The Impact of the Internet on Personal Autonomy

An STS Research Paper
presented to the faculty of the
School of Engineering and Applied Science
University of Virginia

by

Connor Anderson

March 27, 2020

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signed: _____

Approved: _____ Date _____
Peter Norton, Department of Engineering and Society

The Impact of the Internet on Personal Autonomy

In the span of a generation, the internet has become a massive part of our lives, with 3.2 billion smartphone users as of 2019 (Newzoo). Tech companies optimize AI to generate revenue by capturing our data and attention. Marketers utilize these systems to generate sales, and politicians utilize them to spread ideas. Left unchecked, these algorithms can drive radicalization, place us in bubbles of like-minded thoughts, and spread disinformation to billions. Foreign actors attempt to manipulate these platforms for their own agendas. Massive databases of personalized data amount to a privacy risk as third parties stand to profit by utilizing the data. These risks push politicians to regulate tech companies if the companies cannot combat these threats. Under pressure by governments to avoid regulation, tech companies further threaten autonomy as they utilize AI to take governance into their own hands. Consequently, modern capitalistic markets produce companies that threaten privacy and autonomy in ways that appear statist, a tendency which may be called the Paradoxical Capitalist Effect. These conflicts pose the question of how the internet affects personal autonomy, "the capacity of an agent to act in accordance with objective morality rather than under the influence of desires" (Lexico, n.d.). I argue that the internet threatens autonomy through disinformation and attention campaigns which are amplified by threats to privacy.

Review of Research

Kwon et al. (2016) found that the average user of social networking sites exhibits rational addictive behaviors. The researchers applied the rational addiction framework introduced by Becker and Murphy (1988) which views addiction as a rational, utility-maximizing behavior

based on economic considerations (Kwon et al., 2016). Addictive behavior regarding social media suggests a threat to autonomy. In a systematic literature review, D'Arienzo et al. (2019) found a significant positive association between insecure attachment styles (anxious and avoidant) and intensive and dysfunctional use of the internet and social media, suggesting some groups may face greater risk to autonomy. Andreasson et al. (2016) found that because internet addiction varies by age, gender, and relationship status, "internet addiction" as a unified term is not a useful construct (2016).

Chistman (2018) says: "Autonomy concerns the independence and authenticity of the desires (values, emotions, etc.) that move one to act in the first place." I utilize this definition of autonomy to investigate how the internet affects the authenticity of desires, values, and beliefs. Ribeiro et al. (2020) found that evidence that the YouTube algorithm systematically progresses users towards more polarizing content. Hoffman et al. (2019) found: "While paid content matters for traditional consumer products, organic engagement remains the bread and butter of political campaigning." Thus, the distribution and censorship of organic disinformation and fake organic disinformation becomes central to autonomy.

The internet's threat to personal autonomy: attention campaigns and privacy threats

The purported goal of many social networks is to supply their users the content they demand. In a 2019 Facebook newsroom post, Facebook stated: "The goal of News Feed is to connect people with the posts they find most relevant. As we've said in the past, it's not about the amount of time someone spends on Facebook, but rather the quality of time spent. That means making sure people see what they want to see – whether that's posts from family and friends or news articles and videos from Pages they follow" (Facebook, 2019). YouTube echoes

a similar goal: “We want to make sure we’re suggesting videos that people actually want to watch” (YouTube, 2019). While these companies’ stated goals are not to maximize users’ time on the site, more content that users want to see inevitably leads to more time on the site. Furthermore, relevant user content yields better personal data. To provide posts from family or friends, Facebook must know who their friends are, and providing the news and articles that users most want to is best accomplished when Facebook knows more about its users. YouTube as well can better suggest videos the more it knows about the individual user. Hence, privacy is inconsistent with the attention economy.

Some advocates claim the human mind is ill equipped to handle the campaigns for attention by social networks, advertisers, and journalists. The Center for Humane Technology (CHT) says humanity is losing the attention race: “Today’s tech platforms are caught in a race to the bottom of the brain stem to extract human attention. It’s a race we’re all losing…. The result: addiction, social isolation, outrage, misinformation, and political polarization” (Harris n.d.). Tristin Harris, the founder of CHT, says our paleolithic brains live in a world of god-like technology: “Technology has outmatched our brains, diminishing our capacity to address the world’s most pressing challenges. The advertising business model built on exploiting this mismatch has created the attention economy” (Harris 2019).

