

# Disguised Propaganda on Social Media: Addressing Democratic Dangers and Solutions

---

JOHAN FARKAS

“THE STRUCTURE OF PRESENT-DAY SOCIETY places the individual where he is most easily reached by propaganda... the technical evolution of this society deepen[s] this situation.”<sup>1</sup> At first glance, this quote seems to aptly capture contemporary debates about the dangers to democracy posed by deception and false information in digital environments. Yet, it predates the internet substantially, appearing in the seminal work of French philosopher Jacques Ellul, *Propaganda: The Formation of Men's Attitudes*, first published in 1962.<sup>2</sup> In recent years, political actors worldwide have grown increasingly concerned with the ways in which new forms of manipulation, propaganda, and “fake news” might subvert and distort public deliberation. These concerns rose to prominence in late 2016 following the British European Union membership referendum and the election of President Donald Trump in the United States. Since then, case after case has provided unsettling glimpses into the dark underbelly of the digital era, unraveling complex layers of deception and disinformation. Subversive actors—from individuals to organizations and even nation states—have weaponized social media in order to achieve political goals. Fake profiles, social bots, and micro-targeted advertisements are only some of the strategies currently employed. The implications of such tactics are difficult to estimate, yet they raise a series of disturbing questions about the current state of liberal democracies. This essay sets

1

---

JOHAN FARKAS is PhD Fellow at Malmö University, Media and Communication Studies. His research revolves around new forms of political propaganda and struggles in digital media. Farkas' work is published in international journals such as *New Media & Society* and *Javnost – The Public*. He is also the author of a forthcoming chapter in the anthology *Fake News: Understanding Media and Misinformation in the Digital Age* (MIT Press).

---

Copyright © 2018 by the *Brown Journal of World Affairs*

out to critically address this fast-developing topic and its threat to democracy.

Ellul's reflections from the mid-twentieth century speak directly to our present situation, epitomizing a simple and often neglected aspect of political ma-

---

**Propaganda is far from a new phenomenon. It is deeply historical and continues to evolve alongside political systems and media technologies.**

---

nipulation and deception: that propaganda is far from a new phenomenon. It is deeply historical and continues to evolve alongside political systems and media

technologies. While manipulation and propaganda certainly take new forms online, mechanisms often remain the same.<sup>3</sup> This teaches us two key lessons. First, it forces us to recognize the roots of propaganda, suggesting that we should not overestimate its novelty in the digital age. Second, it lays the foundation for a more nuanced discussion of how modern democracies can address propaganda. If we know what kinds of approaches and solutions failed in the past, we can avoid repeating those mistakes. Instead of reusing flawed ideas, falling prey to moral panics and technological quick fixes, we can have an informed conversation about our current predicament.

2

Some past lessons might seem obvious today. However, as this article will showcase, recent attempts to stop disguised propaganda have largely failed to take these lessons into consideration and have proven unable to address digital propaganda's root causes. At best, these measures and solutions might prove ineffective and at worst they might end up hurting democracy in the process of trying to save it. Indeed, one of the most pervasive solutions offered today, not least by social media companies, is to automate censorship with little to no public oversight. This leads to less transparency, limiting the possibility of taking preventive action and informing citizens. Drawing on propaganda theory, this article engages equally with the democratic dangers of disguised propaganda on social media, weaknesses of current solutions to the problem, and potential paths forward. Departing from the 2016 U.S. presidential election and the (still evolving) case of Russian interference, the article outlines how insights from propaganda theorists, developed in response to mass media, can help inform current problems and future solutions.

## **DEFINING PROPAGANDA: A CONCEPTUAL VOCABULARY**

In order to address new forms of propaganda, it is essential to establish a com-

mon vocabulary. In contemporary debates, clear definitions are few and far between. The vague and prevalent notion of fake news exemplifies this.<sup>4</sup> Theories of twentieth century propaganda have largely been neglected in recent discussions, perhaps because they seem outdated in relation to our present media landscape. Yet, these theories provide a powerful starting point for analyzing digital propaganda. They not only help us define its boundaries, but also give us a better grasp of how we might understand its different forms.

Throughout the twentieth century, definitions of propaganda changed considerably and were subject to intense debate. After World War II, propaganda became intrinsically linked to fascism, war, and genocide, although this was not always the case. In 1928, Edward Bernays—the American “father of public relations” and nephew of Sigmund Freud—argued that propaganda represented a “perfectly wholesome word, of honest parentage, and with an honorable history.”<sup>5</sup> In Bernays’ view, modern propaganda includes instruments of shaping public opinion through mass media. Depending on the aim, it can successfully unite or divide citizens by creating shared perceptions of events, ideas, and people. As with any other instrument, Bernays argued, propaganda can be misused. However, in itself, it merely represents a tool for shaping worldviews, which can even serve an important role in liberal democracies.<sup>6</sup> As societies grow in complexity, citizens face overwhelming amounts of choices, potentially causing confusion and conflict. Bernays saw propaganda as vital for reducing complexity and finding “new ways to bind and guide the world.”<sup>7</sup> Instead of rejecting propaganda, he prescribed clear ethical guidelines for its function and purpose. Sources of propaganda have to be “clearly stated and the facts accurately presented.”<sup>8</sup> Additionally, democracies should “be in a position to deal effectively with rumors and suspicions, attempting to stop them at their source.”<sup>9</sup> Ivy Lee, another advocate of propaganda and public relations, similarly argued that “the essential evil of propaganda is failure to disclose the source of information,” as in the case of private corporations disguised as civil society groups.<sup>10</sup>

