



Program on Extremism

THE GEORGE WASHINGTON UNIVERSITY

LESSONS FROM THE INFORMATION WAR:
APPLYING EFFECTIVE TECHNOLOGICAL
SOLUTIONS TO THE PROBLEMS OF ONLINE
DISINFORMATION AND PROPAGANDA

This paper, part of the Legal Perspectives on Tech Series, was commissioned in conjunction with the Congressional Counterterrorism Caucus

J.D. MADDOX

SEPTEMBER 2019

About the Program on Extremism

The Program on Extremism at George Washington University provides analysis on issues related to violent and non-violent extremism. The Program spearheads innovative and thoughtful academic inquiry, producing empirical work that strengthens extremism research as a distinct field of study. The Program aims to develop pragmatic policy solutions that resonate with policymakers, civic leaders, and the general public.

About the Author

J.D. Maddox is an adjunct professor of national security studies at George Mason University's Department of Information Sciences and Technology. He recently served as the Director of Analytics at the interagency Global Engagement Center, and has led counterterrorism activities at Central Intelligence Agency, Department of Defense, National Nuclear Security Administration, and Department of Homeland Security.

The views expressed in this paper are solely those of the author, and not necessarily those of the Program on Extremism or the George Washington University.

The Emergence of Technological Tools Against Foreign Propaganda and Disinformation Online

One of the most consequential events in modern Information Warfare occurred on February 3, 2015.

Throughout 2014, the terrorist group Islamic State ISIS enjoyed seemingly continuous battlefield victories and manufactured a popular narrative of “remaining and expanding.”¹ They had taken the cities of Sinjar and Kobani, demonstrating their intent to develop a geographic caliphate, and along the way they tweeted constantly, earning a reputation for torturous executions, rape and enslavement – all of which triggered *supportive* audience reactions.² Researchers estimated 46,000 mostly uncontested ISIS-controlled accounts on Twitter, posting regularly, with about 1,000 supporters each.³

In December 2014, a Royal Jordanian Air Force F16 pilot named Muath Safi Yousef al-Kasasbeh crashed his jet near Raqqa and was captured by ISIS. ISIS initially used him in its *Dabiq* magazine for propaganda, and then falsely offered to exchange him for ISIS prisoners. By January, ISIS asked its Twitter followers for execution recommendations, using the hashtag #SuggestAWayToKillTheJordanianPilotPig to generate support. And by January 3rd, ISIS propagandists recorded a theatrically orchestrated execution film in which Lieutenant al-Kasasbeh was burned alive in a cage, with cleanly uniformed ISIS militants positioned as a seemingly disciplined unit to witness the execution.⁴

ISIS released Lieutenant al-Kasasbeh’s execution video on February 3, 2015. Everyone who was involved in the Coalition effort to counter ISIS propaganda watched the video closely.⁵ It was remarkable for its orchestration and for its broad dissemination. The Middle East was captivated by the video, and although anti-ISIS viewers were enraged,⁶ pro-ISIS tweets appeared to *increase* ten-fold in the month afterward, with ISIS’s capture of Tikrit in March bolstering their narrative.⁷ This was the peak of ISIS’s activity on social media and the pressure to counter them was acute.

Although the effort against ISIS's online presence was underway, the al-Kasasbeh propaganda event hyper-focused policymakers on opportunities to undermine terrorist use of social media at scale.⁸ It also reinforced the importance of Information Warfare, forcing the small Information Operations community to reconsider the importance of these tactics within the civil-military toolkit. And it encouraged the community to pursue solutions with social media industry partners: in the months after the al-Kasasbeh propaganda event, the community regularly and openly called upon Twitter, Facebook, and other platforms to suspend pro-ISIS accounts. The U.S. Government's demands gained strength in the following months, culminating with a meeting of the Global Coalition Against ISIL Communications Working Group, including representatives of the major social media platforms, in October 2015.⁹

The effort to suspend ISIS accounts on Twitter – which offers the most accessible data for analysis – paid off quantifiably, with “devastating reductions” in ISIS follower accounts from June to October 2015. Average tweets per day per ISIS account during this period peaked at 14.5 per day in June and dropped to 5.5 per day by October.¹⁰ Naysayers had derided these efforts as a game of “whack-a-mole” because ISIS Twitter accounts could be replicated rapidly and required repeated suspensions,¹¹ but the effect was a net loss of ISIS social media presence.

