THE BROOKINGS INSTITUTION

BROOKINGS CAFETERIA PODCAST

A NEW SOCIAL CONTRACT FOR BIG TECH

Washington, D.C.

Friday, July 3, 2020

PARTICIPANTS:

Hosts:

FRED DEWS
Managing Editor, Podcasts and Digital Projects
The Brookings Institution

ROBERT WICKS
Publicity Manager
Brookings Institution Press

Guest:

DIPAYAN GHOSH
Pozen Fellow, Shorenstein Center on Media Politics and Public Policy at the Harvard Kennedy School

* * * * *

P R O C E E D I N G S

DEWS: Welcome to the Brookings Cafeteria, the podcast about ideas and the experts who have them. I'm Fred Dews. In this world of endless technology that permeates all our lives how can individuals, institutions and governments harness its positive contributions for protecting each of us no matter who or where we are?

That's a central question addressed by the guest expert on this episode in his new book from Brookings Institution Press titled, Terms of Disservice: How Silicon Valley is Destructive by Design.

Author Dipayan Ghosh is Pozen Fellow at the Shorenstein Center on Media, Politics and Public Policy at the Harvard Kennedy School. A Computer Scientist by training, he has served as a Technology and Economic Policy Advisor in the Obama White House, and as a Privacy and Public Policy Advisor at Facebook. He's interviewed here by my Brookings Press colleague, Robert Wicks.

You can follow the Brookings Podcast Network on Twitter @PolicyPodcasts to get information about and links to all of our shows. Including, Dollar & Sense, the Brookings Trade Podcast, The Current and our Events Podcasts.

And now, here is Robert Wicks with Dipayan Ghosh.

WICKS: Well, Dipayan, thanks for making the time to talk today. I know there's been a lot going on, obviously, in the country with regards to big tech and what the book is about. So we're excited to have it coming out on June 16th.

GHOSH: Thanks, Robert, for having me. And no doubt there is the COVID-19 pandemic and the protests which are front and center of everyone's attention, rightly so, but at the center of it all, is how we all interact with each other, and a big part of that today is technology.

WICKS: Yeah. So, obviously, the big news concerning tech regulation recently is that President Trump issued an executive order towards the end of May, attempting to regulate big tech for what he considered violations of free speech against conservative viewpoints. So there's obviously a lot to unpack there, but could you walk us through what Trump's order proposes to do, and how likely it is to get any traction?

GHOSH: Yeah. Well, backing up a sec, social media companies today have such huge influence over how we all talk with each other, communicate with each other, consume media, view the news, and these companies often recommend certain posts, or news articles, and oftentimes those are President Trump's tweets themselves. And of course he has a massive following on both Twitter and Facebook.

And a couple of weeks ago, President Trump tweeted about mailing ballots, and suggested that even though we might need them now because of coronavirus, having a system of mailing ballots might actually rig the election. In other words, skew the results against his political interests, his interest to get reelected. And of course, there is no truth to this. And Twitter was quick to react. It always has had this authority to flag a post, but it did so for the first time against this tweet from President Trump, and marked it as a political lie, and linked to information that you could go see about mailing ballots, which many people are now going to use this year to vote.

Trump's response was swift, it was an Executive Order that contented that, well, I want to take the authority from social media companies like Twitter to moderate my content, away. And I want to transfer it over to, potentially, the Federal Communications Commission.

Now, there a dozen problems with this executive order, which we don't need, necessarily, to go into here, but it's just legally such a mess. And for a President to try to issue an executive

order suggesting that tech companies cannot moderate its content is just ridiculous on so many counts because, first of all, a President shouldn't be tweeting out political lies and divisive content. And second, from a legal perspective, the executive order just doesn't hold any water.

So, Twitter didn't necessarily react to the executive order, but the next day I believe, Trump tweeted out something in regard to the George Floyd protests, and said that "When the looting starts, the shooting starts," suggesting that, for protesters who take a particular approach, or others who take a particular approach in response to the killing of George Floyd Trump might send military police out.

