Microtargeting as Information Warfare

Jessica Dawson, Ph.D.

ABSTRACT

Foreign influence operations are an acknowledged threat to national security. Less understood is the data that enables that influence. This article argues that governments must recognize microtargeting—data informed individualized targeted advertising—and the current advertising economy as enabling and profiting from foreign and domestic information warfare being waged on its citizens. The Department of Defense must place greater emphasis on defending servicemembers' digital privacy as a national security risk. Without the ability to defend this vulnerable attack space, our adversaries will continue to target it for exploitation.

INTRODUCTION

In September 2020, General Paul Nakasone, NSA Director and Commander of U.S. Cyber Command, called foreign influence operations "the next great disruptor."[1] Nearly every intelligence agency in the United States government has been sounding the alarm over targeted influence operations enabled by social media companies since at least 2016, even though some of these operations started earlier. What often goes unstated and even less understood is the digital surveillance economy underlying these platforms and how this economic structure of trading free access for data collection about individuals' lives poses a national security threat. Harvard sociologist Shoshana Zuboff calls this phenomenon "surveillance capitalism [which] unilaterally claims human experience as free raw material for translation into behavioral data."[2] This behavioral data is transformed into increasingly accurate micro-targeted advertising.[3] The new surveillance capitalism has enabled massive information warfare campaigns that can be aimed directly at target populations. The predictive power of surveillance capitalism is not only being leveraged for advertising success but increasingly harnessed for mass population control[4] enabled by massive amounts of individually identifiable, commercially available data with virtually no oversight or regulation.

Jessica Dawson is an Assistant Professor and Research Scientist at the Army Cyber Institute. She holds a Ph.D. in sociology from Duke University and her research is focused on the intersection of social cohesion, narratives, and technology.

This is not to say there is no oversight—data use and collection by the intelligence community is subject to significant oversight and regulation. This article, critically, is not about data use laws and areas that are already regulated. Technology companies such as Facebook or Google exist in ungoverned spaces and are not subject to regulations like specific industries such as banking, education, or health care providers. For example, medical companies are clearly bound by Health Insurance Portability and Accountability Act (HIPAA) and the banking industry is bound by Sarbanes Oxley, which includes data regulation components. Conversely, the tech companies actually have a shield from liability based on the Communications Decency Act, Section 230.[5] This law places tech companies outside of regulatory restrictions rather than providing any meaningful limit on their actions and as a result creates a national security risk for the Department of Defense (DoD).

For example, Facebook has acknowledged its platforms'[1] abilities to help political campaigns target voters to defeat ballot initiatives[6] and, more recently, Channel 4 News in the United Kingdom reported on how political action committees (PACs) in the US targeted voters to decrease opposition turnout using the Cambridge Analytica dataset.[7] These incidents, and others have caused people to look at the concentrated power companies leveraged via these platforms. This article argues microtargeting allows individual-level messaging to be deployed to influence voting behavior and is able to be leveraged for more insidious dis/misinformation campaigns. What started as a way for businesses to connect directly with potential customers has transformed into a disinformation machine at a scale that autocratic governments of the past could only imagine. The US must recognize the current advertising economy as enabling and profiting from information warfare being waged on its citizens and address the threat.

[1] Facebook also owns Instagram, Oculus, and WhatsApp.

Fundamentally, domestic digital privacy is a national security issue. The DoD should place greater emphasis on defending servicemembers' digital privacy as a national security threat. This is not a hypothetical issue. China recently accused a staff sergeant of being patient zero in the COVID-19 pandemic, which unleashed a torrent of attacks online against her.[8] Targeting of key individuals by foreign agents has always been a national security threat, and yet the current advertising ecosystem is not currently widely recognized as an attack space. Consider a defense contractor that targets a senior military leader in order to sway his/her decision on an acquisition. What if a missile systems operator is identified and targeted for digital blackmail by North Koreans? Worse, consider if China is successful in convincing key US military officers that it poses no threat in the Pacific, leading to changes in the force posture that work in China's benefit. The murder of a Mexican American soldier and subsequent social media outrage at Fort Hood in 2020 demonstrates the impact a local incident can have on the national scale. All of this is enabled, with surgical precision, by the microtargeting advertising environment, fed by data gathered through apps, cell phones, games, and more.

UNDERSTANDING DATA

Everyone who has ever bought a car or house, or applied for a credit card, understands that companies gather data about you, the consumer. An individual's credit report shows what accounts they have, and the balances owed, and helps lenders determine if an individual is at high risk (low credit score) or low risk (high credit score) of paying back the loan. In a way, this is quantified trust. Credit reports are also auditable—every American is entitled to free credit reports each year to ensure that no one has opened accounts in their name or to ensure that nothing on the report is erroneous.

Expanding further, companies such as Mastercard know everything an individual has purchased on their credit card. Amazon knows what you have purchased on Amazon as well as how you paid for it. Companies have been gathering data on their customers for years, but the key element is that Mastercard knows one piece of this information, Amazon another, and so on. They do not know how you voted, for example, nor should they include that information in whether you get approved for a credit card. All of this changed as data became more ubiquitous and storage became cheaper.

