Tracy Pinkham
Prof. Lodge
HTY 365
25 February 2020

Internet Regulation Recommendations in the Age of Disinformation

In its early stages, the internet it was viewed as a "common" in which the freedom of information had been greatly expanded. As it has become an ever-present part of our daily lives, corporations and governments have exploited data which internet users have generated for government controls and security capitalism. While countries such as China have used those controls to align internet use within their country to their national interests and social norms, regulations in the US have not done so. They have allowed tech firms such as Facebook and Google to extract information from our citizens unfettered. Those data sets have been exploited by foreign governments and national campaigns in micro-targeting schemes to spread disinformation. In order to fight these micro-targeted disinformation schemes the US needs to implement regulations that allow internet use to align with our national values as countries such as China have done. The US should implement internet privacy laws, akin to the EU's General Data Protection Regulation (GDPR), that could prevent the abuse of personal data as in such cases as Cambridge Analytica. It should also work to promote algorithmic accountability within platforms such as YouTube and Facebook. Content should not be kept from the internet, but the ability for it to be amplified should be restricted by code architecture.

There is no doubt that fake news, or disinformation, has been spread across the internet for years. After the 2016 election cycle it became a topic of national interest, for good reason. In 2017 Congress held hearings into meddling in the election through social media. It was revealed during this process that "nearly 150 million American Facebook and Instagram users were

exposed to Russian-generated content, which consisted of paid ads, free posts, and even event notices." (Jamieson 69) Russian meddling reached across many other platforms with over one thousand videos uploaded to YouTube. Twitter reported 3,814 accounts linked to the Russian Internet Research Agency (IRA), as well as more than 50,000 bots (Jamieson 70). There were also a number of domestic imposter news sites such as Infowars and Breitbart. These varied sources of imposter news helped concerted efforts of Russian hackers to steer the national conversation in mainstream coverage, and even frame at least one debate question. It cannot be known exactly how many votes these disinformation campaigns changed, but it is clear that they are a threat to democratic health in the U.S. and across the globe.

Disinformation on the internet should not be taken lightly. It should also not induce a moral panic, (Jarvis) that causes citizens to hand over their rights in democratic societies. Joshua Tucker pointed out that while disinformation is an issue on the internet, it may not be as widespread as some perceive (Tucker). The research he presented from Social Media and Political Participation found that "over 90% of our respondents shared no stories from fake news domains." (Guess 1) As such it is crucial that the US does not go overboard in enacting internet content regulation.

Some of the regulations enacted in other countries to fight cybercrime and disinformation are also a threat to democratic health. These laws are being used to censor journalists, activists and citizens. This is taken to an extreme in China, where the laundry list of barred speech is extensive:

> No organization or individual may produce, duplicate, announce or disseminate information having the following contents: being against the cardinal principles set forth in the Constitution; endangering state security, divulging state secrets, subverting state

> power and jeopardizing national unification; damaging state honor and interests; instigating ethnic hatred or discrimination and jeopardizing ethnic unity; jeopardizing state religious policy, propagating heretical or superstitious ideas; spreading rumors, disrupting social order and stability; disseminating obscenity, pornography, gambling, violence, brutality and terror or abetting crime; and other contents forbidden by laws and administrative regulations. (Deibert 180)

These policies, along with a wide array of other internet regulations such as licensing requirements, state ownership and identification of users, all work towards the government's goal to create a "bordered internet subject to national policy (Deibert 181). China, Turkey and Egypt, are the world leaders in jailing journalists. According to Courtney Radsch, results of a Committee to Protect Journalists' survey show that "nearly three-quarters of the 262 journalists in prison around the world are being held on anti-state charges" (Radsch). Further, such laws also work to effect self-censorship of the millions of Chinese internet users: average citizens, activists and journalists alike. (Deibert 181) While a bordered internet may align with the authoritarian norms and values of the Chinese government, it certainly does not align with those of Western Democracies such as the US.

China is by no means alone in its attempts to regulate the internet, and it is not only authoritarian regimes that have done so. The Philippines, a democracy, "where press freedom is highly valued and the media are considered an active influence in keeping government in check," (Deibert 118) has also passed laws to censure freedom of speech on the internet. In 2012 The Cybercrime Act was passed. It was greeted with large protests from netizens within the country as well as many international human rights advocacy groups. At the time of these protests Melanie Pinlac of the Center for Media Freedom and Responsibility asserted: "While we

[CMFR] and other critics agree that there is a need to punish those who use the internet to harm children and women. Or steal identities and data for illegal use. We also believe the government has no right to impose limitations on freedom of expression in exchange for security and safety on the web." (Robie) The CMFR, and other groups challenged the law through the court system, and while some aspects were ruled unconstitutional, most of the law was allowed to come into effect in 2014.