The internet can pose a more serious threat to autonomy for certain groups. Christman (2018) distinguishes autonomy in a general sense from situational autonomy: social media addicts are normally autonomous individuals whose autonomy is impaired by social media. But social media’s threat to autonomy is not limited to situational autonomy. Christman (2018) distinguishes freedom from autonomy: “Autonomy concerns the independence and authenticity of the desires (values, emotions, etc.) that move one to act in the first place.” Therefore, any

curtailment of authentic desires, values, and emotions also curtails autonomy. In *The Filter Bubble: What the Internet is Hiding From You,* Eli Pariser (2011) claims: "Personalization filters serve up a kind of invisible autopropaganda, indoctrinating us with our own ideas, amplifying our desire for things that are familiar and leaving us oblivious to the dangers lurking in the dark territory of the unknown." Pariser coined *filter bubbles* to describe unique universes of information created by algorithms that learn and predict individuals' preferences, thereby reinforcing them. The extent to which filter bubbles impact beliefs and desires is therefore the extent to which filter bubbles impact general personal autonomy. One researcher, Harold Holone (2016) compared personalization filters to an invisible in-car navigation system which "instead of suggesting the direction you should follow, simply takes control of your car and takes you where it thinks you want to go" (Holone 2016). To work, filter bubbles must compromise privacy, as algorithms can make better predictions when they use more personalized information as input. While threats to privacy strengthen the internet's threats to autonomy, even with perfect privacy, the internet would still threaten autonomy due to the vulnerabilities of the human mind.

The value of personal data indicates economic pressure in opposition to privacy as evidenced by Facebook (2019) which generates 98.5% of their revenue from advertising. A British parliamentary committee released internal Facebook emails and documents which reveal discussions on how to best profit from its data between 2012 and 2015 (Collins, 2018). Several companies were leveraging Facebook's friend data to add significant value to their own products, and Facebook was in the works determining how to reclaim that value. Facebook decided to change its developer platform to limit access to their friend API (Collins, 2018). The value of the API can be seen by Badoo, a dating app, that wrote to Facebook about the impact this change would have on their products: "We have been compelled to write to you to explain the hugely

detrimental effect that removing friend permissions will cause to our hugely popular (and profitable) applications Badoo and Hot or Not" (Collins, 2018). Facebook decided to give full access to this API to some developers, and removed access from others including Vine (Collins, 2018). Internally, Facebook decided to limit access to their data unless companies were willing to spend on Facebook's advertising product NEKO: "Communicate in one-go to all apps that don't spend that those permission will be revoked. Communicate to the rest that they need to spend on NEKO $250k a year to maintain access to the data" (Collins, 2018). In 2012, Mark Zuckerberg discussed another strategy called data reciprocity which meant that Facebook would share their data only if other companies were willing to share data back to Facebook, thus increasing the value of the Facebook network: "Sometimes the best way to enable people to share something is to have a developer build a special purpose app or network for that type of content and to make that app social by having Facebook plug into it. However, that may be good for the world but it's not good for us unless people also share back to Facebook and that content increases the value of our network" (Collins, 2018). The value of data can be further explained by the risks Facebook was willing to take to obtain call logs and user text messages: "the growth team is planning on shipping a permissions update on Android at the end of this month. They are going to include the 'read call log' permission.... They will then provide an in-app opt in NUX [New User Experience] for a feature that lets you continuously upload your SMS and call log history to Facebook.… This is a pretty highrisk thing to do from a PR perspective but it appears that the growth team will charge ahead and do it" (Collins, 2018). Facebook took big risks for the sake of data, and even needed to rethink their relationships with companies in order to reclaim the value those companies were gaining from Facebook's data. Those actions were motivated by the growth team which was focused on the value of Facebook's personalized data.

Markets which sell individuals' data further demonstrate the value of personal data. These markets were made visible through Vermont's Act 171 of 2018 which requires all data brokers to register with Vermont's Secretary of State (Vermont Office of the Attorney General, 2018). Data brokers were defined as "a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship." (Vermont Office of the Attorney General, 2018). As of March 2020, the Vermont Secretary of State had 148 businesses registered as active data brokers (Vermont Secretary of State, 2020). Cortera, one of the data brokers in the database, said on their "What We Do" page that the company is in business to "Increase profitability with more informed credit decisions upfront and identify the potential for default in time to act." Lucid, a marketplace which aggregates personal information from over 250 suppliers, says on their website: "Lucid monetization solutions maximize your revenue by matching your community with high-paying researchers that want to survey your user base" (Lucid, n.d.). Lotame runs a private data exchange which sells second party data, the first party data of another organization. Their website states "Selling your first-party data in a second-party data marketplace is an excellent additional source of revenue" (Lotame, 2019). These companies and marketplaces demonstrate the value of personal information for industries including credit lending, advertising, marketing, and risk mitigation. As these industries compete for personal data, advertising attention campaigns and filter bubbles threaten autonomy as they leverage this data.