In the early days of the Internet, advertising paved the way to support platforms' ability to be "free" —in exchange for access, customers gave up certain data. In turn, these companies used the data to better target advertising to potential buyers. First Google, then Facebook, figured out how to monetize all the information on individuals. Facebook quickly realized how much information it had on individuals and how much it could continually gather. Other data brokers, such as Experian, Axiom, Magellan, and others, "followed people throughout their digital lives, through every move and every purchase, collecting as much as possible in order, ostensibly, to provide credit scores but also to make a profit in selling that information."[9] Despite

initial outrages over privacy invasion, it became second nature to expect everything for free or low-cost subscriptions—music in terms of apps like Pandora, Spotify, or YouTube in terms of free music videos, tv shows etc., or Tiktok, allegedly the last happy place on the Internet. All this entertainment was accessed for free—or was it? The old adage that if you are not paying for a product you are the product is not entirely true. Not only are we the product but every aspect of our daily lives provides the raw material for this entire economic model. Companies are making billions of dollars off everyday life events with functionally no oversight, no regulation, and no meaningful ability to opt out.[10]

ADVERTISING THEN AND NOW

There is an old quote in advertising that about 50% of it works, but advertisers don't know which 50%.[11] Advertising has always been only "one small piece of getting consumers to buy"[12] and exists within a larger cultural framework. The holy grail of advertising has always been "bring a particular message to a particular moment to have a high probability of influencing their behavior."[13] That desired behavior change has typically been targeted toward purchasing a product, and "mass behavior medication techniques [were defined as] unacceptable threats to individual autonomy and the democratic order."[14] This instrumentarian power has been justified as unavoidable and inevitable in the pursuit of more targeted advertising. Yet, only once the power of this data began being used for political purposes did governments and people slowly begin to realize the level of influence a few private companies exert over their perception. Over the last 20 years, new "more complex means of behavior modification" have emerged along with a new, logic-based "instrumentarian power [which] knows and shapes human behavior towards other's ends."[15] While culture is a highly contested concept, for this article, it will be defined as "an attention-focusing institution."[16] Social media design has been focused on capturing and selling access to that attention by better targeting content to keep people engaged.[17] Political advertising has benefited tremendously from this new, highly detailed information about potential voters.

Social science research typically uses demographic groups such as race, gender, and political affiliations to identify social groups' patterns and trends. For example, the 1980 election was the first time there was a significant gender gap between women and men voters in support for President Reagan.[18] Prior to surveillance capitalism enabling targeted advertising, political advertising was similar to other social science research. People were broken into large categories using variables that served as proxies for meaningful behavior.[19] Women were more likely to vote for education and healthcare than men, who were more likely to be motivated by national defense issues and the economy. Republicans were motivated by different issues than Democrats.[20] However, these categories have historically been large and imprecise, which meant messaging had to be broad, and, as a result, broad messages would not necessarily resonate with the intended audience.

In order to understand why the transition to surveillance capitalism has enabled a new form of information warfare, we must first understand microtargeting as enabled by algorithms. These algorithms—computer code that shapes outcomes and records the responses—should be understood as "products of social forces."[21] These algorithms did not always reflect such detailed knowledge about individual users; however, as more and more users "shared" more and more details about their lives, Facebook realized it had tremendous pools of new data from which to glean—and monetize—insights. "When people signed on to play games such as Candy Crush on Facebook, and clicked "yes" to the terms of service for that third-party app, they were opting in to give their data and the data of all their friends, for free, to the app developers and then, inadvertently, to everyone with whom that app developer had decided to share the information."[22]

Data-driven insights could be used to better target advertising in more and more effective ways. In his book *Mindf*ck*, Cambridge Analytica whistleblower Chris Wylie describes discovering suburban women who do yoga, shop at Whole Foods, and yet attend anti-LGBTQ churches and donate to anti-gay causes.[23] Messages targeted to a voter in this demographic would have to be wholly different than messages targeted toward women who match those same demographic characteristics but do not attend anti-LGBTQ churches. A Facebook employee was stunned to discover that advertisements for TikTok that looked like they would be better targeted toward teen girls were in fact accurately targeted toward his demographic: middle aged men were being targeted with videos of teen girls dancing. The accuracy of these algorithms is still being investigated by researchers but evidence suggests that "based on only sixty-eight Facebook 'likes' an individual user might have garnered...those few 'likes' [could] predict skin color, sexual orientation, political party affiliation, drug and alcohol use, and even whether a person had come from an intact or a divorced household."[24] Data-enhanced modeling is arguably more accurate than human assessments.[25] The more data available to these companies, the greater accuracy that these messages can be targeted to drive desired behavior. There is a saying that "Google knows you better than your mother" because it has access to nearly every aspect of an individual's online activity from appointments, to meetings to photos and searches, which may be highly embarrassing if they were ever to become public.[26] The Facebook newsfeed is not displaying articles and updates in chronological order—users are seeing content that is continually tested to capture more of the user's attention and spark emotional response.[27]

FROM MICROTARGETING POLITICAL MESSAGES TO SOCIAL CONTROL

As early as 2011, the Defense Advanced Research Projects Agency (DARPA) researched social media information-sharing patterns and social media psychological profiling.[28] Combining demographic information with psychological profile information like the Big Five Personality test apparently increased the accuracy of voting messaging.[29] The Big Five Personality trait test measures people along five-axes: openness, agreeableness, conscientiousness, neuroticism,

and excitableness.[30] For example, according to Cambridge Analytica's research, Republicans tend to rate higher on conscientiousness than Democrats. The 2008 Obama campaign was one of the first to purchase additional data such as magazine subscriptions and automobile buying history to provide "more context to each voter…yielding far more accurate information."[31] The possibilities for using this detailed information to inform political messaging were realized early on by the Obama campaign, which was the first to use the term "persuadables" in attempting to quantify how likely some voters were to be persuaded to cast their vote for Obama.[32] A key aspect of these efforts is a form of experimentation known as A/B testing to find the right content to elicit the desired response.

