

Social Media Lies: User's Private Information and the Spread of Misinformation and Disinformation

Christina Roberts, Keith Ludwick, Ph.D.

ABSTRACT

Social media is becoming more and more integrated with everyday life. Individuals around the globe use social media to stay connected with family and friends, conduct business, market products, run political campaigns, and a myriad of other activities. Unfortunately, the integration of social media with daily life is becoming so ubiquitous as to numb users to the possibility that the companies controlling our access to social media might be using the private information gleaned from individual users to help spread misinformation/disinformation (MIDI). This paper asks: How does the use of private information by social media companies lead to the spread of misinformation or disinformation? Using a Grounded Theory approach and examining three instances of social media companies accessing users' private information (Cambridge Analytica, Russian interference in the 2016 U.S. Presidential Election, and the January 6th insurrection at the U.S. Capitol), this paper interprets these incidents to determine the extent of culpability of the company's use of private user information. The findings indicate a strong link between these companies' private, personal information use and the spread of MIDI. The study finishes with policy recommendations and suggestions for future research.

Keywords: social media; disinformation; cognitive warfare; advertising; consent

Mentiras en las redes sociales: información privada del usuario y difusión de información errónea y desinformación

RESUMEN

Las redes sociales están cada vez más integradas en la vida cotidiana. Personas de todo el mundo utilizan las redes sociales para mantenerse en contacto con familiares y amigos, realizar negocios, comercializar productos, realizar campañas políticas y muchas otras

actividades. Desafortunadamente, la integración de las redes sociales con la vida diaria se está volviendo tan omnipresente que insensibiliza a los usuarios ante la posibilidad de que las empresas que controlan nuestro acceso a las redes sociales puedan estar utilizando la información privada obtenida de usuarios individuales para ayudar a difundir información errónea/desinformación (MIDI). Este artículo pregunta: ¿Cómo el uso de información privada por parte de las empresas de redes sociales conduce a la difusión de información errónea o desinformación? Utilizando un enfoque de teoría fundamentada y examinando tres casos de empresas de redes sociales que acceden a información privada de los usuarios (Cambridge Analytica, la interferencia rusa en las elecciones presidenciales de EE. UU. de 2016 y la insurrección del 6 de enero en el Capitolio de EE. UU.), este artículo interpreta estos incidentes para determinar el grado de culpabilidad del uso por parte de la empresa de información privada del usuario. Los hallazgos indican un fuerte vínculo entre el uso de información personal y privada de estas empresas y la difusión de MIDI. El estudio finaliza con recomendaciones de políticas y sugerencias para futuras investigaciones.

Palabras clave: redes sociales; desinformación; guerra cognitiva; publicidad; consentir

社媒谎言：用户私人信息与错误及虚假信息的传播

摘要

社交媒体越来越融入日常生活。全球各地，人们使用社交媒体与家人和朋友保持联系、开展业务、营销产品、开展政治活动以及进行无数其他活动。不幸的是，社交媒体与日常生活的融合变得如此普遍，以至于用户对一种可能性变得麻木，即控制我们访问社交媒体的公司可能会利用从个人用户收集的私人信息来帮助传播错误信息/虚假信息(MIDI)。本文的研究问题是：社交媒体公司对私人信息的使用如何导致错误信息或虚假信息的传播？通过使用扎根理论法并研究社交媒体公司获取用户私人信息的三个实例（“剑桥分析”事件、俄罗斯干预2016年美国总统选举、以及1·6美国国会暴乱事件），本文对这些事件进行了诠释，以确定公司使用私人用户信息一事的责任程度。分析结果表明，这些公司对个人信息的使用与MIDI的传播之间存在密切联系。本研究最后提出了政策建议和对未来研究的建议。

关键词：社交媒体，虚假信息，认知战，广告，同意

Introduction

The meteoric rise of social media into the fabric of global society over the past twenty years has been unprecedented. Not since the internet itself has technology become as quickly intertwined with daily life. The benefits of social media are well documented: from connecting friends, organizing advocacy groups, and communicating with victims of disaster, to forums to share information and listing employment opportunities, social media offers a myriad of ways to help society (George, Rovniak, and Krashnewski 2013; Houston et al. 2015; Sethi 2013). However, there is a darker side: scammers, misinformation/disinformation (called MIDI) campaigns from individuals and nation-states, as well other criminals all take advantage of the unregulated and ubiquitous nature of social media platforms.

Nevertheless, while these nefarious individuals taking advantage of social media represent a threat to the everyday user, a bigger threat is just starting to come to light, that of the social media conglomerates and corporations themselves. March through October of 2021, the U.S. Congress held the first hearings of its kind investigating the potential of social media companies using their respective platforms to gather private information on customers, allow the spread of MIDI, and other practices for which their users might be unaware (“Disinformation Nation: Social Media’s Role in Promoting Extremism and Misinformation” 2021). From their inception, most of the companies

(e.g., Facebook—now Meta—, Twitter, YouTube) took a “hands-off” approach with the argument that social media were platforms of free speech, and all voices should be heard (Brannon 2018). But that began to change somewhat in the 2010s as social media became platforms for hate speech and radicalization for groups such as white supremacists and Islamic terrorists (Asongu and Orim 2019).

Cries from politicians on both sides of the aisle began to surface that social media companies were supporting these violent organizations with their absence of censorship. Facebook CEO Mark Zuckerberg famously responded that social media’s role should be dedicated to the free expression of ideas (Abril 2019). These shouts from politicians and the public were amplified during the COVID pandemic, when Facebook and other platforms were accused of either spreading MIDI about vaccines or squashing alternative views on the efficacy of vaccines or other medicines (Cascini et al. 2022). During 2019-2021 in particular, the role of social media platforms and the spread of (at worst) deliberately fabricated information or (at best) incorrect information innocently passed along started to come more into question.

The issue of social media companies’ responsibility to help stop the spread of MIDI has yet to resolve, nor is it likely to be fully addressed in the near term. Whether self-management by the companies will come into play or by government regulation will offer changes remains to be seen; however, the fact that these social media con-

glomerates play *some* role in spreading MIDI is undeniable. How these companies attract and keep users staring at computer screens and mobile phones is often a closely guarded secret as it relies on finely tuned algorithms that continue to evolve with the sole purpose of keeping users glued to their electronic devices. While it varies somewhat from company to company, the end result is that if users take part in social media platforms, their hosts subject them to advertising specifically targeted to users' needs or wants (Brannon 2018). By feeding users information that incentivizes them to keep viewing similar information, social media companies continue to generate revenue.