One of the most concerning aspects of the law is that of cyber libel. Under the law a person convicted of cyber libel could face up to twelve years in prison. This is onerous in its own right, but especially when compared to libel in traditional media, which only carries a maximum sentence of six years. It was under this law that Maria Ressa was arrested in February of 2019 (though some of her many arrests have been made under the auspices of different laws, such as tax evasion, and foreign ownership of her media company Rappler). The February charge for cyber libel was for an article published before the Cyberlaw Act of 2012 was even passed. Ressa was not the author of the article in question, but it was published by her blog Rappler. The trumped-up charge relied on the fact that the story had been updated in 2014. (The Economist)

The charges against Maria Ressa affect not only her and the media company she helms. They also add to the process of 'libel chill' across the Philippines, wherein journalists and publishers alike practice self-censorship in fear of reprisal from the government. The manipulation of the Cybercrime Act to suit the needs of the current administration to silence its critics should come as a stern warning to other democracies looking to fight the flow of disinformation on the internet. It is clear that even if the intent of the law is to limit the dissemination of disinformation, the effect of such laws can be used to stifle legitimate criticism of the government and erode the institution of journalism. In the United States journalism

institutions are already on the decline due in part to the decrease of traditional revenue sources. If they were forced to spend large amounts of money on legal fees to fight such cyber libel laws, that decline could be further accelerated.

China, the Philippines and many other countries have enacted laws that strip citizens, as well as institutions, of their rights. The European Union has trended in the other direction. The EU attempted to restore rights to privacy and the right to be forgotten with the landmark General Data Protection Regulation (GDPR). The regulation allows citizens to obtain their personal data for free. It also allows them to withdraw their consent for data collection and forces the company to delete their data upon request. Companies need to have a business reason for collecting data, rather than trying to monetize it later. They must revise their complicated terms and conditions agreements with easy to understand consent forms, and it is required that withdrawing consent is also a simple process. Companies are also required to notify users of a data breach within 72 hours of its occurrence. The regulation also enables regulators to levy significant fines, up to four percent of a company's global revenues. (Solon) According to David Carroll, an associate professor at Parsons School of Design in New York, "It makes companies become much more thoughtful and rigorous about the data they collect and what they use it for." (Solon) While the law is not perfect, it is a good first step in securing a semblance of privacy rights of citizens in the age of surveillance capitalism.

Nicco Mele expressed at the 2020 Camden Conference that the First Amendment is obsolete in its ability to protect citizens against the disinformation and vitriol that is spread on the internet (Mele). In a passage of the book, *Surveillance Capitalism,* Shoshana Zuboff articulates a similar sentiment to Mele's in regard to the Fourth Amendment and data collection:

> When US scholars and jurists assess the ways in which digital capabilities challenge existing law, the focus is on the Fourth Amendment doctrine as it circumscribes the relationship *between individuals and the state.* It is of course vital that the Fourth Amendment protections catch up to the twenty-first century by protecting us from search and seizure of our information in ways that reflect contemporary realities of data production. The problem is that even expanded protections from the state do not shield us from the assault on sanctuary wrought by instrumentarian power and animated by surveillance capitalism's economic imperatives. The Fourth Amendment as currently constructed does not help us here. (Zuboff 481)

Zuboff and others do not have a lot of confidence that the US will follow the EU's lead with the GDPR. However, she does look to it as hopeful example of steps towards reigning in the asymmetrical power that tech companies hold in society. While it is not at the federal level, a step in this direction has been taken in the US. A California law entitled the California Consumer Protection Act, (CCPA) took effect in January of 2020. It is the first of its kind in the US. The CCPA is less stringent than the GDPR in many regards, but it does surpass it in at least one arena. The law requires companies to provide a "'Do Not Sell My Personal Information' link in a clear and conspicuous location on their websites. Under GDPR, by comparison, businesses do not necessarily need the individual's consent to collect and use data." (Paul)

Although data privacy concerns may not instinctively be seen as a way to halt the spread of disinformation on the internet, they could potentially be a powerful tool in that regard. A great deal of disinformation is spread through micro-targeting. This was true on multiple fronts in the 2016 US general election. The varied sources of Russian interference employed this technique across many platforms. "It's clear that they were able to able to drive a relatively significant

following for a relatively small amount of money. It's why this activity appears so pernicious," stated Facebook's general counsel, Colin Stretch, in front of the House Intelligence Committee in 2017. (Jamieson 69) While he was referring to Russian interference in the election, it is clear that this holds true for Cambridge Analytica as well.

