The University of Texas at Austin
Center for Media Engagement
Moody College of Communication

GENAI, DISINFORMATION, AND DATA RIGHTS IN U.S. ELECTIONS

Author: Jacob Gursky

Editors: Inga Trauthig and Samuel Woolley

EXECUTIVE SUMMARY

Five main trends regarding AI and the 2024 US presidential elections stand out:

- Many cases of generative AI used during the 2024 U.S. election are **extensions of mis- and disinformation strategies from previous elections.**
- Both proposed and actual uses of GenAI during the U.S. contest rely upon **manipulation of information related to electoral processes**, offices and vendors via a range of media formats (video, image, audio, and text).
- Actors behind these use cases work to leverage the cachet of **trusted messengers and messages** shared via a trusted mode of communication — i.e., in a particular language or cultural vernacular.
- Conversely, as with prior digital propaganda campaigns, such AI-driven efforts focus upon **eroding public trust in institutions** as a goal in and of itself.
- They take advantage of **Big Tech's ineffective mitigation measures** and lax government regulation.

SUGGESTED CITATION:

Gursky, Jacob. GenAI, disinformation, and data rights in U.S. elections. Series on Generative Artificial Intelligence and Elections. Eds. Inga Trauthig and Samuel Woolley. Center for Media Engagement, October 2024, https://mediaengagement.org/research/generative-artificial-intelligence-and-elections

NOTEWORTHY HIGHLIGHTS

Two reasons underpin concerns about voter manipulation in the US with Artificial Intelligence (AI) content in the 2024 presidential election:

- Prominent stakeholders have been sharing AI-generated false content already. One prominent example was previous president Donald Trump sharing alleged endorsements by Taylor Swift on social media.
- High sophistication of US campaigning. US campaigners, political marketers and strategists are amongst the most-organized and well-funded around the world. In addition, campaigning for US presidential elections runs for multiple months which opens the door for testing several different tactics over this time – compared to e.g., the UK where the national election took place 25 working days after it was announced.

Two unique findings stand out:

- Data rights, and associated laws, are evolving and corresponding AI policies are on the horizon. 19 U.S. states now have comprehensive privacy laws, all of which include a right to delete one's data. 17 of them contain some form of right against automated decision making. Those working to create laws at the intersection of data privacy and AI are struggling to contend with the rapid speed of innovation and sheer size of data gathering in the industry.
- Some firms working in the political GenAI space are non-transparent about how they leverage voter data, who they target with their technology, and how their models are trained and maintained. New data rights provide those most likely to be targeted with disinformation and/or hyper-individualized political messaging with the opportunity to hold both Big Tech and political campaigns accountable.

One important, underreported finding emerged:

- Requested synergy between the message and the messenger for impactful political campaigning. While GenAI can create effective messaging, it does not have abilities on the same scale to become a trusted messenger in tightly knit communities. This leaves room for interventions on behalf of trusted messengers who are embedded/trusted in communities and whose online messaging hence carries more value over other content seen online.

KEY TERMS

- *Generative Artificial Intelligence (GenAI)* refers to computer systems that draw on extremely large datasets to make statistical inferences about the relationship between words in a body of text or pixels from an image. From these inferences, GenAI systems can produce human-like content quickly in response to human-provided prompts.
- *Large language models (LLMs)* are a form of GenAI that are trained on billions of words of human-produced text. For example, ChatGPT is powered by an LLM.
- *Synthetic Media*, or "deepfakes," can be created by generative AI in the form of imagery, audio, or video.

INTRODUCTION

There is an irony in discussing the role of generative artificial intelligence (GenAI) in spreading political propaganda, as "AI" is itself a propaganda term in part designed to obfuscate and confound the reality of the technology.[1] 2024 has seen a variety of tools labeled as GenAI (tools that can generate content such as text and images based on prompts) come into increasingly common use by political campaigns in the United States. GenAI offers new challenges for organizations and individuals seeking to mitigate the harm of political misinformation (false content unintentionally spread) and political disinformation (false content intentionally spread).

However, the usage of GenAI tools in United States politics is only sporadically documented, and much of the writing about their impact is speculative. Through a review of publicly available reporting about GenAI's documented and potential political uses, this paper presents both an argument and a question about the role of these tools in the election cycle of the United States: it argues that many of the proposed and documented use cases of GenAI in the election cycle of the United States can be understood as extensions of mis- and disinformation strategies from earlier election cycles, and it asks how voters and civil society orgs can use recently acquired data rights as new paths to accountability when GenAI is used to spread mis- and disinformation in their communities.

NEW METHODS FOR OLD TRICKS

The Cybersecurity and Infrastructure Security Agency (CISA) has outlined a taxonomy of risks from GenAI in the United States during the 2024 election cycle, which may target election processes, offices, or vendors.[2] These risks are: video (text to video, deepfakes); image (text to image, AI altered image); audio (text to speech, voice cloning); and lastly, text (text to text, generated by large language models, or LLM).

In addition, Wired.com has started a database of GenAI content in the 2024 US election cycle. As of writing, this database contains 15 examples of various image, audio, chatbot, video, and text-based GenAI content that has been used or shared by political figures or official political accounts. There are more examples from the current election cycle than what are covered in Wired's database, but the database acts as a summary and cross section of the types of manipulation that are utilizing AI strategies. Reporting like this acts as context for what systemic risks discussed later in this paper look like in practice. The database examples are distributed as follows:[3] 3 image-based examples, 4 audio-based examples, 3 chatbots, 4 video examples, and 1 text-based example.

This paper first considers both the CISA framework and Wired's examples, then argues for a new understanding of GenAI in the 2024 U.S. elections: it argues that without minimizing the new and unique risks posed by GenAI, we can understand it, in part, as an extension of existing strategies from previous election cycles. This paper bridges the gap between existing conversations about mis- and disinformation and the new ones instigated by the mass availability of GenAI tools. The following sections therefore categorize CISA's taxonomy of the risks of GenAI in relation to previously documented mis- and disinformation strategies.

The CISA framework and the Wired database employ similar taxonomies of the types of content generated by AI systems. However, the CISA taxonomy has a focus on "foreign nation state actors" and "cybercriminals". The Wired database, while discussing the same types of content, primarily consists of domestic political actors using these strategies. The sections below contextualize AI tools as an extension of existing strategies used often by domestic political actors.