The other part of this model is the collection of personal user information. Few people read the ubiquitous "Terms and Agreements" page when downloading a social media app, but buried in the text is the acknowledgment that all activity conducted by a user while using an application is captured and stored (Thompson 2015). While things like names, dates, and photos seem obvious, many of today's users would be shocked to know that social media companies capture minute granular information such as how long a user stays on a particular story or video, the content that they "like" or comment on, the type of cell phone they are using, and time of day when browsing through various stories/postings (Lee and Willett 2021). This private information is captured, analyzed, and often used for targeting advertising, algorithm fine-tuning, or possibly even sold to other companies (Lee and Willett 2021)

Following this line of thinking, it stands to reason that personal user information gathered by social media companies is somehow, at least partially, responsible for the spread of MIDI. This leads to the query addressed in this paper, how does the use of private information by social media companies lead to the spread of misinformation or disinformation? Ultimately, this study hypothesizes that social media companies use of private information has a significant and measurable impact on the spread of disinformation and misinformation due to targeting algorithms and social media companies' financial incentives.

Purpose Statement

This research aims to bring attention to the growing problem of disinformation and misinformation being spread by social media companies use of customers' personal and private information. It is presumed that the spread of MIDI is universally acknowledged to be a negative consequence of the growth of social media over the past decade. What current research has not addressed is how companies are using individuals' private information to help support the spread of MIDI. Investigations into how this occurs, and the ramifications of the use of private information for the spread of "bad" information, will ultimately help academics further understand the far-reaching impact of the use of private information as well as aid policymakers in possible regulatory approaches to help stem the rising tide of a possible increase in spreading MIDI

by all types of individuals, whether their motives are criminal or to influence nation-states.

Consider Facebook's role in the spread of antivaccine rhetoric. Researchers from a U.S.-based human rights nonprofit organization ran a two-day test with brand new Facebook accounts to see how quickly Facebook's algorithm sent them down an antivaccine "rabbit hole" (Avaaz 2021). One account searched for the word "vaccine" and liked pages recommended to the account, including antivaccine content, while the other liked a single well-known page that shared antivaccine content (2021). In both cases, the researchers found that Facebook's "you may also like" recommendations included antivaccine content marked with Facebook's warning label for misinformation about COVID-19 or vaccines (2021). During the two-day course of the research, Facebook recommended over 109 antivaccine pages, with a total of 1.4 million followers to the two accounts (2021). This small test demonstrates the concerning pattern Facebook has of promoting disinformation and misinformation to raise the engagement numbers and increase advertising revenue.

As another example involving antivaccine rhetoric, the Center for Countering Digital Hate (CCDH) found that over 65% of the disinformation about COVID vaccines seen on Twitter and Facebook came from what they coined "the disinformation dozen" (CCDH 2021). Previous research found that social media platforms consistent-

ly failed to act on 95% of COVID and vaccine disinformation reported to the platforms (2021). This includes Facebook's failure to remove posts sharing content from the Disinformation Dozen, such as YouTube videos. As of July 2021, half of the YouTube channels identified by the CCDH were still available, searchable, and posting more content (De Vynck and Lerman 2021). The failure to act on known disinformation indicates the platforms lack significant incentives to remove such information.

Literature Review

Research into social media and its impact on culture, community, and society is nascent but growing rapidly. Entire journals are now dedicated to investigating social media and its impact on the psychological, sociological, cultural, and political aspects of global society (e.g., see *Social Media + Society*, *Journal of Digital & Social Media Marketing*, and *Journal of Social Media and Society*). This blossoming field of inquiry is currently "finding its way" toward consensus on various issues, including the psychological impact of social media on adolescents (Smith, Leonis, and Anandavalli 2021), the use of social media in intelligence/military operations (Sufi and Alsulami 2022), and business development (Tourani 2022). While these various topics are relevant, because of the broad spectrum of academic discourse available, it is necessary to narrow the literature down accordingly; therefore, the research posed by this paper will focus on social media and the intersection between private in-

formation and its use in the spread of MIDI by companies.

The literature surrounding the specific aspects of privacy, social media, and MIDI is broad. However, this study has three themes of interest: personal information privacy, MIDI, and fact-checking within social media. While the academic debate is still ongoing regarding these themes, some thoughts can be generalized.

Personal information/Privacy

As users scroll through Facebook, they can reshare content, create new posts with text or images, react to posts using emojis, “like” or “dislike” postings, leave comments, or send messages to other users (Franz et al. 2019). Each of these actions creates data (2019). Data includes three types: data the user gives voluntarily, purchased data (from a data broker or other organization), and auto-generated data like user analytics (psychological profiles created from what a user interacts with or quizzes they take) (Unger 2020). Unger takes the approach that the absence of personal data privacy protection is the “root cause” of MIDI (Unger 2020, 309). He argues that there is a systematic effort, particularly in political campaigns, to spread MIDI based on the lack of data privacy protection (Unger 2020).

Data privatization may offer different levels of anonymity to varying degrees of success. In Ghazaleh Beigi’s Ph.D. dissertation, she concurs to an extent with Unger but draws out a different conundrum, that of privacy vs. utility (Beigi 2020). She used several meth-

ods to anonymize a set of social media users’ data. Despite anonymizing the structural and textual aspects of a social media data set, the Athd-Improved algorithm reidentified at least 56% of the users in the anonymized dataset (Beigi 2020). This research demonstrates a lack of ability to successfully anonymize to the level needed to maintain privacy and utility. This leads to the question of whether users understand the value of their data or the need for data privacy.

A 2019 survey of 2,416 Americans found that the median consumer would pay only \$5 a month for data privacy but would want an \$80 purchase price before being willing to share that data (Winegar and Sunstein 2019). The researchers surmised that the high disparity between “willingness to pay” (\$5) and “willingness to accept” (\$80) illustrates a significant lack of understanding, on the consumers’ behalf, about the worth of their data privacy (2019). This disparity constructs the current paradox of consumers valuing their privacy when offered to them but showing a lack of inclination to add privacy to their budgets.

A survey of 530 university respondents by Gary Hunter and Steven Taylor found that the more people value anonymity, the more likely they spend time on social media. Although, respondents who particularly valued seclusion and privacy spent less time on social media (Hunter and Taylor 2019). While this survey was small, it may predict similar patterns within the general population. The next question is whether options exist for those valuing priva-

cy to limit the use of their data by others effectively.

Misinformation and Disinformation

Misinformation is false, erroneous, or incorrect knowledge or evidence; actors spread misinformation due to mistakes, errors, or false beliefs in good faith (Wilczek 2020). Disinformation poses as a more nefarious cousin to misinformation, where malicious actors intentionally spread malicious information to cause harm or achieve objectives (Wilczek 2020; Baptist and Gluck 2021). Disinformation consists of everything from false stories and deceptive advertising to government propaganda websites impersonating more reputable information sources (Goldstein 2021; Fallis 2015). Disinformation is deliberate, whereas misinformation stems from incorrect beliefs or mildly obscured truths (Goldstein 2021; Li and Li 2013). For example, a state-sponsored messaging campaign to promote falsehoods about vaccine harm would constitute disinformation, but in misinformation, a person would share a meme from the disinformation campaign in good faith, fully believing what they read and shared (Barnes 2021; University of Washington 2021).

Fact-Checking

Fact-checking is the effort by an organization to verify the veracity of information from sources. Fact-checkers can be in-house or contracted out and have long been a staple of traditional journalism (Cotter, DeCook, and Kanthawala 2022). In recent years, in part to

appease politicians and an ever-growing skeptical public, social media companies and other less well-known information dealers have started to employ fact-checkers to help them establish some boundaries on published information. These fact-checkers can be automated, which comes with its own set of problems.