Following the 2016 presidential election, people became aware of the scale and detail associated with microtargeting political campaigns. As a result, Cambridge Analytica became one of the most notorious examples of data-assisted political microtargeting. It took traditional voter research and aggregated it with unprecedented levels of data. Cambridge Analytica developed an app called "My Personality…to build the first precise models of millions of Facebook users."[33] It combined census data with political affiliation with shopping preferences. From Experian, it purchased "airline memberships, media companies, charities, amusement park attendances as well as government licenses."[34] Combing all of this along with social media information, church attendance behavior, personality information, and voter polling provided a level of detailed analysis on individuals broken down by voting district.[35] By framing messaging according to "psychometric profiles," behavior modification can be achieved more reliably. "Persuasive appeals that were matched to people's extraversion or openness to experience level resulted in up to 40% more clicks and up to 50% more purchases than their mismatching or un-personalized counterparts."[36] Some of the marketing material claimed to have up to 750 data points per person. The company also used traditional social science research methods like focus groups to determine what issues on the ground people cared about rather than relying on representative surveys. This gave its analysts powerful underlying knowledge of their target audiences. For example, the slogan "Drain the Swamp" rose out of focus groups conducted two years before the 2016 election.[37]

Beyond domestic political campaigns, governments like the People's Republic of China are using data-driven analytics to exert social control over their own population. Over 1 billion Chinese users conduct over 60% of their transactions through the app WeChat,[38] giving the Chinese Communist Party (CCP) data not only about what people are buying but also the opportunity to deny people the ability to make purchases. WeChat "is state-recognized, electronic social-security identification and ID card" that "is the dream of the surveillance state."[39] China has used WeChat to crack down on anything which poses a threat to the harmony and stability of the state. For example, it has 75 behavioral indicators such as growing a beard or calling a relative overseas that allegedly indicate potential religious radicalization.[40] This is not merely a concern for China's citizens. Tencent, a China owned company that is one of the largest gaming companies in the world, owns major stakes in popular games like Fortnite (console-based), Riot

Games (pc games), and Supercell (mobile). Recently, the U.S. Congress has begun questioning what data is being gathered and collected by the company and sent back to China's servers.[41] Tiktok and Zoom have also come under scrutiny due to lack of clarity over what is gathered from individuals' devices and sent back to China. While Chinese data collection is perceived as a national security threat, domestic data collection is viewed as a digital privacy issue—these are not separate issues. Domestic digital privacy is fundamentally linked to national security.

MICROTARGETING AS INFORMATION WAR

The main difference between political microtargeting and military information operations is who is doing the targeting and who is the target. Information warfare is defined as "planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives."[42] There is very little difference between the methods of analysis, data collection, and actions used to influence behavior. Information warfare campaigns develop "insights on how best to persuade the target to change its behavior to one that is more favorable to US interests."[43] Consumer patterns used in advertising help reveal additional insights about a population such as life course events. One now notorious story about successful digital targeting of advertising is the story of a father who received advertising for babies only to discover that his daughter was pregnant. The algorithm knew before she had told him.[44]

The fact that one is used on perceived foreign adversaries, whereas one is used to sell the latest hot holiday toy or to influence elections, is a distinction without a difference. The objective of surveillance capitalism-enabled advertising and information warfare is the same: to influence an individual's behavior change in support of someone else's goals. In advertising, the goal is to motivate someone to make a purchase or sign up for a mailing list or otherwise take action related to the sale of a product. What happens when these tools are used for darker purposes?

Social media reveals what people attach themselves to and data-aggregated microtargeting has allowed it to be weaponized.[45] In the US, the digital advertising market is estimated to be worth over 32 billion as of 2017, and the vast majority of this spending is concentrated on Facebook and Google.[46] This is only the advertising spending—not the value of the data gathered and purchased. Recent independent investigations have raised questions about the accuracy of the ad campaigns on Facebook with Uber revealing they had cut their advertising budget by two thirds and saw no change in their engagement. The actual scope and value of this market are surprisingly difficult to measure, but using proxies, they can be estimated. For example, the smart home market, which includes things like Nest thermostat or Ring doorbell, is estimated to be worth "36 billion dollars in 2018 and expected to reach 151 billion by 2023."[47] The smart home market is an excellent example of the scale and scope of surveillance technologies.

Consider when Sarah Huckabee Sanders, the White House press secretary, tweeted about her 2-year-old being able to buy toys via Alexa.[48] Sanders informed the entire world that she—a person with direct daily access to the President of the United States—had what was functionally a listening device *in her home*. While there is no evidence her smart speaker was hacked, it remains a potent vulnerability for everyone.

The information extracted by the surveillance economy has granted anyone with the means to access these systems "direct access to the minds and lives of guards, clerks, girlfriends...a detailed trail of personal information that would previously have taken months of careful observation to gather."[49] Individual cell phone users can be tracked using location-based information updated in real time.[50] Recently, undergraduates at Harvard combined information available on the dark web with a purchased Experian database to identify nearly 1,000 high-net worth individuals in Washington, DC. "They were able to identify 1,000 people who have a high net worth, are married, have children, and also have a username or password on a cheating website. Another query pulled up a list of senior-level politicians, revealing the credit scores, phone numbers, and addresses of three U.S. Senators, three U.S. Representatives, the mayor of Washington, DC, and a Cabinet member."[51] The sheer magnitude of information commercially available on individuals at scale makes it critically important that researchers understand "which behaviors of large groups of people can be influenced by applying psychological mass persuasion—both in their interest and against their best interest."[52] This information is available legally from a wide variety of data brokers to anyone, including US adversaries.

ALGORITHMIC POLARIZATION

Fake news spreads faster than accurate news,[53] breaking down trust in institutions[54] that was already eroding over the last 40 years of growing economic inequality.[55] Following the Senate investigation into Russian election interference, the bipartisan, unclassified report detailed how Russian operatives targeted infrastructure during the 2016 US election using Facebook-targeted advertising.[56] Additionally, Russian active measures used social media to exacerbate existing cultural tensions within the US.[57] Not everyone was caught unaware: Black feminists online realized some accounts were masquerading as Black activists and quickly began working together to identify misinformation attempts with the hashtag #yourslipisshowing.[58] Social media content is optimized to produce polarizing content[59] and researchers have demonstrated the contagion effect of highly emotional content.[60] The social contagion effect of social media has been well documented. Facebook suffered an incredible backlash when it was revealed that it had manipulated people's emotions by choosing happy or sad post updates and then monitoring people's subsequent reactions.[61] Other research has demonstrated the contagion effect of domestic terror groups.[62] The US military is not immune to these polarization effects, creating a significant attack surface for adversaries to weaponize against DoD. And yet, the ability to understand the attack surface within DoD is limited by law, some of the only legal restrictions that exist restricting who can access these data.