Autonomy and privacy advocates view big tech as an industry that seeks to control people's time and data for internal motives. RescueTime is a company that sells software products with the goals of giving people control back over their time. Their website states: "Join

over 2 million people who are taking back control of their time with RescueTime" (RescueTime, n.d.). According to RescueTime, the most frequently blocked websites from their tools are Facebook and YouTube (MacKay, 2019). Ghostery, a company that provides tools to block online trackers, says on their blog: "Almost every interaction you have with the internet leaves a trace, and these traces can be valuable. Website and platform owners, advertisers, search engines, and data aggregators try to get their hands on as much data as possible to optimize their business and increase profits" (Kalkhof, 2020). On March 16th, 2020, Dr. Johnny Ryan, Chief Policy & Industry Relations Officer of *Brave Software* issued a legal complaint stating that Google is violating the General Data Protection Regulation (GDPR) which is legislation in the EU and the European Economic Area (Ryan v. Google, 2020). The lawyers summarized: "In breach of their obligations under Articles 5(1)(b), 12(1), 13(1)(c), 14(1)(c) and 15(1)(c) [of the GDPR], Google have failed to identify the purposes for which they collect and process Dr. Ryan's data in a sufficiently specified, explicit and transparent manner", and they call for the Data Protection Commission to "prohibit further unlawful activity and prevent what is an 'internal data-free-for-all' that results from Google's processing activities" (Ryan v. Google, 2020).

The internet's threat to autonomy through disinformation campaigns

Politically motivated disinformation campaigns that achieve wide circulation or publication on legitimate news sources threaten autonomy as they influence the authenticity of beliefs. Facebook (2020) has been removing and reporting coordinated inauthentic behavior from its site for several years (fig. 1). In February 2020, Facebook removed five networks of accounts that engaged in foreign or government interference associated with India, Egypt, Russia, Iran, and

Vietnam. These networks spent $1.2 million in advertising, and spanned 467 Facebook accounts, 1,245 Instagram accounts, 248 Facebook Pages, and 49 Facebook Groups (Facebook, 2020).

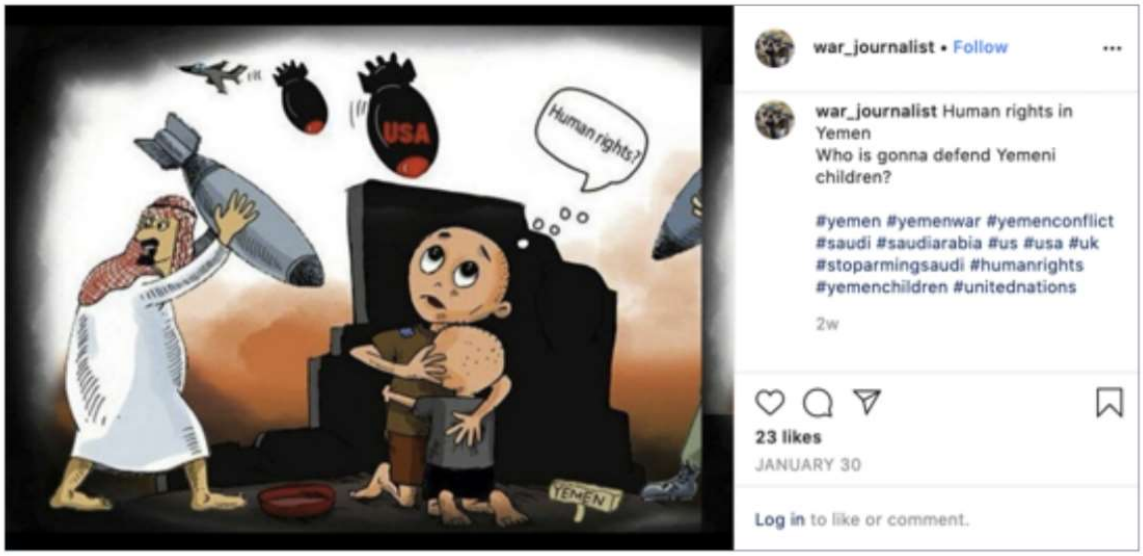

Figure 1. A post removed by Facebook (Facebook, 2020).