Cotter et al. state that “...ensuring that the global public are well-informed requires assurance that platform fact-checking functions effectively and in the public’s best interest” (Cotter, DeCook, and Kanthawala 2022, 1). Generally, people think of fact-checking as a positive step in the quest for unadulterated information published in social media and other venues, but questions remain as to the standards (which vary from company to company) and intent (Cotter, DeCook, and Kanthawala 2022).

Dubois et al. take a similar approach by demonstrating how the employment of fact-checkers helps eliminate the “echo chamber” effect often seen as the root of the problem of social media (Dubois and Blank 2018). Dubois et al. further state that social media platforms generate trust for users by employing fact-checkers, but until standards are created and met, user doubts will remain (Dubois and Blank 2018).

Gaps

As mentioned earlier, plenty of resources and research are available exploring privacy and social media. As researchers begin to investigate the various aspects of this huge domain, they

are making progress, but large gaps in knowledge remain. Specifically missing is how the privacy of personal information is interrelated to the discussion using social media to spread dis/misinformation. This effort will address a piece of that puzzle.

Methods

To investigate “How does the use of private information by social media companies lead to the spread of disinformation or misinformation?” this paper undertakes a qualitative study utilizing Grounded Theory to examine several instances of the spread of MIDI. Because research into social media is relatively new and accepted theories are rare, Grounded Theory offers an excellent tool to help discover commonalities and develop theory. As Glaser and Strauss point out, Grounded Theory offers outstanding theory generation, especially in new and emerging fields (Glaser and Strauss 2010).

The data used by this study consists of three well-developed examples of the spread of MIDI caused by social media corporations using private information. Descriptions of each instance will begin with some general background information to inform the reader, followed by discussing the financial incentive of the company. This is important: as stated earlier, the algorithms used by social media corporations are designed to keep users on their electronic devices to generate ad revenue. More importantly, the longer an individual is on their device using a social

media application, the more personal data is generated, captured, and ultimately used by the social media corporation. Thus, intimately tying financial incentives to collecting personal information. After discussing the financial incentives, the section will conclude with a discourse of the outcomes.

The researchers collected information regarding the individual instances from a variety of sources, including mainstream news sources and recent journal articles. They then compared the different articles to ensure consistency of the information. Each instance was then reviewed numerous times, using a cyclical methodology, to tease out common themes and data points. The ultimate goal was to determine if there were some commonalities between the different instances that could demonstrate social media companies using personal information to spread MIDI. The cases consist of the Cambridge Analytica case, the Russian interference in the 2016 presidential election, and the insurrection attempt on January 6, 2020.

Cambridge Analytica

Background

The political manipulation enabled by loose data privacy in the Cambridge Analytica incident pushed users into different worlds in an extraordinary way. Cambridge Analytica worked for the Trump presidential campaign, using unique advertising theories combined with incredibly personal datasets to shape their part of his campaign strategy (Rosenberg, Confessore, and

Cadwalladr 2018). The company used the concept of “micro-targeting” to profile individual users and target ads to specific individuals based on these psychological profiles across the whole of the United States (ur Rehman 2019). The personality profile application they used had access to users’ Facebook data and data from all their connections even though none of the connections agreed to share that data (ur Rehman 2019). The process used by Cambridge Analytica involved users completing the “thisisyourdigitallife” quiz (2019). Cambridge Analytica then recorded data from the quiz, the user’s profile, and scraped the profiles of all the user’s connections (2019). At no point did this request permission or acceptance from the user’s connections for their data, taking data from up to 87 million users (2019). Cambridge Analytica targeted users with ads specific to their profile (2019). According to a previous Cambridge Analytica employee, the company based ad targeting around 253 predictions about the user’s personality (Hern 2018). Cambridge Analytica crafted these ads and messages using “dog whistles” to create ads that meant something different to each target group, swapping messages around to have one effect on person X and the opposite effect on person Y and suppress voting intentions (2018). The former employee, Christopher Wylie, also stated that Cambridge Analytica “absolutely” made use of fake news in their tactics (BBC News 2018). Because of the targeted ads created with unethically accessed personal information, one can interpret that the campaign

essentially showed the voters two different sets of facts about candidates to manipulate their votes. The MIDI came into play with the content of the ads as they preyed on specific users’ fears (as understood from the 253 data points) to show them false information with the most impact on that user (Heawood 2018; BBC News 2018; ur Rehman 2019). Cambridge Analytica presented something extra insidious by being less obvious than fake news lacking personalization (Heawood 2018). Nonetheless, Cambridge Analytica’s operation did not last forever, and the company filed for bankruptcy in spring 2018 (Confessore and Rosenberg 2018). A U.S. Senate hearing on the matter ended with an unprecedented \$5 billion fine on Facebook from the Federal Trade Commission (Hu 2020).

Financial Incentive

Although, on the surface, social media offers free connection with friends, family, and acquaintances, therein lies a strong profit motivation to connect users’ data with advertisers. In 2018, when Cambridge Analytica came to light, Facebook had a worth of over \$540 billion (ur Rehman 2019). Out of the \$85.965 billion in revenue in 2020, \$ 84.169 billion (over 97%) came from advertising (“Facebook - Financials” 2021). Based on those numbers, one can assume a significant incentive for Facebook to use data for advertising, regardless of privacy violations, since greed makes a powerful motivator (Crusius, Thierhoff, and Lange 2021). Those privacy violations ripen opportunities for

exploitation via political manipulation, as seen with Cambridge Analytica's influence on the Trump campaign.

Outcome/Responses

Responses to Cambridge Analytica varied considerably, but several surveys showed it did affect public opinions on data privacy. A small Israeli survey of 51 adults (half before and half after Cambridge Analytica) noted a shift from viewing data privacy as a commodity to trade for services in the online world or a fundamental right to something one must give up to participate in the online world and something that regulation cannot enforce (Afriat et al. 2021). Another US-based in-depth interview study of 10 undergraduate students found that although none chose to leave Facebook permanently, several reported a reduction in Facebook use (Brown 2020). A New York Times article from a few weeks before the Senate hearing interviewed several people who chose to leave Facebook permanently – a decision many users found difficult but necessary to protect their privacy (Hsu 2018). Although these three sources might have predicted an adverse change in users for Facebook, the financial disclosures show a continuously increasing profit since 2018 (“Facebook - Financials” 2021). Nevertheless, Cambridge Analytica is not the only way Facebook's use of data has encouraged false information.

Russian Exploitation of Engagement Algorithms for Election Interference

Background

During the 2016 election campaign cycle, Russian operatives used Facebook to target American voters with over 129 phony political events (Timberg and Dwoskin 2018). Probably the most interesting one Facebook exposed details about was a double rally, planned and advertised by two separately controlled Russian Facebook groups (2018). The Heart of Texas “Stop Islamization of Texas” rally at the same time and place as their planned “Save Islamic Knowledge” rally hosted by the Russian-controlled group United Muslims of America occurred on May 21, 2016 (2018). Over 12,000 people viewed one paid promotion, and 2,700 viewed the other (Bertrand 2017). Details about the event came from the Senate Intelligence Committee (2017). The Heart of Texas page garnered over 225,000 followers, allowed the group to purchase ads for their events, and had real people show up to the events before Facebook shut it down (2017).

