The Facebook Conundrum: Is it Time to Usher in a New Era of Regulation for Big Tech?

Sara M. Smyth[1]
La Trobe University, Australia

Abstract
Transparency is one of the great promises of technology. Yet, big tech monopolies, like Amazon, Facebook, Google and Apple, cultivate monopolies, covertly influence our behavior, give some types of information preference over others, and secretly disclose our personal information to other entities. They do this every day with virtually no oversight, transparency, or informed consent, irrespective of what they choose to disclose to the public. These data-driven monopolies have, actually, derived much of their success from their hidden surveillance of users, the persistent monitoring of their activities, and their ever-expanding dossiers about their users in the marketplace. Traditional thinking is to let the market be free and unencumbered by government regulation that might have the effect of stifling innovation and creativity. Yet, regulators throughout the world are now waking up to the idea that this 'hands off' approach is dangerously unworkable. The question remains: is it time to usher in a new era of regulation for Big Tech?.

Keywords: Facebook, Technology, Google, Apple, Data.

Introduction

The process of collecting and organizing information is now a tremendous source of economic, political and cultural power. Data makes us more malleable, easier to predict, and extremely prone to influence. For retailers and marketers, being able to understand their customers' behaviours, preferences and aversions – so they can predict their needs and provide more targeted sales pitches – is the Holy Grail.

The Internet is now saturated with bots, artificial intelligence, and links to all 'things' in society. And, a large part of it is managed by a small handful of global conglomerates - Facebook, Google, Amazon and Apple. These are the four most influential companies on the planet; and, they're worth an astounding $2.3 trillion USD (Galloway, 2017, p. 1). Together, they're responsible for an array of products and services that are woven into the daily lives of billions of people around the globe. What does their unprecedented scale

[1] Associate Professor; Coordinator of Masters of Cyber-Security Program (Law), La Trobe Law School, College of Arts, Social Sciences and Commerce, La Trobe University, Bundoora Victoria 3086, Australia. Email: S.Smyth@latrobe.edu.au

and influence mean for the future of the Internet economy? How does the concentration of companies at the top effect our experience and access to the Internet?

When it comes to social networking sites like Facebook (which makes money from helping companies market products and services to particular demographics), the individual is caught within a web of inter-locking social and commercial relationships over which he or she has very little autonomy and control (Rifkin, 2003, p. 103). The norm is widely-distributed electronic openness; and, you have to deliberately carve out limited zones of privacy (Mitchell, 2004, p. 29). Indeed, we've already been going down a path toward a future in which people are monitored around-the-clock and there's scarcely any personal privacy left.

When combined with facial recognition technologies and a web of other data, like one's Facebook or Tinder profile, government identification, workplace, medical history, and more, a single snapshot can create a detailed picture of a person that traces their entire lifespan. With credit card data you can also get picture of a person's spending habits and track their movements 24/7. China is currently leading the way when it comes to this type of omnipresent surveillance; but, it's possible for Western countries to follow in China's footsteps, especially since the underlying technology keeps improving.

While promising to be helpful and even thoughtful, the pervasive power and persistence of advertising platforms embraced by tech giants like Facebook has become downright creepy. Some ads now seem more like stalkers than helpful friends – if, say, you've been online searching for a new pair of jeans, now those same pants begin to follow you around the Web, prodding you to take another look and luring you with progressively better deals and rewards (Wu, 2016, p. 323). Thanks to AI, we can now track behavior at a level and scale previously unconceivable (Galloway, 2017, p. 196).

Rhetorically, the big tech companies peddle individuality and empowerment of the user; but they really want to see their algorithms automating our way of life in exchange for vast catalogues of our intentions, motivations and aversions (Foer, 2017, p. 323). At the same time, there's rarely a clear picture about how they operate. In fact, they cultivate monopolies, covertly influence our behavior, give some types of information preference over others, and secretly disclose our personal information to other entities. They do this with virtually no oversight, transparency, or informed consent, irrespective of what they choose to disclose to the public.

