The Great Hack:

Can Democracy Survive the Internet?

The Great Hack (2019), is a Netflix documentary film that explores the 2018 Facebook/Cambridge Analytica scandal and the influence of social media in political elections. It cites that C.A. used their collection of data points for over 87 million Facebook users as a means of "politcal voter surveillance" in countries around the world, including the U.K's Brexit campaign and the 2016 United States elections.

1. Brittany Kaiser

The movie opens up with a young woman at the Burning Man festival in Black Rock City, Nevada writing the words "Cambridge Analytica" on the Galaxia temple before tying a whistle to it.

We soon learn that this young woman is Brittany Kaiser, the former business development director for the British political consulting firm, Cambridge Analytica, that used data brokers and an online app to accumulate information on tens of millions of Facebook users, gathering data on a massive scale.

I wanted to talk about this scene because it should be noted that the director's choice to open the movie this way was likely to foreshadow Kaiser's complicated role in the scandal. In *The Great Hack*, Kaiser plays the part of the villain, hero, martyr, and confused protagonist all at once. Her role--in the film and in reality--is ultimately to reflect on her actions at Cambridge Analytica and show how her testimony and whistle-blowing would help shape (or RE-shape) our views of democratic elections in the age of social media.

This opening scene is actually metaphorical: Although the main focus at Burning Man is the burning a wooden effigy (called "The Man"), the burning of the temple is equally revered by "burners"--a place to share hopes, fears and loss before letting them burn away to ash.

So when we see Kaiser write on the temple, we can see her participating in a self-cleansing, trying to sever her ties with C.A. (at least spiritually). This ultimately sets the stage for the ominous questions *The Great Hack* explores:

"How did the dream of the connected world tear us apart?"

"Who was feeding us fear and how?"

"Who controls our personal data?"

"And how can it be used against us?"

2. Chris Wylie

One of the other key figures of *The Great Hack*'s was Chris Wylie, the first whistleblower of the Facebook/CA data scandal. At 24 years old, Wylie came up with an idea that led to the foundation of Cambridge Analytica or, as he describes it in the film, a "full service propaganda machine".

In a 2018 interview with *The Guardian* (prior to the release of *The Great Hack*), Wylie explains how the idea to combine big data and **"information operations"** (an established military methodology) came to fruition:

"Wylie's job title was research director across the SCL group, a private contractor that has both defence and elections operations and is the parent company of Cambridge Analytica. Its defence arm was a contractor to the UK's Ministry of Defence and the US's Department of Defense, among others. Its expertise was in "psychological operations" – or psyops – changing people's minds not through persuasion but through "informational dominance", a set of techniques that includes rumor, disinformation and fake news" [(Click here for full article)](#)

The term **Psychological Operations** (Psy Ops) refers to any action which is practiced mainly by psychological methods with the aim of evoking a planned psychological reaction in other people. **Psychological warfare** is believed to have migrated from Germany to the United States in 1941, but **Psy Ops** have existed in the military since World War I--using newspapers, posters and airborne leaflets to distribute propaganda. Later the DOI used radio, magazines and cinema, then television and--finally--the web.

The [Special Activities Division](#) (SAD) is a division of the CIA's [National Clandestine Service](#), responsible for Covert Action and "Special Activities". These special activities include covert political influence (which includes psychological operations) and paramilitary operations. **SAD's political influence group is the only US unit allowed to conduct these operations covertly and is considered the primary unit in this area.**

To be clear though, the use of PsyOps is not exclusive to the military branches of government. Many PsyOp techniques have been used by everyone from a group of 4chan users and Campaign data strategists like Matt Braynard (as we saw last week with Pepe the Frog) to third party political strategists like those we see in *The Great Hack* and conspiracy theorist groups like QAnon which we will talk about next week.

Question to Consider:

- Though some champion psychological warfare for its non-violent or non-lethal ethos, we have seen terrorists groups like ISIS use social media platforms to disseminate their propaganda, using [polarizing internet videos](#) both to subvert and recruit. **Is the use of social media for military PSYOPS really more humane?**

- How does Cambridge Analytica and other "online marketing groups" using PsyOps to influence voters differ from the television and radio ads of previous generations? Are these methods ethical (why or why not)?