OPERATIONAL VULNERABILITIES

DoD is legally restricted from "collecting intelligence against US persons" by Executive Order (E.O.) 12333.[63] This, along with service-specific regulations like Army Regulation 381-10, has been interpreted to restrict analysis of publicly available data such as the data gathered on social media platforms or other data brokers. While there are exceptions to these legislative restrictions, the Army has largely kept hands off of domestic social media or its understanding of the underlying data. The result of this is that there is no agency within the Army charged with understanding the ways in which US adversaries can manipulate the domestic information warfare space. Despite the fact that this data about US forces is readily available to our adversaries, the Army is unable to assess or respond to threats in the social media space. For example, when a recent case at Fort Hood involving missing soldier Vanessa Guillen went viral, Army leaders did not have the appropriate tools to understand the domestic social media situation, i.e., how the message was being amplified and spread.[64]

The restraint on the US government's ability to understand its own population's social media and digital footprint ignores the ability of other governments and other agencies to engage in this same behavior. *The New York Times* recently purchased cell phone data on over two million users and showed how it was able to individually track people to and from work at the Pentagon.[65] This regulatory gray zone also ignores how government agencies can contract around these restrictions. Recently, *The Wall Street Journal* reported that the Department of Homeland Security (DHS) had purchased commercially available cell phone location data to target undocumented immigrants.[66] The DoD is not completely unaware of these vulnerabilities and has purchased some of these databases in order to aid foreign operations.[67] After a Strava database leak revealed forward operating base perimeters due to personal GPS training devices, the military banned its use in deployed environments.[68] It has also banned the China-owned app TikTok from government cell phones but has not taken steps to prohibit soldiers from having it on their personal devices.[69] These are good first steps, but the implications are much bigger than specific apps or locations.

The misinformation environment is not only an overseas operational concern. The considerable misinformation surrounding masks during the COVID pandemic negatively impacted training and readiness for the military. Entire ships were docked as the crew became infected and the military infection rate in some cases exceeded the national level.[70] The military is made up of regular Americans and is not immune to the political debate about masks and freedom.[71] Algorithmic targeting of servicemembers with misinformation has a very different impact on national defense than on other communities, and these consequences do not disappear within the geographic boundaries of the US.

Military social media guidance offers limited utility in protecting users' data from data collection. Other than the U.S. Special Operations Command privacy quick reference guides sheets, there is no policy or directive outlining how soldiers can or should remove their information

from public databases such as Spokeo or others. Servicemembers are not advised to avoid popular but famously insecure email services like Gmail, Yahoo, or MSN. Soldiers receive no advanced warning about the risks of installing Facebook's Messenger on their phones, which gives the company access to their photos, contacts, location data, and messages.[72] Given the notorious difficulty of using DoD systems, forcing soldiers off free tools would likely backfire, but beyond that, any guidance targeted at the individual level is destined to fail. Collective efforts are necessary.

RECOMMENDATIONS

There is no way for any individual to tackle the surveillance economy.[73] Individual privacy is networked and connected.[74] Even if an individual does not have a Facebook account, Facebook has a shadow account for them,[75] collected from friends' phones, contact lists, and emails as well as data Facebook itself purchases. Privacy is not an individual effort; it is networked and requires networked solutions.[76] Location data cannot be turned off due to user requirements to ping the nearest cell phone tower and most apps fail to work if they don't have location data enabled. Additionally, the no/low cost of the current ad supported model enables public entities like schools to pivot online with little cost. Google Classroom, for example, offers cash-strapped school districts digital access but at the cost of children's privacy.[77] These tools are not inherently evil, but the lack of control and oversight over who can access their data, and with what data sets they can be combined, should be more highly scrutinized and regulated by governments. These tools are far beyond any individual's ability to manage.

The European Union's General Data Protection Regulation (GDPR) and the State of California have taken meaningful action to regulate the data privacy market, but these protections are only the beginning of what is required.[78] DoD should engage with the major social media companies to have them remove military servicemembers and their immediate family members from algorithmic targeting. DoD should also work with data brokers to prevent any servicemembers and their immediate families from having their data collected or sold. Companies that sell smart devices should be required to segregate data that comes from military households to prevent it from being converted into covert surveillance,[79] much as Furbies were once banned from secure facilities. The California Consumer Privacy Protection Act, which went into effect in 2020, allows individuals to request their information be deleted—DoD should preemptively do this for all servicemembers and families. Deleting this data would make it more difficult for individuals to be targeted for an online harassment campaign such as the sergeant accused by China of being COVID patient zero.[80] Preventing the data from being bought and sold would be another layer of protection for individuals.

Another recommendation is to limit the level of experimentation that social media companies conduct on the population. Social media companies should be subject to the same human experiment restrictions as academic institutions and medical companies. Facebook has

conducted psychological experiments on emotional contagion,[81] and the platforms are constantly being tested and revised to optimize for capturing attention. More insidiously, however, are reported Cambridge Analytica experiments that evaluated the relationships between personality and political outcomes[82] and also targeted "those who were more prone to impulsive anger or conspiratorial thinking"[83] with messages designed to inflame and provoke them, all without any meaningful informed consent. Medical companies and academic institutions are not allowed to conduct research on human subjects without informed consent and oversight to determine whether the value of the experiment is greater than the potential harm. Human subjects research was first limited after the horrors of the experimentation conducted under the Nuremberg Laws. Psychological manipulation research by the government, universities, and hospitals is dramatically limited due to concerns over individual autonomy, meaningful consent, and abusive practices.[84] Social media companies' experiments on populations should be held to the same oversight and regulation as hospitals and academic research in order to provide oversight and prevent harm.

