STATEMENT OF

JOAN DONOVAN, PHD
RESEARCH DIRECTOR AT HARVARD KENNEDY SCHOOL'S SHORENSTEIN CENTER ON MEDIA, POLITICS AND PUBLIC POLICY

HEARING ON "ALGORITHMS AND AMPLIFICATION: HOW SOCIAL MEDIA PLATFORMS' DESIGN CHOICES SHAPE OUR DISCOURSE AND OUR MINDS"

BEFORE THE SENATE COMMITTEE ON THE JUDICIARY SUBCOMMITTEE ON PRIVACY, TECHNOLOGY, AND THE LAW

APRIL 27, 2021

From "Get Big Fast" to "Move Fast and Break things" and Back Again.

Before there was "move fast and break things," there was another animating ethic of the tech industry: "Get big fast!" This philosophy has proven to be good for the industry, but bad for the world. Over the last decade, social networking (connecting people to people) morphed into social media (connecting people to people *and* to content), which resulted in exponential profits and growth. Most people don't know the difference between social networking and social media, but this transition was the key to products like Facebook, Twitter, and YouTube dominating global markets in mass communication. In short, *networks are the wealth of society*. Networks are where the rich and powerful derive their importance and high status, hence saying "he or she is connected" when referencing someone you do not want to mess with. When social media is the vector of attack against our democracy and public health, a small group of highly motivated and connected actors can manipulate public understanding of any issue simply by using these products they are as designed.

How social media companies got big fast was a combination of lax consumer regulation, eschewing risks, buying out the competition where possible, and a focus on scale that made for poor security decisions. Beyond connecting people and content, products like Facebook, YouTube, and Twitter rely on other companies and individuals to provide them with more data, increasing the scale in this massive and sprawling data infrastructure across the web. Mapping, tracking, and aggregating people's social networks made social media a viable business because companies could sell data derived from interactions or monetize those relationships as other products, such as advertising, targeted posts, and promoted messages. Social media data should be legally defined at some point, but for now, I am referring to information about people, how they behave online, interactions with people and content, and location tagging.

But, it wasn't enough just to collect and sort data on the product: targeted advertising and data services only become useful when paired with other kinds of data. For example, in Nov. 2012, when looking at different models for monetizing Facebook, Zuckerberg wrote in a company email that allowing developers access to data without having these companies share their data with Facebook would be "good for the world, but bad for us."[1] This is because Facebook knew, even back then, that their products could threaten privacy on a scale society had never reckoned with before. Now, these social media products that favor runaway scale and openness threaten not only individual rights, but also the future of democracy and public health.

By leveraging people's networks and content at the same time, a business model emerged where key performance indicators included:

(1) growth of daily and monthly active users,

(2) increasing engagement metrics, and

(3) advertising revenue.

The last decade has been marked by these companies expanding exponentially on all of these indicators. In a *PC Mag* article from 2011 about the best mobile apps, Facebook and Twitter were both ranked lower than an app that turns your camera into a flashlight.[2] In 2011, Twitter had approximately 100 million users, Facebook had 845 million, and YouTube had 800k.[3] By 2020, Twitter reports 353 million active users, Facebook reports 2.7 billion active users, and 2.29 billion for YouTube.[4] Advertising revenue continues to grow across all of these products, where Google ($146 billion) and Facebook ($84 billion) dominate.[5]

Using accounts as a key performance indicator drove a shadow industry of growth hacking, which eventually was integrated directly into the products—allowing a

---

[1] Solon, Olivia, and Cyrus Farivar. 2019. "Thousands of Leaked Facebook Documents Show Mark Zuckerberg as 'Master of Leverage' in Plan to Trade User Data." NBC News. https://www.nbcnews.com/tech/social-media/mark-zuckerberg-leveraged-facebook-user-data-fight-rivals-help-friends-n994706

[2] Segan, Sasha. 2011. "The Top 10 Free BlackBerry Apps 2011." PC Mag. https://www.pcmag.com/news/the-top-10-free-blackberry-apps-2011.

[3] Wasserman, Todd. 2012. "Twitter Says It Has 140 Million Users." Mashable. https://mashable.com/2012/03/21/twitter-has-140-million-users/.
Associated Press. 2012."Number of Active Users at Facebook over the Years." https://finance.yahoo.com/news/number-active-users-facebook-over-years-214600186--finance.html?guccounter=1.

[4] Statista. 2021. "Most Used Social Media 2021." Statista. Accessed April 26, 2021. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.

