A Social (Media) Contract

Reconciling American Freedom and Security in an Age of Online Radicalization and Extremism

By Tony Formica

INTRODUCTION: ONCE UPON A TIME IN AMERICA

2018 was proclaimed the most violent year for deaths caused by domestic extremists since the 1995 Oklahoma City Bombing, closing out with eleven Americans murdered in the Tree of Life Synagogue massacre.[1] Extremist groups have been on the rise for the past four years, and an uptick in extremist-related violence has followed in their wake.[2] Prominent social media platforms have been tacitly implicated in these attacks, facilitating extremist recruitment, disseminating propaganda, and spreading disinformation.

Neither leaders in our nation's capital nor Silicon Valley have proposed meaningful solutions to address this threat. Should Congress regulate tech firms? Criminalize certain types of online behavior? Trust in private sector self-regulation? These questions reveal an underlying tension between sacrosanct American public liberties, venerated corporate rights, and the desire of American citizens to be secure in their daily lives.

Censorship and surveillance will not solve this dilemma; they seem likely to exacerbate it. We need a paradigmatic shift in how we view the intersection of online extremism with protected liberties and corporate rights. Domestic extremism is an unquestionable threat to national security, but the best way to deal with it lies in framing it as a public health issue and encouraging and reinforcing industry-led self-regulation. This approach optimally synchronizes tech sector know-how with governmental oversight practices in a manner that promotes public safety without abandoning our nation's bedrock principles.

Social media platforms such as Twitter face enormous challenges fighting extremist recruitment, propaganda, and disinformation on their sites. Photo by Sara Kurfeß.

ADMIT IT, AMERICA: YOU HAVE A PROBLEM

Congress is dedicating an increasing share of its attention to the relationship between social media platforms and online extremism. Several hearings since 2017 suggest that Congressional focus on extremism is also shifting from traditional concerns (such as the recruitment of Americans to jihadist movements) to the blossoming threat of domestic extremist violence and proliferation of hate groups in the United States. Representative Jerrold Nadler convened a hearing in 2019 to examine whether social media firms' efforts are sufficiently tackling hate speech and extremism on their platforms that are resulting in real-world deaths.[3] As Representative Cedric Richmond put it: "There are real families being destroyed; there are real people dying because of this."[4]

Islamic terrorism is quantitatively and qualitatively a lesser threat to American domestic tranquility and security than home-grown radicalized extremists.

The data supports these warnings: Islamic terrorism is quantitatively and qualitatively a lesser threat to American domestic tranquility and security than home-grown radicalized extremists.[5] Domestic extremists accounted for nearly 74 percent of all extremist-related fatalities within the United States over the past decade, while Islamic terrorism claims slightly more than 23 percent.[6] Domestic extremists would have a monopoly on fatal violence had not one of the perpetrators "switched from white supremacist to radical Islamist beliefs prior to committing [his] murder."[7] As their overall share of the violence increases, domestic extremists are also killing more Americans year-on-year. There was a 35 percent increase in the number of Americans killed by such groups from 2017 to 2018.[8] This violence was accompanied by a surge in hate groups, hate group recruitment, and hate crimes, which have run unchecked since 2015.[9] Right-wing extremist groups, in particular, are responsible for the majority of fatal domestic violence, presenting both hate group ideologies and extremist violence tendencies.[10]

By comparison, since after September 11, 2001, through to 2018, Muslim Americans killed 141 of their fellow citizens; non-Islamic extremists killed 49 Americans in 2018 alone.[11] There has been an overall downward trend in arrests of Muslim Americans for alleged involvement with violent extremism since 2015.[12] This information suggests that narratives and radicalization pathways from overseas are less effective than homegrown varieties at enticing Americans to extremist violence.

These trends are driven at least in part by political polarization, anti-immigrant sentiment, and technologies such as social media, which help spread propaganda.[13] Interestingly, today's extremists prefer to operate as lone actors, employing firearms and bladed weapons.[14] This is in stark contrast to bombings or arson, which predominated extremist violence in the United States throughout the 1990s and early 2000s.[15] Today's radicalized individuals have a clear preference for violence that is up close and personal.

What these observations do not provide is an understanding of the mechanisms which allow online antipathies to metastasize into real-world violence. Is there a causal link between violent behavior online and the demonstrated preference for intimate, close-range violence by domestic extremists? Social media's distortion of our conceptions of physical space is at the core of understanding this connection.