During the 2016 election cycle, Facebook hosted more than 3,000 ads about the U.S. presidential election created and purchased by the Russian Internet Research Agency (Isaac and Shane 2017). The Internet Research Agency, or IRA, spreads Kremlin-linked disinformation and propaganda for Russia, with various political aims linked to Russian goals (Isaac and Shane 2017; Permanent Select Committee on Intel-

ligence 2018). Over 10 million people saw these ads, with 44% seen before election day and the remainder before congress requested to see the ads in 2017 (Isaac and Shane 2017). This highly coordinated, nation-state campaign demonstrates how little vetting Facebook gives to those who purchase ads from the company.

Financial incentive

The revenue generation mechanisms of social media are prone to spreading disinformation by relying on user engagement and viral content to garner revenue through advertising (O'Neil 2021; Walker, Mercea, and Bastos 2019). User engagement metrics come from the amount of time users are active on Facebook, the content they look at, and what they share, like, or comment on (Kim 2021). Facebook provides a particularly potent example of how these metrics feed into disinformation and misinformation spreading through their use of engagement algorithms. The metric of user engagement forms a particular threat because it offers financial incentives through advertising to psychologically exploit users and keep them looking at the platform — since engagement increases when users have an emotional reaction to content, the algorithm feeds users content they react to emotionally (Unger 2020). The algorithm personally curates each user's feed based on the user's viewing habits, interactions, and engagements with the platform (Oremus et al. 2021). Facebook's data collection does not stop with platform interactions either. The company uses cross site tracking to see what users purchase,

login to, view, and interact with on their browser (O'Flaherty 2021). Depending on user settings, or if they have the app on their phone, this tracking may even extend beyond the browser to cross-application tracking (2021). User settings, browser type, and whether or not users download the Facebook application can impact this part of the data collection. However, per Facebook's data use policy, the only people who can opt out of any private data processing are users protected by the European Union's General Data Protection Regulation, but these protections are unavailable to anyone else (Facebook 2022). This means all other users are subject to their data functioning as part of the engagement algorithm. Taking this data to target negative emotions appears to be the most effective method of increasing engagement. As noted by a recent Washington Post article, "The theory was simple: Posts that prompted lots of reaction emoji tended to keep users more engaged, and keeping users engaged was the key to Facebook's business" (Oremus and Merrill 2021, 2). 98% of Facebook's revenue generation in 2020 came through advertising (SEC 2021). Keeping users on the platform means they view more ads and increase revenue.

Outcome/Responses

"The company's data scientists confirmed in 2019 that posts that sparked angry reaction emoji were disproportionately likely to include misinformation, toxicity and low-quality news." (Oremus and Merrill 2021, 2). "Inducing reliance on emotion resulted

in greater belief in fake (but not real) news stories compared to a control or to inducing reliance on reason” (Martel, Pennycook, and Rand 2020, 1). As seen by these sources, anger and misinformation based on user data form the backbone of Facebook’s engagement algorithm, which is how they stay in business. Besides the examples of fake news spreading, the most significant outcome is users’ emotional reaction to fake news.

January 6th

Background

The attempted insurrection on January 6th, 2021, and the associated social media activity renewed interest and attention to how social media affects politics. A New York Times article from a few weeks after the attack noted that approximately 140 police officers were injured, Officer Brian Sicknick died, and a total of four other cops committed suicide after the events (Schmidt and Broadwater 2021; Cameron 2022). Consider how one news article noted that former President Trump’s Tweets fanned the flames of this attempt, and another noted evidence of plans to attack placed visibly on social media (Dilanian and Collins 2021; Miller, Jaffe, and Nakhlawi 2021). This case study starts with Twitter’s financial incentives for pushing MIDI content to users, how the algorithm works with private user data, and then explores how this impacted the insurrection.

Financial Incentive

In 2016, Twitter changed the way its feed works from a reverse chronological timeline to one created by a ranking, or engagement, algorithm (Koumchatzky and Andryeyev 2017). This new algorithm functioned similarly to how Facebook’s algorithm works by gathering user-specific data to create a personalized platform for each individual (2017). Some of this user data is the more public data such as likes, comments, and posts (2017). Other pieces of this data come from “[t]weets you found engaging in the past, how often and how heavily you use Twitter” and data that most users may not even realize Twitter is collecting – much less how they use it to manipulate what things the user sees first (2017). Unfortunately, this deep learning algorithm causes a similar problem to that seen in the Facebook engagement algorithm case study. A 2018 article from the Brookings Institute put it succinctly, saying, “we’re more likely to react to content that taps into our existing grievances and beliefs, inflammatory tweets will generate quick engagement” (Meserole 2018, para. 10). A Cornell study estimated Twitter had over 10.64 million tweets and 35.84 retweets regarding election fraud claims (Abilov et al. 2021). A Pew Research study found that the average top 25% of Tweepers receive one retweet per month (Mcclain et al. 2021). Based on the Cornell numbers, each tweet about election fraud received roughly 3.36 retweets (Abilov et al. 2021). Retweets accounted for roughly 77% of engagement regarding election fraud

(2021). On average, only 49% of tweets shared on Twitter are retweets, with an additional 33% of engagement coming from replies (Mcclain et al. 2021). Since the Cornell study numbers do not include replies, this would suggest a higher-than-average secondary engagement for election MIDI content (Abilov et al. 2021). As mentioned earlier, increased engagement drives advertising which forms 89% of Twitter's revenue, according to their fiscal year 2021 financial disclosures (Twitter 2022a). If the election fraud tweets did indeed have a higher engagement rate, then Twitter would have a financial incentive to promote them above other tweets. Twitter's algorithm, based on engagement, would also be more likely to promote such tweets.

Twitter offers extremely limited options for opting out of personalized ads using such user data. This year, a blog post from the company stated, "Opting out of Twitter's interest-based ads won't stop you from seeing Twitter ads altogether. For example, you may still see ads on Twitter that are personalized based on other information, including what you Tweet, who you follow, what type of phone you use, where you are, and the links you click on Twitter." (Twitter 2022b). A 2018 article from MIT found that advertising may be responsible for as much as 75% of fake news spread (Relihan 2018).

To summarize, private data leads to social media companies (Twitter in this case) figuring out what content creates maximum engagement and emotional responses, advertising reve-

nue incentivizes the company to create maximum engagement, and maximum engagement means pushing MIDI content to users. Election-related MIDI is no exception to this cycle. In two examples, a member of the group the Proud Boys and a Florida leader of a similar group, the Oath Keepers, both stated they went to the Capitol on January 6th because Trump had told them to be there (Feuer 2022). One of Trump's tweets on January 5th praised those who had already traveled to the capital, stating, "Washington is being inundated with people who don't want to see an election victory stolen by emboldened Radical Left Democrats. Our Country has had enough, they won't take it any-more! We hear you (and love you) from the Oval Office. MAKE AMERICA GREAT AGAIN!" (Trump 2021).