[5] H. Tankovska, "Facebook's advertising revenue worldwide from 2009 to 2020." https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/#:~:text=In%202020%2C%20Facebook%20generated%20close,of%20the%20social%20network's%20revenue.
Joseph Johnson, "Advertising revenue of Google from 2001 to 2020," February 5, 2021, Statista, https://www.statista.com/statistics/266249/advertising-revenue-of-google/#:~:text=In%202020%2C%20Google's%20ad%20revenue%20amounted%20to%20146.92%20billion%20US%20dollars.

massive and known vulnerability of sock puppets, or fake accounts, to persist.[6] For those who understood how to manipulate this vulnerability, increasing engagement meant delivering more novel and outrageous content, which is why false news, harassment, and defamation thrive on social media. For social media companies, decisions about profit drive innovation, not higher principles like access to truth, justice, or democracy. As a result, these products are not only a parasite on our social networks feeding off every click, like, and share, but they also cannot optimize for the public interest. It did not have to be this way. Back in 2011, mobile was developing quickly and there were many ways in which social media could have been designed to foster community safety and to maximize privacy. Instead, the drive to maximize the number of users, engagement, and revenue led us here.

Most crucially the entire internet infrastructure needs an overhaul, so that companies are not able to siphon data and leverage it to maximize an advantage over consumers.[7] But, users are not necessarily the customers, advertisers are.[8] The structure of online advertising pipelines systematically advantages these companies at the expense of several industries, most importantly journalism. By becoming the gateway to news audiences, top social media companies hoard advertising revenue that belongs to those who create engaging content for display on their products, most notably journalists.

When criticized about the squeeze their products have placed on journalism, Facebook and Google will cite their various news initiatives. But, these initiatives pick and choose partners and then channel journalists labor directly back into their products. Facebook's fact-checking program, for instance, partners with several reputable news outlets, but labelling has done little to disincentivize fake news. Moreover, fact-checking is ad-hoc and will never rival supporting independent investigative journalism, a bedrock of a strong democracy. Instead, this initiative expands Facebook's ever-growing web of influence over news as it becomes increasingly more difficult to criticize the corporation for fearing of losing resources.

Nevertheless, as journalism wanes, social media serves **misinformation-at-scale** to hundreds of millions of daily active users instantaneously, especially odious when misinformation is promoted in trends and recommendations. In October 2020, I testified about conspiracies and misinformation having similar harmful societal impacts as secondhand smoke.[9] Post-2020, we see misinformation-at-scale's deadly effects in the US. Scammers and grifters use social media to sell bogus products and push conspiracies—including monetizing the pandemic in grotesque ways to sell fake cures or to scaremonger.[10] Going into the pandemic, anti-vaccination activists had a huge

---

[6] Donovan, Joan, and Brian Friedberg. n.d. "Source Hacking: Media Manipulation in Practice." Data & Society (blog). Accessed January 5, 2020. https://datasociety.net/output/source-hacking-media-manipulation-in-practice/.
[7] Noble, Safiya Umoja. 2018. Algorithms of Oppression: How Search Engines Reinforce Racism. New York: NYU Press.
[8] Anthony Nadler, and Joan Donovan. 2018. "Weaponizing the Digital Influence Machine." Data & Society. Data & Society Research Institute. October 17, 2018. https://datasociety.net/library/weaponizing-the-digital-influence-machine/.
[9] Donovan, Joan. 2020. "Thank You for Posting: Smoking's Lessons for Regulating Social Media | MIT Technology Review." https://www.technologyreview.com/2020/10/05/1009231/social-media-facebook-tobacco-secondhand-smoke/.
[10] Donovan, Joan. 2021. "Without Leadership on Vaccine Rollout, Scams Are Inevitable | MIT Technology Review." https://www.technologyreview.com/2021/01/06/1015813/florida-eventbrite-vaccine-scam-inevitable/.

advantage over public health officials, where anti-vaccination activists were able to leverage already dense and sprawling networks across social media products. As a result, they attached their strikes to breaking news cycles by attacking public confidence in science. There was nothing public health officials could do to stop the torrent of misinformation drowning doctors and hospitals, as evidenced by the reporting of Brandy Zadrozny and Ben Collins at *NBC News*.[11] The same situation holds for other public servants, like election officials, who continue to bear the costs of election disinformation and are leaving their jobs because its managing misinformation-at-scale is unsustainable.[12]

For journalists, researchers, and everyone trying to mitigate misinformation, the experience is like trying to put your hands up against a growing ocean swell as it washes over you. Journalists, universities, public service, and our healthcare professionals take on the true costs of misinformation-at-scale, which isn't an existential statement. There are millions of resources lost to mitigating misinformation-at-scale, where the cost of doing nothing is even worse. For example, take the blatant lie that the vaccines have microchips. To counter it, journalists traded off covering other stories, while public health professionals continue to explain that there are no microchips in the vaccine.[13]

The only way to fix a problem like motivated misinformers involves platforms enforcing existing policies, researchers and journalists working together as tech watchdogs, and policymakers opening the way for a public interest internet. Regulators should introduce public interest obligations to social media newsfeeds and timelines so that timely, local, relevant, and accurate information reaches the masses-at-scale. Together, we must make a public interest internet a whole-of-society priority.