A PATHOLOGY OF VIRTUAL HATRED AND REAL VIOLENCE

Social media disrupts conceptions of the physical and emotional distances between its users. An individual might feel tremendous affinity for someone in their Star Trek fan blog, perhaps feeling more affinity for his digital compatriot than for his next-door neighbor. Indeed, an individual might earnestly despise their neighbor, but there are social consequences for giving those feelings full expression. For example, screaming about your neighbor's car parking might entice your neighbor to scratch up your car with his keys the next morning. However, no such inhibitions exist online because we are unlikely to encounter our online counterparts physically. The low risk of reciprocation produces no consequences for employing vitriolic or violent language against others online. In all of these cases, our conception of physical proximity in the digital world distorts the emotional attachments we develop with our online acquaintances.

These dynamics are not novel and underlie every modality of digital interaction. However, they interact with human cognition in dangerous and powerful ways when an individual is vulnerable to radicalization. Individuals, both on and offline, tend to seek out, share, and recall information that is compatible with their worldview and cultural commitments.[16] Individuals search for information as motivated consumers, rather than as passive aggregators. People do not generally become extremists by happenstance online encounters.[17] Instead, extremist-prone individuals tend to have affinities and worldviews, which lead them to actively search for online content that reinforce their beliefs. These preferences may be sourced as disinformation, misinformation, or extremist propaganda.

Social media algorithms note and log these extremism-prone search preferences, and subsequently steer users towards more of the same.[18] This mechanism comprises the entire social media business model: algorithms learn about user preferences and steer them into communities of similar individuals with similar consumption patterns and preferences, and who collectively generates more clicks and revenue.[19] A primary consequence of this process is the reduction of information-sharing across tribal units, including and especially in the case of extremist groups.[20] The result is a communications environment where an individual's information diet is restricted almost exclusively to the biases and preferences of people to whom they have been algorithmically guided.

Insular cultural nodes produced by this filtering effect are hard to break. While it is not impossible to acquire a diverse range of perspectives online, social media algorithms are programmed to keep users anchored to profit-maximizing communities. Human psychology amplifies the problem. Once an individual has a tribal allegiance, he tends to apply cultural cognition to reconcile any dissonance between his emotional commitments and perception of facts.[21] Any countervailing information which breaks through the filters is discredited and discounted in the pursuit of ideological coherence at the expense of civic cohesion.

While these effects are amplified for extremist-prone individuals, even those less at-risk have a demonstrated tendency to abandon their inhibitions against uncivil rhetoric when engaging perceived adversaries online.[22] The paucity of information from outside groups, paired with the recurrent discrediting of any such information that does enter the tribe's media feed, results in the dehumanization of external "others."[23] Viciousness against the tribe's perceived enemies quickly becomes confused with virtuous defense of the tribe's values. The dynamic reinforces when rival Tribe B punches back at Tribe A, confirming Tribe A's suspicion that Tribe B's members are irrational, ignorant, and, after enough iterations, malfeasant.[24] Cognitive dissonance resolution mechanisms will persuade Tribe A's members that their original savaging of Tribe B was not only justified, but also insufficient: Tribe B remains ignorant and irrational, thus meriting further abuse.[25] The result is a digital commons of shouting parties and individuals, locked in perpetual digital combat, where neither side can agree on basic facts nor perceive each other as well-intentioned fellow citizens.

Social media allows them to spread their message and guarantees people sympathetic to that message will find it.

These interactions significantly increase the emotional distance between warring individuals online, increasing the probability that opponents eventually come to see their rivals as less human. That becomes more likely when an individual is entrenched in an online extremist group—such as a white nationalist movement—that specifically categorizes other groups as enemies or sub-humans. The distortion of physical proximity wrought by digital communications—individuals rarely, if ever, see their rivals in the real world—makes this perception tenable. The radicalization of emotional commitments and concomitant animosities makes it dangerous. Emotional and physical distance between killer and target are two of the most potent natural inhibitions human beings have against killing members of our own species.[26] Military formations, for example, undertake significant desensitization efforts to cause their own soldiers to view the enemy as less than human.[27] Unfortunately, social media can serve the same function for online warring tribes.

It is, therefore, no wonder that extremist and hate groups, and the crimes associated with them, have been on the rise: social media allows them to spread their message and guarantees people sympathetic to that message will find it. A percentage of these individuals will become sufficiently radicalized through

escalating intertribal conflict to become convinced that their enemies are malfeasant subhumans deserving of violence, and a smaller percentage will be motivated to translate their online conflict into acts of physical violence in the real world.