Outcome/Responses

Shortly after the election, CISA (Cybersecurity and Infrastructure Security Agency) put out a joint statement declaring, "There is no evidence that any voting system deleted or lost votes, changed votes, or was in any way compromised" (CISA 2020). According to the Department of Homeland Security, "The November 3rd election was the most secure in American history" (Al-Arshani 2020). Yet a Cornell study collected over 7.6M tweets and 25.6M retweets from 2.6M users related to voter fraud claims, and by their estimates, that was only 60% of the data (Abilov et al. 2021). Former President Trump himself tweeted over 300 times about election fraud before Twitter suspend-

ed him a few days after the insurrection (Qiu 2020; Abilov et al. 2021). Twitter cited incitement of violence and fear of further incitement of violence among their reasoning (Twitter 2021). His Facebook posts on mail-in voting fraud received roughly 3.8 million interactions (Unger 2020). Twitter suspended only 7.8% of accounts promoting such MIDI at the time of the Cornell dataset collection (Abilov et al. 2021). YouTube still had the top ten election MIDI spreading channels, and all of the top videos were online and visible as of Jan 11 (2021). The study found that such claims, and the spread through social media, undermined confidence in the election and played a significant role in the occurrence of the January 6th insurrection (2021). This creates the same issue as seen with Facebook, where emotional reactions prompt engagement, engagement feeds ad revenue, and engagement is highest when the algorithm presents dis- or misinformation - creating a financial incentive to continue the behavior (Oremus and Merrill 2021; Unger 2020). Although it is impossible to know exactly how much of the engagement regarding the election fraud claims twitter's algorithm drove, it seems clear that it had an important impact in fomenting the required emotions and belief for people to show up to the capitol on January 6th with intent to stop election proceedings. This instance exemplifies how Facebook and Twitter's engagement algorithms spread false information about the election being stolen and the impact it had on January 6th.

Bias and Limitations

Because of the secretive nature of social media conglomerates and their proprietary algorithms, getting exact data and examples is extremely difficult. This study relies heavily on secondary sources to evaluate instances of companies' use of private information, which can cause problems and inconsistencies. Additionally, these instances used in this qualitative study have yet to be fully detailed and documented as new information is coming to light almost daily.

Results

Each case study demonstrated a different violation of data privacy. Cambridge Analytica relied on microtargeting from personal datasets and psychological profiles, including data taken from individuals' connections (friends) without permission (Rosenberg, Confessore, and Cadwalladr 2018; ur Rehman 2019). Facebook's engagement algorithm relies on increased engagement as tracked by user viewing habits, interactions, and engagements with the platform - essentially tracking every mouse click and movement (Oremus et al. 2021). This includes cross-site tracking, where Facebook tracks purchases, logins, time spent viewing articles clicked on from Facebook posts, and other browser interactions (O'Flaherty 2021). It may also include cross-app tracking, depending on user settings and whether or not the user has the Facebook app (2021). Twitter uses similar engagement

data to Facebook, tracking clicks, views, location, type of phone, and whom the user follows without options to change that tracking within the platform (Twitter 2022b).

Conclusion

Combining the everyday use of social media as a political messaging platform with currently available (and accurate) profiling allows a new exploit for disinformation campaigns that harm democratic institutions (Krafft and Donovan 2020). Analyzing the evidence presented in these case studies indicates that if an informed electorate is a vital part of democracy and advertising revenue disincentivizes private companies to encourage correct information, democracy cannot continue to exist as it has in the past. For years politicians have used social media platforms to curate semi-personal messages aimed at large masses (Sobieraj et al. 2020). Although disinformation campaigns are nothing new, the methods enabled by data privacy violations (personal profiling) and the megaphones social media gives users present a unique threat to democracy through the political incivility caused by these uses of social media (Unger 2020).

At the time of this writing, the congressional January 6th committee is still uncovering new information, the COVID-19 pandemic has left lingering effects and a society uncertain of where it stands on mandatory vaccinations, polio may be making a comeback, and a new health threat, monkeypox, is

emerging (Plummer 2022; Cheng 2022; January 6th Committee 2022; Haseltine 2022). Future research should consider these latest variables and updated information. Ideally, more information will also come to light about how Twitter, Facebook, YouTube, and other social media giants use their algorithms.

As seen in the case studies, after the platforms collate this data, they use it to personalize advertising, increase engagement, and increase advertising revenue. Frequently, this comes at the cost of spreading MIDI due to the emotional reaction false information causes, which leads to increased engagement. The fake news then increases political incivility, in some cases leading to civil unrest based on falsehoods, which negatively effects democracy.

Policy Implications

As mentioned earlier, the only exceptions Facebook applies to their data handling are for users who fall under the protection of the GDPR (Facebook 2022). The GDPR, or general data protection regulation, is a European Union (EU) regulation that advertises itself as the toughest in the world and includes hundreds of pages of requirements applicable to any organization targeting EU users or data related to EU citizens (“Data Protection under GDPR” 2021). The legislation offers consumer protections, including regulations regarding obtaining consent for data processing, what types of data companies can process, and data transfer (“Data Protection under GDPR” 2021). This forward-thinking legislation gives users

a say in how their data is handled and prevents scenarios like the case studies discussed in this paper from occurring by stopping the problems at the source – the data.

As opposed to the protections in the EU, data privacy legislation in the United States is currently a patchwork effort of minimal federal efforts and some state laws, unlike the consumer protections offered in the European Union. Although data broker sounds like something from a sci-fi dystopia, it is currently a billion-dollar industry in the U.S. lacking necessary federal regulation regarding the collection or use of said data (Martin 2020). In the United States, California passed the California Consumer Privacy Act of 2018 governing knowledge about what data businesses are collecting, options to opt-out of data sharing, and the right to delete personal information the businesses collected (“California Consumer Privacy Act (CCPA)” 2018). Vermont also passed H.764 to give consumers the right to opt out of data collection and the right to know more about data brokers’ collection practices (“Bill Status H.764 (Act 171)” 2021). Current federal regulations include the Health Insurance Portability and Account-

ability Act or HIPAA (which applies to healthcare data) (“Health Information Privacy” 2015), and the Gramm-Leach-Bliley Act (applied to financial data) (“Gramm-Leach-Bliley Act” 2021). In comparison with other data privacy-conscious governments, the next logical step would involve a comprehensive legislative effort for consumer privacy protections at the federal level, like the GDPR.

In addition to regulating data privacy, congress should also consider adopting ethical AI (Artificial Intelligence) legislation to correct malicious, ill-informed or negatively consequential AI. Last year, the Department of Defense mandated five principles to ensure the ethical, legal, and safe use of AI in warfighting and business applications (Hicks 2021). These include ensuring AI is responsible, equitable, traceable, reliable, and governable (2021). In context of the social media algorithms and the harm they cause the most important of these is traceability which would allow both the company, and if congress mandated it, governmental regulatory bodies to understand how these algorithms work and ensure they do not cause harm for individuals or democracy as a whole.