The success of ISIS account suspensions in those “early days” encouraged stronger efforts by social media companies acting on their own and according to their own terms of service. The U.S. Government took the position – as it does now – that it should not directly censor online communications, in support of free speech.¹² Twitter reported suspending over 1,200,000 accounts between 2015 and 2018 for “violations related to the promotion of terrorism” and only .2 percent of those suspensions were based on U.S. Government reports.¹³

The ISIS propaganda effort persists today at a lower level, with decreased press attention.¹⁴ In the past few years, media attention seems to have shifted to Russian propaganda and disinformation activities on social media. The Russian Internet Research Agency (IRA) has conducted a complex campaign across multiple social media platforms reinforcing U.S. political divisions, peaking in 2017. For example, in 2017 the

IRA posted about 6,000 Instagram posts per month; about 4,000 Facebook posts per month; and over 59,000 Twitter posts per month. Over 30,000,000 users interacted with IRA content on Facebook and Instagram in 2015-2017.¹⁵

Frustration with this abuse of social media by ISIS and state actors such as the IRA underlies recent calls for increased account suspension efforts by social media platforms.¹⁶ Social media platforms commonly refer to these activities as “content moderation” – originally developed over a decade ago to combat copyright theft – and rely on Section 230 of U.S. Code 47 for “protection for private blocking and screening of offensive material.”¹⁷ In July 2018, Twitter released a suspended data set of 2,973,371 tweets from 2,848 handles, run by the IRA from February 2012 to May 2018.¹⁸ These content moderation efforts have undoubtedly impacted Russian disinformation campaigns against U.S. audiences, but online disinformation campaigns by state and non-state actors continue.

The success of content moderation against ISIS and the IRA is promising, but seems to have encouraged *overreliance* on this process as a singular solution to the problem of disinformation and propaganda efforts on the internet. For example, the May 2019 Christchurch Call mandated a closer content moderation relationship between signatory governments and social media companies, with the goal of eliminating the kind of violent content that was posted on Facebook and 8chan before and during the March 15, 2019, shooting attack at a mosque in Christchurch, New Zealand.¹⁹ The Call seems to aspire to a “sophisticated algorithm” that ensures efficient suspensions, but Facebook’s recent explanation of their processes shows that content moderation is extraordinarily complex and doesn’t guarantee the kind of instantaneous results that would have been needed to prevent the dissemination of the Christchurch attacker’s propaganda.²⁰ The video uploaded during the Christchurch attack could still be found online weeks afterwards.

The Promise of New Technologies to Address Audience Vulnerabilities to Propaganda and Disinformation

Content moderation's greatest use may be its contribution to addressing propaganda and disinformation *in combination with* other technologies that address the underlying psychological and sociological factors at play. One set of academic researchers tells us that news consumers tend to seek out information that aligns with their own views,²¹ while another group tells us that news consumers fall prey to disinformation because they are cognitively lazy.²² These academic perspectives are refinements of enduring theories of human cognitive bias such as selective exposure, confirmation bias, and motivated reasoning. No matter which academic camp we choose, there are new technologies that can aid online information consumers by identifying the origins of the information they are seeing, offering context for the information, warning of artificiality of information, and arming them with better cognitive tools to judge information veracity.

Content Validation

The problems of disinformation and propaganda are often problems of attribution. In the case of videos and other imagery, propagandists sometimes misidentify the origins of an image in order to develop a false narrative about the image, and this misattribution threatens to confuse and misguide media consumers.²³ One possible solution to the misattribution of content is blockchain-based information validation. Blockchain-based information validation systems digitally “fingerprint” a video or image when it is recorded and immutably store the fingerprint to the blockchain, so that anytime a user of that system accesses the video, they are assured of its origins. Insurers, for example, have begun to use these blockchain-based information validation systems to verify evidence of claims. Critics of these systems are quick to point out, though, that proving the origins of an image file does not prove the truth of the image itself, and that these systems are only useful for counter-disinformation if they are employed at scale.

De-Anonymized Social Media Accounts

Most of the major social media platforms have experimented with account validation. Facebook and Twitter have used checkmark symbols to indicate whether an account holder has voluntarily documented their identity.²⁴ This voluntary self-documentation by users has been mostly for reputation management by the famous, but could have advantages in countering disinformation originators if the process were popularized among all users. The process could be strengthened even more by encouraging social media users to feature their real names. Most of the Russian disinformation distributed online during the 2016 U.S. elections was distributed by fake-name accounts whose origins were indiscernible to average social media users.²⁵ While account validation offers some clear opportunities against disinformation and propaganda, detractors argue that the anonymity of the internet is what makes it so successful, and that de-anonymization would undermine the fair use of the internet by otherwise suppressed voices.