And this was seen as a violent act by Twitter. And so Twitter flagged that tweet as well, suggesting that this is potentially violent. It was just incredible. Incredible to see this back and forth between a President and a leading tech company, and I'm very glad that Twitter took this very protective to democracy stance.

WICKS: Something that stood out to me is the idea that's almost morbidly funny, but your book calls for regulation, it's just a much more focused, constructive form of regulation than what could be proposed in an executive order. So could you maybe talk about what are the regulatory goals that we would want from smart laws that are meant to protect us?

GHOSH: Yeah. And it's a great question because I see that there are probably two major problems with tech companies right now. So Facebook has been at the center of controversy because, while Twitter has flagged Trump's posts, Facebook has done nothing about them, and Mark Zuckerberg himself has said that: I'm not going to be the arbiter of truth. And this is why we've seen employee walkouts, and employees resigning from their jobs at Facebook, and this is a huge problem.

I would call these problems, broadly speaking, content policy problems. That's to say,

content that appears on social media platforms, and other internet platforms, publicly-available information needing to be moderated in some way. That's to say we need to protect our media environment and people from misinformation and disinformation, we need to protect people, especially marginalized communities, from hate speech, from a violent conduct, of course, from child exploitative material.

So, there's all these forms of offending content out there, we need tech companies, especially companies that have the billions of users that Facebook and Google have, to protect its user population from that offending content. And that's this practice of content policy moderation, flag posts, relegate posts, take them down if necessary, especially of course they're child exploitative, for example.

I would call that a major problem, but it's one of two broad problems that I see. The other broad problem is systemic economic exploitation by the dominant tech platforms, Facebook, Amazon, Google, et cetera, where, they've designed a business model that prioritizes the uninhibited collection of data, the use of that data to develop algorithms, pick ways (phonetic) at the expense of people.

And the holding of rivals, potential rivals, at bay through anti-competitive means, along with other practices. And I think it's a set of practices that's not policed, that's not scrutinized, partly because in the United States we don't have the regulatory authorities positioned well to scrutinize those practices. And so I would call this second broad problem, issues of economic concern.

So, we have content policy concerns, and we have economic concerns. And the response would be through potential content policy reform, potentially by doing things like reforming Section 230 for the first set of problems, and for the second, the economic reforms, potentially

things like privacy, like competition, like transparency over these tech platforms.

WICKS: The book tries to lay out these two problems especially looks at the second set of problems, which I see as the set of problems that really is at the heart of all of the concern that we have over the internet today.

GHOSH: Well, yeah. It does seem as though the economic model at its core thrives on controversy, on posts that get circulated, and the posts that get circulated tend to be more extreme. So, it seems like the content problem, is derived directly from the economic problem, because it behooves them, it makes them money to sort of foment this content controversy instead of directly addressing the economic.

WICKS: That's exactly what I try to contend which is that, if you really want to do something about content policy, if you really want to diminish this problem of President Trump tweeting out violent material, then don't look at the negative externalities, don't look at the surface level harms, problems that the machine produces. Instead, look at the machine, look at the nature of the machine itself, and treat the business practices that, at root level, produce those content policy problems.

GHOSH: In a sense, we have a machine, let's call it Facebook, and which is a machine, it has servers, it has the physical infrastructure, and it has an algorithmic and infrastructure, it's a very complicated machine that's designed to optimize profits for shareholders.

It has a set of business practices, core pillars that are, again, focused around collection of data, analysis of that data, development of algorithms to create content, keep people engaged and understand who the individual users are. And a set of corporate policies and development practices to maintain the company's position in the market.

So, it's a machine of sorts, and this machine operates in unpoliced ways through the

collection of data, through the development of algorithms, through anti-competitive measures to restrict the activities and rivals, the threat of rivals. And through platform growth, uninhibited platform growth to try to essentially take over social media around the world, take over the media environment around the world. That is a machine because of the way part of this is around understanding who you are as a consumer, and keeping you scrolling on your smartphone, that is part and parcel of this machine.

How does that happen? The data collection allows Facebook to understand who you are, and your preferences and beliefs, and interests, and dislikes, and likes, routine behaviors?