This article consists of four parts. Following the introduction, Part I considers the evolution of Big Tech from the hippie counterculture movement of the 1960s through to today. Part II examines our current online world of mass surveillance, data harvesting and targeted marketing. As global tech giants like Google, Amazon and Facebook expanded their reach across the Internet to mine, repurpose and monetize data, they have created giant networks of surveillance and tracking, which feed into localized centres of control. Part III looks at the recent Cambridge Analytica scandal that prompted investigations into Facebook by the Federal Trade Commission (FTC) and widespread calls for the regulation of Big Tech. Part IV examines the lack of trust and accountability that Facebook now faces from its users and regulators. Currently, the FTC is investigating Facebook for privacy violations which relate to how the company shared data with outside developers in the past. Lastly, conclusion briefly looks at the way forward.

I. How it All Began

Ironically, Silicon Valley's penchant for monopoly dates back to the hippie counterculture of the 1960s where it emerged from the spirit of idealism, transformation and cooperation (Foer, 2017, p. 12). Once the Internet was released to the masses, it was no longer just a technology – it was a movement. There was an expectation of a great transformation; and, a belief in something truly extraordinary. The Internet would serve as 'a new global commons,' liberating us from the enslavement of television and the isolating, anti-social act of reading books that tech theorists like Marshall McLuhan disdained. It would counteract the destructive forces of individualism and usher in an era of creativity and collaboration. How this might work in practice remained prophetically vague – it would take decades to see how it would unfold (Wu, 2016, p. 253).

Stewart Brand (1989) was a hippie for the ages. As the founder of the *Whole Earth Catalogue*, Brand was at the center of some of the most intriguing events of the 1960s: he hung out with the writer Ken Kesey and his band of Merry Pranksters; he featured in Tom Wolfe's travelogue *The Electric Kool-Aid Acid Test*; and, he was one of the organizers of the infamous Trips Festival in San Francisco, which featured six thousand hippies, plenty of LSD, and the Grateful Dead (Rheingold, 2000, p. 26). Brand (1989) also inspired a revolution in computing which profoundly shaped the future of technology (Foer, 2017, p. 13).

The early network culture of the Internet had an egalitarian spirit and a left-leaning socialist mission, whereby the system – and the information it provided - was open, public and free. In his 1987 book *The Media Lab*, Brand quoted Howard Rheingold's (2000) reflection on the existence of computer-linked communities as relaxed, friendly, welcoming 'places':

> There's always another mind there. It's like having the corner bar, complete with old buddies and delightful newcomers and tools waiting to take home and fresh graffiti and letters, except instead of putting on my coat, shutting down the computer, and walking to the corner, I just invoke my telecom program and there they are. It's a place (Brand, 1989, p. 24).

Everything the hippie culture despised – the mindless submission of the worker, the tyranny of bureaucracy and the oppressiveness of centralised control – could be overcome in a virtual network where the individual had the freedom to find his inspiration, shape his environment, and share his passions and interests with likeminded people (Foer, 2017, p. 19). The existence of these computer-linked communities was, in fact, predicted in 1968 by J.C.R. Linklater, one of the research directors for the Department of Defense's Advanced Research Project Agency (DARPA) – the precursor to the Internet. Linklater wrote that, "life will be happier for the on-line individual because the people with whom one interacts most strongly will be selected more by commonality of interests and goals than by accidents of proximity (Rheingold, 2000, p. 19)." As such, these digital communities could become the agorae of modern life and empower individuals to be more open, expressive and free.

Spiritual prophesies about the revolutionary potential of technologies, and the underlying manifesto they preached – which saw technology as a tool of liberation and

collaboration – have been echoed by leading technology firms ever since. The spirit of egalitarianism and openness imbued within hippie culture are still apparent in the fact that big tech leaders typically eschew corner offices, preferring to sit amongst their staff in open spaces wearing the same T-shirts and jeans as those who are far beneath them on the pay grid (Foer, 2017, p. 20). And, by and large, they continue to view themselves as powerful agents of change – liberating the masses and creating new places where communities can flourish in a new era of openness and cooperation.

Another powerful metaphor that was popular in the early days of online communities depicted the first inhabitants of cyberspace as venturing into a new electronic frontier. For instance, in the early to mid-1990s, John Perry Barlow wrote a number of columns in *Wired* magazine in which he maintained that cyberspace is an independent "frontier" with its own rules and norms and that it would be impossible for any government to regulate it.

Like Brand (1989), Barlow was not your stereotypical computer geek. He worked as a cattle rancher in Wyoming and also wrote lyrics for the Grateful Dead. He was the first person to use William Gibson's science fiction term *cyberspace* – first coined in the 1984 novel *Neuromancer* - to describe this innovative domain. And, also like Brand (1989), he channelled the spiritual yearnings of his generation into musings about cyberspace.