Automated Website Ratings

A handful of self-described independent organizations have begun to market their services as neutral judges of disinformation originators online. These services are sometimes enhanced by artificial intelligence, which promises to instantaneously identify disinformation originators. These services are intended to help social media platforms avoid unintentionally amplifying false or problematic information and are intended to help advertisers avoid placing their ads on counterproductive websites. These services are not new, though: for over a decade, researchers have aggregated data on problematic ad originators and malware originators, and they have published their research openly to help content originators and advertisers avoid problematic associations.²⁶ While these services may now carry the label of “black list,” any organization that has posted an ad online has indirectly used these services for years.

Crowdsourced Information Verification

The internet often works to a propagandist's advantage because it enables broad dissemination of information with little opportunity for direct refutation. As a result, media consumers may see only one side of an argument. Recent research indicates, however, that online groups can be effective judges of source reliability when they are primed to think critically, and can ably see through biased presentations.²⁷ New crowdsourcing technology helps overcome the tyranny of one-sided presentations by providing a forum for critical "meta-conversations" – conversations occurring literally atop the original information, almost anywhere on the internet. This technology is currently popular with academics, who use it to discuss research papers posted online, for example. This technology requires much broader mainstream adoption, however, before it could counter propaganda and disinformation at scale.

Online Advertisement and Content Attribution

Under the assumption that malign influencers would take advantage of lax advertising standards to deliver disinformation in the run-up to European elections – as they have during previous elections²⁸ – some social media providers recently began to require advertisers to clearly identify the origins of politics-related advertisements.²⁹ By requiring advertisers to declare their allegiances with a "paid for by" statement, Facebook intended to address the problems of disinformation and propaganda on the supply side, before ads reach consumers – perhaps offering one of the most scalable solutions to the problem. Similarly, YouTube places overlay ads on videos it identifies as coming from state-funded broadcasters.³⁰ Ad attribution, like other de-anonymization efforts, promises a new level of transparency, but for the time being the rules for these ads seem limited and circumventable. For example, an ad intended to influence voters during an election by focusing on voters' underlying psychological vulnerabilities – indirectly affecting their voting behavior – may evade new advertising transparency rules.

“Yellow Alerts”

A number of analytic teams persistently research the online propaganda of groups like ISIS and the IRA, leveraging sophisticated social media monitoring systems, and they produce impressive reports of their findings. These reports typically are read only by a small audience, though, and the findings are lost on the majority of general internet users who might benefit from warnings of malign influence campaigns erupting online. Issuing succinct "yellow alerts" of these malign campaigns on social media platforms – where media consumers are most likely to encounter disinformation – could prepare consumers to encounter such campaigns critically. This concept often receives strong resistance, however, because the judgment of what is propaganda and what is truth can be subjective.³¹ Therefore, a warning system of this kind would only be politically feasible if it focused on objective facts of the deceptive techniques of a campaign. For example, a warning could describe ISIS's duplicitous use of false identities online, but a warning could not defensibly judge the truthfulness of an ISIS statement. However, social media platforms may hesitate to support a system that seems to imply a vulnerability of their own platforms.

Tech-Enabled Media Literacy Training

To judge by recent press, the public is mentally defenseless against online disinformation.³² While this is an exaggeration, information consumers do sometimes fall prey to disinformation and propaganda because it is well hidden, seemingly indistinguishable from fact.³³ Proponents of media literacy training promise to solve that problem by training and retraining information consumers in the art of factual discernment online. A handful of counter-disinformation games are online now, and a few non-profit organizations offer more intensive classroom and online training curricula. These games and classes take students through the process of applying rigorous sourcing standards to the information they are encountering, encouraging

stronger critical thinking. But perhaps the most limiting factor of these programs is their popularity – they remain “nice to have” features of education systems; furthermore, these effects of these programs will likely only be felt in the long term.