3. Carole Caldwalldr

Another of the film's protagonists (and writer of the above article), Caldwalldr's role centers around the perspective of the media and free press. Through her we learn more about how the story was covered, and the headwinds and challenges the media faced covering it. She points out that the future of her country was actually decided in Silicon Valley, where there's no accountability for the tech platforms (like Facebook and Google) that are used to undermine democratic elections

She also speaks about the inadequacy of election laws to battle the use of fake news and other social media–weaponizing tactics.

In her lengthy and detailed article in *The Guardian* (linked above), Caldwalldr quotes [Paul-Olivier Dehaye](#) – a data expert and academic based in Switzerland, who published some of the first [research into Cambridge Analytica's processes who](#)states it's become increasingly apparent that Facebook is "abusive by design" and that the company has "failed time and time again to be open and transparent."

In one scene near the end of the film, Cadwalladr takes to the TED stage to confront Zuckerberg, Jack Dorsey, and other tech leaders. Addressing "the gods of Silicon Valley," she pleads with them to consider the harm they've done, and change their ways for the sake of democracy.

"This technology that you have invented has been amazing, but now it's a crime scene, and you have the evidence," says Cadwalladr. "And it's not enough to say that you will do better in the future."

Questions to Consider:

- As Cadwalldr asks in the movie, is it still possible to have "a fair election" in the age of social media and big data?
-
- Do you think the CEOs of Twitter and Facebook will voluntarily become accountable for their users actions? Should they? What about sites where users are anonymous like 4chan?

4. David Carroll

"Who has seen an ad that has convinced you that your microphone is listening to your conversations?"

This is the question Professor David Carroll asks his students at the beginning of *The Great Hack.* He laughs nervously as almost every hand in the classroom shoots up.

Another protagonist in the story, Carroll spends his screen time fighting to get his own data back from Cambridge Analytica and has become a leading advocate for data rights in the United States.

While Chris Wylie represents the political machine that was Cambridge Analytica. Carroll is the voice of the everyday social media user who was being exploited by the networks and companies like Cambridge Analytica for gains based upon his data.
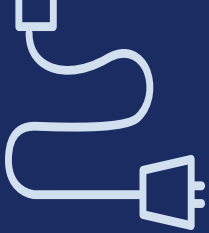
In an interview with *Business Insider* from August 2018, Caroll talks about the future of data rights and the importance for online users to demand transparency:

"Data protection is a structural problem. We don't have effective ways to hold companies accountable and to enforce when they commit data crimes because we don't even have a way to define, let alone prosecute, these data crimes....Europeans have data rights. Americans don't have the same rights. In the charter of human rights that founded the EU, data protection rights are listed as a fundamental right that's equivalent to freedom of speech, freedom to marry, all these other basic human rights. That's why Europe has a 20-year lead on creating the infrastructure for businesses to provide for these rights." (qtd. in Fischer)   (Click here to read the whole article)

Question to Consider:

- David Carroll wants the U.S. to enact more legislation to protect our data and online users, however if the politicians and lawmakers are the ones using big data and psychological profiling as a way to gain voters, can we trust them to regulate big tech companies to be more transparent about their algorithms and what else goes on "under the hood"?

#1: THE GREAT HACK VS. THE SOCIAL DILEMMA

Much like *The Social Dilemma* (which we watched in Week 3), *The Great Hack* Illustrates how giant tech companies like Facebook and Google, founded with good intentions to connect us all, are not preserving the ideals of the open society to which they owe their success.

They also show us the potential consequences when we trade our privacy and data for the "free" usage of various online platforms:

…Remember This?

/the
democracy
dilemma_

- *Fake news spreads 6x faster than accurate news on Twitter, and falsehoods are 70% more likely to be retweeted*

- *The number of countries with political disinformation campaigns on social media doubled in the past 2 years.*

- *Google search results can shift the voting preferences of undecided voters by 20% or more — up to 80% among some demographics.*

- *An internal memo to Facebook senior executives in 2018, which was largely ignored, read, "Our algorithms exploit the human brain's attraction to divisiveness. If left unchecked, [they'll feed users] more and more divisive content in an effort to gain user attention & increase time on the platform."*

In the Week 3 lesson that accompanied **The Social Dilemma,** I provided information on three of the major consequences of exploitative technologies (like Facebook) outlined in the movie. One of them was **The Democracy Dilemma**--a problem rooted in political polarization and divisiveness due to the creation and widespread dissemination of content that promotes outrage, deception, and conspiracy is promoted as a way to drive more engagement.