Furthermore, the algorithms being used are opaque and not widely understood. Recent research has demonstrated how the Russians have weaponized fake military profiles against constitutional foundations such as the right to protest or certain political parties,[85] eroding US citizens trust in their military and their government. These social media companies have "allowed attack vectors on our societal cohesion...[given] direct access to the minds of US citizens."[86] Given that social media has been linked to genocide,[87] any future changes to the platforms should be halted until the algorithms' effects on individuals and society are better understood.[88] No military in its right mind would allow its servicemembers to be experimented on; yet, that is exactly what happens every day with misinformation on social media.

Part of this oversight should be to require researchers be given direct access to data and algorithms in order to understand the social and psychological aspects of social media microtargeting. There are very real questions about the validity of the claims made by these marketing companies.[89] If data is not the promised new oil but rather snake oil, governments have an obligation to reign in a potentially fraudulent market.[90] Currently, researchers are limited to what data is released by the platforms and are unable to meaningful replicate studies to test whether private companies like Cambridge Analytica actually manipulated election outcomes.[91]

Academic researchers are unable ethically to conduct the same experiments Facebook and other companies have performed and these companies should be required to grant access to universities and government agencies in order to determine what worked and how to defend against these tactics in the future. Access to this data should be highly restricted given national security concerns.

CONCLUSION

Information microtargeting, surveillance capitalism, modern advertising, and foreign influence operations are essentially synonymous and represent a national security concern that DoD and the rest of the federal government must address. In today's media environment, however, "if you make it trend, you make it true."[92] The ability to target the trending message toward people more likely to be receptive to it reduces national security and further erodes already weakened trust in institutions. Because nearly all of this data is available for purchase by anyone, surveillance capitalism has opened up an information warfare attack space on the American people, one the DoD is currently unprepared to defend. While there are limitations to what messages the US government can target at its citizens,[93] there are very few limitations on what foreign governments can target toward other populations. Current limitations are based on terms of service violations rather than national security concerns. This should stop. Facebook founder Mark Zuckerberg has stated that his company will not fact check political advertisements.[94] It has outsourced its content moderation to contractors, several of whom suffer from PTSD due to the horrors of the content to which they have been exposed.[95] Zuckerberg argues that Facebook's success is patriotic in order to stand as a bulwark against China's dominance[96]—this a deflection attempt disguising the fact that Facebook serves its own ends and not national interests.[97] There is bipartisan acknowledgment that Russia sponsored several disinformation campaigns within US geographic boundaries during the 2016 campaign.[98] Facebook initially dismissed these claims, but, as evidence mounted, it was forced to acknowledge abuse of its system.[99]

The microtargeting environment enabled by surveillance capitalism sacrifices collective security in the name of a free-market economy. Governments must wrestle with the implications of the surveillance economy sooner rather than later. This pits the interests of the companies—profit—against the Constitution and interests of national security. This is a false dichotomy. Profit tends to do better in a stable society—destabilized societies do not buy things on the Internet. There is nothing in the Constitution that prevents the government from regulating industries, especially dangerous industries and their products. For all the good these technologies have enabled, there is ample evidence that they are enabling the erosion of the foundations of freedom and democracy. Since most of these companies are based in the US, taking meaningful action to limit their reach and power over American citizens' digital lives would have meaningful global impact. It would also reestablish the US global commitment to values such as freedom and democracy by reigning in tools currently being used to undermine both. It would also offer an alternative to the global worldview of the People's Republic of China that prioritizes harmony aligned with China's interests over any conception of human rights and uses vast digital surveillance to accomplish this compliance.

NOTES

1. Bryan Sparling, "The Zhenhua Leak, IOS 14 and National Security.," LinkedIn, September 24, 2020, https://www.linkedin.com/pulse/zhenhua-leak-ios-14-national-security-bryan-sparling.
2. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power,* 1st edition (Location?PublicAffairs, 2019), 8.
3. Christopher Wylie, *Mindf*ck: Cambridge Analytica and the Plot to Break America* (New York: Random House, 2019); Brittany Kaiser, *Targeted: The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again* (Location?Harper, 2019); Sasha Issenberg, *The Victory Lab: The Secret Science of Winning Campaigns,* Reprint edition (New York: Broadway Books, 2013).
4. Zeynep Tufekci, *Twitter and Tear Gas: The Power and Fragility of Networked Protest*, Reprint edition (New Haven, CT: Yale University Press, 2018).
5. "Communications Decency Act," 47 U.S. Code § 230, accessed November 19, 2020, https://www.law.cornell.edu/uscode/text/47/230.
6. Facebook, "Case Study: Reaching Voters with Facebook Ads (Vote No on 8)" (Menlo Park, CA: Facebook for Government, Politics & Advocacy, July 2011), https://www.facebook.com/notes/us-politics-on-facebook/case-study-reaching-voters-with-facebook-ads-vote-no-on-8/10150257619200882.
7. Channel 4 News InvestigationsTeam, "Revealed: Trump Campaign Strategy to Deter Millions of Black Americans from Voting in 2016," Channel 4 News, September 28, 2020, https://www.channel4.com/news/revealed-trump-campaign-strategy-to-deter-millions-of-black-americans-from-voting-in-2016.
8. Dan Patterson, "Trolls Are Spreading Conspiracy Theories That a US Army Reservist Is 'COVID-19 Patient Zero,' China Is Amplifying That Disinformation," *CBS Evening News*, April 30, 2020, online edition, https://www.cbsnews.com/news/coronavirus-patient-zero-china-trolls/.
9. Brittany Kaiser, *Targeted: The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again*, Harper, 2019, 57.
10. Tim Hwang, *Subprime Attention Crisis: Advertising and the Time Bomb at the Heart of the Internet* (New York: FSG Originals, 2020); Zeynep Tufekci, "Opinion | The Looming Digital Meltdown," *The New York Times*, January 6, 2018, https://www.nytimes.com/2018/01/06/opinion/looming-digital-meltdown.html.
11. Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, 1st edition (New York: W.W. Norton & Company, 2016).
12. Michael Schudson, *Advertising, The Uneasy Persuasion: Its Dubious Impact On American Society*, Reprint edition (New York: Basic Books, 1986), xx.
13. Zuboff, T*he Age of Surveillance Capitalism*, 78.
14. Zuboff, 20.
15. Zuboff, 8.
16. Schudson, *Advertising, The Uneasy Persuasion,* xxi.
17. Hwang, *Subprime Attention Crisis*; Vincent F. Hendricks and Mads Vestergaard, "The Attention Economy," in Reality Lost: Markets of Attention, Misinformation and Manipulation, ed. Vincent F. Hendricks and Mads Vestergaard (Cham, Switzerland: Springer International Publishing, 2019), 1-17, https://doi.org/10.1007/978-3-030-00813-0_1.
18. Martin Gilens, "Gender and Support for Reagan: A Comprehensive Model of Presidential Approval," American Journal of Political Science 32, no. 1 (1988): 19-49, https://doi.org/10.2307/2111308.
19. Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Reprint edition (New York: Broadway Books, 2017).
20. Cambridge Analytica, "Key Case Studies" (Cambridge Analytica, 2015).
21. David Beer, "The Social Power of Algorithms," I*nformation, Communication & Society* 20, no. 1 (January 2, 2017): 4, https://doi.org/10.1080/1369118X.2016.1216147.
22. Kaiser, *Targeted,* 136.
23. Wylie, *Mindf*ck*.
24. Craig Silverman and Ryan Mac, "Facebook Gets Rich Off Of Ads That Rip Off Its Users," BuzzFeed News, December 10, 2020, https://www.buzzfeednews.com/article/craigsilverman/facebook-ad-scams-revenue-china-tiktok-vietnam.
25. Kaiser, *Targeted*, 398.
26. Robert L. Mitchell, "What Google Knows About You," Computerworld, May 11, 2009, https://www.computerworld.com/article/2551008/what-google-knows-about-you.html.