False Election Information Spread Through Trusted Sources and in Various Languages

The CISA taxonomy describes the following AI content as a risk to election processes: "Chatbots, AI-generated voice, or videos could be used to spread false information about time, manner, or place of voting via text, email, social media channels, or print."

It has been verified that false information about elections is being created by GenAI. For example, AP News reports that inaccurate voting information is being generated by chatbots.[4] However, the reporting on this topic focuses on the mistakes made by the GenAI, not on the ways in which this misinformative messaging may be targeted at voters by political actors.[5] While of course there is a risk when any individual treats GenAI as a trusted source for election info (and GenAI chatbots exist that claim to guide users through understanding elections and candidates), in the context of political campaigning, a message is useless if it cannot be delivered. Who is targeting this inaccurate information at voters?

In 2020, a popular new strategy among many political consultants was a form of hyper targeting called relational organizing.[6] This strategy uses data to identify a trusted member of a community and then targets that trusted community member to deliver an inaccurate message, sometimes knowingly (disinformation) and sometimes unknowingly (misinformation). This method was used in 2020 to spread false information about voting rules[7]— no GenAI required.

The lesson of relational organizing is this – effective political messaging often requires the right message and the right messenger. GenAI that is trained and fine-tuned on a specific population's vernacular[8] has potential to create effective messaging. However, GenAI does not have the ability to easily become a trusted messenger in tightly knit communities, such as those that primarily rely on encrypted messaging apps. The parallels between the strategies prominent in 2020 and the risks identified by CISA demonstrate that, while GenAI may offer new ways to create messaging, the strategies for disrupting elections often remain the same.

While there is evidence that foreign actors are using GenAI to target Americans with political messaging, it is unclear if it is more effective than other forms, either in its scale or in its ability to persuade a specific population.[9] GenAI's ability to produce or parse information at scale seems to be an advantage in some situations. For example, an article from Chatham House discusses a specific technique, known as rumor bombing,[10] that is made easier through the use of GenAI, as it relies on the mass production of specifically crafted content for messages. In addition, some political data consultants state that the sheer number of data points about voters that campaigns now hold cannot be made useful by a human, but can be leveraged by GenAIs[11] that can use this data to create targeted messages.

The question of whether GenAI is more effective at persuading particular populations is less clear. Some speculate that GenAI may be used in American elections to increase information accessibility through translation.[12] Mis- and disinformation tactics in the U.S. often use translation and taking advantage of language capabilities as a vector,[13] for non-English language communities traditionally receive less oversight[14] from Big Tech companies when

tech tools are used to target them with harmful content. (These are often the same Big Tech companies that are releasing GenAI tools to the public: Meta is an example of this.[15]) Another potential avenue for using GenAI to persuade particular populations is in the targeting of local, rather than national, politicians. While deepfakes of national figures are becoming increasingly common,[16] there are far fewer reports of AI imitation of local politicians. GenAI trained on the data of specific populations may increase this type of propaganda localization.

Eroding Trust is the Goal

Those spreading disinformation in U.S. elections often seek to sow general distrust in media and journalists:[17] the danger of GenAI disinformation does not rely on the quality of any single post, but on increasing the perception that all media is untrustworthy. As CISA notes, surveys have confirmed that the public perception of the political risks from GenAI content is as much a part of the issue as GenAI content itself, for this perception of risk is eroding the public trust in media.[18] This holds even more true when the actual risks of GenAI—such as its ability to generate hyper-targeted messaging—are overblown[19] or misrepresented by marketers.

Hype around GenAI is thus a part of this trust erosion. Propagandists rely on hype around new technologies to sow fear and to gain the trust of those in positions of political power. According to reporting from Business Insider,[20] some political actors hold that GenAI can now or will soon be able to predict public opinion; the article references a preprint research paper indicating that this is indeed possible.[21] However, without transparency and explainability[22] of the models and from campaigners using GenAI, these claims are difficult to validate. The fundamental questions here are the same as those underlying the Cambridge Analytica scandal:[23] something is wrong here, this data should not be used in this way, but what is the actual effect of this misuse, and how do we distinguish that effect from the effect of the hype around it?

According to research at the University of Chicago, the perception of manipulation by GenAI may be a bigger issue than actual microtargeting accomplished through GenAI, and the perception of manipulation may be exacerbated as a small number of powerful tech companies centralize power and control of GenAI models and how they are used and moderated.[24] As reported by Brookings,[25] GenAI may also contribute to the so-called "liar's dividend"—the ability to persuasively claim that "true information is false by relying on the "belief that the information environment is saturated with misinformation."

In addition, bias, or perceived bias, of GenAI chatbots has become a flashpoint, and new publicly available bots are closely examined for bias.[26] However, this is an extension of

existing distrust of social media companies, which frequently are accused of political bias and of manipulating their algorithms to express that bias. This extends to GenAI; just as users may fail to trust information on a social media platform because they perceive the platform to be biased, they may disbelieve actual true information, assuming instead that it is false information, created with or manipulated by GenAI.

Some efforts have been made to measure the bias and reliability of publicly available GenAI services. For example, a journalist from Fast Company queried chatbots with political questions relating to the US election cycle, seeking to assess which (if any) of the publicly available options was reliable. This is one example of a relatively common genre of political reporting this election cycle, where journalists demonstrate the biases and efficacy of various chatbots by prompting them with political questions.[27]

Another use case for GenAI is to aid in running bot networks to manipulate the algorithms of social media companies.[28] This tactic—coordinated manipulation of social media algorithms—is already a known strategy for political actors.[29] When GenAI is used to create content to manipulate not at the individual level but at the platform level by spreading many messages containing similar viewpoints, it can be seen as an extension of this existing strategy.

GenAI tools are not homogeneous, and it is currently difficult to understand whether the abilities of any of particular tool in generating content that can manipulate political discourse has been overblown. As discussed in the following section, this requires a level of transparency that is not currently accomplished through self or government regulation.

Taking Advantage of Big Tech's Ineffective Mitigation Measures and Lax Government Regulation

In response to the controversies around the use of GenAI in elections, some GenAI companies attempt to ban chatbots from answering election related questions at all.[30] However, this may contribute to the general sense of distrust engendered by GenAI (thus increasing general distrust of the media, as previously mentioned); it may also have unintended consequences, such as when GenAI chatbots, in an effort to avoid political topics, inadvertently fuel Republicans' narrative that the 2020 election was "stolen" by refusing to state that Joe Biden legitimately won the 2020 election.[31]

ChatGPT has worked to prepare for the 2024 US Presidential election by, for example, adding "attribution and links." This is a step forward. However, due to the size of the platform and the nuance and unpredictability of its results, the technology can still be used by political actors.[32] It is difficult for GenAI companies to enforce bans on political uses of their services

in practice.[33] For one thing, these policies fail to address the role of data rights (addressed in the next section), such as deletion and objection to automated decision making; they focus on the output of the model rather than how the model is created, which is at the core of the issue.