THE IMBROGLIO OF PUBLIC-PRIVATE ROLES AND RESPONSIBILITIES

The psychological pathology analysis above suggests two remedies for the threat posed by online radicalization and extremism. The first entails disrupting the radicalization process at its inception, via some form of intervention when a consumer searches for content linked to extremist perspectives, thus curbing the forces driving individuals into extremist enclaves. The second remedy entails platform operators employing a process that would allow them to identify, adjudicate, and remove extremist content on their sites, thus reducing the ability of motivated consumers to find harmful content catering to extremist preferences.

Unfortunately, sensationalism and division on social media platforms sell: no emotion goes viral faster than rage, and furious netizens are consistent platform users.[27]

Social media firms are concerned with promoting their bottom line and expanding their consumer base. These interests may conflict with a responsibility to promote public security. This responsibility lies with the government.

However, traditional government tools to combat online extremism—Foreign Intelligence Surveillance Act (FISA)-derived measures, Executive Order 12333 and related orders—have significant operational shortcomings.[28] First, they are slow and outdated. Radicalization on social media platforms occurs faster than federal law enforcement agencies are capable of legally monitoring. Simply getting a FISA request approved to initiate Federal Bureau of Investigation (FBI) surveillance requires extensive evidence from multiple types of sources, vetting through several layers of organizational hierarchy and typically several rounds of editing between the Bureau and the Department of Justice (DOJ).[29] Critically, a FISA warrant cannot "…be opened 'solely on the basis of First Amendment activities,'" precluding the monitoring of American citizens simply because they visit or associate with unsavory individuals, either on or offline.[30]

Fundamentally, traditional government tools for surveilling extremism assume that Americans worthy of monitoring are working with or being manipulated by a hostile foreign actor; they offer little guidance on how to proceed when great numbers of Americans are being radicalized by their fellow countrymen. The greatest difficulty of government surveillance tools in the context of home-grown extremism is the threat these tools pose to the protected liberties of American citizens and their trust in government.[31] These liberties do not simply concern the private citizen either. America's commitment to free speech in the public forum is at the heart of our understanding of the public discourse required for effective democratic governance.[32] Government-mandated social media censorship, whether it be removing content or blocking users, would represent a betrayal of First Amendment principles. Social media firms would justifiably see such restrictive regulatory approaches not only as threats to liberties, but also to profits, and in any event would deploy their legions of corporate lobbyists.

Frankly, social media firms possess the technical capabilities and capacity to expeditiously implement meaningful changes on their platforms.

The current impasse in dealing with social media-derived domestic extremism stems from an outdated conception of government's roles and responsibilities where national security clashes with private liberties. Furthermore, social media firms are critical to the implementation of any feasible policy solution. Frankly, social media firms possess the technical capabilities and capacity to expeditiously implement meaningful changes on their platforms. These firms must be integrated into any usable framework and that framework must entail more than simply a threatening ultimatum from Congress.

A more fruitful approach could entail observing past government approaches to regulating products inimical to public interest. Domestic online extremism

is a national security issue, but the most effective mitigation strategy does not lie within national defense or intelligence. It lies in industrial self-regulation.

RECOMMENDATIONS: DIGITAL DUTIES AND OBLIGATIONS

Industries often adopt voluntary self-regulatory procedures when they receive pressure from both lawmakers and the public.[33] This has been observed in industries spanning from tobacco to marine fisheries.[34] Social media firms currently face this dilemma. While effectiveness and earnestness of self-regulation will vary by industry, a rigorous self-regulatory framework is key: successful frameworks emphasize transparency, benchmarks, oversight, and accountability.[35]

Industries often adopt voluntary self-regulatory procedures when they receive pressure from both lawmakers and the public.