The hacker credo 'information wants to be free' was a battle cry for the liberation of the Internet. These sentiments undoubtedly inspired many who designed significant social projects – without any expectation of profit – such as Linux, Wikipedia and the Creative Commons (Foer, 2017, p. 26). Paradoxically, they've also been trumpeted by powerful tech giants like Facebook. For example, if you walk through Facebook's headquarters in Menlo Park, California, you'll find a two-story mural - it looks like a massive totem pole filled with abstract shapes, and in the middle, there's a single word: *hack* (McMillan, 2015).

Yet, if we assume that information is 'disembodied' – that it floats freely through digital networks, unaffected by social, legal, political and cultural contexts - much is overlooked (Lyon, 2008b, p. 506). The general decline of face-to-face relationships that networked technologies promote has actually led to a demand for more 'tokens of trust' – in the form of social insurance numbers, PINs, barcodes, photo IDs and, increasingly, biometrics (Lyon, 2008a, p. 36). Thus, in the modern state, networked communications are increasingly dependent upon data that are said to be 'about me (Lyon, 2008b, 507).'

The comparison of data from different sources is now routinized, as we leave traces of our data behind whenever we engage in the routine transactions of modern society (Bennett, 2008, p. 52). David Lyon has thus suggested that surveillance systems 'bring back' disappearing bodies, by making them visible to organizations, agencies and authorities: "[t]he existence of contemporary surveillance systems in a sense reconnects bodily persons with data about them, by constituting them as high-value consumers, terror suspects, loan defaulters, free-flight eligibles or whatever (Lyon, 2008b, p. 507)."

Another, more practical, reason for the perceived lack of control in cyberspace owes itself to the free-market optimism that animated so much thinking about the Internet, information law and policy. From the beginning, there was intense worry about the risks of state intervention and coercion, combined with astonishing inattentiveness to the ramifications of what might happen if the Internet pioneers were left alone to accumulate

enormous amounts of power and wealth (Cohen, 1930). Much of the credit for economic boom during the mid-to-late 1990s was attributed to e-commerce and new opportunities for selling and delivering goods and services online (Regan, 2003, p. 14). The idea was to let the market be free and unencumbered by government regulation that might have the effect of stifling innovation and creativity (Regan, 2003, p. 14).

Various calls for intervention and regulation sparked intense criticism; and, the primary idea for a policy solution was simply that of "self-regulation." The theory was that if privacy is important to consumers, online organisations would respond and provide protection. In essence, the market would police itself and outside regulation would not be necessary. Yet, the online world does not represent a perfect market; and, vast power and information asymmetries need to be corrected. Nevertheless, concerns about stifling market and technological innovation surpassed concerns about the commodification and misuse of personal information.

Yet, the idea of the Internet as a true marketplace of ideas, or even a confessional corner, was actually quite vulnerable. The institutional forces that ultimately overcame this utopian dream came from the Internet itself – thus, there was nothing about its code that would keep it free, open and non-commercial forever (Wu, 2016, p. 275). And, rather than creating a practical manifestation of the counterculture's ideals, massive amounts of effort and resources have been directed toward replicating the world as it is and perpetuating its social, political and economic ills, rather than remedying it for the better.

Over time, this business model proved to be enormously successful. Before long, one company – Google – became the source of all knowledge; another – Facebook – became the portal to all social connections; and, a third – Amazon – became Earth's biggest store (Foer, 2017, p. 28). Make no mistake about it, we're not the customers of these big tech giants; we're the product they sell to their real customers – fortune 500 companies. This hidden marketing agenda was bluntly revealed in an open letter to customers by Apple's CEO Tim Cook in 2014: "…when an online service is free, you're not the customer. You're the product (Selk, 2018)." Indeed, we are little more than "tenant farmers" for the big tech companies, "working their land by producing data that they in turn sell for a profit (Schneier, 2015b)."

Facebook has invested a lot of money in developing metrics to convince its advertisers that their ads are valuable because even when users aren't clicking on them, they're seeing the product content (Wu, 2016, p. 300). It also allows advertisers to create their own pages, and to buy space in users' news feeds; and, with the 'like' button feature, users can freely promote and endorse products to their friends (Wu, 2016, p. 300). More sneakily, Facebook's heavy investment in tracking technologies enables it to follow users around the Web and report back to their advertisers – "she's looking at airline tickets!" – which allows, for example, US Airways to bombard the user with targeted ads on Facebook advertising airfares and, perhaps, even a free upgrade on her news feed (Wu, 2016, p. 300).