A GenAI may also provide users with false political information that the user does not know is false.[34] This is a form of misinformation. As reporting in The Verge has pointed out,[35] OpenAI's policies rely on users identifying and reporting on inaccurate content. This, too, is an existing trick deployed through new technology; there was a similar lack of transparency in existing political SMS texting in 2020 that made it difficult or impossible for voters to vet information without the help of outside reporting.[36] Again, attribution and sourcing are indeed an issue with GenAI, but they are not a new issue, for they have been part of mis- and disinformation in US elections since long before the normalization of GenAI.

To remedy this issue, OpenAI again attempts to address the content of its output, not the creation of the model; while it seeks to provide only authoritative election information[37] and to provide transparency about where the information comes from, it does not offer transparency about the creation of the model itself. It is unclear whether OpenAI's "authoritative voting information" is being used to train the model so that it returns accurate synthetic answers to political queries, or whether users are manually redirected to certain resources when they use certain keywords. (It is common for GenAIs to have filters applied to their output that are not generated by or from the model itself.) In the same way, Meta focuses on transparency of generated content,[38] not on transparency about models themselves.

Just like in previous elections cycles in 2016 and 2020, with GenAI, much of the decision making about what content is or is not allowed to be disseminated online lies in the hands of small number of people making decisions at a small number of powerful companies[39]—the companies who build GenAI tools and the companies that are used by disinformation spreaders to maintain their messaging infrastructure and reach. In some cases, such as Meta, the same companies provide both; the platforms that provide GenAI tools are the same platforms where mis- and disinformation spreads.

According to research from the Center for Media Engagement,[40] political consultants are considering using GenAI to build region-specific phone banks for voice calling. It is unclear if this will increase the scale of political phone banking, or just remove the human actors from the picture. Again, we see that this is not an entirely new strategy, but a new tool to accomplish an old strategy: these GenAI phone banks parallel the SMS phone banks that existed in 2020, which were semi-automated tools that auto-filled SMS messaging and required human actors to click the send button at a rapid pace to circumvent regulations.[41]

GenAI regional phone banks might parse bigger data sets to target people or use personalized text generated by GenAI for the messages, and might even do away with the need for human actors to personalize text and click the send button. The generation of regionalized text, voices, vernacular, and languages potentially makes these strategies more viable with smaller teams of volunteers or paid phone bankers.

One difference is that, according to analysis from Brookings,[42] AI makes the generation of content easier at scale. Twilio, one of the largest providers of automated anonymous political text messaging for the 2020 election, is already integrating a GenAI into its platform, built on OpenAI.[43] It remains unknown how much GenAI will expedite the process of creating false content, for it is possible that even at scale, human moderation and fine tuning will remain a necessary step.[44]

As demonstrated by the history of political SMS texting, political actors experimenting with new technologies understand that they don't have to be faster than U.S. regulators, just fast enough to get through an election cycle. In state-level regulatory bills, we again see the pattern emerge: these bills focus on transparency around already-created content (such as requiring disclaimers on GenAI created media) rather than on transparency around the data used to train and create models.[45]

Regulations of GenAI political campaigning should take a comprehensive approach that considers official campaigns, unofficial actors, GenAI companies whose primary clients are political actors, and general purpose models whose tools are being co opted for political purposes. For instance, even if states or the federal government regulate official campaigns' use of GenAI, there remains the question of how it will be used by PACs and dark-money organizations.[46] Often, the risk comes not from the company that created the model but the company that licenses it.[47] This is true of GenAI just as it is of the semi-automated political texting apps like Twilio that underly much SMS misinformation and disinformation: the company makes the tech, and those who use the tech can create whatever content and choose whatever targets they wish, without regulation interfering in meaningful ways.[48]

As we approach the 2024 election, many mitigation strategies for political usage of GenAI have been proposed and are being explored. Recommendations from Stanford and the University of Chicago offer insight into some potential mitigations.[49] During the elections, some civil society organizations could demand that political actors publicly pledge not to use deceptive GenAI content, and organizations that represent the political interests of minority communities can be incorporated into the building of GenAI models that target those specific communities. Campaign regulations could be changed to require political actors to be transparent about which model is being used so that affected populations seeking transparency can audit for biases by querying the model themselves.[50] While there

is little evidence that those building or using GenAI models in the 2024 cycle are adopting or responding to these proposed mitigations, there is one potential avenue to explore: part two of this paper explores a new path for accountability that is open to communities whose data is being used to train GenAI models: focusing on claiming and protecting their data rights.

DATA RIGHTS, OR WILL THEY RETRAIN THE MODEL?

As of this writing, 19 U.S. states have passed comprehensive privacy laws. All 19 of these laws including a right to delete one's data, and 17 contain some right against automated decision making.[51] AI-specific laws are following close behind.[52] Privacy rights and AI-related rights overlap in many places,[53] such as in the regulation of algorithmic fairness,[54] though in some places privacy laws are not sufficient in mitigating the use of AI because of the speed with which AI companies collect and incorporate data.[55]

The use of data rights to regulate AI use has some drawbacks. It is unclear whether existing disclosure requirements—the requirement that content created with GenAI be labeled for transparency—will extend to GenAI when it is used to target a voter, or require the disclosure of the specific company whose AI was used to do the targeting, including for politically focused GenAI firms, such as Votivate.[56] For example, if a political organization uses a model to generate a message, the disclosure may include the name of the organization without the name of the company who owns the model, or vice versa. Both pieces of information are necessary to effectively carry out data rights.

Data rights requests require voters and civil society organizations to know which models are being used to generate hyper-targeted content.[57] As the number of models available to the public grows, relying on self-regulation (which is already lax and narrow) by the largest providers of general purpose models becomes less viable. Currently, cheaper and cheaper AI models are being released,[58] a trend that is sometimes referred to as the "democratization" of GenAI; as cheaper models and specialized models built by political consultants become more commonplace, increased transparency can ensure that users know who to contact to assert their data rights.