NOTES

27. Hendricks and Vestergaard, "The Attention Economy"; Zeynep Tufekci, "View of Engineering the Public: Big Data, Surveillance and Computational Politics | *First Monday*," First Monday 19, no. 7 (2014), https://firstmonday.org/ojs/index.php/fm/article/view/4901/4097.
28 DARPA, "Narrative Networks,". Defense Advanced Research Projects Agency, 2011, https://www.darpa.mil/program/narrative-networks.
29. Wylie, *Mindf*ck*; Kaiser, *Targeted*; Cambridge Analytica, "Key Case Studies."
30. Alan S. Gerber et al., "The Big Five Personality Traits in the Political Arena," *Annual Review of Political Science* 14, no. 1 (June 15, 2011): 265-87, https://doi.org/10.1146/annurev-polisci-051010-111659.
31. Wylie, Mindf*ck, 24.
32. Kaiser, *Targeted*; Wylie, *Mindf*ck*; Issenberg, *The Victory Lab.*
33. Kaiser, *Targeted*, 398.
34. Wylie, M*indf*ck*, 72.
35. Wylie, *Mindf*ck.*
36. S. C. Matz et al., "Psychological Targeting as an Effective Approach to Digital Mass Persuasion," Proceedings of the National Academy of Sciences 114, no. 48 (November 28, 2017): 12714, PAGE Number? https://doi.org/10.1073/pnas.1710966114.
37. Wylie, *Mindf*ck.*
38. Kai Strittmatter, *We Have Been Harmonized: Life in China's Surveillance State* (LOCATION?Custom House, 2020), 186.
39. Strittmatter, 187.
40. Strittmatter, *We Have Been Harmonized.*
41. Jenny Leonard, Saleha Mohsin, and David McLaughlin, "Tencent's Gaming Stakes Draw U.S. National Security Scrutiny," MSN, 2020, https://www.msn.com/en-us/money/other/tencents-gaming-stakes-draw-us-national-security-scrutiny/ar-BB199H8k.
42. "Joint Publication 3-13.2: Military Information Support Operations" (U.S. Department of Defense, December 20, 2011), https://www.bits.de/NRANEU/others/jp-doctrine/JP3-13.2C1(11).pdf.
43. "Joint Publication 3-13.2: Military Information Support Operations."
44. Schneier, *Data and Goliath.*
45. Wylie, *Mindf*ck*, 67.
46. Hwang, *Subprime Attention Crisis*, 13.
47. Zuboff, *The Age of Surveillance Capitalism*, 6.
48. Anna Giaritelli, "Sarah Sanders Warns Amazon about Its Echo Device: 'We Have a Problem,'" *Washington Examiner*, January 15, 2018, https://www.washingtonexaminer.com/sarah-sanders-warns-amazon-about-its-echo-device-we-have-a-problem.
49. Wylie, *Mindf*ck*, 49.
50. Stuart A Thompson and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy," *The New York Times,* December 19, 2019, Online Edition edition.
51. Adam Zewe, "Imperiled Information: Students Find Website Data Leaks Pose Greater Risk than Most People Realize," Harvard John A. Paulson School of Engineering and Applied Sciences, January 17, 2020, https://www.seas.harvard.edu/news/2020/01/imperiled-information.
52. Matz et al., "Psychological Targeting as an Effective Approach to Digital Mass Persuasion," 12714.
53. Sandeep Suntwal, Susan A. Brown, and Mark W. Patton, "How Does Information Spread? A Study of True and Fake News," n.d., 10.
54. Francesca Polletta and Jessica Callahan, "Deep Stories, Nostalgia Narratives, and Fake News: Storytelling in the Trump Era," *American Journal of Cultural Sociology* 5, no. 3 (October 2017): 392-408, https://doi.org/10.1057/s41290-017-0037-7.
55. Joseph E. Stiglitz, *The Price of Inequality: How Today's Divided Society Endangers Our Future,* 1 edition (New York: W. W. Norton & Company, 2012).do you have a page number?
56. 116th Congress, "REPORT OF THE SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE ON RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION," Senate Report (Washington, DC: United States Senate Intelligence Committee, 2017), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