And then, with that information Facebook can determine what should be the optimal ranking of your newsfeed, for example. And that is an algorithm, that's a machine designed to keep you engaged. And what the company has found, through machine learning, not even through independent human analysis, but machine analysis, is that misinformation, other kinds of lies, violence, hatred, these are among the most engaging forms of content out there.

And the tech industry is profiting off of that, because there are echo chambers that feed off of this kind of material, and not even echo chambers, this material travels faster and farther than the truth, than more mundane information. Such as: the Knicks beat the Lakers last night, or that President Obama said such and such.

What researchers have found is that this kind of violent, or misinforming material travels faster and farther than the truth and less offending content, and the tech companies are profiting out of that.

WICKS: It also seems like they've created an addiction and they're feeding it. It seems like that feeds into why it's so hard to generate public interest, because it seems like despite the fact that this is an issue that literally touches all of our lives, public interest in fixing the problem

seems tepid, at best.

People know that elections have been meddled with, they know their data has been breached countless times. You know, you can almost this national yawn when we talk about the dangers inherent in this. So how do we mobilize the public on this issue, keeping in mind that the very platforms needed to mobilize people, or controlled by the digital robber barons?

GHOSH: It's such a difficult question. Let's just take the individual case of privacy reform, which wouldn't address the entire business model of tech, but at least would start to address things like Facebook collecting millions of data points on a particular user from across the internet, and through location data, and through third party, web cookies, et cetera, et cetera.

Privacy can start to address how Facebook, and in forms of data Facebook can collect, as well as, potentially, how Facebook can use that kind of data. That's what a privacy law might do. And yet, we all know the privacy harms that can arise from the tech industry. We witnessed the Snowden disclosures, we witnessed the Cambridge Analytica revelations, Europe has acted based on those two events and others, and yet in the United States, let's say, erratically capitalistic, open economy, we are not able to do anything about it, despite our seeing these incidents, and despite all this we have completely failed.

President Obama introduced the Consumer Privacy Bill of Rights Act of 2015, a legislative proposal developed by Obama and his White House, and the Commerce Department, sent over to Congress, and there were no bites in Congress, no one wanted to cosponsor this thing, in the House or the Senate, Republicans or Democrats.

Why is that the case? Well, of course in that particular case, it's complicated, that bill was criticized. But I think more broadly, there is reticence to push on privacy reform in this country because consumers don't really see the threat from data collection immediately.

There's a thing in the book that I call the privacy paradox, whereby we often tend to look at the exchange that's happening here and now, without thinking about the economic and social repercussions that can result days, or months, or years down the line, where we get access to Instagram, immediately after signing up, we enjoy it, and we fail to see that there could be bigger economic harms that can come down the line.

I honestly don't know how you start to create this conversation at a broader level, and start to educate the public that, well, perhaps we need to pass a privacy law once and for all. And I actually don't think that that should necessarily be a goal, because I think it's such a difficult conversation to have at a broad level.

This is a complex industry, these practices around data collection are so complicated themselves. Instead, I think we need our national leaders, we need politicians to stand up, and take a stand for consumers.

WICKS: Yeah. It seems like we're not very good at identifying threats that aren't going to hurt us immediately, like global warming, and fixing the health care system, but every once in a while, something happens, a flashpoint, the pandemic has shown us that the health care system does need to be reformed. It took the death of George Floyd to set off the is wave of calls for justice and police reform.

It's like we need an event to show us how bad things can get before we say okay, we need to fix this problem. In your mind, is there a nightmare scenario? Something that could happen that would make all of us wake up and say: oh, my, god, we actually have to do something about our cybersecurity?

GHOSH: It's hard to imagine anything worse than what has already happened. We saw the Snowden disclosures, we witnessed the fact that the United States Government was

collaborating with a bevy of technology firms, of the leading firms in Silicon Valley, siphoning in information and conducting a massive surveillance program. We saw Russia pushing disinformation, establishing essentially coordinated disinformation campaign against American voters, which was a direct attack to our political process and American democracy.