Currently, though, smaller GenAI firms offer very little transparency. Firms such as Civox[59] (which was actively used to generate content for a Pennsylvania campaign) and Votivate (which, as reported by The Nation, claims to offer "high-quality individualized media aimed at moving voters to action") offer very little transparency about where their data comes from and how their proprietary AI models are trained and maintained. This also leaves open the question of how voters and organizations can request transparency and assert their data rights when smaller firms go out of business, do not reply to queries, or lack the internal infrastructure to in good faith reply to queries meaningfully. In a scenario where political

propagandists are relying on many smaller firms and models, making data deletion requests to all of them becomes less feasible. For example, as of this writing, the previously mentioned Votivate, offers a data rights form that does not mention anything about its GenAI models.[60]

However, this proliferation and fragmentation of the market does not mean that the data rights approach is not viable. Enforcement of regulation combined with the systemic use of data rights can make this approach work. First, organizations with fewer resources—the very groups most likely to need to rely on GenAI to create content—are also likely to rely on one or two of the most popular and easily available public models. These organizations may attempt to circumvent self regulation of these large models. Systemic strengthening and data rights at the level of state authorities, combined with system use by data subjects, may be an effective way to increase transparency and audit whether or not these self-regulations against political usage are being effective.

Strengthening data rights at the federal and state levels could also help to address the problem of data brokers: to assert their data rights with data brokers, users must currently reach out to many different organizations one by one.[61] This is a similar situation to a fragmented AI market, where a users must make individual requests to many different companies running smaller models. Similar strategies to those developed to help individuals use their data rights with data brokers, such as the data broker registries created in California and Vermont[62], can enable voters to understand which GenAI companies are used to target their communities with messaging. Similar registries for GenAIs used in politics will help make data rights effective as localized models become more commonplace. This would compensate for a lack of self-regulation from smaller GenAI firms, which are less likely than large firms to have any form of processing in place for data rights. For example, the company Civox mentioned earlier in this report does not offer information about privacy rights on its website.[63]

OpenAI and ChatGPT are already being openly used for political purposes, as when ChatGPT was used in Philadelphia to generate fabricated positive news stories about a sheriff.[64] And these two, being among the largest, most popular tools, are also likely to be used to facilitate cyber attacks on elections, where malicious actors iterate on publicly available tools to find what is most useful to their ends. This further bolsters the idea that these models are a point at which data rights could be asserted to achieve accountability.[65] These companies cannot be relied upon for effective self-regulation. Communities that are being effected by AI generated political messaging can use data rights to systemically hold them accountable and push for transparency. State level authorities can employ the new privacy laws' enforcement mechanisms to ensure the responses from these large companies are meaningful, and this will set the standard for the smaller firms creating localized models. Access to data is already

becoming a battleground that intersects with the politics of GenAI use for both large scale models[66] and models developed specifically for politics.

Political organizations that use data for hypertargeting have long played a game of keep away with transparency and user rights. It is very difficult to get data from data brokers or from centralized databases that are controlled by an individual party, and even when a user can identify the source of a message, they are unable to identify where or how their data was used to inform it. There is a parallel between this and AI generated messaging targeted at a specific group. Communities are already self organizing to counter mis- and disinformation[67] on platforms that are vulnerable to chatbots, and these communities are advised to enlist legal support [68] to also mitigate GenAI related harms.

The assertion of deletion rights depends on an increased level of transparency from both the providers of GenAI tools and the political actors who use the tools. For example, both Meta and OpenAI already provide self service tools to request the deletion of data from training models. However, both of these companies employ a very narrow view of what can be deleted. Both companies require users to provide both the prompt and the output that generated their personal data. This is an insufficient and non compliant approach for several reasons. First, people should be able to opt out of having their data used to train models without concrete evidence that the model will output their identifiable personal data. Second, requiring a user to figure out how to prompt the model to produce their personal data is onerous. Just because an individual cannot construct the proper prompt does not mean that it is impossible to do so. This approach thus puts an unfair burden on a user, who may not even know what kind of data for which to prompt for. Third, in this scenario, if the user is not the one who queried the model, then they cannot request that their data be deleted. This scenario is particularly problematic for the use of GenAI in politics, because it is the campaigners who are using and potentially generating personal data, not the voters.

For these and other reasons, collective action around data rights may be more feasible for civil society organizations attempting to hold GenAI accountable within the US presidential election cycle than individual requests. Collective actions and collective deletion requests may detour around these companies' purposefully difficult request portals and policies.

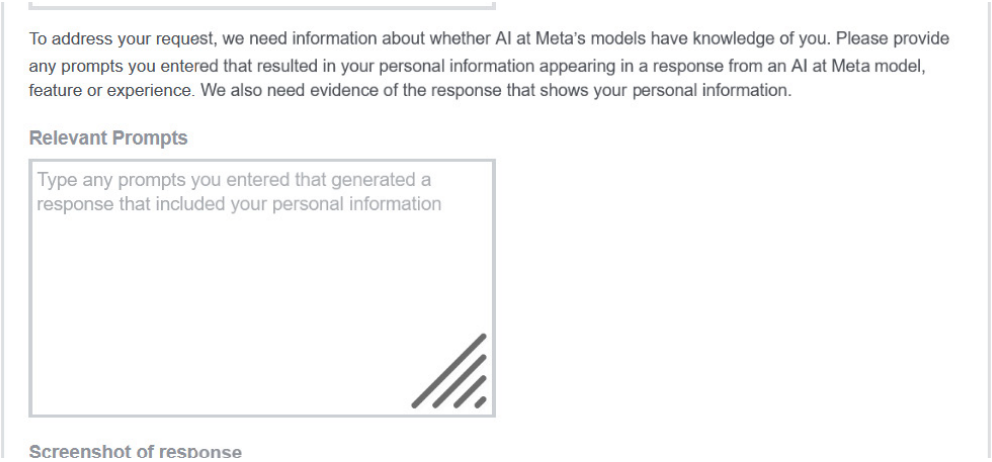

Figure 1: Meta requires the ability to query their models in order to use data rights.

Collective assertion of their data rights can enable communities to object to their data being used to generate and target personalized harmful messages in their vernacular.