Facebook (2019) also removed several posts connected to a Russian campaign on May 6, 2019 (fig. 2).

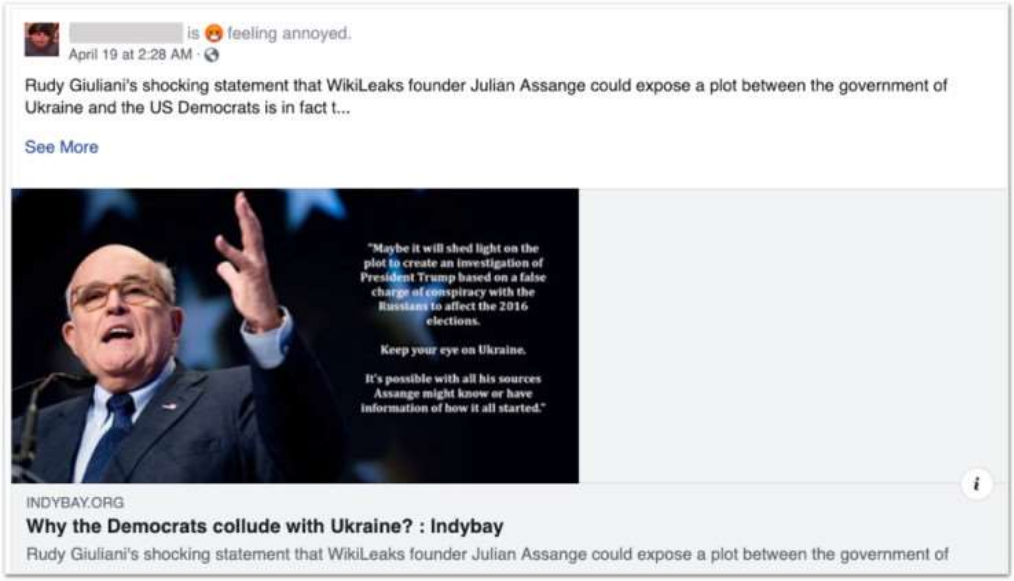

Figure 2. A post Facebook removed in May 2019 (Facebook, 2019).

In December 2019, Reddit (2019) announced a campaign on its site that was thought to be connected to the Russian campaigns reported by Facebook. Reddit identified several accounts that coordinated to promote politically motivated posts. The majority of the manipulated posts did not receive much attention except for a single post that included leaked documents from the UK. The Atlantic Council's Digital Forensic Research Lab (DFRLab) dubbed the Russian-based operations "Secondary Infektion" due to the striking resemblance to the soviet era "Operation Infektion" that "planted the fake story in distant media before amplifying it through Soviet channels: it ultimately spread through genuine news media around the world and was often reported as fact" (Atlantic Council, 2019). Operation Infektion caused 15% of Americans in 1995 to believe that the AIDS virus was created by the US military (Boghardt, 2009). The perpetrators of modern disinformation campaigns take great measures to conceal their identities and often create new accounts to post a single article, and then abandon the account (Atlantic Council, 2019). The associated accounts therefore do not build up large amounts of followers or credibility that might lend the articles to be shared to larger audiences. Articles promoted by political disinformation campaigns pose the greatest threat to autonomy when they are circulated through genuine news media due to a greater ability to influence peoples' desires and beliefs.

Unconstrained algorithms that optimize for engagement, and thereby profit, eventually promote organic, provocative content. Mark Zuckerberg (2018) stated: "One of the biggest issues social networks face is that, when left unchecked, people will engage disproportionately with more sensationalist and provocative content." Ribeiro et al. (2020) found that: "A large percentage of users who consume Alt-right content now consumed Alt-lite and I.D.W. [Intellectual Dark Web] content in the past", which is evidence that the YouTube algorithm systematically progresses users towards more polarizing content. Roger McNamee (2019), an

early Facebook investor and former mentor to Mark Zuckerberg, said: “One of the best ways to manipulate attention is to appeal to outrage and fear, emotions that increase engagement.”