References

- Abilov, Anton, Yiqing Hua, Hana Matatov, Ofra Amir, and Mor Naaman. 2021. "VoterFraud2020: A Multi-Modal Dataset of Election Fraud Claims on Twitter." arXiv. <http://arxiv.org/abs/2101.08210>.
- Abril, Danielle. 2019. "Mark Zuckerberg Calls Facebook a Free-Speech Zone as Critics Demand More Restrictions." *Fortune*. October 17, 2019. <https://fortune.com/2019/10/17/facebook-ceo-mark-zuckerberg-freedom-of-expression-speech/>.
- Afriat, Hagar, Shira Dvir-Gvirsman, Keren Tsurriel, and Lidor Ivan. 2021. "'This Is Capitalism. It Is Not Illegal': Users' Attitudes toward Institutional Privacy Following the Cambridge Analytica Scandal." *The Information Society* 37 (2): 115–27. <https://doi.org/10.1080/01972243.2020.1870596>.
- Al-Arshani, Sarah. 2020. "The Department of Homeland Security Breaks from Trump and His Baseless Claims of Election Fraud, Calling This Year's Presidential Race 'the Most Secure in American History.'" *Business Insider*. November 12, 2020. <https://www.businessinsider.com/dhs-breaks-from-trump-2020-election-most-secure-in-history-2020-11>.
- Asongu, Simplice A, and Stella-Marie I Orim. 2019. "Terrorism and Social Media: Global Evidence." *AGDI Working Paper*, 30.
- Avaaz. 2021. "A Shot in the Dark: Researchers Peer under the Lid of Facebook's 'Black Box,' Uncovering How Its Algorithm Accelerates Anti-Vaccine Content." https://avaazimages.avaaz.org/fb_algorithm_antivaxx.pdf.
- Baptist, Jeffrey, and Julian Gluck. 2021. "The Gray Legion: Information Warfare Within Our Gates." *Journal of Strategic Security* 14 (4): 37–55. <https://doi.org/10.5038/1944-0472.14.4.1928>.
- Barnes, Julian E. 2021. "Russian Disinformation Targets Vaccines and the Biden Administration." *The New York Times*, August 5, 2021. <https://www.nytimes.com/2021/08/05/us/politics/covid-vaccines-russian-disinformation.html>.
- BBC News. 2018. "Cambridge Analytica Planted Fake News." *BBC News*, March 20, 2018. <https://www.bbc.com/news/av/world-43472347>.
- Beigi, Ghazaleh. 2020. "Protecting User Privacy with Social Media Data and Mining." Dissertation, Arizona, USA: Arizona State University.

Bertrand, Natasha. 2017. "Russia Organized 2 Sides of a Texas Protest and Encouraged 'Both Sides to Battle in the Streets.'" *Business Insider*. November 1, 2017. <https://www.businessinsider.com/russia-trolls-senate-intelligence-committee-hearing-2017-11>.

"Bill Status H.764 (Act 171)." 2021. 2021. <https://legislature.vermont.gov/bill/status/2018/H.764>.

Brannon, Valerie C. 2018. "Free Speech and the Regulation of Social Media Content." R45650. Washington D.C.: Congressional Research Service. <https://doi.org/10.1201/b22397-4>.

Brown, Allison J. 2020. "'Should I Stay or Should I Leave?': Exploring (Dis)Continued Facebook Use After the Cambridge Analytica Scandal." *Social Media + Society* 6 (1): 2056305120913884. <https://doi.org/10.1177/2056305120913884>.

"California Consumer Privacy Act (CCPA)." 2018. State of California - Department of Justice - Office of the Attorney General. October 15, 2018. <https://oag.ca.gov/privacy/ccpa>.

Cameron, Chris. 2022. "These Are the People Who Died in Connection With the Capitol Riot." *The New York Times*, January 5, 2022, sec. U.S. <https://www.nytimes.com/2022/01/05/us/politics/jan-6-capitol-deaths.html>.

Cascini, Fidelia, Ana Pantovic, Yazan A. Al-Ajlouni, Giovanna Failla, Valeria Puleo, Andriy Melnyk, Alberto Lontano, and Walter Ricciardi. 2022. "Social Media and Attitudes towards a COVID-19 Vaccination: A Systematic Review of the Literature." *EclinicalMedicine* 48 (June): 101454. <https://doi.org/10.1016/j.eclinm.2022.101454>.

CCDH. 2021. "The Disinformation Dozen: Why Platforms Must Act on Twelve Leading Anti-Vaxxers." https://252f2edd-1c8b-49f5-9bb2-cb57bb47e4ba.filesusr.com/ugd/f4d9b9_b7cedc0553604720b7137f8663366ee5.pdf.

Cheng, F.K. 2022. "Debate on Mandatory COVID-19 Vaccination." *Ethics, Medicine, and Public Health* 21 (April): 100761. <https://doi.org/10.1016/j.jemep.2022.100761>.

CISA. 2020. "Joint Statement from Elections Infrastructure Government Coordinating Council & the Election Infrastructure Sector Coordinating Executive Committees." November 12, 2020. <https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election>.

Confessore, Nicholas, and Matthew Rosenberg. 2018. "Cambridge Analytica to

File for Bankruptcy After Misuse of Facebook Data.” *The New York Times*, May 2, 2018, sec. U.S. <https://www.nytimes.com/2018/05/02/us/politics/cambridge-analytica-shut-down.html>.

Cotter, Kelley, Julia R. DeCook, and Shaheen Kanthawala. 2022. “Fact-Checking the Crisis: COVID-19, Infodemics, and the Platformization of Truth.” *Social Media + Society* 8 (1): 205630512110690. <https://doi.org/10.1177/20563051211069048>.

Crusius, Jan, Josephine Thierhoff, and Jens Lange. 2021. “Dispositional Greed Predicts Benign and Malicious Envy.” *Personality and Individual Differences* 168 (January): 110361. <https://doi.org/10.1016/j.paid.2020.110361>.

“Data Protection under GDPR.” 2021. Your Europe. 2021. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm.

De Vynck, Gerrit, and Rachel Lerman. 2021. “Facebook and YouTube Spent a Year Fighting Covid Misinformation. It’s Still Spreading.” *Washington Post*, July 22, 2021. <https://www.washingtonpost.com/technology/2021/07/22/facebook-youtube-vaccine-misinformation/>.

Dilanian, Ken, and Ben Collins. 2021. “Feds Aren’t Using Posts about Plans to Attack the Capitol as Evidence.” *NBC News*. April 20, 2021. <https://www.nbcnews.com/politics/justice-department/we-found-hundreds-posts-about-plans-attack-capitol-why-aren-n1264291>.

“Disinformation Nation: Social Media’s Role in Promoting Extremism and Misinformation.” 2021. Washington D.C.