According to the Stanford University report "Regulating AI Through Data Privacy," "consumer rights to delete and correct must extend to data embedded within such models in order to be meaningful."[69] This report describes how deletion rights can be implemented without retraining entire models. In addition, some state privacy laws contain provisions allowing organizations to assert privacy rights on a user's behalf.[70] These provisions can be leveraged by organizations in diaspora and minority communities in the United States to facilitate mass deletion requests. We might think of these organizations as what Katharine Miller of Stanford calls "data intermediaries," a collective that negotiates for the data rights of a group.[71] There is existing precedent for the use of data rights as a leverage tool in both collective governance and in attempts to hold Big Tech companies accountable to vulnerable populations.[72]

CONCLUSION

In summary, GenAI creates new challenges for organizations that have been attempting to counter mis- and disinformation since the 2020 election cycle. However, just as GenAI has changed the landscape of mass scale political messaging, new data rights are changing the landscape of ways to fight back, providing a way for the populations most likely to be beset by hyper-targeted GenAI-created messaging to hold accountable both the Big Tech companies that produce the technology and the political campaigners who exploit it.

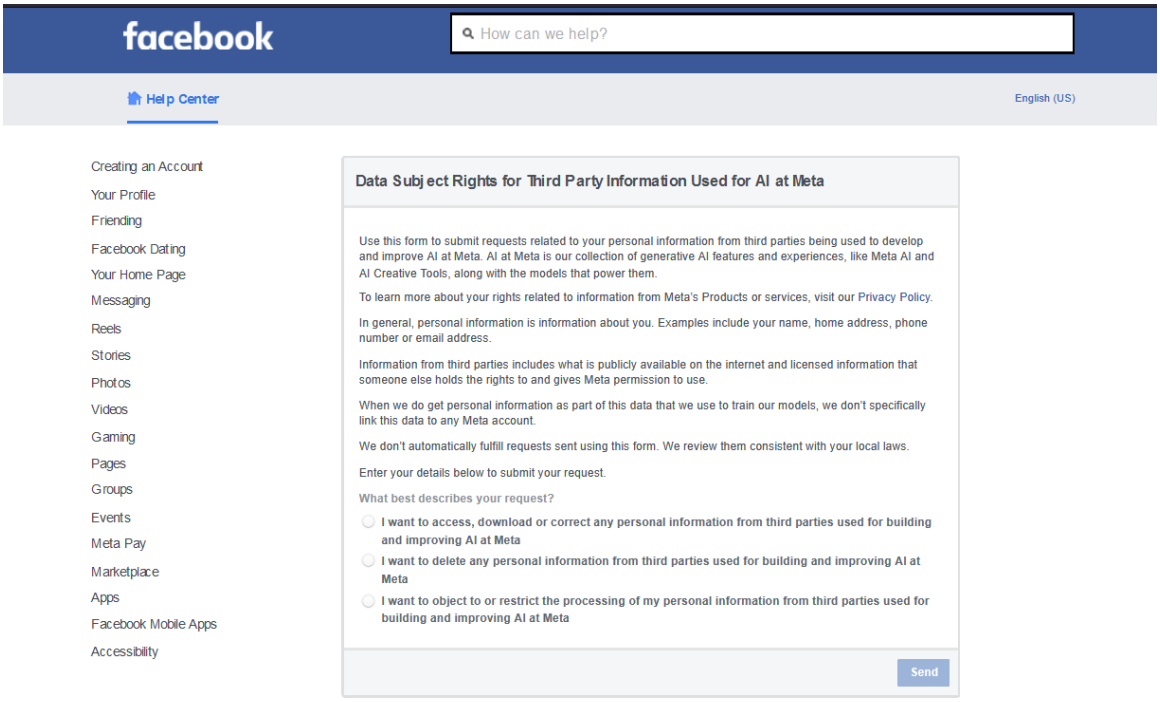

Figure 2: Meta's portal to request the deletion of Third Party Information from its GenAI tools

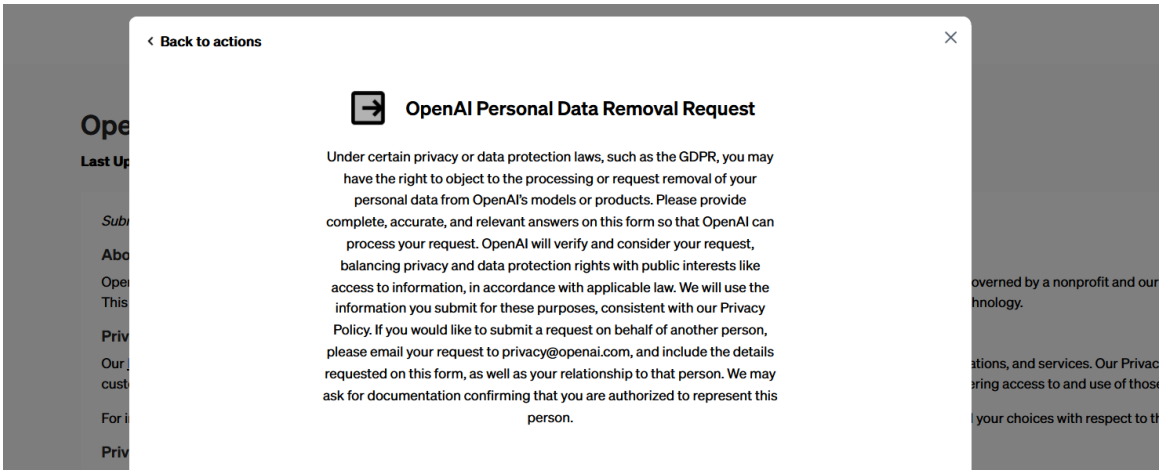

Figure 3: OpenAI's Personal Data Removal Request form

ACKNOWLEDGEMENTS

This report is part of a series commissioned by editors Dr. Inga Trauthig and Dr. Samuel Woolley. The series compiles short investigations into the role of generative artificial intelligence (GenAI) before, during and after several key elections in 2024: national elections in India, Mexico, South Africa, the U.S. and European Elections (U.K. and French snap elections and European Parliament). Individual authors were free to choose their analytic focus depending upon the given region and context. This series adds both analyses of standing literature and empirical insights into the potential impacts of GenAI on key democratic processes. These insights are critical to groups working to sustain and advance democracies in the face of constant transformation of the digital environment and associated communication processes. The series is a project of the Propaganda Research Lab, Center for Media Engagement at The University of Texas at Austin.

Executive summaries and noteworthy highlights for each report were drafted independently by the editors Trauthig and Woolley. These summaries do not necessarily represent the views of the report authors.