Companies generally rely on two strategies to combat disinformation: AI and human moderation teams. Reddit said in an official post: “We do have systems in place for catching coordinated behavior on the platform” and “We really encourage users, moderators, and 3rd parties to report things to us as soon as they see them.” Facebook takes a similar stance: “We have significantly ramped up our efforts to proactively enforce our policies using a combination of artificial intelligence doing the most repetitive work, and a much larger team of people focused on the more nuanced cases”, with the team consisting of 30,000 people (Zuckerberg, 2018). Twitter (n d.) uses a similar strategy: “Using machine-learning tools, we can spot and take action on entire networks of malicious automated accounts.” In February 2020, Twitter created a new policy that: “You may not deceptively share synthetic or manipulated media that are likely to cause harm” (Twitter, 2020). Content that meets this criterion is very likely to be removed, but content that is deceptively altered or fabricated is likely to be applied a label which warns users of disinformation (Twitter, 2020). Twitter now warns users before liking or retweeting labeled content, and it reduces the visibility of the tweet and/or prevents it from being recommended (Twitter, 2020). Disinformation campaigns modify the content that people see, thereby affecting the beliefs that people form. Algorithmic bias influences autonomy through this mechanism.

The government pressures tech companies to protect privacy and security for fear of regulation. In 2016, Mark Zuckerberg told Techonomy Media (2017): “I think the idea that fake news on Facebook, of which you know is a very small amount of the content, influenced the [2016] election in any way, I think is a pretty crazy idea.” It wasn’t until September 2017 that Facebook’s Chief Security Officer Alex Stamos (2017) acknowledged the Russian interference

with the election that occurred on its platform. Stamos told the Washington Post: “We decided that the responsible thing to do would be to make clear that our findings were consistent with those released by the U.S. intelligence community, which clearly connected the activity in their report to Russian state-sponsored actors” (Timberg, 2017). Twitter, Facebook, and Google testified on Capitol Hill in October 2017 regarding the Russian influence on the 2016 elections. Senators Mark Warner (D-Va.), Amy Klobuchar (D-Minn.), and John McCain (R-Ariz.) pressed the companies on a bill named “The Honest Ads Act” (Hamza, 2017) that would require “digital platforms with at least 50,000,000 monthly visitors to maintain a public file of all electioneering communications purchased by a person or group who spends more than $500.00 total on ads published on their platform” (Warner, n.d.). Mark Zuckerberg appeared on Capitol Hill in 2018 to testify regarding the Cambridge Analytica scandal where the data of 87 million Facebook users was sold to the political consulting firm by a researcher (The New York Times, 2018). Facebook failed to inform the users about the incident despite learning about it in 2015 (The New York Times, 2018). Senator Richard Blumenthal (D-Conn.) expressed a desire to regulate Facebook: “The old saying: There ought to be a law. There has to be a law. Unless there’s a law, their business model is going to continue to maximize profit over privacy” (The New York Times, 2018). Senator John Thune (R-SD), had a similar view: “In the past, many of my colleagues on both sides of the aisle have been willing to defer to tech companies’ efforts to regulate themselves. But this may be changing” (The New York Times, 2018).

Large tech companies such as Facebook must carefully regulate their websites due to opposing profit and security motives. Mark Zuckerberg (2018) explained: “One of the biggest issues social networks face is that, when left unchecked, people will engage disproportionately with more sensationalist and provocative content.” Engagement translates to profits, but when it

is connected to disinformation, it can become a security threat that motivates governments to regulate the industry. Sandy Parakilas, a Facebook employee who worked on privacy said: “The people whose job is to protect the user always are fighting an uphill battle against the people whose job is to make money for the company” (Perlroth, 2018). Mark Zuckerberg (2018) outlined his plan for content governance which included removing harmful content, discouraging borderline content, and working with regulators. In the comment section, an unorganized group of Facebook censorship opposers emerges. Comments included (Zuckerberg, 2018):