After World War II, Bernays’ notion of politically neutral or benign propaganda largely fell from grace in the public. Nazi Germany’s explicit use of the term in Joseph Goebbels’ *Reich Ministry of Public Enlightenment and Propaganda* linked propaganda intimately with fascism. Still, many of Bernays’ core arguments continued to be used by scholars. In his seminal work, Ellul argued that any form of “democratic propaganda must be essentially truthful,” echoing Bernays.<sup>11</sup> Yet, he contended, “the true propagandist must be as cold, lucid, and rigorous as a surgeon... [t]here is, therefore, no ‘democratic’ propaganda.”<sup>12</sup> Propaganda and democracy can coexist in theory; however, as a successful propagandist needs

to exploit any means necessary, propaganda will always be undemocratic in practice. Ellul nonetheless saw how some forms of propaganda could represent greater threats than others. He took disguised propaganda as being especially sinister, as it pushes citizens “in a certain direction without their being aware of it.”<sup>13</sup> To Ellul, this danger was not to be underestimated, especially in the context of enemy nations, as propaganda “has such an ability to effect psychological transformations and such an impact on the very core of man that it inevitably has military force when used by a government and directed to the outside.”<sup>14</sup>

Written in different times and contexts, the works of Bernays and Ellul point to a series of fundamental challenges for democracies posed by propaganda in the age of mass communication. While media technologies changed considerably in the period from Bernays’ 1920s to Ellul’s 1960s, propaganda campaigns prevailed, not least in the form of fabricated sources—prevalent, for example, in clandestine radio channels during World War II and the Cold War.<sup>15</sup> With the rise of digital media at the end of the twentieth century, insights from these theorists were largely forgotten. Nonetheless, recent developments remind us that propaganda continues to adapt to evolving media landscapes. While some things change, others stay the same.

4

In propaganda theory, the use of disguised sources as a means of promoting political agendas is often characterized as either *grey* or *black* propaganda. Within grey propaganda, sources are deliberately obfuscated, making them difficult or impossible to identify. In black propaganda, propagandists carefully create fake identities that are “presented by the propagandizer as coming from a source inside the propagandized.”<sup>16</sup> Both grey and black propaganda stand in contrast to *white* propaganda, which has clear and overt authorship. While covert and overt sources are often deployed in tandem, distinguishing between different types is a productive way of understanding and addressing them.<sup>17</sup>

One of the key questions raised by propaganda—especially in its grey and black forms—is to what extent it proves effective. As Ellul already noted in the 1960s, this is essentially “impossible to measure” due to its often ephemeral, covert, and deeply contextual nature.<sup>18</sup> This does not, however, imply that disguised propaganda should not be studied. Rather, it suggests that the starting point for understanding grey and black forms cannot be their scale, size, and effect. Instead, we have to investigate their underlying technological and political conditions and causes: Why are they there? What purposes do they serve? And what are their modes of operation?

These insights remain key in our contemporary digital age, as tech companies increasingly turn to automated measures and machine learning to solve their

problems. These kinds of solutions do little to help our current predicament. Instead of addressing the structural causes of disguised propaganda, they largely work as opaque, ad hoc fixes. This not only decreases transparency, but also fails to help us understand the complexity of manipulation in digital environments and prevent its influence on democratic processes, such as elections.

## DISGUISED PROPAGANDA IN SOCIAL MEDIA

As the dust from the Cold War was still settling, optimism about the democratic potentials of digital technologies was widespread among scholars and media professionals. While authoritarian regimes could exercise tight control over mass media (radio and television), the internet presented a new and highly decentralized form of communication. It had the potential to empower oppressed groups and usher in a new wave of democracy. This optimism continued with the rise of social media such as Facebook and Twitter in the mid-to-late 2000s. These platforms made it easier for any citizen with a digital device and internet connection to engage in “mass self-communication” and potentially influence change.<sup>19</sup> Boler and Nemorin reflected this optimism in 2013, arguing that “the proliferating use of social media and communication technologies for purposes of dissent from official government and/or corporate-interest propaganda offers genuine cause for hope.”<sup>20</sup> In

this narrative, social media represented a democratizing tool that would foster participation and bottom-up initiatives. Social media companies themselves were quick to jump on this band-

wagon, promoting their platforms as spaces of participation, connectivity, decentralization, and spontaneous interaction. For example, the CEO of Facebook, Mark Zuckerberg, argued that the company aimed at giving “people the power to share and making the world more open and connected.”<sup>21</sup>

Fast-forward to 2018: things seem to have changed quite a bit. In the wake of the 2016 U.S. presidential election and the Brexit referendum, widespread criticism erupted among citizens, scholars, journalists, and political actors, all of whom argued that social media companies had failed to live up to their democratic rhetoric. Whereas platforms such as Facebook and Twitter had originally been seen as vehicles of democracy, attention turned to their ability to support

---

**Whereas Facebook and Twitter had originally been seen as vehicles of democracy, attention turned to their ability to support new and powerful forms of disguised propaganda.**

---

new and powerful forms of disguised propaganda. It became clear that malicious groups and organizations could use social media to orchestrate large-scale grey and black propaganda campaigns—often disguised as originating from within a target country. It also became clear that the decentralized structure of social media supports such efforts, while simultaneously making it difficult to recognize and address them.