The Propaganda Research Lab at UT Austin's Center for Media Engagement (CME) is supported by grants from the John S. and James L. Knight Foundation, Omidyar Network, and Open Society Foundations. Any opinions, findings, conclusions, and recommendations expressed in series are those of the authors and editors and do not reflect the views of these funding bodies.

ENDNOTES

[1] Will Douglas Heaven, "What Is AI?" MIT Technology Review, July 10, 2024, https://www.technologyreview.com/2024/07/10/1094475/what-is-artificial-intelligence-ai-definitive-guide/.

[2] Cybersecurity & Infrastructure Security Agency (CISA), "Risk in Focus: Generative A.I. and the 2024 Election Cycle," January 18, 2024, https://www.cisa.gov/resources-tools/resources/risk-focus-generative-ai-and-2024-election-cycle.

[3] Vittoria Elliott, "The WIRED AI Elections Project," Wired, May 30, 2024, https://www.wired.com/story/generative-ai-global-elections/.

[4] Garance Burke, "Chatbots' Inaccurate, Misleading Responses about US Elections Threaten to Keep Voters from Polls," Associated Press News, February 27, 2024, https://apnews.com/article/ai-chatbots-elections-artificial-intelligence-chatgpt-falsehoods-cc50dd0f3f4e7cc322c7235220fc4c69.

[5] Haley Ott and Emmet Lyons, "ChatGPT Gave Incorrect Answers to Questions about How to Vote in Battleground States," CBS News, June 25, 2024, https://www.cbsnews.com/news/chatgpt-chatbot-ai-incorrect-answers-questions-how-to-vote-battleground-states/.

[6] Pema Levy, "The Secret to Beating Trump Lies with You and Your Friends," Mother Jones, November–December 2020, https://www.motherjones.com/politics/2020/10/relational-organizing/.

[7] Jacob Gursky, Martin J. Riedl, and Samuel Woolley, "The Disinformation Threat to Diaspora Communities in Encrypted Chat Apps," Brookings, March 19, 2021, https://www.brookings.edu/articles/the-disinformation-threat-to-diaspora-communities-in-encrypted-chat-apps/.

[8] Zelly Martin, Dean Jackson, Inga Kristina Trauthig, and Samuel C. Woolley, "Political Machines: Understanding the Role of AI in the U.S. 2024 Elections and Beyond," Center for Media Engagement, June 6, 2024, https://mediaengagement.org/research/generative-ai-elections-and-beyond/.

[9] Elise Thomas, "Pro-CCP 'Spamouflage' Network Pivoting to Focus on US Presidential Election," Institute for Strategic Dialogue, February 15, 2024, Digital Dispatches, https://www.isdglobal.org/digital_dispatches/pro-ccp-spamouflage-net-work-focuses-on-us-election/.

[10] Helen Fitzwilliam, "How AI Could Sway Voters in 2024's Big Elections," Chatham House, September 29, 2023, https://www.chathamhouse.org/publications/the-world-today/2023-10/how-ai-could-sway-voters-2024s-big-elections/.

[11] Donie O'Sullivan and Yahya Abou-Ghazala, "The AI Political Campaign Is Here," CNN, May 3, 2023, https://www.cnn.com/2023/05/02/politics/ai-election-ads-2024/index.html.

[12] Rachel Curry, "How 2024 Presidential Candidates Are Using AI inside Their Election Campaigns," CNBC, December 17, 2023, https://www.cnbc.com/2023/12/17/how-2024-presidential-candidates-are-using-ai-in-election-campaigns.html.

[13] Gretel Kahn, "AI, Lies and Conspiracy Theories: How Latinos Became a Key Target for Misinformation in the US Election," Reuters Institute for the Study of Journalism, March 25, 2024, https://reutersinstitute.politics.ox.ac.uk/news/ai-lies-and-conspiracy-theories-how-latinos-become-key-target-misinformation-us-election.

[14] Gabriel R. Sanchez and Carly Bennett, "Why Spanish-Language Mis- and Disinformation Is a Huge Issue in 2022," Brookings, November 4, 2022, https://www.brookings.edu/articles/why-spanish-language-mis-and-disinformation-is-a-huge-issue-in-2022/.

[15] Will Knight, "Meta's New Llama 3.1 AI Model Is Free, Powerful, and Risky," Wired, July 23, 2024, https://www.wired.com/story/meta-ai-llama-3/.

[16] Reis Thebault, "Deepfake Kari Lake Video Shows Coming Chaos of AI in Elections," March 24, 2024, https://www.washingtonpost.com/politics/2024/03/24/kari-lake-deepfake/.

[17] Hugh Jones, "Will ChatGPT Influence the 2024 Election?" *Newsweek*, March 17, 2023, https://www.newsweek.com/will-chatgpt-influence-2024-election-opinion-1787435.

[18] Lucia Mackenzie and Mark Scott, "How People View AI, Disinformation and Elections — in Charts," Politico, April 16, 2024, https://www.politico.eu/article/people-view-ai-disinformation-perception-elections-charts-openai-chatgpt/.

[19] Aden Barton, "AI and Democracy," *Harvard Magazine*, October 13, 2023, https://www.harvardmagazine.com/node/84864.

[20] Hasan Chowdhury, "The Next Election Can't Handle a World Powered by ChatGPT," *Business Insider,* May 18, 2023, https://www.businessinsider.com/ai-and-chatgpt-pose-risks-for-2024-presidential-election-2023-5.

[21] Chu, Eric, Jacob Andreas, Stephen Ansolabehere, and Deb Roy, "Language Models Trained on Media Diets Can Predict Public Opinion." Preprint, arXiv, March 28, 2023. https://doi.org/10.48550/arXiv.2303.16779.

[22] P. Jonathon Phillips, Carina A. Hahn, Peter C. Fontana, Amy N. Yates, Kristen Greene, David A. Broniatowski, and Mark A. Przybocki, "Four Principles of Explainable Artificial Intelligence," National Institute of Standards and Technology, September 2021, 9, https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8312.pdf?trk=public_post_comment-text

[23] Matt Weinberger, "Facebook Just Gave Us a New Kind of Scandal — and It's Going to Get Weirder from Here," *Business Insider* Nederland, November 11, 2017, https://www.businessinsider.nl/facebook-cambridge-analytica-artificial-intelligence-augmented-reality-2018-3/.

[24] Galen Druke, "2024 Is the 1st 'AI Election.' What Does That Mean?" *ABC News*, December 1, 2023, https://abcnews.go.com/538/2024-1st-ai-election/story?id=105312571.