Dubois, Elizabeth, and Grant Blank. 2018. “The Echo Chamber Is Overstated: The Moderating Effect of Political Interest and Diverse Media.” *Information, Communication & Society* 21 (5): 729–45. <https://doi.org/10.1080/1369118X.2018.1428656>.

Facebook. 2022. “Facebook Data Policy.” January 4, 2022. https://m.facebook.com/privacy/explanation/?_se_imp=1B8bi41uKqU3YqgfM.

“Facebook - Financials.” 2021. 2021. <https://investor.fb.com/financials/default.aspx>.

Fallis, Don. 2015. “What Is Disinformation?” *Library Trends* 63 (January): 401–26. <https://doi.org/10.1353/lib.2015.0014>.

Feuer, Alan. 2022. “Three Characters at the Heart of an Unsettling Jan. 6 Narrative.” *The New York Times*, June 10, 2022, sec. U.S. <https://www.nytimes.com/2022/06/09/>

[us/politics/jan-6-proud-boys-capitol-police.html](https://www.washingtonpost.com/politics/jan-6-proud-boys-capitol-police.html).

Franz, Daschel, Heather Elizabeth Marsh, Jason I. Chen, and Alan R. Teo. 2019. "Using Facebook for Qualitative Research: A Brief Primer." *Journal of Medical Internet Research* 21 (8): e13544. <https://doi.org/10.2196/13544>.

George, Daniel R., Liza S. Rovniak, and Jennifer L. Kraschnewski. 2013. "Dangers and Opportunities for Social Media in Medicine." *Clinical Obstetrics and Gynecology* 56 (3): 10.1097/GRF.0b013e318297dc38. <https://doi.org/10.1097/GRF.0b013e318297dc38>.

Glaser, Barney G., and Anselm L. Strauss. 2010. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. 5. paperback print. New Brunswick: Aldine Transaction.

Goldstein, Neal D. 2021. "Misinformation." *American Journal of Public Health* 11 (2). <https://www.proquest.com/docview/2486203133>.

"Gramm-Leach-Bliley Act." 2021. Federal Trade Commission. 2021. <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act>.

Haseltine, William A. 2022. "There May Be A New Polio Epidemic On Its Way- If So, What We Can Do: Part III." *Forbes*. June 28, 2022. <https://www.forbes.com/sites/williamhaseltine/2022/06/28/there-may-be-a-new-polio-epidemic-on-its-way-if-so-what-we-can-do-part-iii/>.

"Health Information Privacy." 2015. Text. HHS.Gov. August 26, 2015. <https://www.hhs.gov/hipaa/index.html>.

Heawood, Jonathan. 2018. "Pseudo-Public Political Speech: Democratic Implications of the Cambridge Analytica Scandal." *Information Polity* 23 (4): 429–34. <https://doi.org/10.3233/IP-180009>.

Hern, Alex. 2018. "Cambridge Analytica: How Did It Turn Clicks into Votes?" *The Guardian*, May 6, 2018, sec. News. <https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie>.

Hicks, Kathleen. 2021. "Implementing Responsible Artificial Intelligence in the Department of Defense." Department of Defense.

Houston, J. Brian, Joshua Hawthorne, Mildred F. Perreault, Eun Hae Park, Marlo Goldstein Hode, Michael R. Halliwell, Sarah E. Turner McGowen, et al. 2015.

“Social Media and Disasters: A Functional Framework for Social Media Use in Disaster Planning, Response, and Research.” *Disasters* 39 (1): 1–22. <https://doi.org/10.1111/disa.12092>.

Hsu, Tiffany. 2018. “For Many Facebook Users, a ‘Last Straw’ That Led Them to Quit - The New York Times.” March 21, 2018. <https://www.nytimes.com/2018/03/21/technology/users-abandon-facebook.html>.

Hu, Margaret. 2020. “Cambridge Analytica’s Black Box.” *Big Data & Society* 7 (2): 2053951720938091. <https://doi.org/10.1177/2053951720938091>.

Hunter, Gary L., and Steven A. Taylor. 2019. “The Relationship between Preference for Privacy and Social Media Usage.” *Journal of Consumer Marketing* 37 (1): 43–54. <https://doi.org/10.1108/JCM-11-2018-2927>.

Isaac, Mike, and Scott Shane. 2017. “Facebook’s Russia-Linked Ads Came in Many Disguises.” *The New York Times*, October 2, 2017, sec. Technology. <https://www.nytimes.com/2017/10/02/technology/facebook-russia-ads-.html>.

January 6th Committee. 2022. “Committee Activity.” Select Committee to Investigate the January 6th Attack on the United States Capitol. July 21, 2022. https://january6th.house.gov/committee_activity.

Kim, Jiyoung. 2021. “The Meaning of Numbers: Effect of Social Media Engagement Metrics in Risk Communication.” *Communication Studies* 72 (2): 195–213. <https://doi.org/10.1080/10510974.2020.1819842>.

Koumchatzky, Nicolas, and Anton Andryeyev. 2017. “Using Deep Learning at Scale in Twitter’s Timelines.” May 9, 2017. https://blog.twitter.com/engineering/en_us/topics/insights/2017/using-deep-learning-at-scale-in-twitters-timelines.

Krafft, P. M., and Joan Donovan. 2020. “Disinformation by Design: The Use of Evidence Collages and Platform Filtering in a Media Manipulation Campaign.” *Political Communication* 37 (2): 194–214. <https://doi.org/10.1080/10584609.2019.1686094>.

Lee, Klara, and Mack Willett. 2021. “Rightly | Giant Tech Companies Following Your Personal Data.” Rightly. February 18, 2021. <https://rightly.ly/our-views-and-opinions/the-privacy-policies-of-social-media-companies-how-do-they-use-your-data/>.

Li, Wei, and Hao Li. 2013. “Misinformation.” *International Economic Review*, 54 (1): 253–77.

Martel, Cameron, Gordon Pennycook, and David G. Rand. 2020. "Reliance on Emotion Promotes Belief in Fake News." *Cognitive Research: Principles and Implications* 5 (1): 47. <https://doi.org/10.1186/s41235-020-00252-3>.

Martin, Brittany A. 2020. "The Unregulated Underground Market for Your Data: Providing Adequate Protections for Consumer Privacy in the Modern Era." *Iowa Law Review* 105 (2): 865–900.

Mcclain, Colleen, Regina Widjaya, Gonzalo Rivero, and Aaron Smith. 2021. "2. Comparing Highly Active and Less Active Tweeters." *Pew Research Center: Internet, Science & Tech* (blog). November 15, 2021. <https://www.pewresearch.org/internet/2021/11/15/2-comparing-highly-active-and-less-active-tweeters/>.

Meserole, Chris. 2018. "How Misinformation Spreads on Social Media—And What to Do about It." *Brookings* (blog). May 9, 2018. <https://www.brookings.edu/blog/order-from-chaos/2018/05/09/how-misinformation-spreads-on-social-media-and-what-to-do-about-it/>.