A large-scale study estimates that, during the 2016 U.S. presidential election, social bots produced close to 19 percent of all debate on Twitter.<sup>22</sup> Social bots are software-driven digital accounts, automatically producing and distributing messages on social media. Bots were found on both sides of the political spectrum, although a majority supported the Republican candidate, Donald Trump.<sup>23</sup> In the context of the British EU membership referendum, research estimates that 13,493 Twitter accounts were bots.<sup>24</sup> One of the key ways bots are used is to spread conspiracy theories and disinformation, popularly referred to as “fake news.”<sup>25</sup> Despite these indications of massive automated deception, identifying the actual producers of bots remains close to impossible, especially without the help of social media companies. We are in a situation today where almost any individual with adequate resources can obtain the knowledge and tools to influence public debate through bots.<sup>26</sup>

6

These developments have led to mounting pressure on social media companies to investigate questions of deceit, particularly as to whether foreign nations interfered in the U.S. and U.K. elections. In response to political demands, Twitter, Facebook, Instagram, and YouTube all found evidence of Russian interference in the 2016 U.S. elections. According to Twitter, a total of 36,746 Russian accounts produced approximately 1.4 million tweets during the elections.<sup>27</sup> Among these accounts, Twitter established that 3,814 accounts were connected to a company known as the Internet Research Agency in St. Petersburg.<sup>28</sup> Facebook similarly found that this company had “consistently used inauthentic accounts to deceive and manipulate people.”<sup>29</sup> The Internet Research Agency is a secretive Russian organization known to orchestrate disguised social media campaigns in multiple European countries and the United States.<sup>30</sup> The company has been dubbed a “troll factory” due to its engagement in social media *trolling*, inciting conflict and hatred based on fake identities.<sup>31</sup> This term, however, has obvious shortcomings, as the agency’s operations go far beyond simply trolling. The Internet Research Agency engages in large-scale disguised propaganda campaigns. Their activities do not rely solely on social bots, however. According to leaked documents from the organization, employees were expected to manage at least six fake Facebook accounts publishing three

posts a day and 10 fake Twitter accounts tweeting 50 times a day in 2014.<sup>32</sup> Interviews with former employees confirmed the existence of these operations, involving hundreds of employees working in 12-hour shifts, writing more than 150 comments each day and maintaining 10 blogs each.<sup>33</sup> By using fake identities, employees would disseminate disguised propaganda, deploying social bots to amplify its effects.<sup>34</sup>

According to Facebook, the Internet Research Agency bought strategic political ads on both Facebook and Instagram during the 2016 U.S. elections. More than half of these ads made explicit references to racial issues and some specifically targeted voters in swing states that were key to the election outcome.<sup>35</sup> Evidence indicates that the company might have had access to social media data on millions of U.S. citizens, shared illegally by the U.K. data analytics firm, Cambridge Analytica.<sup>36</sup> The Internet Research Agency systematically focused their efforts on specific demographics, including the Black Lives Matter movement organizing against police oppression of African Americans. According to Facebook and Twitter, the Russian company controlled several leading social media accounts within this movement and targeted its members with advertisements, discouraging African Americans from voting in the elections.<sup>37</sup> Ads on Instagram read, “Hillary Clinton does not deserve Black voters” and “a great number of black people support us saying that #HillaryClintonIsNotMyPresident.”<sup>38</sup>

7

A leading hypothesis is that the goal was to sow discord and suppress Democratic votes to strengthen the Republican candidate, Donald Trump.<sup>39</sup> In the context of the 2016 British EU membership referendum, Twitter found evidence of similar propaganda activity, though on a significantly smaller scale. Facebook did not find evidence of such coordinated foreign propaganda in the British referendum.<sup>40</sup> At the time of writing, further investigations are still underway.

In 2018, the U.S. Justice Department indicted 13 Russian individuals affiliated with the Internet Research Agency, accusing the company of engaging “in political and electoral interference operations” and employing “hundreds of individuals for its online operations” with an annual budget totaling “the equivalent of millions of U.S. dollars.”<sup>41</sup> The indictment specifies that the organization carried out “information warfare” in the elections based on “fictitious U.S. personas on social media platforms and other Internet-based media.”<sup>42</sup> At the time of writing, the prosecution has yet to lead to any convictions. Yet, revelations have already led to numerous promises and actions from social media companies. Following accusations of Russian interference in the U.S. elections, Twitter and Facebook first responded defensively. In the days after Donald

Trump's election as President, the CEO of Facebook, Mark Zuckerberg, called the notion of Russian interference a "pretty crazy idea."<sup>43</sup> As more evidence emerged, his defense shifted to an apology, leading to his statement in 2018 that Facebook's slow response to Russian meddling was one of his "greatest regrets in running the company."<sup>44</sup> Following public apologies, both Twitter and Facebook announced that they were implementing a range of technical innovations to prevent similar malicious practices in the future.<sup>45</sup> Both companies promised that these changes would be wide-ranging, increase transparency, and prevent disguised propaganda from taking hold. In practice, however, the overwhelming response from both companies has been *decreased transparency* and *technological solutionism*. As the following section will discuss, these actions largely fail to address the complicated cultural and political nature of disguised propaganda, potentially even causing more harm than good for liberal democracies.