The Complexity of Technology Implementation in the Context of the U.S. Constitution

The U.S. government-industry relationship regarding online propaganda and disinformation has traditionally been informational. Both groups have relied upon formal information-sharing forums such as the Global Internet Forum to Counter Terrorism, the Global CT Forum, or Tech Against Terrorism to enable discussions of strategic intent. And when the U.S. Government is aware of an imminent threat of violence online, it may legally inform the social media platforms.³⁴ But the social media industry has historically appeared to keep governments at arm’s length to retain control of their own business processes and to reinforce their images as independent and free information-sharing platforms.³⁵

The seven technologies above may offer mutually beneficial opportunities for collaboration between government and industry, with the goal of limiting the effects of online propaganda and disinformation. Together, these technologies avoid the trap of politically judging the content appearing online, they offer new market opportunities for social media platforms and related developers, and they offer the government an opportunity to demonstrate resolve by driving broad adoption. Perhaps most importantly, these technologies are market-driven, and are not punitive, encouraging continued growth of an important business sector.

While the technological solutions provided here would intentionally support collaboration between government and industry, the international community seems to be heading in the other direction. Governments are enacting legislation that empowers them to punitively direct social media platforms to take down harmful content online. The definition of “harmful” is subjective and based on malleable government policy.

Singapore's new Protection From Online Falsehoods and Manipulation bill, for example, enables the state to enforce removal of "false" content on apps such as WhatsApp or Telegram.³⁶ Germany's 2018 Network Enforcement Act holds social media companies responsible for content considered illegal under Germany's existing hate speech laws, such as "incitement to hatred".³⁷ And the latest, the Christchurch Call, requires social media companies to voluntarily respond to reports of "terrorist and violent extremist" content online.³⁸

These directive content moderation policies conflict with the U.S. public's sense of free speech rights and even conjure nightmares of totalitarianism.³⁹ Yet commentators consistently complain of the threat of ceding online content review to a commercial industry. While the German Network Enforcement Act initially received strong constituent approval, the legislation now seems to be under litigative assault, perhaps demonstrating the limits of societal support.⁴⁰ The reality of enforcement seems to have diverged radically from the original intent of the legislation, and that lesson is important to any U.S. technology implementation in this area: technology may be applied as a helpful tool for addressing skin-deep propaganda and disinformation symptoms, but not as a comprehensive solution to the deeper illness.