In the case of self-regulation, *transparency* refers to standards which are created by expert organizations external to the industry with widespread understanding and acceptance of these standards.[36] *Benchmarks* are quantifiable measures of both performance and effectiveness;. for example, the number of extremists detected on the platform, or the efficacy of content removal tools.[37] *Oversight* demands regular reporting, and allows regulatory authorities to examine progress against defined benchmarks periodically.[38] Finally, *accountability* mandates reports be available to the broader public with a mechanism for external parties to register dissatisfaction with self-regulatory procedures.[39]

Two major social media firms have implicitly recognized that self-regulation in response to online extremism and radicalization on their platforms is favorable. Facebook launched its Community Standards, which establishes guidelines governing violent, objectionable, and inauthentic content on the platform, among others.[40] Violations can result in content being flagged or removed, or lead to users being blocked from the platform, all ostensibly to create a safe online environment.[41] Facebook has updated its standards to target not only Islamic extremism, but also white nationalism and white separatism.[42]

Google's parent company Alphabet, meanwhile, has used its Jigsaw subsidiary to pioneer The Redirect Method, which functionally serves as a targeted intervention against prospective radicalization victims whenever they seek out flagged extremist content online.[43] As the project's own descriptive page reads, "The Redirect Method…focuses on the slice of ISIS's audience that is most susceptible to its messaging, and redirects them towards curated YouTube videos debunking ISIS recruiting themes."[44] Jigsaw employed former ISIS members to develop an understanding of prevalent extremist propaganda themes, narratives, and content, and then augmented that understanding with digital targeting tools to both flag suspected extremist content and identify countervailing media content from across the internet.[45]

Both Facebook's Community Standards and The Redirect Method are commendable at face value from a purely counter-extremism perspective. Both solutions attempt to deal with the motivated cognition problem discussed earlier by intercepting content before it reaches extremist-susceptible parties. The Redirect Method also disrupts filtering processes by redirecting individuals actively seeking engagement with online extremist communities to more moderate voices.

While commendable, both initiatives also fall short on several key components of optimal self-regulation. Facebook's Standards are virtually entirely contrived in-house, and report only raw numbers for content that has been flagged or removed without regard to measures of effectiveness. This strategy brings the firm's commitment to transparency and the relevance of its benchmarks into question. Moreover, Facebook does not go out of its way to report its success against its own benchmarks, which limits the potential for oversight. However, Facebook has demonstrated a receptiveness to public and Congressional demands that it do better. Its proclaimed willingness to adopt the Honest Ads Act's provisions as well as its recent commitment to tightening restrictions on white nationalist content are both encouraging signs of increasing accountability.

The Redirect Method performs better from a self-regulatory perspective. Jigsaw developed the technology and human capital for the Redirect Method in consultation with many external think tanks and experts, and its measures of performance and effectiveness are easy to access and appear valid.[46] Yet The Redirect Method is hampered by a lack of clear commitment to oversight and

accountability from the public sector or, if such oversight and accountability exists, it is not clearly outlined in public materials. More fundamentally, The Redirect Method targets victims of Islamic extremism's radicalization efforts and does little to combat home-grown, domestic extremist movements in the United States.

Recognizing that firms' self-regulatory efforts are imperfect is not cause for casting these efforts as either misguided or ineffective. It simply indicates an opportunity for public-private cooperation in combating online extremism and radicalization. We need the government to commit itself to regulatory approaches which complement the laudable existing efforts of these two social media giants, while also avoiding entanglements with First Amendment protections. Five recommendations are prudent.

1. Name the threat: Any governmental enhancement of private self-regulatory frameworks vis-à-vis online extremism and radicalization should explicitly name the threat: domestic extremist movements. A standard understanding of what constitutes domestic extremism, shared by the public and private sectors, must be adopted before any further regulatory frameworks can be implemented by the government.

2. Enforce transparency as a consumer health issue: The Honest Ads Act's (HAA) most significant provision is its requirement that social media firms provide and update a public database on who purchases ads on their platforms.[47] This is functionally equivalent to the FDA certification processes for food and drugs: it allows consumers to know that the products they are using are safe. By recasting online extremism as a matter of industrial regulation, the government can avoid allegations of censoring free speech and create social support for the HAA or equivalent legislation. The HAA or equivalent legislation should ensure that it addresses ad purchases by domestic extremist movements in addition to foreign adversaries with known histories of promoting divisive social issues online.

3. Enforce accountability as a consumer health issue: The Emergency Planning and Community Right-to-Know Act requires firms to report all hazardous chemicals stored and dumped to state and local governments.[48] This approach enforces accountability by mandating negative externalities generated by private industrial practices be made accessible to the public. A similar piece of legislation requiring social media companies to report the number of domestic extremists identified on, removed from, or redirected by their platforms would illuminate the prevalence of the threat posed by these individuals, and how effective firms are at dealing with this threat.