#### PROBLEMS WITH CURRENT SOLUTIONS

As it became evident that Russian Twitter accounts produced approximately 1.4 million tweets during the U.S. elections, Twitter first responded by refusing to share any content from deleted accounts with researchers and journalists, thus avoiding public scrutiny.<sup>46</sup> In order to analyze the propaganda and inform citizens about the intricacies of the propaganda, anonymous researchers, assisted by journalists, had to break Twitter's policies by sharing deleted data fragments.<sup>47</sup> While this produced some new insights, the published data had severe limitations due to fragmentation and missing contexts. Among other problems, researchers could not assess whether the data was a representative sample of the operations carried out by the Internet Research Agency. Similar to Twitter, Facebook refused to share any data on the political ads that the Internet Research Agency had bought on its platforms. The company stated that "federal law places strict limitations on the disclosure of account information," and when asked by confounded journalists which law the company was referring to, Facebook did not respond.<sup>48</sup> Later on, ads were made public thanks to U.S. lawmakers who argued for the democratic importance of transparency: as stated by Democratic member of the House of Representatives, Adam Schiff, "Ultimately, by exposing these advertisements, we hope to better protect legitimate political expression and discussions."<sup>49</sup> Under continued pressure from political and civic actors, Twitter eventually released a substantial dataset on the Internet Research Agency's activities in October 2018, a full year after the company admitted to the existence of disguised propaganda operations on their



platform.<sup>50</sup> As with the datasets provided by Facebook, Instagram, and YouTube, however, Twitter's data "lacked core components that would have provided a fuller and more actionable picture."<sup>51</sup>

Despite promising otherwise, increased transparency has not been the primary response from social media companies. In addition to refusing to share disguised propaganda content, Facebook announced in the spring of 2018 that it was dramatically restricting data access through the platform's APIs, causing hundreds of research projects to come to a complete halt overnight. An API, or Application Programming Interface, represents a point of contact between computer programs. On Facebook, a series of APIs define what external developers, including academic researchers, can and cannot do on the platform.

Facebook's data shutdown came in the wake of the Cambridge Analytica scandal, revealing that this company had obtained Facebook data on millions of Americans and used it to analyze and target them with political ads during the elections. Facebook persistently labelled these practices as abuse and a breach of trust, downplaying how the data was obtained based on Facebook's own tools and policies at the time. In 2013–14, when Cambridge Analytica's data was obtained, Facebook allowed software developers to collect data not only from people who used their applications, but also from all of their friends.<sup>52</sup> Already in 2011, Austrian lawyer and activist Max Schrem criticized Facebook for these practices, filing a complaint to the EU's Data Protection Commissioner.<sup>53</sup> As Schrem pointed out, Facebook violated users' privacy by not clearly indicating that "if a 'friend' installs an application, the application can automatically access their profile picture, name and other basic information."<sup>54</sup> Eventually, in 2014–15, Facebook discontinued this practice, approximately three years before the Cambridge Analytica scandal took off.<sup>55</sup>

When Facebook shut down access to its APIs in 2018 it did not put an end to the "loophole" (or deliberate policy) that enabled app developers to obtain data on millions of users through their Facebook friends. It did, however, drastically limit public scrutiny of Facebook, a move that could ironically strengthen producers of disguised propaganda; as researchers warned: "restricting access to data is likely to facilitate further weaponization by turning Facebook into a de facto black box that is largely unaccountable to external oversight."<sup>56</sup>

This brings us to the technological solutions announced by social media companies in response to disguised propaganda. In 2018, Facebook announced that it would start implementing new forms of "machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself."<sup>57</sup> Ac-

According to Facebook, this innovation would prevent political manipulation by automatically detecting and deleting it. The company did not reveal details on how this would work in practice or how they would handle such content, besides deleting it. As previous research indicates, this potentially enables producers of disguised propaganda to continue their efforts without ever facing legal consequences.<sup>58</sup> In regards to transparency, Facebook did not set any goals for increased transparency in their new and automated content moderation system.

The solution from Twitter was equally technical, although slightly different in scope. According to the company, previous efforts to counter misinformation and manipulation had too narrowly focused on content removal, rather than addressing the roots of the problem. In the future, the company assured, a new technological system would be developed that can measure the “health” of online debates, preventing destabilizing forces from corroding public discourse. Jack Dorsey, CEO of Twitter, compared this new approach to a medical examination:

If you want to improve something, you have to be able to measure it. The human body has a number of indicators of overall health, some very simple, like internal temperature. We know how to measure it, and we know some methods to bring it back in balance. What we know is we must commit to a rigorous and independently vetted set of metrics to measure the health of public conversation on Twitter.<sup>59</sup>

10

In order to counter misinformation and deception, Twitter argued, you have to be able to measure it. Still, the company did not detail how this would solve the problem of disguised propaganda. Yet Twitter promised that it would “commit to sharing our results publicly to benefit all who serve the public conversation.”<sup>60</sup> As the company only shared tweets from the Internet Research Agency after a year of public pressure, the sincerity of this commitment is yet to be determined.