In this week's film, we see the Democracy Dilemma play out in great detail, exploring the impact on democracy when our data (a trillion-dollar-a-year industry) is used without our knowledge or consent to manipulate political behavior/ideologies.

QUESTIONS TO CONSIDER:

In an interview with Justin Rosenstein in *The Social Dilemma*, he said:
"You look over at the other [political] side, and you start to think, 'How can those people be so stupid? Look at all of this information that I'm constantly seeing. How are they not seeing that same information?' And the answer is: they are not seeing that same information."
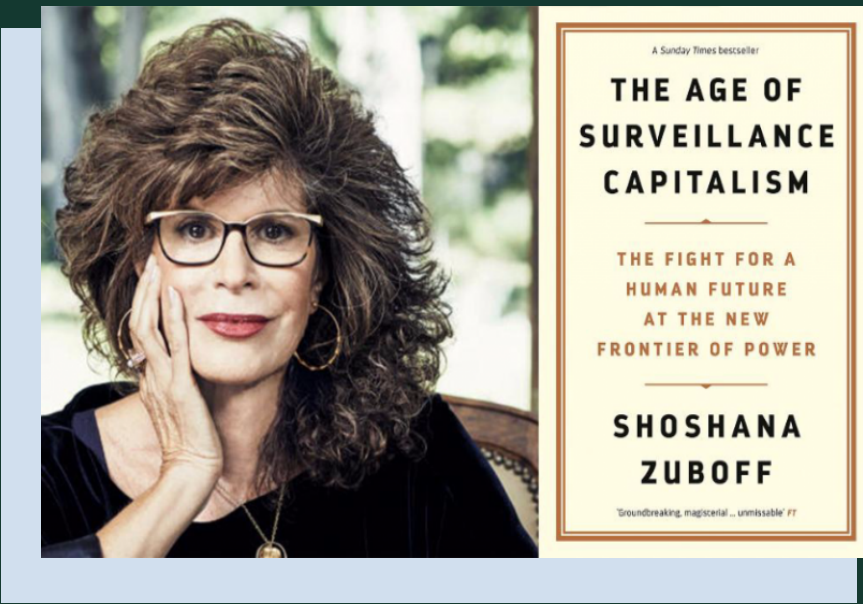
We learn from *The Great Hack* that Cambridge Analytica targeted Facebook users whose minds they thought they could change (referred to in the documentary as "persuadables"), with individually-tailored ads featuring propaganda and/or misinformation.

- Do you think this kind of targeted-advertising falls under the umbrella of free speech? Is the lack of accountability for tech platforms that are used to undermine democratic elections a violation of our civil liberties and human rights?

Another parallel from *The Social Dilemma* that comes into play here is the concept of **Surveillance Capitalism**--a term coined by Harvard Business School professor and author Shoshana Zuboff (remember her?)

As she defines it, Surveillance Capitalism is an economic "logic of accumulation" that involves extracting personal data in often-unrecognizable ways, creating "new markets for behavioral prediction, modification, and control" that exploit this data as its primary resource.