4. Check firms' work: Princeton University's Web Transparency and Accountability Project creates bots to masquerade as real people, places them online, and tracks how long it takes for those bots to suffer some form of discrimination, whether in job applications, academic admissions, or medical treatment.[49] The government should mirror this practice to collect their own data on how effective firms are at meeting their own benchmarks for countering extremism on their platforms. Instead of assessing the time between a bot's creation and its first experience of discrimination, this project would seek to identify the time and pathways to achieve radicalization. This would go a long way towards ensuring government oversight and accountability.

Corporate self-interest should suffice to motivate desired organizational change.

5. Name and subsidize good actors: Firms that voluntarily take meaningful steps towards self-regulation with the explicit purpose of combating extremism and radicalization on their platforms should be recognized and rewarded. The government should prepare a tiered system of subsidies for firms which voluntarily adopt measures, such as the HAA, which are not yet law. These subsidies should be specifically targeted to help companies implement further measures to increase their transparency, ability to create meaningful benchmarks through collaboration with external expertise, achieve governmental oversight, and ultimately create private accountability to the public welfare. Companies receiving these subsidies should be publicly reported as actively promoting the public's health and welfare.

Companies which do not implement sufficiently rigorous self-regulatory procedures will not be penalized. They simply will not receive federal support and risk being implicitly shamed for not being interested in promoting the public's welfare.[50] Corporate self-interest should suffice to motivate desired organizational change.

CONCLUSION: TOWARDS A NEW SOCIAL (MEDIA) CONTRACT

The complexity of the threat posed by online extremism and radicalization to American domestic security is significant, both technologically and legally. This paper's recommendation to refocus federal efforts through a public health lens holds the promise of employing governmental tools beyond restrictions to individual liberties, but such a paradigm shift is neither a panacea nor guaranteed smooth sailing, particularly in our current political climate. Potential points of contention are addressed below.

First, Congress is reluctant to pass new regulation, and is generally slow to do so. Even when legislators do manage to impose regulatory restrictions on large industries, exemptions and loopholes proliferate rapidly. However, regulation is still a viable option for two reasons, one philosophically idealistic while the other utterly practical. Philosophically, the mere fact that regulation is difficult ought not to preclude its use by liberal democratic law-making institutions. If Congressional leaders make the case to the public that social media platforms are contributing to the loss of American lives, there is a chance that the voters will respond with an increased demand that legislators regulate and reward those legislators who do so effectively. Practically, the recommendation to create a tiered system of subsidies for companies that voluntarily implement self-regulation is more a palatable form of regulation compared to traditional approaches: providing incentives instead of imposing restrictions.

The violence spawned by this process is real, and it threatens us all equally.

A second point of contention is that social media companies may not get on board with self-regulation, effectively quashing the notion through collective inaction. However, our case studies suggest this is not the trend. Google and Facebook, the predominant social media players by most metrics, have clearly recognized the value of self-regulation. Their efforts, while imperfect, send a strong message from industry leaders that the status quo is unacceptable. The policy recommendations made in this paper, if adopted, will only strengthen the self-regulation regime. Moreover, the practice of naming good actors and implicitly shaming noncompliant ones (inherent in several of the legislative approaches recommended here) places pressure on recalcitrant firms if they are perceived by customers as unsafe or untrustworthy. One need only look at the penalty Facebook has already incurred due to customer concerns about their privacy to understand how significant a motivator these risks can be once the public becomes aware of them.[51]

The third shortcoming of these recommendations is they do not address how law enforcement agencies might best adapt their current techniques and procedures to the digital world to identify, intervene, or apprehend online extremists. This is an important topic for further research, but it goes beyond the scope of this paper. Nevertheless, synchronizing law enforcement's efforts with social media firms' practices in dealing with extremism on their platforms would be considerably easier if the measures proposed here were adopted by Congressional leadership, in particular, the recommendation to standardize the definition of extremism across government and the private sector.