While the technological solutions from Facebook and Twitter are still to be implemented and evaluated, propaganda theory predicts their likely failure. As Ellul argued more than 50 years ago, “it is impossible to measure the effectiveness of ‘black’ propaganda due to its subversive and hidden nature.”<sup>61</sup> Addressing propaganda through quantitative means will always be close to impossible, as quantification requires some form of decontextualization. In order to evaluate content objectively, measurements have to rely on some form of universal standard. This fails to accommodate how successful propaganda is always deeply interwoven with its cultural and political context. Propaganda relies on a snowball effect in which ideas and thoughts are not merely propagated one way from a

sender to a receiver. Propaganda instead guides public opinion in specific directions by continually adjusting to contexts, goals, and available means. The idea of measuring the “health” of conversations in order to address disguised propaganda, as proposed by Twitter, misses the point. Measuring the “health” of debates around the Black Lives Matter movement, for example, would not have identified the grave democratic threat posed by systematic infiltration from the Internet Research Agency.

The same applies for the numerous calls for increased media literacy in public debates, promoting the idea that citizens can somehow learn to spot manipulation.<sup>62</sup> If disguised prop-

---

**A first step, then, is to stop idealizing technological quick fixes and instead approach the issue as a systemic challenge requiring political solutions in the form of national and supranational legislation.**

---

aganda is well made, as was the case with the Internet Research Agency, users, however literate, will have no way of spotting it. This has become increasingly clear in the wake of the Russian campaign against the United States.<sup>63</sup> While technological systems for detecting social bots and fake accounts might help identify and poke holes in the surface of the problem, addressing its roots will rely on increased scrutiny and informed political action. Thus, a first step is to stop idealizing technological quick fixes and instead approach the issue as a systemic challenge requiring political solutions in the form of national and supranational legislation.

#### **POTENTIAL WAYS FORWARD: PREVENTION AND SCRUTINY**

In order to minimize the potential threat of disguised propaganda in contemporary democracies, political solutions need to focus on preventing future campaigns and ensuring open scrutiny in cases of attack. In relation to prevention, increased funding for national security agencies represents one important step toward tracking down and disarming disguised operations before they influence political discourse and elections. This type of solution has already been proposed or implemented in both Europe and the United States.<sup>64</sup> In March 2018, the U.S. federal government unveiled a spending bill containing \$380 million for safeguarding U.S. voting systems and a \$307 million increase in the FBI’s budget for “counter-intelligence efforts to protect against Russia cyber attacks.”<sup>65</sup> Increased funding represents an important step. However, far less


attention has been given to the equally important issue of handling attacks if, or rather when, they occur. A key solution to minimizing the corrosive effect of disguised propaganda lies in transparent public scrutiny, both to maintain an informed public sphere and to inform appropriate political responses to a continually evolving threat.

Without thorough examination and analysis, disguised propaganda can potentially wreak havoc: not only through its online operations, but also through misinformed and corrosive public debates, technological quick fixes, and flawed policy responses. Propaganda theory teaches us that disguised campaigns are continually evolving, adapting to political contexts and technologies. In cases of attack, informed responses are vital. Ineffective solutions might potentially cause more harm than good. The goal of propaganda, such as that of the Internet Research Agency, is to create division and polarization. Misguided solutions might increase this effect by censoring or blaming particular voter groups. Democratic governments and international political bodies need to have clear goals for ensuring transparency and thorough examination in cases of attack. In this regard, legislation is critical, as social media companies have clear incentives to counteract openness. In the case of disguised propaganda in the U.S. elections, fragmented information has only become public due to immense political pressure and protests against social media policies from journalists and scholars. In future cases, perhaps in countries with less legislative influence over Facebook and Twitter, it is even more doubtful that these companies will cooperate transparently. Lawmakers need to proactively ensure such cooperation.

12

In order to understand why social media companies oppose openness, we must look at their business models. From a business perspective, platforms have to walk a line between maximizing engagement and avoiding public backlash. User engagement represents the basic currency of companies such as Facebook and Twitter, and their aim is to maximize it. Engagement is crucial not only because it enables more exposure to ads, but also because it enables companies to obtain more information about their users, which can be used to make ads more precise. If companies invest large amounts of resources in content removal, they hurt their own business model, as this content might have been highly engaging. At the same time, publicity around misinformation and propaganda might discourage users from interacting on platforms and result in increased regulation. As a result, social media platforms have little incentive to increase transparency even if this could help address the complex democratic threat of disguised propaganda. Before the recent public backlash against social media, content removal practices were already highly obscure and inconsistent. They

furthermore relied almost exclusively on users to report cases of violations.<sup>66</sup> Political solutions to disguised propaganda must counteract these opaque practices and ensure transparency in cases of attack. Citizens across the political spectrum should demand legislation—whether national or international—from their politicians. Companies like Twitter and Facebook should be legally obligated to investigate the risk of disguised propaganda operations in all democratic countries in which they operate. If they identify such activities, companies should be legally obliged to put forth this information and make the data available for public scrutiny. Otherwise, it will be impossible to address the roots of the ever-evolving democratic threat of disguised propaganda.