The scandal around the company Cambridge Analytica came to light when a whistleblower from the company brought the story to *The Guardian.* When all of the details came to light, it revealed a huge breach of privacy on the part of both Cambridge Analytica and Facebook.

> Cambridge Analytica, or companies linked to Cambridge Analytica, had used the personal data of about 200,000 Facebook users to build up detailed psychological profiles of up to 87 million Facebook users. Whilst the initial 200,000 users had voluntarily completed a personality test, they had not necessarily known how their answers would be used, and the 87 million users who were profiled had most certainly not given their informed consent for this. Cambridge Analytica used this massive database to help political campaigners in the United Kingdom, the United States and other countries to target Facebook users with highly specific messages. (Heawood 429)

The Trump campaign employed Cambridge Analytica to help him win the 2016 US election, by targeting persuadable individuals through Facebook ads. These ads may not have made up a significant proportion of political engagement across social media platforms during the 2016 campaign, but they were effective in influencing the election because, "political targeting works by delivering messages to susceptible voters in locations that mater. Efficient means of audience identification reduce the amount of communication needed to influence an election." (Jamieson 132)

The harm of micro-targeting to the health of a democracy can be explained in a number of ways. First is the exploitation of mass amounts of data, which amount to a psychological profile, without consent. Second, micro-targeted ads often conceal that they are even ads. Thus, when people scroll by the information on Facebook, they are less likely to examine it as critically as if they had known its true purpose. Third, if false claims are made in a private ad, they cannot be openly debated in the marketplace of ideas because they have not been presented in the broader marketplace. Fourth, it allows politicians to make incompatible claims or promises to different individuals without those incongruencies being exposed in public. "These incompatible promises clearly cannot both be fulfilled and, as a result, a party might lack a clear mandate if it were elected to government." (Heawood 431) Fifth and finally, it allows for foreign actors to target voters with disinformation, such as the IRA did during the 2016 US election.

Micro-targeting "trades on our expectations of public communications to be smuggled through private messages," (Heawood 432) and disrupts the standards and norms of public communication within a democracy. If the GDPR or the CCPA had been in place during the runup to the 2016 US Election or the Brexit vote in the UK, the massive privacy breaches of Cambridge Analytica would have had the possibility of being exposed. If a journalist could have gained access to their data sets, there is a chance they could have ferreted out the connection. As it stood then, and as it stands now in most of the US, gaining access to that data was/is nearly impossible. The US cannot continue to allow such valuable information to be exploited by opaque tech platforms at the expense of our democracy.

Access to one's data is not the only regulation that should be put into place. Philip N. Howard put forth several other pathways to help end tech platform's opaque ways and aid the health of democracies. In addition to access to personal data, Howard suggests four other

reforms. The first addresses a concern raised by Joshua Tucker at the Camden Conference. If stringent privacy laws are passed and data collection by third parties is ended, it wipes out an opportunity for researchers to access that information and use it for research purposes, all while the tech platforms still have access to the information (Tucker). Howard suggests that data portability be coupled with the ability of citizens to donate their data to journalists, medical researchers or other civic groups. This would create an "opportunity for civic expression by allowing citizens to share it with whichever organizations and causes they want to support--not just the ones that can afford to buy it, as is the case today." (Howard) He also suggests that tech platforms and companies should be required to "tithe for the public good," by allocating ten percent of ad space on their platforms for public service announcements and transmitting ten percent of their data to civic institutions for research.

Another important reform Howard calls for is the regular audit of platforms' algorithms. Though these companies may assert that this is proprietary information, there is a precedent in the fact that the government already conducts audits of algorithms of financial trading and video gambling machines. Social media sites and platforms such as Google have become central to everyday public life and, as such, "Users should have access to clear explanations of the algorithms that determine what news and advertisements they are exposed to, and those explanations should be confirmed by regular public audits. Moreover, all ads, not just political ones, need to be archived for potential use by public investigators." (Howard) Algorithmic accountability could help slow the spread of disinformation on the internet. It could also help halt the amplification of racism, misogyny and other forms of hate speech that have been magnified on platforms for years. A decrease in amplification of disinformation and hate speech could go a long way in mitigating their negative impacts on society without taking the drastic measure of

regulating speech and content on the internet. Placing internet ads in a public database could also ameliorate the many problems associated with micro-targeted ads.