References

- ¹ ISIS used its *Dabiq* magazine to officially announce its Remaining and Expanding propaganda theme in August 2014. See ISIS. "Remaining and Expanding." *Dabiq*. October 2014. <https://clarionproject.org/docs/isis-isis-islamic-state-magazine-issue-5-remaining-and-expanding.pdf>.
- ² Badawy, Adam and Emilio Ferrara. "The rise of Jihadist propaganda on social networks." *Journal of Computational Social Science* (2018): <https://arxiv.org/abs/1702.02263>.
- ³ Berger, J.M. and Jonathon Morgan. "The ISIS Twitter Census." *The Brookings Project on U.S. Relations with the Islamic World* (2015): https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf.
- ⁴ Chen, Ronald. *The Death of Muath al-Kasasbeh: The Politics of Mourning, Memory, Identity & Power*. <https://mei.nus.edu.sg/wp-content/uploads/2018/03/politicsofalkasasbeh.pdf>: Yale-NUS College, National University of Singapore, 2018.
- ⁵ The author led the US Government's short-lived Information Coordination Cell (ICC) within the Center for Strategic Counterterrorism Communications at the time. The ICC was intended to coordinate all counter-propaganda efforts against ISIS. Comments on the Information Operations community's activities are based on this perspective.
- ⁶ Chen, Ronald. *The Death of Muath al-Kasasbeh: The Politics of Mourning, Memory, Identity & Power*. <https://mei.nus.edu.sg/wp-content/uploads/2018/03/politicsofalkasasbeh.pdf>: Yale-NUS College, National University of Singapore, 2018.
- ⁷ Badawy, Adam and Emilio Ferrara. "The rise of Jihadist propaganda on social networks." *Journal of Computational Social Science* (2018): <https://arxiv.org/abs/1702.02263>.
- ⁸ The al-Kasasbeh propaganda event occurred just after ISIS's 7 January 2015 *Charlie Hebdo* attack, which certainly contributed to the intensity of the moment. The al-Kasasbeh attack, however, stood out as a culmination of ISIS's propaganda.
- ⁹ Foreign and Commonwealth Office. "UK holds meeting of representatives from the Global Coalition against ISIL." 28 October 2015. *gov.uk*. <https://www.gov.uk/government/news/uk-holds-meeting-of-representatives-from-the-global-coalition-against-isil>.
- ¹⁰ Berger, J.M. and Heather Perez. "The Islamic State's Diminishing Returns on Twitter: How suspensions are limiting the social networks of English-speaking ISIS supporters." *GWU Program on Extremism* (2016): https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/Berger_Occasional%20Paper.pdf.
- ¹¹ Among the articles decrying the "whack-a-mole" approach at the time was Makuch, Ben. "Banning Islamic State Jihadists From Twitter Is Like Playing Whack-a-Mole." *Vice*. 21 August 2014. https://www.vice.com/en_us/article/z4mzbj/isis-twitter-whack-a-mole. 7 May 2019.
- ¹² Perhaps the most prominent recent example of this policy is the US Government's abstention from the Christchurch Call. See Romm, Tony and Drew Harwell. *White House declines to back Christchurch call to stamp out online extremism amid free speech concerns*. 15 May 2019. https://www.washingtonpost.com/technology/2019/05/15/white-house-will-not-sign-christchurch-pact-stamp-out-online-extremism-amid-free-speech-concerns/?utm_term=.2f9883fac9ab.
- ¹³ Twitter. *Expanding and building #TwitterTransparency*. 5 April 2018. https://blog.twitter.com/en_us/topics/company/2018/twitter-transparency-report-12.html.
- ¹⁴ Information Operations analysts continue to describe a flourishing ISIS propaganda effort, despite the group's geographic losses. One useful assessment is Milton, Daniel. "Down, but Not Out: An Updated Examination of the Islamic State's Visual Propaganda." The Combating Terrorism Center at West Point (2018): <https://ctc.usma.edu/app/uploads/2018/07/Down-But-Not-Out.pdf>
- ¹⁵ Howard, Philip, et al. "The IRA, Social Media and Political Polarization in the United States, 2012-2018." *Computational Propaganda Research Project* (2018): <https://comprop.oii.ox.ac.uk/research/ira-political-polarization/>.
- ¹⁶ Calls for regulation of the social media industry, at their root, are normally demands for increased content moderation. The most prominent recent example of these is a call for content moderation, in the guise of increased regulation, after a derisive video of US House of Representatives Speaker Nancy Pelosi surfaced on the internet. See Condliffe, Jamie. "The Week in Tech: Disinformation's Huge Inaction Problem." *New York Times*. 31 May 2019. <https://www.nytimes.com/2019/05/31/technology/facebook->