[25] Zeve Sanderson, Solomon Messing, and Joshua A. Tucker, "Misunderstood Mechanics: How AI, TikTok, and the Liar's Dividend Might Affect the 2024 Elections," Brookings, January 2, 2024, https://www.brookings.edu/articles/misunderstood-mechanics-how-ai-tiktok-and-the-liars-dividend-might-affect-the-2024-elections/.

[26] Will Knight, "My Surprisingly Unbiased Week With Elon Musk's 'Politically Biased' Chatbot," Wired, December 24, 2023, https://www.wired.com/story/fast-forward-elon-musk-grok-political-bias-chatbot/.

[27] Theo Burman and Daniel Orton, "Who Would Best Replace Joe Biden? We Asked ChatGPT," *Newsweek*, July 13, 2024, https://www.newsweek.com/joe-biden-replace-chatgpt-us-election-2024-donald-trump-ai-tool-1923961.

[28] The Economist, "AI Will Change American Elections, but Not in the Obvious Way," August 31, 2023, https://www.economist.com/united-states/2023/08/31/ai-will-change-american-elections-but-not-in-the-obvious-way.

[29] Maurice Jakesch, Kiran Garimella, Dean Eckles, and Mor Naaman, "Trend Alert: A Cross-platform Organization Manipulated Twitter Trends in the Indian General Election," in *Proceedings of the ACM on Human-computer Interaction* 5, no. CSCW2 (2021): 1-19.

[30] Sarah Taaffe-Maguire, "OpenAI's ChatGPT Stops Answering Election Questions after Giving Wrong Answers," Sky News, June 6, 2024, https://news.sky.com/story/openais-chatgpt-stops-answering-questions-on-election-results-after-wrong-answers-13148929.

[31] David Gilbert, "Google's and Microsoft's AI Chatbots Refuse to Say Who Won the 2020 US Election," Wired, June 7, 2024, https://www.wired.com/story/google-and-microsofts-chatbots-refuse-election-questions/.

[32] Sara Fischer, "OpenAI Unveils Plans for Tackling Abuse Ahead of 2024 Elections," Axios, January 15, 2024, https://www.axios.com/2024/01/15/chatgpt-openai-2024-elections.

[33] Zelly Martin, Dean Jackson, Inga Kristina Trauthig, and Samuel C. Woolley, "Political Machines: Understanding the Role of AI in the U.S. 2024 Elections and Beyond," Center for Media Engagement, June 6, 2024, https://mediaengagement.org/research/generative-ai-elections-and-beyond/.

[34] Shannon Bond, "Tech Giants Pledge Action against Deceptive AI in Elections," NPR, February 16, 2024, sec. Untangling Disinformation, https://www.npr.org/2024/02/16/1232001889/ai-deepfakes-election-tech-accord.

[35] Alex Cranz, "Here's OpenAI's Big Plan to Combat Election Misinformation," The Verge, January 15, 2024, https://www.theverge.com/2024/1/15/24039333/openai-chatgpt-dalle-ai-2024-election-misinformation-plan.

[36] Tony Romm and Isaac Stanley-Beckre, "Trump-Associated Firm Tied to Unmarked Texts Urging Vote Protests in Philadelphia," The *Washington Post*, November 6, 2020, https://www.washingtonpost.com/technology/2020/11/06/trump-text-messages-philadelphia/.

[37] OpenAI, "How OpenAI Is Approaching 2024 Worldwide Elections," OpenAI, January 15, 2024, https://openai.com/index/how-openai-is-approaching-2024-worldwide-elections/.

[38] Nick Clegg, "How Meta Is Planning for Elections in 2024," Meta (blog), November 29, 2023, https://about.fb.com/news/2023/11/how-meta-is-planning-for-elections-in-2024/.

[39] Rishi Iyengar, "What AI Will Do to Elections," Foreign Policy (blog), August 7, 2024, https://foreignpolicy.com/2024/01/03/2024-elections-ai-tech-social-media-disinformation/.

[40] Martin, Jackson, Trauthig, and Woolley, "Political Machines."

[41] Katlyn Glover, Jacob Gursky, Katie Joseff, and Samuel C. Woolley. "Peer-to-Peer Texting and the 2020 U.S. Election: Hidden Messages and Intimate Politics," University of Texas at Austin Center for Media Engagement, October 27, 2020, https://mediaengagement.org/research/peer-to-peer-texting-and-the-2020-election/.

[42] Darrell M. West, "How AI Will Transform the 2024 Elections," Brookings, May 3, 2023, https://www.brookings.edu/articles/how-ai-will-transform-the-2024-elections/.

[43] Twilio, "Twilio To Deliver Customer-Aware Generative AI Through New OpenAI Integration." Twilio, August 3, 2023, https://www.twilio.com/en-us/press/releases/twilio-to-deliver-customer-aware-generative-ai-through-new-opena.

[44] The Economist, "How Worried Should You Be about AI Disrupting Elections?" August 31, 2023, https://www.economist.com/leaders/2023/08/31/how-artificial-intelligence-will-affect-the-elections-of-2024.

[45] Shannon Bond, "AI Fakes Raise Election Risks as Lawmakers and Tech Companies Scramble to Catch Up," NPR, February 8, 2024, sec. Elections, https://www.npr.org/2024/02/08/1229641751/ai-deepfakes-election-risks-lawmakers-tech-companies-artificial-intelligence; Adam Edelman, "States Turn Their Attention to Regulating AI and Deepfakes as 2024 Kicks Off," NBC News, January 25, 2024, https://www.nbcnews.com/politics/states-turn-attention-regulating-ai-deepfakes-2024-rcna135122.

[46] Lauren Camera, "Artificial Intelligence Brings 'Nightmare' Scenario to 2024 Presidential Campaign Analysts," U.S. News, July 7, 2023, https://www.usnews.com/news/the-report/articles/2023-07-07/artificial-intelligence-brings-nightmare-scenario-to-2024-presidential-campaign-analysts.

[47] Panditharatne, Mekela. "The Election Year Risks of AI." TIME, April 10, 2024. https://time.com/6965299/risks-ai-elections/.

[48] Katlyn Glover, Jacob Gursky, Katie Joseff, and Samuel C. Woolley, "Peer-to-Peer Texting and the 2020 U.S. Election: Hidden Messages and Intimate Politics," University of Texas at Austin Center for Media Engagement, October 27, 2020, https://mediaengagement.org/research/peer-to-peer-texting-and-the-2020-election/; Katie Joseff, Jacob Gursky, and Samuel Woolley, "Texts From Politicians Could Be More Dangerous Than Ever," Wired, April, 2020, https://www.wired.com/story/opinion-texts-from-politicians-could-be-more-dangerous-than-ever/.