NOTES

57. Claire Allbright, "A Russian Facebook Page Organized a Protest in Texas. A Different Russian Page Launched the Counterprotest," *The Texas Tribune*, November 1, 2017, https://www.texastribune.org/2017/11/01/russian-facebook-page-organized-protest-texas-different-russian-page-1/; Andrew Weisburd, Clint Watts, and JM Berger, "Trolling for Trump: How Russia Is Trying to Destroy Our Democracy," *War on the Rocks*, November 6, 2016; Ryan Browne, "Russian Trolls Tried to Convince African Americans Not to Vote in 2016, US Senate Says," CNBC, October 9, 2019, https://www.cnbc.com/2019/10/09/senate-intel-report-russian-trolls-targeted-african-americans-in-2016.html.
58. Rachelle Hampton, "Years Ago, Black Feminists Worked Together to Unmask Twitter Trolls Posing as Women of Color. If Only More People Paid Attention," *Slate Magazine*, April 23, 2019, https://slate.com/technology/2019/04/black-feminists-alt-right-twitter-gamergate.html.
59. Zeynep Tufekci, "Opinion | YouTube, the Great Radicalizer," *The New York Times*, March 10, 2018, https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html.
60. Amit Goldenberg and James Gross, "Digital Emotion Contagion," accessed October 8, 2019, https://doi.org/10.31219/osf.io/53bdu; A.D.I. Kramer, J.E. Guillory, and J.T. Hancock, "Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks," *Proceedings of the National Academy of Sciences* 111, no. 24 (June 17, 2014): 8788-90, https://doi.org/10.1073/pnas.1320040111.
61. Adam D.I. Kramer, "The Spread of Emotion via Facebook," in *Proceedings of the 2012 ACM Annual Conference on Human Factors in Computing Systems - CHI '12* (the 2012 ACM annual conference, Austin, TX: ACM Press, 2012), 767, https://doi.org/10.1145/2207676.2207787; Kramer, Guillory, and Hancock, "Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks."
62. Alex Goldenberg and Joel Finkelstein, "Cyber Swarming, Memetic Warfare and Viral Insurgency: How Domestic Militants Organize on Memes to Incite Violent Insurrection and Terror Against Government and Law Enforcement" (Princeton, NJ: Network Contagion Research Institute, 2020).
63. William Johnson, ed., *Operational Law Handbook* (Charlottesville, VA: Judge Advocate General's Legal Center and School, 2013), 105.
64. Heather Osborne and Jessica Priest, "Vanessa Guillen's Killing at Fort Hood Leaves Family Grieving, Grasping for Clues," MSN, July 18, 2020, Online edition, https://www.msn.com/en-us/news/us/vanessa-guillens-killing-at-fort-hood-leaves-family-grieving-grasping-for-clues/ar-BB16RNIl; Jim Hice, "New Leadership Named on Fort Hood in Response to Vanessa Guillen Case," MSN, September 1, 2020, https://www.msn.com/en-us/news/us/new-leadership-named-on-fort-hood-in-response-to-vanessa-guillen-case/ar-BB18ByD7.
65. Thompson and Warzel, "Twelve Million Phones, One Dataset, Zero Privacy."
66. Byron Tau and Michelle Hackman, "WSJ News Exclusive | Federal Agencies Use Cellphone Location Data for Immigration Enforcement," *The Wall Street Journal*, February 7, 2020, sec. Politics, https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600.
67. Joseph Cox, "How the U.S. Military Buys Location Data from Ordinary Apps," Vice.com, November 16, 2020, https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.
68. Matt Burgess, "Strava's Data Lets Anyone See the Names (and Heart Rates) of People Exercising on Military Bases," *Wired UK*, January 30, 2018, https://www.wired.co.uk/article/strava-military-bases-area-51-map-afghanistan-gchq-military.
69. Josephine Wolff, "The Military's Ban of TikTok Is Just the Beginning," *Slate Magazine*, January 6, 2020, https://slate.com/technology/2020/01/military-tiktok-ban-strava-genetic-testing.html.
70. Gina Harkins, "6 Big Takeaways from the Full Navy Investigation into a Carrier's COVID Outbreak," Military.com, September 19, 2020, https://www.military.com/daily-news/2020/09/19/6-big-takeaways-full-navy-investigation-carriers-covid-outbreak.html; Meghann Myers, "Military's COVID-19 Cases Growing at Twice the Nationwide Rate," *Military Times*, July 13, 2020, https://www.militarytimes.com/news/your-military/2020/07/10/militarys-covid-19-cases-growing-at-twice-the-nationwide-rate/.
71. Eric Taylor Woods et al., "COVID-19, Nationalism, and the Politics of Crisis: A Scholarly Exchange," *Nations and Nationalism*, July 19, 2020, https://doi.org/10.1111/nana.12644.
72. Zak Doffman, "Why You Should Stop Using Facebook Messenger," *Forbes*, July 25, 2020, https://www.forbes.com/sites/zakdoffman/2020/07/25/why-you-should-stop-using-facebook-messenger-encryption-whatsapp-update-twitter-hack/.
73. Zeynep Tufekci, "Opinion | Think You're Discreet Online? Think Again," *The New York Times*, April 21, 2019, https://www.nytimes.com/2019/04/21/opinion/computational-inference.html.