Going Down the Rabbit Hole

What I have learned studying the internet over the last decade is simple: *everything open will be exploited*. There is nothing particularly new about misinformation and conspiracies circulating. After all, there is no communication without misinformation. However, over the last decade the design of social media itself created favorable conditions for reaching millions instantaneously while also incorporating financial and political incentives for conducting massive media manipulation campaigns. The most dangerous aspects of these products come to light when we analyze who gains an advantage when openness meets scale.

---

[11] Zadrozny, Brandy, 2020."They're on the Misinformation Front Line. Here's What They Predict about the Virus." NBC News. https://www.nbcnews.com/tech/social-media/these-disinformation-researchers-saw-coronavirus-infodemic-coming-n1206911.
Zadrozny, Brandy, and Ben Collins.et al. 2020. "Whitmer Conspiracy Allegations Tied to 'boogaloo' Movement." NBC News. https://www.nbcnews.com/tech/tech-news/whitmer-conspiracy-allegations-tied-boogaloo-movement-n1242670.
Zadrozny, Brandy. 2020. "Anti-Vaccination Movement Gets Traction in Unlikely Source: Local News." NBC News.. https://www.nbcnews.com/tech/tech-news/anti-vaccination-groups-target-local-media-after-social-media-crackdowns-n1251485.
[12] CNN, Fredreka Schouten and Kelly Mena. n.d. "High-Profile Elections Officials Leave Posts after a Tumultuous 2020." CNN. Accessed April 26, 2021. https://www.cnn.com/2021/02/19/politics/election-officials-lose-and-leave-jobs/index.html.
[13] Donovan, Joan, Brian Friedberg, Gabrielle Lim, Nicole Leaver, Jennifer Nilsen, and Emily Dreyfuss. 2021. "Mitigating Medical Misinformation: A Whole-of-Society Approach to Countering Spam, Scams, and Hoaxes," 52.

I often joke nervously that "my computer thinks I'm a white supremacist." One only needs to look at my homepage on YouTube to illustrate this point. On the homepage, YouTube clearly displays your interests and makes recommendations. Daily, it recommends me content from a white supremacist who they have already banned, yet recent videos of his livestreams are continuously recommended. I first learned of the pandemic in January 2020 from a conspiracist and nationalist YouTuber, who was excited by shutting down the borders to stop the "Wu Flu." I had spent countless hours down the rabbit hole with this YouTuber before, who that night in January 2020 spent over three hours extoling his xenophobic views. Racialized disinformation continues to be a critical source of political partisanship in the US because it is so easy to manipulate engagement on race and racism—and it's profitable.[14]

While some debate the existence of "the rabbit hole" on social media, our research team at Shorenstein has been looking deeper at this phenomenon. Going down the rabbit hole means getting pulled into an online community or subculture, where the slang, values, norms, and practices are unfamiliar, but nevertheless engrossing. There are four aspects of the design of social media that lead someone down the rabbit hole. They are:

(1) repetition relates to seeing the same thing over and over on a single product,

(2) redundancy is seeing the same thing across different products,

(3) responsiveness is how social media and search engines always provide some answer unlike other forms of media, and

(4) reinforcement is the ways that algorithms work to connect people and content so that once you've searched for a slogan or keyword, algorithms will reinforce these interests.

Nowhere is this more prevalent than on YouTube, where any search for conspiracy or white supremacist content, using their preferred keywords of the in-group, will surface numerous recommendations. It's a misconception that these online echo chambers or filter bubbles are hyper-personalized and conclusively shape individual behavior in a specific direction. Instead, what algorithms tend to do is group people with homogeneous characteristics into buckets, who are served similar content in batches. From 9/11 conspiracies, to the "vaccines cause autism" meme, to QAnon, some conspiracist communities have been thriving on social media for decades. But, it is a misnomer, albeit a popular one, to imagine social media as an attention economy, where individual users are making independent choices of where to spend their time.