In the midst of these developments, there are also positive initiatives that should be applauded. In June 2018, Facebook launched a new tool that makes it possible to view all ads currently run on the platform. The system, open for all, lets users search for political ads dating back seven years.<sup>67</sup> Both Facebook and Twitter also eventually shared data on the Internet Research Agency's operations and took measures to inform the hundreds of thousands of Facebook users that were targeted. As outlined, however, these changes only came after grave political pressure. Accordingly, social media companies are unlikely to commit to any long-term solutions, as their business models simply do not incentivize democratic oversight. This especially holds true outside the United States, where companies like Facebook and Twitter are far more detached from democratic governments. If disguised propaganda campaigns take hold in Europe, Asia, South America, Africa, or Australia, it is unlikely that companies will collaborate as willingly and transparently as with U.S. lawmakers. Consequently, it remains crucial for political actors and civil society to demand transparency through new regulation that ensures it, not just in the United States but in democracies worldwide. While prevention is crucial, thorough public analysis and awareness in cases of attack is equally fundamental for democracy. 

13

## NOTES

1. Jacques Ellul, *Propaganda: The Formation of Men's Attitudes* (New York: Vintage Books, 1965), 9.
2. Published in French in 1962 and in English in 1965.
3. Johan Farkas and Christina Neumayer, "Disguised propaganda from digital to social media," in *The Second International Handbook of Internet Research*, ed. Jeremy Hunsinger, Lisbeth Klastrup, and Matthew M. Allen (New York: Springer, 2018).
4. Johan Farkas and Jannick Schou, "Fake News as a Floating Signifier: Hegemony, Antagonism and the Politics of Falsehood," *Javnost – The Public* 25, no. 3 (2018).
5. "Edward Bernays, 'Father of Public Relations' And Leader in Opinion Making, Dies at 103," *New York Times*, March 10, 1995; Edward L. Bernays, *Propaganda* (New York: Horace Liverlight, 1928).
6. Bernays, *Propaganda*, 159.

7. *Ibid.*, 10.

8. *Ibid.*, 153.

9. *Ibid.*, 43–4.

10. Martin J. Manning and Herbert Romerstein, *Historical Dictionary of American Propaganda* (Westport: Greenwood Press, 2004), 163.

11. Ellul, *Propaganda: The Formation of Men's Attitudes*, 239.

12. *Ibid.*, 241.

13. *Ibid.*, 16.

14. *Ibid.*, 239.

15. John Nichols and Lawrence C. Soley, *Clandestine Radio Broadcasting: A Study of Revolutionary and Counterrevolutionary Electronic Communication* (New York: Praeger, 1987).

16. Howard Becker, "The Nature and Consequences of Black Propaganda," *American Sociological Association* 14, no. 2 (1949): 221.

17. As noted by Professor of Sociology, Jessie Daniels, however, the terminology has obvious drawbacks due to its unfortunate racial connotations: see Jessie Daniels, "Cloaked Websites: Propaganda, Cyber-Racism and Epistemology in the Digital Era," *New Media & Society* 11, no. 5 (2009): 659–83.

18. Ellul, *Propaganda: The Formation of Men's Attitudes*, 262.

19. Manuel Castells, *Networks of Outrage and Hope: Social Movements in the Internet Age* (Cambridge: Polity Press, 2012), 6.

20. Megan Boler and Selena Nemorin, "Dissent, Truthiness, and Skepticism in the Global Media Landscape: Twenty-First Century Propaganda in Times of War," in *The Oxford Handbook of Propaganda Studies*, ed. Jonathan Auerbach and Russ Castronovo (Oxford: Oxford University Press, 2013), 411.

21. Anna Lauren Hoffmann, Nicholas Proferes, and Michael Zimmer, "Making the World More Open and Connected: Mark Zuckerberg and the Discursive Construction of Facebook and Its Users," *New Media & Society* 20, no. 1 (2016): 199–218.

22. Alessandro Bessi and Emilio Ferrara, "Social Bots Distort the 2016 US Presidential Election Online Discussion," *First Monday* 21, no. 11 (2016).

23. Bence Kollanyi, Philip N. Howard, and Samuel C. Woolley, "Bots and Automation over Twitter during the U.S. Election," ComProp Data Memo, 2016, <http://politicalbots.org/wp-content/uploads/2016/10/Data-Memo-First-Presidential-Debate.pdf>.

24. Marco T. Bastos and Dan Mercea, "The Brexit Botnet and User-Generated Hyperpartisan News," *Social Science Computer Review* (2017): 1–18.

25. Chengcheng Shao et al., "The Spread of Fake News by Social Bots," *ArXiv*, July 24, 2017, <https://arxiv.org/abs/1707.07592v2>.

26. Bessi and Ferrara, "Social Bots Distort the 2016 US Presidential Election Online Discussion."

27. Natasha Bertrand, "Twitter Will Tell Congress That Russia's Election Meddling Was Worse than We First Thought," *Business Insider*, October 30, 2017.

