based only on general zip codes or broad age ranges, and blocking targeting based on behaviours, interests, or sensitive psychographic traits (Goodman and Rysman 2021).

10. Conclusions

The use of Artificial Intelligence, Big Data and campaign financing has permanently changed America's political culture for the worse. Due to the lack of personal data regulation, microtargeting has become an incredibly powerful tool for manipulating the masses. While both tech companies and political campaigns alike hide behind the first amendment, evidence shows that such practices do much to obstruct the freedom of the press as well as the freedom of speech. The right to informational privacy is not a right that should be sacrificed on the altar of free speech, instead it should be seen as an integral part of it. In order to have an open society with due process under the constitution, America cannot continue to see the manipulation of citizens via algorithms as free speech. A careful balancing act must be achieved by congress in order to ensure that campaign finance and data selling do not dominate the democratic process as they do now. If nothing is done, future elections will only grow more divided and polluted by AI generated propaganda, creating increasingly extreme informational bubbles.

References

- Appelman, Naomi, and Ronan Ó Fathaigh. 2022. The Law and Policy of Political Microtargeting: An Analysis of the US and EU Frameworks. *Journal of Internet Law* 25 (8): 3–7.
- Bahi, S. 2024. Social Media Strategies and the 2024 U.S. Election Campaigns. *Medium*. <https://medium.com/@shabbybahi123/social-media-strategies-and-the-2024-u-s-election-campaigns-6892207af840>
- Balkin, Jack M. 2020. How to Regulate (and Not Regulate) Social Media. *Journal of Free Speech Law* 1 (1): 85–88.
- Barocas, Solon, and Helen Nissenbaum. 2014. Big Data's End Run around Anonymity and Consent. In *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, edited by Julia Lane, Victoria Stodden, Stefan Bender, and Helen Nissenbaum, 44–75. Cambridge University Press. <https://doi.org/10.1017/CBO9781107590205.004>
- Bennett, Colin J., and David Lyon. 2019. Data-Driven Elections: Implications and Challenges for Democratic Societies. *Internet Policy Review* 8 (4). <https://doi.org/10.14763/2019.4.1433>
- Bhagwat, Ashutosh. 2022. *Our Democratic First Amendment*. Cambridge University Press. <https://doi.org/10.1017/9781108676373>
- Burkell, Jacquelyn, and Priscilla M. Regan. 2021. Voter Preferences, Voter Manipulation, Voter Privacy: Contextualizing Political Microtargeting. *Internet Policy Review* 10 (4): 7–10.
- Cadwalladr, Carole, and Emma Graham-Harrison. 2018. Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach. *The Guardian*, March 17, 2018. <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>
- Catalan, David. 2026. *Data Leak: How the Lack of Federal Data Privacy Protections Leaves Both Citizens and Non-citizens Vulnerable*. Policy Briefs & White Papers. Congressional Hispanic Caucus Institute (CHCI). <http://chci.org/wp-content/uploads/2026/03/2026-David-Catalan.pdf>
- Chander, Anupam, Margot E. Kaminski, and William McGeveran. 2021. Catalyzing Privacy Law. *Minnesota Law Review* 105 (4): 1735–38.
- Chemerinsky, Erwin. 2023. *Constitutional Law: Principles and Policies*. 7th ed. Aspen Publishing.
- Chester, Jeff, and Kathryn C. Montgomery. 2017. The Role of Digital Marketing in Political Campaigns. *Internet Policy Review* 6 (4): 4–7. <https://doi.org/10.14763/2017.4.773>
- Dobber, Tom, Ronan Ó Fathaigh, and Frederik Zuiderveen Borgesius. 2021. The Regulation of Online Political Micro-targeting in Europe and the United States. In *Free Speech, Privacy and Media: Comparative Perspectives*, edited by Russell L. Weaver, Mark D. Cole, Steven I. Friedland, Duncan Fairgrieve, András Koltay, and Arnaud Raynouard, 145–49. Carolina Academic Press.
- Electronic Frontier Foundation (EFF). 2020. Privacy and Political Campaigns. <https://www.eff.org/issues/privacy-and-political-campaigns>
- Federal Trade Commission. 2019. FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook. Press release. <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook>
- Franks, Mary Anne. 2020. *The Cult of the Constitution*. Stanford University Press.

- GDPR. 2016. General Data Protection Regulation (Rozporządzenie o Ochronie Danych Osobowych, RODO). <https://eur-lex.europa.eu/PL/legal-content/summary/general-data-protection-regulation-gdpr.html>
- Hasen, Richard L. 2016. *Plutocrats United: Campaign Money, the Supreme Court, and the Distortion of American Elections*. Yale University Press.
- Hasen, Richard L. 2022. *Cheap Speech: How Disinformation Poisons Our Politics—and How to Cure It*. Yale University Press.
- Hersh, Eitan D. 2015. *Hacking the Electorate: How Campaigns Perceive Voters*. Cambridge University Press. <https://doi.org/10.1017/CBO9781316212783>
- López Ortega, Alberto. 2022. Are Microtargeted Campaign Messages More Negative and Diverse? An Analysis of Facebook Ads in European Election Campaigns. *European Political Science* 21 (3): 335–58. <https://doi.org/10.1057/s41304-021-00346-6>
- Persily, Nathaniel. 2017. The 2016 U.S. Election: Can Democracy Survive the Internet? *Journal of Democracy* 28 (2): 63–76. <https://doi.org/10.1353/jod.2017.0025>
- Post, Robert. 2022. Data Privacy and the First Amendment. *Yale Law Journal* 131 (6): 1820–24.
- Rehagen, Tony. 2024. Candidate AI: The Impact of Artificial Intelligence on Elections. Emory University News Center. <https://news.emory.edu/features/2024/09/candidate-ai-impact-artificial-intelligence-elections/>
- Repp, Stefan. 2026. *The Strategic Use of Microtargeting: The Case of the German Federal Elections of 2025*. IPE Working Papers, no. 270/2026. Institute for International Political Economy (IPE) Berlin. <https://www.econstor.eu/handle/10419/341421>
- Richards, Neil. 2021. *Why Privacy Matters*. Oxford University Press.
- Sernani, Paolo, Angela Cossiri, Giovanni Di Cosimo, and Emanuele Frontoni. 2025. Analyzing Digital Political Campaigning Through Machine Learning: An Exploratory Study for the Italian Campaign for European Union Parliament Election in 2024. *Computers* 14 (4): 126. <https://doi.org/10.3390/computers14040126>
- Solove, Daniel J., and Paul M. Schwartz. 2020. *Information Privacy Law*. 7th ed. Wolters Kluwer.
- Sunstein, Cass R. 2021. *#Republic: Divided Democracy in the Age of Social Media*. Princeton University Press.
- Susser, Daniel, Beate Roessler, and Helen Nissenbaum. 2019. Technology, Autonomy, and Manipulation. *Internet Policy Review* 8 (2): 4–6. <https://doi.org/10.14763/2019.2.1410>
- Voinea, Cristina. 2024. Political Campaigning, Microtargeting, and the Right to Information. *Practical Ethics* (blog), Uehiro Centre for Practical Ethics, University of Oxford. <https://blog.uehiro.ox.ac.uk/2024/01/political-campaigning-microtargeting-and-the-right-to-information/>
- Zuiderveen Borgesius, Frederik J., Damian Trilling, Judith Möller, Balázs Bodó, Claes H. de Vreese, and Natali Helberger. 2018. Online Political Microtargeting: Promises and Threats for Democracy. *Utrecht Law Review* 14 (1): 84–86. <https://doi.org/10.18352/ulr.420>