The internet is not a net good or a net bad. It is a neutral tool that can be used by activists and journalists to help spread their message, just as it can be exploited by governments to help censor them. (Tucker) It is therefore important that the US does not fall prey to a moral panic and regulate away our First Amendment right to free speech within its domain. The internet has given society social movements such as #BlackLivesMatter and #MeToo. These movements encapsulate important stories of the American experience that had long been ignored by media gatekeepers. The US needs to maintain the freedom of speech that allowed these and other movements to flourish. It is also important that the US restore rights of privacy of its citizens against tech platforms which have exploited unfettered access to personal information for decades. If the US can accomplish both preserving and restoring these rights on the internet, perhaps we can begin to repair and reimagine the rotting institutions of American Democracy.

References

Backer, Larry Cata. "China's Social Credit System: Data-Driven Governance for a 'New Era'." *Current History* (September 2019): 209-214.

Deibert, Ronald, John Palfrey, Rafal Rohozinski, Jonathan Zittrain. *Access Contested: Security, Identity, and Resistance in Asian Cyberspace (Information Revolution and Global Politics)*. Cambridge: The President and Fellows of Harvard College, 2012.

Guess, Andrew, Johnathan Nagler, Joshua Tucker. "Less than you think: Prevalence and predictors of fake news dissemination on Facebook." 2019. https://smappnyu.org/wp-content/uploads/2019/01/Fake_News.pdf.

Heawood, Jonathan. "Pseudo-public political speech: Democratic implications of the Cambridge Analytica scandal." *Information Polity:The International Journal of Government & Democracy in the Information Age* (2018): 29-34. https://web-a-ebscohost-com.wv-o-ursus-proxy05.ursus.maine.edu/ehost/pdfviewer/pdfviewer?vid=1&sid=701b7575-a916-4030-a2d2-d30bc2ce46e5%40sessionmgr4007.

Howard, Philip N. "Our Data, Ourselves: How to stop tech firms from monopolizing our personal information." *Foreign Policy 229* (July 2018): 27+. Gale Academic OneFile, https://link-gale-com.wv-o-ursus-proxy05.ursus.maine.edu/apps/doc/A549156208/AONE?u=maine_augusta&sid=AONE&xid=b0931ae3. Accessed 2 Mar. 2020.

Jamieson, Kathleen Hall. *Cyberwar: How Rusian Hakers and Trolls Helped Elect a President; What we don't, can't and do know*. New York: Oxford University Press, 2018.

Jarvis, Jeff, “Hands Off Our Net!” (lecture, Camden Conference, Camden Opera House, Camden, ME, February 22, 2020).

Mele, Nicco “Rule 1: It Will Get Crazier” (lecture, Camden Conference, Camden Opera House, Camden, ME, February 21, 2020).

Paul, Kari. "California's groundbreaking privacy law takes effect in January. What does it do?" *The Gaurdian* 30 December 2019. https://www.theguardian.com/us-news/2019/dec/30/california-consumer-privacy-act-what-does-it-do.

Radsch, Courtney C. ""When Fighting Fake News Aids Censorship."." *Project Syndicate* 1 March 2018. ProQuest, https://library.umaine.edu/auth/EZproxy/test/authej.asp?url=https://search.proquest.com/docview/2009298797?accountid=28933.

Robie, David, and Del M. Abcede. "Cybercrime, criminal libel and the media: from 'e-martial law' to the Magna Carta in the Philippines." *Pacific Journalism Review, vol. 21, no. 1 SE* (2015): 211+. Gale Academic OneFile, https://link-gale-com.wv-o-ursus-proxy05.ursus.maine.edu/apps/doc/A425460025/AONE?u=maine_augusta&sid=AONE&xid=8bdb1b99. Accessed 2 Mar. 2020.

Solon, Olivia. "How Europe's 'breakthrough' privacy law takes on Facebook and Google." *The Guardian* 19 April 2018. https://www.theguardian.com/technology/2018/apr/19/gdpr-facebook-google-amazon-data-privacy-regulation.

The Economist. "Stopping the press; Media freedom in the Philippines." *The Economist, vol. 430, no. 9130* 16 February 2019: 34+. Gale General OneFile, https://link-gale-com.wv-o-ursus-proxy05.ursus.maine.edu/apps/doc/A574101591/ITOF?u=maine_augusta&sid=ITOF&xid=b70621df. Accessed 2 Mar. 2020.

Tucker, Joshua, "Social Media, Democracy, Fake News and Fact-Checking" (lecture, Camden Conference, Camden Opera House, Camden, ME, February 22, 2020).

Zuboff, Shoshan. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs Hachette Book Group, 2019.