28. "Update on Twitter's Review of the 2016 U.S. Election," Twitter, 2018, [https://blog.twitter.com/official/en\\_us/topics/company/2018/2016-election-update.html](https://blog.twitter.com/official/en_us/topics/company/2018/2016-election-update.html).

29. Alex Stamos, "Authenticity Matters: The IRA Has No Place on Facebook," Facebook, April 3, 2018, <https://newsroom.fb.com/news/2018/04/authenticity-matters/>.

30. Economist Staff, "Russian Disinformation Distorts American and European Democracy," *Economist*, February 22, 2018; Olga Bugorkova, "Ukraine Conflict: Inside Russia's 'Kremlin Troll Army,'" *BBC News*, March 19, 2015, <https://www.bbc.com/news/world-europe-31962644>.

31. Alec Luhn, "Inside the Russian 'Troll Factory' That Reached Millions of US Voters with Inflammatory Ads," *Telegraph*, October 20, 2017, <http://www.telegraph.co.uk/news/2017/10/20/inside-russian-troll-factory-reached-millions-us-voters-inflammatory/>; W. Lance Bennett and Steven Livingston, "The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions," *European Journal of Communication* 33, no. 2 (2018): 122–39.

32. Max Seddon, "Documents Show How Russia's Troll Army Hit America," *BuzzFeed News*, June 2, 2014, <https://www.buzzfeednews.com/article/maxseddon/documents-show-how-russias-troll-army-hit-america>.

33. Bugorkova, "Ukraine Conflict: Inside Russia's 'Kremlin Troll Army.'"
34. Research is still to uncover the exact strategic uses of bots by the IRA, but bots were likely deployed both as means of spreading messages further on social media platforms and for creating credibility through large amounts of followers, likes, and shares related to key profiles operated by the agency.
35. Jessica Guynn, Nick Penzenstadler, and Brad Heath, "We Read Every One of the 3,517 Facebook Ads Bought by Russians. Here's What We Found," *USA Today*, March 13, 2018; Issie Lapowsky, "How Russian Facebook Ads Divided and Targeted Us Voters Before The 2016 Election," *Wired*, April 18, 2018.
36. Ryan Browne, "Cambridge Analytica Whistleblower Says Facebook Users' Data Could Be Stored in Russia," *CNBC*, April 9, 2018; Isobel Asher Hamilton, "Cambridge Analytica's Facebook Data Was Accessed in Russia," *Business Insider*, July 18, 2018.
37. P.R. Lockhart, "The Mueller Indictment Offers New Details on How Russian Trolls Stoked Racial Tensions," *Vox*, February 16, 2018.
38. Alana Abramson, "Here's What We Learned From the Ads Bought by Russian Trolls in 2016," *Time Magazine*, May 19, 2018.
39. Charles M. Blow, "Attacking the 'Woke' Black Vote," *New York Times*, February 18, 2018; Matt Burgess, "Twitter Has Admitted Russian Trolls Targeted the Brexit Vote (a Little Bit)," *Wired*, February 8, 2018.
40. Matt Burgess, "Twitter Has Admitted Russian Trolls Targeted the Brexit Vote (a Little Bit)," *Wired*, February 8, 2018.
41. Grand Jury for the District of Columbia, "Indictment," 2018, <https://www.justice.gov/file/1035477/download>.
42. Grand Jury for the District of Columbia, 6.
43. Olivia Zolon, "Facebook's fake news: Mark Zuckerberg rejects 'crazy idea' that it swayed voters," *Guardian*, November 11, 2016, <https://www.theguardian.com/technology/2016/nov/10/facebook-fake-news-us-election-mark-zuckerberg-donald-trump>.
44. Smith David, "Mark Zuckerberg Vows to Fight Election Meddling in Marathon Senate Grilling," *The Guardian*, April 11, 2018, <https://www.theguardian.com/technology/2018/apr/10/zuckerberg-facebook-testimony-latest-news-regulation-congress>.
45. "Russian Ads Released by Congress," Facebook, May 18, 2018, <https://newsroom.fb.com/news/2018/05/russian-ads-released-by-congress/>; Tessa Lyons, "Increasing Our Efforts to Fight False News," Facebook, June 21, 2018, <https://newsroom.fb.com/news/2018/06/increasing-our-efforts-to-fight-false-news/>; David Ingram, "Twitter changes strategy in battle against internet 'trolls'," *Reuters*, May 15, 2018, <https://www.reuters.com/article/us-twitter-harassment/twitter-changes-strategy-in-battle-against-internet-trolls-idUSKCN1IG2HK>.
46. Alex Hern, "Russian Troll Factories: Researchers Damn Twitter's Refusal to Share Data," *The Guardian*, November 15, 2017, <https://www.theguardian.com/world/2017/nov/15/russian-troll-factories-researchers-damn-twitters-refusal-to-share-data>.
47. Ben Popken, "Twitter Deleted 200,000 Russian Troll Tweets. Read Them Here," *NBC News*, February 14, 2018.
48. Jack Morse, "Mark Zuckerberg's Refusal to Make Russia-Linked Facebook Ads Public Is a Disgrace," *Mashable*, September 22, 2018, <https://mashable.com/2017/09/21/zuckerberg-russia-ads-release-public/#prHPqyzkVaq>.
49. Issie Lapowsky, "House Democrats Release 3,500 Russia-Linked Facebook Ads," *Wired*, October 5, 2018.
50. Vijaya Gadde and Yoel Roth, "Enabling Further Research of Information Operations on Twitter," Twitter, October 17, 2018, [https://blog.twitter.com/official/en\\_us/topics/company/2018/enabling-further-research-of-information-operations-on-twitter.html](https://blog.twitter.com/official/en_us/topics/company/2018/enabling-further-research-of-information-operations-on-twitter.html).
51. Renee DiResta et al., "The Tactics & Tropes of the Internet Research Agency," *New Knowledge*, 2018.
52. Will Oremus, "The Real Scandal Isn't What Cambridge Analytica Did," *Slate*, March 20, 2018; Sam Meredith, "Facebook-Cambridge Analytica: A timeline of the data hijacking scandal," *MSNBC*, April 10, 2018.