Largely unbeknownst to the general public, Facebook has become extremely rich from this business model, by which it cleverly mines and exploits the enormous trove of demographic data its users have given it free access to. To illustrate: in its 2017 annual financial report, Facebook revealed, "We generate substantially all of our revenue from

selling advertising placements to marketers (Borchers, 2018)." In fact, $39.94 billion of Facebook's $40.65 billion in total revenue — 98 percent — came from ads.

The profit-making power now held by tech giants like Facebook and Google is what keeps fierce corporate rivalry at bay – start-ups, for example, no longer aspire to displace these companies, but launch with the hope of getting bought up by the few goliaths in the marketplace (Foer, 2017, p. 31). Indeed, Facebook bought the five-year old, fifty employee instant messaging firm WhatsApp for a whopping $20 billion USD (Galloway, 2017, p. 7). It also owns Instagram which, along with WhatsApp and Facebook, are three of the five platforms that accumulated 100 million users the fastest (Galloway, 2017, p. 96). Aside from family, work and sleep, billions of people now spend more time on these platforms than any other activity (Galloway, 2017, p. 96).

The importance of free and open networks, which appealed to many in the early days of the digital revolution, has clearly been flaunted by companies like Google and Facebook, which are subject to little regulation or market competition (Schneier, 2015a, 60). Hidden within this agenda – of making information freely accessible to everyone – was always a price: the collection of our personal data in increasingly aggressive yet covert ways (West, 2017, p. 17). These companies have made billions of dollars promoting the idea that transparency is an inherent good, and, conversely, that secrets are intrinsically bad; yet, this only extends to their user-base, not to themselves. As Cory Doctorow observed: "…if it's a bargain, it's a curious, one-sided arrangement (Doctorow, 2012, p. 1)."

Cyberspace has become one of the most centralized mediums on the planet. The big tech companies that power most of the online content - Google, Amazon, Facebook and Apple – are the most powerful gatekeepers the world has ever known (Foer, 2017, p. 5). Indeed, sixty-two percent of Americans get their news from social media – primarily from Facebook; and, a third of all traffic to media sites flows through Google (Foer, 2017, p. 6). Of course, we highly reward entrepreneurship in Big Tech culture. We elevate the executives running these companies to hero or even God-like status. Yet, it's far more than just 'entrepreneurship' at work here. We have long celebrated extremely powerful and wealthy companies, like Facebook and Google, and allowed them to become larger, richer, and more powerful, without any competition or alternative for consumers.

How did this happen? The collection of user data didn't begin with Google or Facebook; in fact, it pre-dates the development of both platforms entirely. First introduced in Netscape Navigator 1.1 in 1995, cookies made it possible for servers to keep track of users' activities in ways that enabled e-commerce and soon led to targeted advertising (West, 2017, p. 8). Banner ads débuted the same month as the cookie; and, although they were touted as helping to "tailor advertising more closely to what consumers want," there were no features allowing users to modify their preferences, much less block them altogether (West, 2017, p. 8). Nevertheless, unlike the blogs and other open and creative spaces that were popular in the early days of the Internet, users channeled their energy into upgrading the value of these commercially-driven platforms (Wu, 2016, p. 301).

By 2010, The *Wall Street Journal* reported that the 50 most-visited sites on the Internet placed more than 3,000 tracking files on users' computers, making it possible for them to track users on pages belong to other sites and, more generally, as they flitted their way across the Web (West, 2017, p. 9). This was only the beginning of the advertising

business model that has become essential to the growth and shape of the Internet, and the origins of the commercial surveillance infrastructure as we now know it. Over time, through the covert technique of "attention arbitrage" the monopolists consolidated their power and influence, while rewarding us enough to keep us hooked (Wu, 2016, p. 301).

Of course, marketers have long been interested in siphoning data about consumers and using it to make predictions about their choices and behaviour – with the hope of eventually influencing them. The growth in the use of customer surveys and polls in the 1950s and '60s was used to render the post-war consumer understandable to researchers, political pollsters and marketers. By the 1980s, the means used to collect data about consumers shifted to the recording of credit card purchases and telephone calls (West, 2017, p. 6).