> “Sounds very communistic. Just saying.” - Sarah Owens Betar
> “Lay off the censorship” - Larry Blankenship
> “Fb censorship sucks like all censorship.” - Stephane St-Pierre
> “If kicking conservatives and Christians off of facebook then yeah, you’ve done a good job. 🙄” - Grace Dawn Fully
> “Stop censoring conservatives! It’s called free speech!” - Marina Bath
> “Just let freedom of expression flow!” - Ben L Jennings
> “Stop the BS. You are against free speech. So many posts without share buttons. Despicable.” - Don Shows
> “not if you use it for a propaganda machine” - William Anderson
> “please uphold everyone's 1st amendment right and stop your employees from censoring conservative thoughts on facebook.” - Vivian Fung
> “FB blocks what wants to when it wants to and allows content that is wrong sadly it is going to happen again and again.” - Dee Murphy
> “Against 1st amendment rights! Hope you lose big time” - Joy Kent
> “Mark, please stop censoring Conservative sites that contradict your political views.” - Barbara Hamann
> “How about giving the people the freedom of speech!!!!!” - Jacqui ‘Ayles’ Rogan

Conclusion

In a relatively free market, tech companies with financial motives are pressured to collect personal data and to govern their own platforms. This tendency may be called the Paradoxical

Capitalist Effect, whereby capitalistic markets in the internet age produce companies that threaten privacy and autonomy in ways that appear statist. These companies must be careful to build trust with their users. Companies can do so through transparency, by using state-of-the-art security measures, by making their AI open source, by detailing how users' data is used or sold, and by disclosing disinformation campaigns and foreign interference. The GDPR is a step toward building trust. It is up to these companies to build trust through transparency; if they fail, governments may force their hand.

References

Andreassen, C. S., Billieux, J., Griffiths, M. D., Kuss, D. J., Demetrovics, Z., Mazzoni, E., & Pallesen, S. (2016). The relationship between addictive use of social media and video games and symptoms of psychiatric disorders: A large-scale cross-sectional study. *Psychology of Addictive Behaviors*, *30*(2), 252–262. doi: 10.1037/adb0000160.

Atlantic Council. (2019, Aug.). Operation "Secondary Infektion": A Suspected Russian Intelligence Operation Targeting Europe and the United States. www.atlantic council.org/wp-content/uploads/2019/08/Operation-Secondary-Infektion_English.pdf.

Becker, G. S., & Murphy, K. M. (1988). A Theory of Rational Addiction. *Journal of Political Economy*, *96*(4), 675–700.

Boghardt, T. (2019). Soviet Bloc Intelligence and Its AIDS Disinformation Campaign. *Studies in Intelligence*, *53*(4), 19. www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol53no4/pdf/U-Boghardt-AIDS-Made in the USA-17Dec.pdf.

Christman, J. (n.d.). Stanford Encyclopedia of Philosophy. In *Stanford Encyclopedia of Philosophy*. plato.stanford.edu/archives/spr2018/entries/autonomy-moral/.

Collins, D. (2018). Note by Chair and Selected Documents Ordered from Six4Three. www.parliament.uk/documents/commons-committees/culture-media-and-sport/Note-by-Chair-and-selected-documents-ordered-from-Six4Three.pdf.

Cortera. (n.d.). Who We Are. www.cortera.com/who-we-are.

D'Arienzo, M. C., Boursier, V., & Griffiths, M. D. (2019). Addiction to Social Media and Attachment Styles: A Systematic Literature Review. *International Journal of Mental Health and Addiction*, *17*(4), 1094–1118. doi: 10.1007/s11469-019-00082-5.

Facebook. (2019, May 6). Removing More Coordinated Inauthentic Behavior from Russia. about.fb.com/news/2019/05/more-cib-from-russia.

Facebook. (2019, May 16). Using Surveys to Make News Feed More Personal. about.fb.com/news/2019/05/more-personalized-experiences/.

Facebook. (2020, Jan. 30). Form 10-K for the fiscal year ended Dec. 31, 2019, p. 56. investor.fb.com/financials/sec-filings-details/default.aspx?FilingId=13872030.

Facebook. (2020, March 2). Feb. 2020 Coordinated Inauthentic Behavior Report. about.fb.com/news/2020/03/february-cib-report/.

Hamza Shaban, C. T. (2017, Oct. 31). Facebook, Google and Twitter testified on Capitol Hill. Here's what they said. *Washington Post.* www.washingtonpost.com/news/the-switch/wp/2017/10/31/facebook-google-and-twitter-are-set-to-testify-on-capitol-hill-heres-what-to-expect.

Harris, T. (2019, Dec. 5). Our Brains Are No Match for Our Technology. *New York Times.* www.nytimes.com/2019/12/05/opinion/digital-technology-brain.html.

Harris, T. (n.d.). Center for Humane Technology. humanetech.com/about-us.