- [disinformation-nancy-pelosi.html?action=click&module=Briefings&pgtype=Homepage](#). Specific to the ISIS problem, see Romm, Tony and Drew Harwell. "White House declines to back Christchurch call to stamp out online extremism amid free speech concerns." *The Washington Post*. 15 May 2019. https://www.washingtonpost.com/technology/2019/05/15/white-house-will-not-sign-christchurch-pact-stamp-out-online-extremism-amid-free-speech-concerns/?utm_term=.2f9883fac9ab.
- ¹⁷ Cornell University. *47 U.S. Code § 230. Protection for private blocking and screening of offensive material*. 8 February 1996. <https://www.law.cornell.edu/uscode/text/47/230#>.
- ¹⁸ Roeder, Oliver. *Why We're Sharing 3 Million Russian Troll Tweets*. 31 July 2018. <https://fivethirtyeight.com/features/why-were-sharing-3-million-russian-troll-tweets/>.
- ¹⁹ New Zealand Ministry of Foreign Affairs and Trade. *Christchurch Call*. 15 May 2019. <https://www.christchurchcall.com/>.
- ²⁰ Fishman, Brian. "Crossroads: Counter-terrorism and the Internet." *Texas National Security Review* (2019): <https://tnsr.org/2019/02/crossroads-counter-terrorism-and-the-internet/>.
- ²¹ Schmidt, Ana Lucia, et al. "Anatomy of news consumption on Facebook." *Proceedings of the National Academy of Sciences of the United States of America* (2017). <https://www.pnas.org/content/114/12/3035>.
- ²² Pennycook, Gordon and David Rand. "Lazy, not biased: Susceptibility to partisan fake news is better explained by lack of reasoning than by motivated reasoning." *Cognition* (2018). <https://static1.squarespace.com/static/51ed234ae4b0867e2385d879/t/5b43b48b03ce6471753c78ba/1531163796071/2018+Pennycook+Rand+-+Cognition.pdf>.
- ²³ Thompson, Nicholas and Issie Lapowski. "How Russian Trolls Used Meme Warfare To Divide America." *Wired* 17 December 2018. <https://www.wired.com/story/russia-ira-propaganda-senate-report/>.
- ²⁴ Lodge, Kristen. *What is a Verified Social Media Account (and How Can You Get It?)*. 2018. <https://www.commonplaces.com/blog/what-is-a-verified-social-media-account-and-why-does-it-matter/>. 8 May 2019.
- ²⁵ US House of Representatives. *Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements*. 2018. Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements. 8 May 2019.
- ²⁶ EasyList. *EasyList*. 2019. <https://easylis.to/#easyprivacy>. 8 May 2019.
- ²⁷ Pennycook, Gordon and David Rand. "Lazy, not biased: Susceptibility to partisan fake news is better explained by." *Cognition* (2018). <https://static1.squarespace.com/static/51ed234ae4b0867e2385d879/t/5b43b48b03ce6471753c78ba/1531163796071/2018+Pennycook+Rand+-+Cognition.pdf>.
- ²⁸ Dawson, Andrew and Martin Innes. *The Internet Research Agency in Europe 2014-2016*. Research Report. Cardiff: Cardiff University Crime & Security Research Center, 2019. <https://static1.squarespace.com/static/57875c16197aea2902e3820e/t/5cd14804104c7bb3cafeaa06/1557219339758/The+Internet+Research+Agency+In+Europe+2014-2016.pdf>.
- ²⁹ Facebook. *Increasing Transparency for Ads Related to Politics in the UK*. 16 October 2018. <https://newsroom.fb.com/news/2018/10/increasing-transparency-uk/>. 3 May 2019.
- ³⁰ Ong, Thuy. "YouTube will start labeling videos from state-funded broadcasters." *The Verge* 2 February 2018. <https://www.theverge.com/2018/2/2/16964190/youtube-state-funded-broadcasters>.
- ³¹ Allen, Barbara. *Poynter*. 2 May 2019. <https://www.poynter.org/letter-from-the-editor/2019/letter-from-the-editor/>. 3 May 2019.
- ³² The New York Times, for example, developed an impossible online quiz asking users to identify fraudulent Facebook postings, implying intellectual helplessness. See Collins, Keith and Sheira Frenkel. "Can You Spot the Deceptive Facebook Post?" *New York Times* 4 September 2018. <https://www.nytimes.com/interactive/2018/09/04/technology/facebook-influence-campaigns-quiz.html>.

³³ US House of Representatives. *Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements*. 2018. Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements. 8 May 2019.

³⁴ Levinson-Waldman, Rachel. "Government Access to and Manipulation of Social Media: Legal and Policy Challenges." *Howard Law Journal* (2018): 523-560.

https://docs.wixstatic.com/ugd/cc2615_23ccb9a7aa1a4098b4742b01e5e443e6.pdf#page=43.

³⁵ It's probably impossible to objectively quantify the divide between Silicon Valley and Washington, DC, but the sentiment is routinely identified by journalists and commentators on the tech beat. See Zegart, Amy and Kevin Childs. "The Divide Between Silicon Valley and Washington Is a National-Security Threat." *The Atlantic* 13 December 2018. <https://www.theatlantic.com/ideas/archive/2018/12/growing-gulf-between-silicon-valley-and-washington/577963/>.

³⁶ Wong, Tessa. "Singapore fake news law polices chats and online platforms." *BBC News* 9 May 2019. <https://www.bbc.com/news/world-asia-48196985>.

³⁷ Tworek, Heidi and Paddy Leerssen. *An Analysis of Germany's NetzDG Law*. Working Paper. Amsterdam: Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, 2019.

https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf.

³⁸ New Zealand Ministry of Foreign Affairs and Trade. *Christchurch Call*. 15 May 2019.

<https://www.christchurchcall.com/>.

³⁹ Tworek, Heidi. "A Lesson From 1930s Germany: Beware State Control of Social Media." *The Atlantic* 26 May 2019. <https://www.theatlantic.com/international/archive/2019/05/germany-war-radio-social-media/590149/>.

⁴⁰ Kinstler, Linda. "Germany's Attempt to Fix Facebook Is Backfiring." *The Atlantic* 18 May 2019.

<https://www.theatlantic.com/international/archive/2018/05/germany-facebook-afd/560435/>.