We saw Cambridge Analytica through which, essentially a Russian researcher gained access to the Facebook data of 87 million people, the vast majority of them Americans, and potentially the fact that that data might have been shared by Cambridge Analytica to third parties. We also know that one of Cambridge Analytica's clients was the Trump campaign at the time.

So, we have seen big issues. I don't know. I don't know what it would take beyond potential rigging of a national election. Maybe the rigging of a national election, as a matter of fact, maybe if we can clearly point someday to the fact that there are disinformation operators out there, they're accessing our data en masse, and they're coordinating campaigns against us, and those campaigns lead to a particular result. Maybe that's the type of thing that would finally set us all off.

WICKS: It's sad though, because it feels like a chicken-egg scenario, where if something like that happened to report it, could be read in some corners as fake news. It seems like, we report on this type of stuff but the reporting can be thought of as fake news, and so it's not taken seriously.

It's like this thing that just kind of keeps going and going, and I know it's not fair to ask you for the solution, because it does seem like it's pretty intractable, but is it really just going to be about this slow, steady process of demanding that our lawmakers care about us, and put the needs of the consumers ahead of straight, monetary value?

GHOSH: I think the good news, to your earlier question, is that perhaps we're starting to see some movement. Because when we look at privacy, even though at the Federal level, it's hard to push something organically because of the privacy paradox, and because of tech lobbying, and because of political alignment, let's say, between the current administration and the tech industry, to an extent.

Despite all of that, we're seeing states move. For example, California has passed the strongest U.S.-based privacy law that currently exists. I think we could say that. It's been described as a GDPR, right, in the sense that Europe has its General Data Protection Regulation which is extraordinarily protective theoretically, although it hasn't been enforced to the word.

And the California law is not quite GDPR. I've heard some privacy advocates suggest that it's only 35 percent there, yet it's the strongest law we have in the U.S., anywhere in the U.S. right now. And I think that it's forcing a national conversation, because the tech industry doesn't want to comply with California, or at minimum wants to assure that no state goes further than California.

And so, there's some impetus behind the tech industry lobby to force a Federal law that essentially wouldn't do much beyond what California does already, but would preempt any state. So, I think there's some movement in privacy.

I think there's some movement in competition policy as well, particularly on antitrust reform, we've seen a couple of big efforts amongst academics, particularly legal experts, lie Fiona Scott-Morton, who have laid out mechanisms by which you could start to investigate an antitrust case against companies like Facebook and Google. We've seen the U.K. put out a few reports on this through its CMA (phonetic), which seem a big report from the University of Chicago.

So I think that there's some movement. There's a possibility that you could start to pack against these three pillars. If you think of a company like Facebook, or Google, or Amazon, part of what I argue in this book, is that there's a consistent business model, no matter what company over the Internet you look at, and more specifically what I describe as the consumer internet.

Those companies that engage in an ongoing dialogue with consumers, like Facebook, like Twitter, that business model involves the collection of data on an uninhibited basis, the use of that data to opaque ends, that's to say to develop algorithms that carried content and target ads, and the engagement in anti-competitive practices to maintain market position.

If you see those as three core pillars of the tech industry, and I believe they're consistent amongst these dominant Internet firms. Right now, the tech industry has unilateral control over those three areas. If you think about your exchange with Facebook, for example, of data, Facebook can kind of do whatever it wants with your data.

When you think about how Facebook uses algorithms to engage you, or target ads at you, Facebook can, again, do whatever it wants really. And the same goes in the competition area. So, if we want to renegotiate the terms that be, if we want to, let's say, take away some of the power from the tech industry, this unilateral control that they have over these economic exchanges with consumers and in the marketplace, then I believe what you need to do, and I believe where the country is going, and indeed the rest of the world is going, is that we need to transfer some of that power away from the tech industry. We need to put it back in the hands of consumers.

WICKS: Well, I feel like a lot of questions I've been asking you, are kind of downers. So, as we wrap up, I want to finish by addressing, you bring up a new social contract in your book with specifics like, the right to be forgotten, data anonymization. Can you walk us through, if we woke up tomorrow and everything was fixed, what would that look like? What would the new

social contract look like in that role?