53. Natasha Lomas, “Facebook was warned about app permissions in 2011,” *TechCrunch*, March 24, 2018.

54. Max Schrem, “Complaint against Facebook Ireland Ltd. – 13 Applications,” August 18, 2011.

55. Josh Constine, “Facebook Is Shutting Down Its API For Giving Your Friends’ Data To Apps,” *TechCrunch*, April 28 2015.

56. Marco Bastos and Shawn T. Walker, “Facebook’s data lockdown is a disaster for academic researchers,” *The Conversation*, April 11, 2018, <http://theconversation.com/facebook-s-data-lockdown-is-a-disaster-for-academic-researchers-94533>.

57. “Russian Ads Released by Congress,” Facebook, May 18, 2018, <https://newsroom.fb.com/news/2018/05/russian-ads-released-by-congress/>.

58. Johan Farkas, Jannick Schou, and Christina Neumayer, “Cloaked Facebook Pages: Exploring Fake Islamist Propaganda in Social Media,” *New Media & Society* 20, no. 5 (2018): 1850–867.

59. Jack Dorsey, “If You Want to Improve Something, You Have to Be Able to Measure It. The Human Body Has a Number of Indicators of Overall Health, Some Very Simple, like Internal Temperature. We Know How to Measure It, and We Know Some Methods to Bring It Back in Balance,” Twitter, March 1, 2018, <https://twitter.com/jack/status/969234283633115137>.

60. Jack Dorsey, “What We Know Is We Must Commit to a Rigorous and Independently Vetted Set of Metrics to Measure the Health of Public Conversation on Twitter. And We Must Commit to Sharing Our Results Publicly to Benefit All Who Serve the Public Conversation,” Twitter, March 1, 2018, <https://twitter.com/jack/status/969234283633115137>.

61. Ellul, *Propaganda: The Formation of Men’s Attitudes*, 262.

62. Gianfranco Polizzi, “Fake news and critical literacy in the digital age: sharing responsibility and addressing challenges,” *LSE Media Policy Project*, May 21, 2018, <http://blogs.lse.ac.uk/mediapolicyproject/2018/05/21/fake-news-and-critical-literacy-in-the-digital-age-sharing-responsibility-and-addressing-challenges/>; “Kate Kaye, “Degrassi, Fake News and Why We Need Media Literacy More than Ever,” *Medium*, June 11, 2018.

63. Johan Farkas and Marco Bastos, “IRA Propaganda on Twitter: Stoking Antagonism and Tweeting Local News,” Proceedings of the 9th International Conference on Social Media & Society (2018): 281–85; Renee DiResta et al., “The Tactics & Tropes of the Internet Research Agency,” *New Knowledge*, 2018; Philip N. Howard et al., “The IRA, Social Media and Political Polarization in the United States, 2012–2018,” *Computational Propoganda Research Project*, 2018.

64. Elana Schor, “Dems demand budget boost to shield midterms from Russian interference,” *Politico*, February 2, 2018; Katja Brandt Andersen, “Regeringen frygter russisk manipulation af dansk valg: Klar med hemmelig plan,” TV2, September 7, 2018, <http://nyheder.tv2.dk/politik/2018-09-07-regeringen-frygter-russisk-manipulation-af-dansk-valg-klar-med-hemmelig-plan>.

65. Dustin Volz, “U.S. Spending Bill to Provide \$380 Million for Election Cyber Security,” *Reuters*, March 21, 2018, <https://www.reuters.com/article/us-usa-fiscal-congress-cyber/u-s-spending-bill-to-provide-380-million-for-election-cyber-security-idUSKBN1GX2LC>.

66. Johan Farkas and Christina Neumayer, “‘Stop Fake Hate Profiles on Facebook’: Challenges for Crowdsourced Activism on Social Media,” *First Monday* 22, no. 9 (2017); Sarah T. Roberts, “Commercial Content Moderation: Digital Laborers’ Dirty Work,” in *The Intersectional Internet: Race, Sex, Class and Culture Online*, ed. Safiya Umoja Noble and Brendesha M. Tynes (New York: Peter Lang, 2016); Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media* (New Haven: Yale University Press).

67. “Russian Ads Released by Congress,” Facebook, May 19, 2018, <https://newsroom.fb.com/news/2018/05/russian-ads-released-by-congress/>.