It's more correct to call the rabbit hole an "algorithmic economy," where algorithms pattern the distribution of content based on signals from millions of people according to generic profiles in buckets, coupled with algorithmic grouping in batches. On its surface, the design is not insidious: the buckets and batches are related to generic interests. For example, if you're a baseball fan and YouTube knows you want more

[14] Freelon, Deen, Michael Bossetta, Chris Wells, Josephine Lukito, Yiping Xia, and Kirsten Adams. 2020. "Black Trolls Matter: Racial and Ideological Asymmetries in Social Media Disinformation." Social Science Computer Review, April, 0894439320914853. https://doi.org/10.1177/0894439320914853.

sports content, that's a great service. But if you've searched for more contentious content, like QAnon, Proud Boys, or Antifa recently, you are likely to enter a rabbit hole, where extracting yourself from reinforcement algorithms ranges from difficult to impossible. While customers, such as advertisers, have lobbied these social media companies for better ad placement, users are not able to easily swap out interests or stop targeted recommendations altogether.

Getting Out of the Rabbit Hole

My last point is about the past five years of social media shaping our public discourse. Social media provides a different opportunity for the enemies of democracy to sow chaos and plan violent attacks. It's fourth generation warfare, where it is difficult to tell the difference between citizens and combatants. The reason why Russia impersonated US social movements in 2016 was expressly because movements elicit lots of engagement, where participants see sharing content and network-making as political acts. That kind of political participation was challenging for city governance during the 2011 Occupy Movement, but that moment—a decade ago—should have taught Facebook, YouTube, and Twitter more about the range of effects their products could have on society. Now we see these products used by authoritarians who leverage a mix of authentic political participation paired with false accounts and fake engagement to win elections.[15]

Cobbled together across products, our new media ecosystem is the networked terrain for a hybrid information war that ultimately enables dangerous groups to organize violent events—like the nationalists, militias, white supremacists, conspiracists, anti-vaccination groups, and others who collaborated under the banner of Stop The Steal in order to breach the Capitol. Last week, a *Buzzfeed* article included a leaked internal Facebook memo on the exponential growth of "Stop the Steal" groups on their platform. The report clearly illustrated that groups exposing violent and hateful content can grow very fast on across the product. Even when Facebook removes groups, it does not stop the individuals running them from trying again. Adaption by media manipulators is a core focus of our research at the Shorenstein Center.[16] Facebook found that their own tools allowed Stop the Steal organizers to leverage openness and scale to grow faster than Facebook's own internal teams could counter.

In short, even when aware of the risks of their product to democracy, Facebook's interventions do little to contain exposure of misinformation-at-scale to the general public. When determined to stop the spread of misinformation, Facebook could not counter it with their internal policies. Misinformation-at-scale is a feature of Facebook's own design and is not easily rooted out. Because Facebook defines the problem of misinformation-at-scale as one of coordinated inauthentic behavior, they were woefully unprepared handle the threats posed by their own products. They were unprepared in

---

[15] Ong, Jonathan, and Jason Vincent Cabañes. 2018. "Architects of Networked Disinformation: Behind the Scenes of Troll Accounts and Fake News Production in the Philippines." Architects of Networked Disinformation: Behind the Scenes of Troll Accounts and Fake News Production in the Philippines, January. https://doi.org/10.7275/2cq4-5396.

[16] Donovan, Joan, Emily Dreyfuss, Brian Friedberg, and Gabrielle Lim. n.d. "A Blueprint for Documenting and Debunking Misinformation Campaigns." Nieman Reports. Accessed November 8, 2020. https://niemanreports.org/articles/a-blueprint-for-documenting-and-debunking-misinformation-campaigns/.

2016 and have since then been unable to handle the new ways that motivated misinformers use their products.

What began in 2016 with false accounts and fake engagement inflaming and amplifying societal wedge issues slowly transformed overtime into a coordinated attack on US democracy and public health. The biggest problem facing our nation is misinformation-at-scale, where technology companies must put community safety and privacy at the core of their business model, ensure that advertising technology is utilized responsibly, and quickly act on groups coordinating disinformation, hate, harassment, and incitement across the media ecosystem. A problem this big will require Federal oversight.

But I am hopeful that another future is possible, if tech companies, regulators, researchers, and advocacy begin to work together to build a public interest internet modeled on the principles that the public has a right to access accurate information on demand.[17] The cost of doing nothing is democracy's end.

[17] Technology and Social Change Research Project. 2021. "Submission to the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression." Media Manipulation Casebook. February 17, 2021. https://mediamanipulation.org/research/submission-un-special-rapporteur-promotion-and-protection-right-freedom-opinion-and.