Ultimately, leaders across all sectors of our nation must reframe their understanding of the threat posed to all of us by social media-enabled radicalization. The violence spawned by this process is real, and it threatens us all equally. We urgently need a common acknowledgment of the duties and obligations Americans have to one another, not merely as members of corporate or government entities, online tribes, or the generic "public," but rather as common citizens with a shared commitment to one another's well-being and security. Silence on this commitment from Congress and Silicon Valley will do nothing to stanch our national bleeding; leadership on it will align our practices with our highest aspirations and values. ■

ABOUT THE AUTHOR

Major Tony Formica graduated from the United States Military Academy at West Point in 2009 with a B.S. in International Relations and East Asian Area Studies. He commissioned as an infantry lieutenant in the U.S. Army and was first posted to Fort Wainwright, Alaska. While there, he deployed and led soldiers in Kandahar Province, Afghanistan before returning to the United States in the spring of 2012. Tony was selected as a U.S. Army Downing Scholar in the fall of 2017 and focuses his graduate studies on the national security implications stemming from the interaction of social media, economic inequality, and political tribalism.

ENDNOTES

1. Anti-Defamation League, "Right-Wing Extremism Linked to Every 2018 Extremist Murder in the U.S., ADL Finds," January 23, 2019, https://www.adl.org/news/press-releases/right-wing-extremism-linked-to-every-2018-extremist-murder-in-the-us-adl-finds; Charles Kurzman, *Muslim-American Involvement with Violent Extremism, 2001-2019*, (Chapel Hill, North Carolina: Triangle Center on Terrorism and Homeland Security, 2020), 1.

2. For the purposes of this paper, the terms "extremist" and "extremism" will be understood by the definition used by the Federal Bureau of Investigation as entailing individuals or movements which "…[encourage], [condone], [justify], or support the commission of violent act[s] to achieve political, ideological, religious, social, or economic goals."; Federal Bureau of Investigation, "What is Violent Extremism?," accessed April 28, 2019, https://cve.fbi.gov/whatis/; Liam Stack, "Over 1,000 Hate Groups Are Now Active in United States, Civil Rights Group Says," *The New York Times*, February 20, 2019, https://www.nytimes.com/2019/02/20/us/hate-groups-rise.html.

3. Tony Romm, "Facebook and Google to be quizzed on white nationalism and political bias as Congress pushes dueling reasons for regulation," *The Washington Post,* April 8, 2019, https://www.washingtonpost.com/technology/2019/04/08/facebook-google-be-quizzed-white-nationalism-politicalbias-congress-pushes-dueling-reasons-regulation/?utm_term=.86e7785e4155.

4. Ibid.

5. Kurzman, *Muslim-American Involvement with Violent Extremism, 2001-2019*, 1.

6. Anti-Defamation League, "Right-Wing Extremism Linked to Every 2018 Extremist Murder in the U.S., ADL Finds."

7. Adam Serwer, "The Terrorism That Doesn't Spark a Panic," *The Atlantic*, January 28, 2019, https://www.theatlantic.com/ideas/archive/2019/01/homegrown-terrorists-2018-were-almost-all-right-wing/581284/.

8. Anti-Defamation League, "Right-Wing Extremism Linked to Every 2018 Extremist Murder in the U.S., ADL Finds."

9. Liam Stack, "Over 1,000 Hate Groups Are Now Active in the United States, Civil Rights Group Says."

10. Global Terrorism Database, National Consortium for the Study of Terrorism and Responses to Terrorism (START), University of Maryland, as cited in Kurzman, *Muslim-American Involvement with Violent Extremism, 2001-2019*, 1.

11. Kurzman, *Muslim-American Involvement with Violent Extremism, 2001-2019*, 1; Anti-Defamation League. "Murder and Extremism in the United States in 2018," accessed March 26, 2020, https://www.adl.org/murder-and-extremism-2018#the-perpetrators.

12. Ibid, 1.

13. Liam Stack, "Over 1,000 Hate Groups Are Now Active in the United States, Civil Rights Group Says," February 20, 2019, https://www.nytimes.com/2019/02/20/us/hate-groups-rise.html.

14. Anti-Defamation League, "Right-Wing Extremism Linked to Every 2018 Extremist Murder in the U.S., ADL Finds."

15. National Consortium for the Study of Terrorism and Responses to Terrorism (START), University of Maryland (2019), Profiles of Radicalization in the United States (PIRUS), [data file], retrieved from http://www.start.umd.edu/data-tools/profiles-individual-radicalization-united-states-pirus.

16. Dan M. Kahan, David A. Hoffmann, Donald Braman, Danieli Evans, and Jeffrey J. Rachlinski, "'They Saw a Protest': Cognitive Illiberalism and the Speech-Conduct Distinction," *Stanford Law Review*, vol. 64, 2012, 8.