[49] Ethan Bueno de Mesquita, Brandice Canes-Wrone, B. Hall Andrew, Kristian Lum, Gregory J. Martin, and Yamil Ricardo Velez, "Preparing for Generative AI in the 2024 Election: Recommendations and Best Practices Based on Academic Research," Stanford Graduate School of Business and the University of Chicago Harris School of Public Policy, November 23, accessed August 4, 2024, https://www.gsb.stanford.edu/faculty-research/publications/preparing-generative-ai-2024-election-recommendations-best-practices.

[50] Jeremy Baum, and John Villasenor, "The Politics of AI: ChatGPT and Political Bias," Brookings, May 8, 2023, https://www.brookings.edu/articles/the-politics-of-ai-chatgpt-and-political-bias/.

[51] Andrew Folks, "US State Privacy Legislation Tracker," International Association of Privacy Professionals, July 22, 2024, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

[52] Cobun Zweifel-Keegan, "US State AI Governance Legislation Tracker," International Association of Privacy Professionals, June 25, 2024, https://iapp.org/resources/article/us-state-ai-governance-legislation-tracker/.

[53] Cameron F. Kerry, "Protecting Privacy in an AI-Driven World," Brookings, February 10, 2020, https://www.brookings.edu/articles/protecting-privacy-in-an-ai-driven-world/.

[54] Cameron F. Kerry, "How Privacy Legislation Can Help Address AI," Brookings, July 7, 2023, https://www.brookings.edu/articles/how-privacy-legislation-can-help-address-ai/.

[55] Jennifer King and Caroline Meinhardt, "Rethinking Privacy in the AI Era: Policy Provocations for a Data-Centric World," Stanford University Human-Centered Artificial Intelligence, February 22, 2024, https://hai.stanford.edu/white-paper-rethinking-privacy-ai-era-policy-provocations-data-centric-world.

[56] Micah L. Sifry, "How AI Is Transforming the Way Political Campaigns Work," *The Nation*, February 1, 2024, https://www.thenation.com/?post_type=article&p=483429.

[57] According to the *Washington Post*, GenAI is already being used to generate content targeted at specific populations; see Cat Zakrzewski, "ChatGPT Breaks Its Own Rules on Political Messages," The *Washington Post*, August 28, 2023, https://www.washingtonpost.com/technology/2023/08/28/ai-2024-election-campaigns-disinformation-ads/.

[58] Alex Perry, "ChatGPT Maker OpenAI Goes Smaller and Cheaper With New AI Tech," *The Wall Street Journal*, July 18, 2024, https://www.wsj.com/tech/ai/chatgpt-maker-goes-smaller-and-cheaper-with-new-ai-tech-0cbcff84.

[59] Martin, Jackson, Trauthig, and Woolley, "Political Machines." Reuters. "Meet Ashley, the First AI Political Campaign Caller," Youtube, N.d., https://www.youtube.com/watch?v=jVrnMZnDfx0. Anna Tong and Helen Coser, "Meet Ashley, the world's first AI-powered political campaign caller", Reuters, 16 December 2023, https://www.reuters.com/technology/meet-ashley-worlds-first-ai-powered-political-campaign-caller-2023-12-12/.

[60] Votivate, "Data subject access request form." Last viewed 25 September 2024, https://app.websitepolicies.com/dsar/view/v20wpba.

[61] Federal Trade Commission, "Data Brokers: A Call For Transparency and Accountability: A Report of the Federal Trade Commission (May 2014)," Federal Trade Commission, May 27, 2014, https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014.

[62] California Department of Justic Office of the Attorney General, "Data Broker Registry", Last viewed 12 September 2024, https://oag.ca.gov/data-brokers; Vermont Secretary of State Business Services Devision, "Data Brokers", Last viewed 12 September 2024, https://sos.vermont.gov/corporations/other-services/data-brokers/.

[63] Civox, "Civox: Reach More. Connect Better.", Last viewed 12 Sepetmber 2024, https://www.civox.com/.

[64] MaryClaire Dale and Ali Swenson, "Philly Sheriff's Campaign Takes down Bogus 'News' Stories Posted to Site That Were Generated by AI," WHYY (blog), February 5, 2024, https://whyy.org/articles/philly-sheriffs-campaign-takes-down-bogus-news-stories-posted-to-site-that-were-generated-by-ai/.

[65] Vera Bergengruen, "Hackers Could Use ChatGPT to Target 2024 Elections," *Time*, February 21, 2024, https://time.com/6717129/hackers-ai-2024-elections/.

[66] Kevin Roose, "The Data That Powers A.I. Is Disappearing Fast," The *New York Times*, July 19, 2024, sec. Technology, https://www.nytimes.com/2024/07/19/technology/ai-data-restrictions.html.

[67] Joao V. S. Ozawa, Samuel Woolley, and Josephine Lukito, "Taking the Power Back: How Diaspora Community Organizations Are Fighting Misinformation Spread on Encrypted Messaging Apps," Harvard Kennedy School Misinformation Review, June 12, 2024, https://doi.org/10.37016/mr-2020-146.

[68] Harris, Norden, Praetz, and Howard. "How Election Officials Can Identify, Prepare for, and Respond to AI Threats."

[69] Eli MacKinnon and Jennifer King, "Regulating AI Through Data Privacy," Stanford University Human-Centered Artificial Intelligence, January 11, 2022, https://hai.stanford.edu/news/regulating-ai-through-data-privacy.

[70] "California Consumer Privacy Act (CCPA)," State of California Department of Justice, Office of the Attorney General, March 13, 2024, https://oag.ca.gov/privacy/ccpa.

[71] Katharine Miller, "Privacy in an AI Era: How Do We Protect Our Personal Information?" Stanford University Human-Centered Artificial Intelligence, March 18, 2024, https://hai.stanford.edu/news/privacy-ai-era-how-do-we-protect-our-personal-information.

[72] Jessica Pidoux, Paul-Olivier Dehaye, and Jacob Gursky, "Governing Work through Personal Data: The Case of Uber Drivers in Geneva," *First Monday* 29, no. 2 (February 2024), https://doi.org/10.5210/fm.v29i2.13576.