In other words, it's the entire M.O. of companies like Facebook and Google, which depend on users providing a constant stream of photos, likes, and other useful data that can be used to map relationships, measure emotional responses, and yes, serve ads. And when it comes to ads, the holy grail of advertising is having the ability to predict peoples' behavior—and thus, manipulate it.
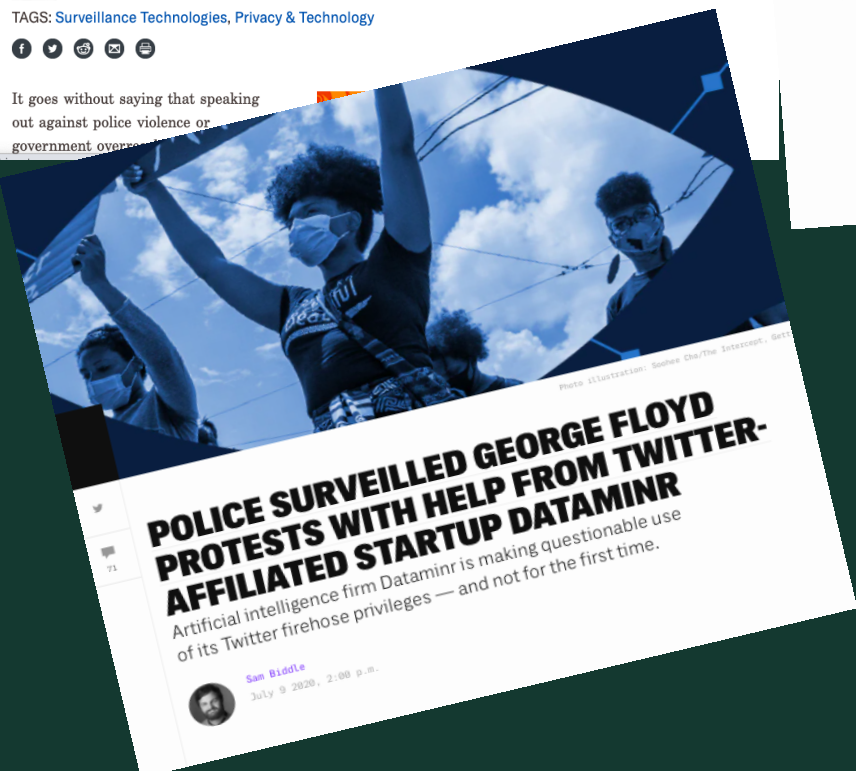
In an interview Zuboff conducted in 2016, she spoke to an anonymous chief data scientist at an unnamed Silicon Valley company that develops applications to improve students' learning who told her:

"The goal of everything we do is to change people's actual behavior at scale. When people use our app, we can capture their behaviors, identify good and bad behaviors, and develop ways to reward the good and punish the bad. We can test how actionable our cues are for them and how profitable for us" (qtd. in Zuboff).

This quote seems to perfectly capture the tech industry ideology, and--perhaps more importantly--illustrates how the technological process for creating the algorithms that help you choose your next Amazon purchase or what to watch on Hulu is the same one used in government surveillance tactics that the majority of U.S. citizens decry.

Nefarious government programs like facial recognition and predictive policing that are frequently used against immigrants, activists, and other marginalized groups don't just come out of nowhere. They are an inevitable consequence of a system that incentivizes the endless accumulation of data for profit.

We saw some of the ways that this this plays in *The Great Hack*, but we are also seeing it again--in real time--during the Black Lives Matter protests across the U.S. in 2020.

Take a second to watch this short clip from *Last Week Tonight with John Oliver* on Facial Recognition software (click here)
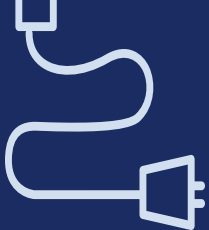
Making technology-driven surveillance part of the police's response to democratic protest sets a dangerous precedent. The risk of giving police these kind of powerful capabilities to target protestors can easily be abused and have a chilling effect on freedom of speech and assembly. (This is particularly true in the case of Black Lives Matter, given alleged evidence of the infiltration of U.S. law enforcement agencies by white supremacists)

QUESTIONS TO CONSIDER:

- Do you think Americans should be guaranteed the right to privacy? If yes, who makes sure that right is upheld?

- The Fourth Amendment to the U.S. Constitution states:
  "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

  Does the Fourth Amendment protect us from the kind of large scale surveillance and monitoring happening now? If it doesn't protect us, are there any laws that do? If there are not, should those laws be created?

#2: THE GREAT HACK VS. FEELS GOOD MAN

One of the things people found so shocking about the Facebook/C.A. scandal was the fact that they had no idea they were being fed content that had been perfectly tailored to pursued them into voting for a specific candidate through targeted advertising-- pretty much in the same way that a company will market you a pair of shoes or a probiotic based on your online activity.

Simultaneously, a group of anonymous self-proclaimed losers on 4chan were pumping out meme after meme that either glorified Trump or condemned Hillary Clinton. Both of these tactics had an impact on the 2016 Presidential campaign, and both of them were done completely legally.

QUESTIONS TO CONSIDER

- Do you feel like these two "campaign tactics" are ethical? Is one less ethical than the other (and why)?