Hoffman, S., Taylor, E., & Bradshaw, S. (2019). *The Market of Disinformation.* oxtec.oii.ox.ac.uk/wp-content/uploads/sites/115/2019/10/OxTEC-The-Market-of-Disinformation.pdf.

Holone, H. (2016). The filter bubble and its effect on online personal health information. *Croatian Medical Journal, 57*(3), 298–301. doi.org/10.3325/cmj.2016.57.298.

Kalkhof, J. (2020, March 3). Defining your digital footprint. www.ghostery.com/blog/ghostery-news/defining-your-digital-footprint.

Kwon, H. E., So, H., Han, S. P., & Oh, W. (2016). Excessive Dependence on Mobile Social Apps: A Rational Addiction Perspective. *Information Systems Research*, *27*(4), 919–939. doi: 10.1287/isre.2016.0658.

Lexico. (n.d.). Autonomy: Definition of Autonomy by Lexico. www.lexico.com/en/definition/autonomy.

Lotame. (2019, Sep. 16). What Is Second Party Data and How Can You Use it? www.lotame.com/what-is-second-party-data.

Lucid. (n.d.). Monetization. luc.id/monetization.

MacKay, J. (2019, Jan. 24). The State of Work Life Balance in 2019 (According to Data). RescueTime. blog.rescuetime.com/work-life-balance-study-2019.

McNamee, R. (2019, Jan. 17). I Mentored Mark Zuckerberg. But I Can't Stay Silent. *Time.* time.com/5505441/mark-zuckerberg-mentor-facebook-downfall.

Newzoo. (2019, Sep. 17). Number of smartphone users worldwide from 2016 to 2021 (in billions). In Statista.

Pariser, E. (2011). The Filter Bubble: What the Internet is Hiding From You. New York: Penguin Press.

Perlroth, N., Frenkel, S., & Shane, S. (2018, March 19). Facebook Exit Hints at Dissent on Handling of Russian Trolls. *New York Times.* www.nytimes.com/2018/03/19/technology/facebook-alex-stamos.html.

Reddit. (2019, Dec. 6). Suspected Campaign from Russia on Reddit. www.reddit.com/r/reddit security/comments/e74nml/suspected_campaign_from_russia_on_reddit.

RescueTime. (n.d.) Online Homepage. www.rescuetime.com.

Ribeiro, M. H., Ottoni, R., West, R., Almeida, V. A. F., & Meira, W. (2020). Auditing radicalization pathways on YouTube. *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency,* 131-41. doi: 10.1145/3351095.3372879.

Ryan v. Google Ireland Limited LLC & Google LLC. (2020). Grounds of Complaint to the Data Protection Commision. brave.com/wp-content/uploads/2020/03/Purpose-Limitation-Google.pdf.

Stamos, A. (2017, Sep. 6). An Update on Information Operations on Facebook. about.fb.com/ news/2017/09/information-operations-update.

Timberg, C., & Dwoskin, E. (2017, Oct. 30). Russian content on Facebook, Google and Twitter reached far more users than companies first disclosed, congressional testimony says. *Washington Post.* www.washingtonpost.com/business/technology/2017/10/30/ 4509587e-bd84-11e7-97d9-bdab5a0ab381_story.html.

Twitter (n.d.). Elections integrity. We're focused on serving the public conversation.about. twitter.com/en_us/advocacy/elections-integrity.html#service-integrity.

Twitter (2020). Synthetic and manipulated media policy. help.twitter.com/en/rules-and-policies/manipulated-media.

Vermont Office of the Attorney General (2018, Dec. 11). Guidance on Vermont's Act 171 of 2018 Data Broker Regulation. ago.vermont.gov/wp-content/uploads/2018/12/ 2018-12-11-VT-Data-Broker-Regulation-Guidance.pdf.

Vermont Secretary of State (2020). Online Services (Business Search with Business Type: Data Broker and Business Status: Active). www.vtsosonline.com/online/.

Warner, M. (n.d.). The Honest Ads Act. www.warner.senate.gov/public/index.cfm/the-honest-ads-act.

YouTube. (2019, Jan. 25). Continuing our work to improve recommendations on YouTube. youtube.googleblog.com/2019/01/continuing-our-work-to-improve.html.

Zuckerberg, M. (2018, Nov. 15). A Blueprint for Content Governance and Enforcement. www.facebook.com/notes/mark-zuckerberg/a-blueprint-for-content-governance-and-enforcement/10156443129621634.