NOTES

74. Sara Bannerman, "Relational Privacy and the Networked Governance of the Self," *Information, Communication & Society* 22, no. 14 (December 6, 2019): 2187-2202, https://doi.org/10.1080/1369118X.2018.1478982; Juniper Lovato et al., "Distributed Consent and Its Impact on Privacy and Observability in Social Networks," *ArXiv:2006.16140 [Physics]*, June 29, 2020, http://arxiv.org/abs/2006.16140; Tufekci, *Twitter and Tear Gas.*
75. Kate Knibbs, "What Is a Facebook Shadow Profile," Digital Trends, July 5, 2013, https://www.digitaltrends.com/social-media/what-exactly-is-a-facebook-shadow-profile/.
76. Tufekci, "Opinion | Think You're Discreet Online?"
77. Sara Morrison, "Google's Education Tech Has a Privacy Problem," Vox, February 21, 2020, https://www.vox.com/recode/2020/2/21/21146998/google-new-mexico-children-privacy-school-chromebook-lawsuit.
78. Xavier Becerra, "California Consumer Privacy Act (CCPA)" (State of California, 2020), https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-third-set-mod-101220.pdf?
79. Kimiko de Freytas-Tamura, "The Bright-Eyed Talking Doll That Just Might Be a Spy (Published 2017)," T*he New York Times*, February 17, 2017, https://www.nytimes.com/2017/02/17/technology/cayla-talking-doll-hackers.html; Lauren Davis, "The NSA Once Banned Furbies as a Threat to National Security," io9, February 20, 2014, https://io9.gizmodo.com/the-nsa-once-banned-furbies-as-a-threat-to-national-sec-1526908210.
80. Dan Patterson, "Trolls Are Spreading Conspiracy Theories That a U.S. Army Reservist Is 'COVID-19 Patient Zero' China Is Amplifying That Disinformation.," CBS News, April 30, 2020, https://www.cbsnews.com/news/coronavirus-patient-zero-china-trolls/.
81. Kramer, "The Spread of Emotion via Facebook."
82. Wylie, *Mindf*ck.*
83. Wylie, 120.
84. "45 CFR 46 (Protection of Human Subjects)" (United States Government, 1991).
85. Dana Weinberg and Jessica Dawson, Ph.D., "From Anti-Vaxxer Moms to Militia Men: Influence Operations, Narrative Weaponization, and the Fracturing of American Identity" (SocArXiv, October 30, 2020), https://doi.org/10.31235/osf.io/87zmk.
86. Renny Gleeson, "Truth Dies First: Storyweapons on the InfoOps Battlefield," *The Cyber Defense Review* (Summer 2020): 71.
87. Marzuki Darusman, "OHCHR | Statement by Mr. Marzuki DARUSMAN, Chairperson of the Independent International Fact-Finding Mission on Myanmar, at the 37th Session of the Human Rights Council" (2018), https://www.ohchr.org/EN/HRBodies/HRC/Pages/NewsDetail.aspx?NewsID=22798&LangID=E.
88. Marietje Schaake, "Trade Secrets Shouldn't Shield Tech Companies' Algorithms from Oversight," Brookings (blog), May 4, 2020, https://www.brookings.edu/techstream/trade-secrets-shouldnt-shield-tech-companies-algorithms-from-oversight/.
89. Hwang, *Subprime Attention Crisis.*
90. Hwang; Jeroen van Zeeland, "Data Is Not the New Oil," *Medium*, December 7, 2019, https://towardsdatascience.com/data-is-not-the-new-oil-721f5109851b; Cory Doctorow, "How to Destroy 'Surveillance Capitalism,'" *Medium*, August 30, 2020, https://onezero.medium.com/how-to-destroy-surveillance-capitalism-8135e6744d59.
91. Vian Bakir, "Psychological Operations in Digital Political Campaigns: Assessing Cambridge Analytica's Psychographic Profiling and Targeting," F*rontiers in Communication* 5 (September 3, 2020): 67, https://doi.org/10.3389/fcomm.2020.00067; Cambridge Analytica, "Key Case Studies"; Doctorow, "How to Destroy 'Surveillance Capitalism.'"
92. Renee DiResta, "Computational Propaganda: If You Make It Trend, You Make It True," *The Yale Review*, October 9, 2018, https://yalereview.yale.edu/computational-propaganda.
93. Mac Thornberry, "H.R.5736 - 112th Congress (2011-2012): Smith-Mundt Modernization Act of 2012," webpage, May 10, 2012, https://www.congress.gov/bill/112th-congress/house-bill/5736.
94. David Klepper, "Facebook Clarifies Zuckerberg Remarks on False Political Ads," AP News, October 25, 2019, https://apnews.com/64fe06acd28145f5913d6f815bec36a2.
95. Casey Newton, "Three Facebook Moderators Break Their NDAs to Expose a Company in Crisis," The Verge, June 19, 2019, https://www.theverge.com/2019/6/19/18681845/facebook-moderator-interviews-video-trauma-ptsd-cognizant-tampa.

NOTES

96. Sarah Frier, "Zuckerberg to Tell Congress Facebook's Success Is Patriotic," Bloomberg, July 27, 2020, https://www.bloomberg.com/news/articles/2020-07-27/zuckerberg-to-tell-congress-facebook-s-success-is-patriotic.
97. Zeynep Tufekci, "Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency," *Colorado Technical Law Journal 13 (2015): 17; Zeynep Tufekci, "Opinion | Facebook's Surveillance Machine," The New York Times, March 19, 2018, sec. Opinion*, https://www.nytimes.com/2018/03/19/opinion/facebook-cambridge-analytica.html.
98. Allbright, "A Russian Facebook Page Organized a Protest in Texas. A Different Russian Page Launched the Counterprotest"; Browne, "Russian Trolls Tried to Convince African Americans Not to Vote in 2016, US Senate Says"; Weisburd, Watts, and Berger, "Trolling for Trump: How Russia Is Trying to Destroy Our Democracy."
99. Tufekci, "Opinion | Facebook's Surveillance Machine"; Carole Cadwalladr and Emma Graham-Harrison, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach," *The Guardian,* March 17, 2018, sec. News, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.