GHOSH: This goes to our discussion just now. A new social contract will counteract this pressure from the industry, this unilateral power from the industry and transfer some of that power. Maybe all of that power to the consumer, so when you think about privacy and the practice of data collection by Google, for example, which has its tentacles everywhere really.

For example, a company like Google can collect information, does collect information through on-platform engagement with Google, that's the same when we've searched for things, obviously Google is keeping a record of what we search, trying to infer our behaviors and our interests from that. But also our location data, also our mobile ecosystem data, because many of us are android users, many of us use Google apps on our iPhones, et cetera.

Also location data, purchase data, what browsing data on third-party websites that have cookies and ad trackers that are connected back to Google, et cetera, et cetera. So Google is collecting all this information about us, most of us are not really aware of all of it, and it's happening all the time everywhere.

And we could say, theoretically, then that Google has 100 percent of the power in this relationship with the consumer. What I would contend is we need a privacy law, whereby users have 100 percent of the control, if they wanted. So, if Google currently is collecting all this information, users should be able to delete any information Google has on them.

Users should be able to opt out of certain kinds of data exchanges that Google might be engaging in. Users should be able to opt out of certain kinds of inferences that Google might be making about them. So that, yes, this might mean that their service might be less personalized, that's a choice that a consumer should have.

And I believe it will reduce the bias that we see over the Internet, and many of the

problems that have been talked about. Because when you put the responsibility back on the user, the user shouldn't technically have any complaints, especially if these are not only opt outs, but opt ins whereby Google can't collect your information, can't use your information in certain ways, unless you practically tell them that they can.

So, I think that that's what a digital social contract would be on privacy issues. That's to say, give users completed decision-making power over what Google can collect, and what Google can do with your information. On transparency, give users complete transparency over what kinds of information Google has, and how Google uses that kind of information for or against a user.

And on competition, really break down this business model, start to understand how this industry really works, because what I will contend is that first of all, these companies are monopolies. When you look across the landscape of the consumer internet, every segment of the internet is controlled by Facebook, Google, or Amazon. When you look at e-commerce, or email, or Internet search, social media, or picture sharing, or online video sharing, each of these segments of the consumer Internet is controlled by one of these three companies, essentially.

So, they have these monopolies, not only that, I believe that they're national monopolies in the sense that there are strong network effects around their presence in these industries, these segments of the consumer Internet market. And what there're able to do is, with that monopoly position, siphon out currency from their consumers which comes in the form of our data and our attention, at a monopoly event, they can take as much of it as they want, and they can charge whatever they want for it from the other side of the market, which is marketers trying to reach us.

So, I think we really need to understand, our policymakers really need to understand this much effectively, and strive to act against it, because if these companies are national monopolies

then they deserve heavy regulation.

WICKS: Dipayan, this has been great. Thank you so much for talking with me. The book is Terms of Disservice: How Silicon Valley is Destructive by Design. The author is Dipayan Ghosh. Dipayan, thank you, again.

GHOSH: Thanks, Robert.

DEWS: The Brookings Cafeteria Podcast is the product of an amazing team of colleagues, starting with Audio Engineer, Gaston Reboredo. Bill Finan and Robert Wicks of The Brookings Institution Press do the book interviews. Thanks also to my colleagues Adrianna Pita, Marie Wilkin, and Chris McKenna for their collaboration. Finally, my thanks to Camilo Ramirez and Emily Horne for their guidance and support.

The Brookings Cafeteria is brought to you by the Brookings Podcast Network, which also produces Dollar & Sense, The Current and our Events Podcasts. Email your questions and comments to me at BCP@Brookings.edu. If you have a question for a scholar, include an audio file and I'll play it and the answer on the air. Follow us on Twitter @PolicyPodcasts. You can listen to The Brookings Cafeteria in all the usual places. Visit us online at Brookings.edu.

Until next time, I'm Fred Dews.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2020