Miller, Greg, Greg Jaffe, and Razzan Nakhlawi. 2021. "A Mob Insurrection Stoked by False Claims of Election Fraud and Promises of Violent Restoration." *Washington Post*, January 9, 2021. https://www.washingtonpost.com/national-security/trump-capitol-mob-attack-origins/2021/01/09/0cb2cf5e-51d4-11eb-83e3-322644d82356_story.html.

O’Flaherty, Kate. 2021. "All The Ways Facebook Tracks You And How To Stop It." *Forbes*. May 8, 2021. <https://www.forbes.com/sites/kateoflahertyuk/2021/05/08/all-the-ways-facebook-tracks-you-and-how-to-stop-it/>.

O’Neil, Cathy. 2021. "Analysis | Facebook’s Algorithms Are Too Big to Fix." *WashingtonPost*, October 8, 2021. https://www.washingtonpost.com/business/facebooks-algorithms-are-too-big-to-fix/2021/10/08/63986860-282f-11ec-8739-5cb6aba30a30_story.html.

Oremus, Will, Chris Alcantara, Jeremy B. Merrill, and Artur Galocha. 2021. "How Facebook Shapes Your Feed." *Washington Post*, October 26, 2021. <https://www.washingtonpost.com/technology/interactive/2021/how-facebook-algorithm-works/>.

Oremus, Will, and Jeremy B. Merrill. 2021. "Facebook Prioritized ‘Angry’ Emoji Reaction Posts in News Feeds - The Washington Post," October 26, 2021. <https://www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm/>.

Permanent Select Committee on Intelligence. 2018. "Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements | Permanent Select Committee on Intelligence." June 2018. <https://intelligence.house.gov/social-media-content/>.

Plummer, Robert. 2022. "Monkeypox: WHO Declares Highest Alert over Outbreak." *BBC News*, July 23, 2022, sec. Health. <https://www.bbc.com/news/health-62279436>.

Qiu, Linda. 2020. "Trump Has Amplified Voting Falsehoods in over 300 Tweets since Election Night." *The New York Times*, November 16, 2020, sec. Technology. <https://www.nytimes.com/2020/11/16/technology/trump-has-amplified-voting-falsehoods-in-over-300-tweets-since-election-night.html>.

Rehman, Ikhtlaq ur. 2019. "Facebook-Cambridge Analytica Data Harvesting: What You Need to Know," 12.

Relihan, Tom. 2018. "Social Media Advertising Can Boost Fake News — or Beat It." MIT Sloan. December 19, 2018. <https://mitsloan.mit.edu/ideas-made-to-matter/social-media-advertising-can-boost-fake-news-or-beat-it>.

Rosenberg, Matthew, Nicholas Confessore, and Carole Cadwalladr. 2018. "How Trump Consultants Exploited the Facebook Data of Millions." *The New York Times*, March 17, 2018, sec. U.S. <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>.

Schmidt, Michael S., and Luke Broadwater. 2021. "Officers' Injuries, Including Concussions, Show Scope of Violence at Capitol Riot." *The New York Times*, February 12, 2021, sec. U.S. <https://www.nytimes.com/2021/02/11/us/politics/capitol-riot-police-officer-injuries.html>.

SEC. 2021. "Facebook FORM 10-K 2020." <https://www.sec.gov/ix?doc=/Archives/edgar/data/1326801/000132680121000014/fb-20201231.htm>.

Sethi, Umong. 2013. "Social Media - A Tool for the Military." *Centre for Land Warfare Studies*, 5.

Smith, Douglas, Trinity Leonis, and S. Anandavalli. 2021. "Belonging and Loneliness in Cyberspace: Impacts of Social Media on Adolescents' Well-Being." *Australian Journal of Psychology* 73 (1): 12–23. <https://doi.org/10.1080/00049530.2021.1898914>.

Sobieraj, Sarah, Gina M. Masullo, Philip N. Cohen, Tarleton Gillespie, and Sarah

J. Jackson. 2020. "Politicians, Social Media, and Digital Publics: Old Rights, New Terrain." *American Behavioral Scientist* 64 (11): 1646–69. <https://doi.org/10.1177/0002764220945357>.

Sufi, Fahim, and Musleh Alsulami. 2022. "A Novel Method of Generating Geospatial Intelligence from Social Media Posts of Political Leaders." *Information* 13 (3): 120. <https://doi.org/10.3390/info13030120>.

Thompson, Cadie. 2015. "What You Really Sign up for When You Use Social Media." CNBC. May 27, 2015. <https://www.cnbc.com/2015/05/20/what-you-really-sign-up-for-when-you-use-social-media.html>.

Timberg, Craig, and Elizabeth Dwoskin. 2018. "Russians Got Tens of Thousands of Americans to RSVP for Their Phony Political Events on Facebook." *Washington Post*, January 25, 2018. <https://www.washingtonpost.com/news/the-switch/wp/2018/01/25/russians-got-tens-of-thousands-of-americans-to-rsvp-for-their-phony-political-events-on-facebook/>.

Tourani, Nazanin. 2022. "Thriving in a Shifting Landscape: Role of Social Media in Support of Business Strategy." *Asia Pacific Management Review*, February, 1–6. <https://doi.org/10.1016/j.apmrv.2021.11.001>.

Trump, Donald. 2021. "Search on Trump Twitter Archive." January 5, 2021. // www.thetrumparchive.com.

Twitter. 2021. "Permanent Suspension of @realDonaldTrump." January 8, 2021. https://blog.twitter.com/en_us/topics/company/2020/suspension.

———. 2022a. "Fiscal Year 2021 Twitter Annual Report." 2022. https://s22.q4cdn.com/826641620/files/doc_financials/2021/ar/FiscalYR2021_Twitter_Annual-Report.pdf.

———. 2022b. "Your Privacy Options for Personalized Ads | Twitter Help." April 28, 2022. <https://help.twitter.com/en/safety-and-security/privacy-controls-for-tailored-ads>.

Unger, Wayne. 2020. "How Disinformation Campaigns Exploit the Poor Data Privacy Regime to Erode Democracy." *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3762609>.

University of Washington. 2021. "Library Guides: News: Fake News, Misinformation & Disinformation." October 2021. <https://guides.lib.uw.edu/c.php?g=345925&p=7772376>.

Walker, Shawn, Dan Mercea, and Marco Bastos. 2019. "The Disinformation Landscape and the Lockdown of Social Platforms." *Information, Communication & Society* 22 (11): 1531–43. <https://doi.org/10.1080/1369118X.2019.1648536>.

Wilczek, Bartosz. 2020. "Misinformation and Herd Behavior in Media Markets: A Cross-National Investigation of How Tabloids' Attention to Misinformation Drives Broadsheets' Attention to Misinformation in Political and Business Journalism | PLOS ONE." *PLOS ONE*, <https://doi.org/10.1371/journal.pone.0241389>, , November. <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0241389>.

Winegar, A. G., and C. R. Sunstein. 2019. "How Much Is Data Privacy Worth? A Preliminary Investigation." *Journal of Consumer Policy* 42 (3): 425–40. <https://doi.org/10.1007/s10603-019-09419-y>.