- After watching *Feels Good Man* and *The Great Hack* (and even Shoshanna Zuboff's thoughts on Surveillance Capitalism in *The Social Dilemma*), do you feel like there should be rules and legalities put into place for using our data in this way?

- **Connecting all three documentaries**: In the three movies we've watched this semester, we've learned about how our phones and apps have learned our habits enough to know when to show us an ad (*The Social Dilemma*), we've learned that companies like Cambridge Analytica have scraped enough user data to know exactly who is persuadable and how to persuade them (*The Great Hack*), and we learned exactly where they are getting the most original, user-created, grassroots content (aka Dank Memes) to use while doing so (*Feels Good Man*). What responsibilities do you think the websites/platforms have to monitor or restrict these things from happening?

- Where do you draw the line between target marketing and surveillance capitalism? What about targeting voters with ads or memes vs. a PsyOp?

Two years after *The Great Hack* was released, surveillance capitalism is alive and well. We see it in targeting advertising, in recommended content, and despite Congressional hearings and Facebook receiving a $5 billion fine from the Federal Trade Commission for the company's long history of privacy violations dating back to 2010, right now Facebook users are still seeing hyper-targeted social media advertising--especially political ads during the 2020 presidential campaigns.

In an article published by *The Independent* in January 2020, Brittany Kaiser wrote:

"The debate between freedom of speech and censorship is being skewed here for political purposes and, it seems to me, as a convenient excuse for Facebook to profit off of allowing extremism on its platform. During the Brexit and Trump campaigns of 2016, I saw virulent racism and unchecked disinformation being channelled directly into voters' Facebook feeds. The world's most powerful democracy is about to elect its next president – yet little has been done to prevent a repeat of history. Worse, Facebook has since made it its official position that it cannot tackle false claims made by politicians. In an era of populism, this is dangerous."

We must act now to protect ourselves as voters, or we will continue to see Facebook profit off the erosion of our freedoms. We need action to protect our digital democracy." (click for full article)

Kaiser's article outlines what she believes are necessary steps in order to protect our digital future and its effect on democracy, one of which being that politicians must be held to the same community standards as every other user.
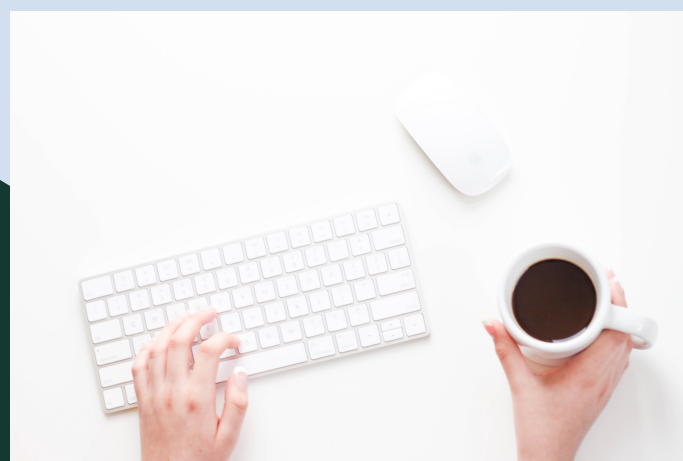
She explains how billions of campaign dollars are spent on Facebook Ads and "none of it, as far as I am aware, will be fact-checked. No content will be blocked or removed, even if it's found to be demonstrably false. Fake news ads from the Trump campaign about his political rival Joe Biden were blocked by CNN, but have been hosted on Facebook for months racking up millions of views by impressionable voters. We should not stand for this" (Kaiser).

The call for accountability--from companies, lawmakers, and users/citizens--dominates the conversation about how to move forward to protect data right, privacy, and the need for transparency and openness in the fields of technological innovations. However the current climate of political and social divisiveness in the U.S. leaves most people pointing the finger and putting the blame on "the other side."

Discussion Board Requirements

Your Post Should Be

- Be a minimum of 350 words
- Include one direct quote *NOT* featured in this lesson with a **CORRECT MLA IN-TEXT CITATION WITH THE TIME STAMP**
- At least one reference or quote from one of our 3 previous readings (Harari, Daniels & Konnikova) or documentaries (*The Social Dilemma* and *Feels Good Man*)
  - Include at least one question for your classmates

You may use any of the "Questions to Consider" in this lesson to get you started but they are not required!

Check the Discussion Board Assignment for due dates