17. Taber & Lodge, as cited in Flynn et al, "The Nature and Origins of Misperceptions: Understanding False and Unsupported Beliefs about Politics," *Political Psychology*, vol. 38, 2017, 10, https://ore.exeter.ac.uk/repository/bitstream/handle/10871/25801/Flynn%20Nyhan%20Reifler%20Advances.pdf?se quence=1&isAllowed=n.

18. Zeynep Tufekci, "YouTube, the Great Radicalizer," *The New York Times,* March 10, 2018, https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html.

19. Cass R. Sunstein, *#Republic: Divided Democracy in the Age of Social Media* (Princeton: Princeton University Press, 2017), 3.

20. Andrew Guess et al., "Avoiding the echo chamber about echo chambers: Why selective exposure to like-minded political news is less prevalent than you think," Knight Foundation, 2018, 8.

21. Kahan et al., "They Saw a Protest," 8.

22. Robert D. Putnam, *Bowling Alone: The Collapse and Revival of American Community* (New York: Simon & Schuster, 2000), 176.

23. Amy Chua, *Political Tribes: Group Instinct and the Fate of Nations*, (New York: Penguin Press, 2018), Chapter 5, eBook.

24. P.W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (New York: Houghton Mifflin Harcourt Publishing Company, 2018), 126.

25. Carol Tavris and Elliot Aronson, *Mistakes Were Made (but not by me): Why We Justify Foolish Beliefs, Bad Decisions, and Hurtful Acts* (New York: Houghton Mifflin Harcourt, 2007), 45.

26. David Grossman, *On Killing: The Psychological Cost of Learning to Kill in War and Society* (New York: Back Bay Books, 2009), 161.

27. Ibid.

28. Executive Order 12333 "…authorizes the Attorney general to promulgate guidelines requiring each element of the Intelligence Community to have in place procedures prescribing how it can collect, retain, and disseminate information about US persons." Richard A. Clark, Michael J. Morell, et al, "Liberty and Security in a Changing World," Report and recommendations of The President's Review Group on Intelligence and Communications Technologies, last modified December 12, 2013, 71.

29. Asha Rangappa, "It Ain't Easy Getting a FISA Warrant: I was an FBI Agent and Should Know," Just Security, March 6, 2017, https://www.justsecurity.org/38422/aint-easy-fisa-warrant-fbi-agent/.

30. Ibid.

31. Clark et al, "Liberty and Security in a Changing Word," 46.

32. Sunstein, *#Republic: Divided Democracy in the Age of Social Media*, 35.

33. Lisa L. Sharma et al, "The Food Industry and Self-Regulation: Standards to Promote Success and to Avoid Public Health Failures," *American Journal of Public Health*, vol. 100, no. 2, 2010, https://ajph.aphapublications.org/doi/pdf/10.2105/AJPH.2009.16090.

34. Ibid.

35. Sharma et al, "The Food Industry and Self Regulation."

36. Ibid.

37. Ibid.

38. Ibid.

39. Ibid.

40. "Community Standards," 2019, www.facebook.com/communitystandards/introduction.

41. Ibid.

42. Louise Matsakis, "Will Facebook's New Ban on White Nationalist Content Work?", *Wired*, March 27, 2019, https://www.wired.com/story/facebook-ban-white-nationalism-separatism-hate-speech/.

43. The Redirect Method, https://redirectmethod.org/.

44. Sharma et al., "The Food Industry and Self Regulation."

45. Ibid.

46. The Redirect Method.

47. Mark R. Warner, "Warner and Klobuchar Call on Google & Twitter to Comply with the Honest Ads Act," April 9, 2018, https://www.warner.senate.gov/public/index.cfm/pressreleases?ID=4AC5CEC9-BE2E-49DC9610-55FBF4CF67C8.

48. Sunstein, *#Republic: Divided Democracy in the Age of Social Media*, 218.

49. Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (New York: Broadway Books, 2017), 210.

50. Warner, "Warner and Klobuchar Call on Google & Twitter to Comply with the Honest Ads Act."

51. Elizabeth Dwoskin, "Zuckerberg says he's going all in on private messaging. Facebook's declining user numbers tell us why," *The Washington Post*, March 11, 2019, https://www.washingtonpost.com/technology/2019/03/11/zuckerberg-says-hes-going-all-in-private-messagingfacebooks-declining-user-numbers-tell-us-why/?utm_term=.947dd160ddf2.