In the commercial world of the 1990s, an important change took place in the collection and use of consumer data. No longer content with survey-style data on existing customers, the goal was to find mathematical models that could identify the unknown individual – the as-yet-unencountered consumer who could be targeted (Amoore, 25). Thus, the modes of identification deployed within contemporary marketing schemes and proposals – particularly when it comes to data mining and social network analysis – have a great deal in common with those used to identify, locate and influence newer - and more narrowly-targeted – audiences based on knowledge of their online transactions and associated patterns of behavior.

II. Mass Surveillance, Data Harvesting and Targeted Marketing

As technologies progressed, those involved in the collection and aggregation of data gained increasing leverage in their ability to track users, generate profiles about them, cross-reference data with other information about them, and sell it to others. Now, most of our electronic clicks, taps and swipes are captured and recorded by someone. Indeed, nearly every mundane aspect of our lives today produces a digital trace – communicating with friends and family, ordering books, buying groceries, going to work, and so on (West, 2017, p. 2). This data is then easily combined with other information from the digital or physical world.

Thus, it is now commonplace for information deemed not to be "sensitive" to be freely compiled, transmitted, and exchanged. Even data about the seemingly trivial aspects of our lives (e.g. pizza orders) has become a valuable commodity and can easily be fed into algorithms and used to predict our behaviour in lucrative ways. These practices provide the means for advertisers to reach, target, and manipulate their audience (Nissenbaum, 1998, p. 590). For many, this comes as a major source of privacy invasion; yet, because the data is eagerly shared, people are, in many cases, complicit in the violation of their own confidentiality (Nissenbaum, 1998, p. 565).

Two factors underlie this trend: the rapid development of information technology coupled with an insatiable desire to know – "whatever may be useful to someone, somewhere, or what may become so in the future (Nissenbaum, 1998, p. 592)." This practice has come to be known as 'data capitalism' – a system in which "the commoditization of our data enables an asymmetric redistribution of power that is weighted toward the actors who have access and the capability to make sense of information (West, 2017, p. 4)." As global tech giants like Google, Amazon and

Facebook expanded their reach across the Internet to mine, repurpose and monetize data, they have created giant networks of surveillance and tracking, which feed into localized centres of control (West, 2017, p. 13).

The real genius behind this system is that they have convinced their customers that they are engaging in social rather than purely economic activity – or, in the very least, the two have become so tightly blurred that it's nearly impossible to distinguish one from the other. Indeed, the targeting for commercial ends is done person-by-person, so it's quite easy for polarizing messages to be widely distributed and masked at the same time. New algorithms let the data infer things about us we've never disclosed. So, I may have never talked about my politics or religious beliefs online, but the things I like or the pages I visit can be used to infer my politics or my religious beliefs. The number of inferences that can be made from the data we reveal is very powerful and can be used to profile us in all sorts of ways.

The news feed provides a reverse chronological index of all the status updates, articles, and photos that your friends have posted on Facebook. It's meant to solve the problem of our growing inability to sift through masses of information; thus, it has been turned into a "personalized newspaper" for users (Foer, 2017, p. 72). In fact, Facebook's algorithms interpret "more than one hundred thousand signals" and sort the information, deciding what we might like to read (Foer, 2017, p. 73). Many users – as many as 60 percent – are apparently completely unaware of this practice (Foer, 2017, p. 73).

Yet, the harvesters of information are keenly aware of the qualitative shift that can occur when bits of data revealed in one context are shifted to another and compiled into profiles. At times, the shift may cross not only contextual lines but temporal lines as information collected in the past is introduced into a current setting (Nissenbaum, 585). So, the data may be willingly disclosed in 2015, but predicting what the implications of that might be down the track – say, in 2020 - can be very difficult for the individual.

In reality, data brokers often act in ways that mask the source of their data, including buying and combining information from other brokers, thereby making it extremely difficult for consumers to retrace the paths through which their data were collected (West, 2017, p. 12). Thus, once the data is freely handed over, its potential use is virtually limitless and consent is un-revocable. Given the uncertainty around technological developments going forward, this should make us extremely nervous. People generally resent the rampant and unauthorized distribution of information about themselves, not only when this violates the integrity of an intimate and highly personal sphere, but also when it breaches contextual and temporal integrity (Nissenbaum, 1998, 586).

Yet, for many consumers, the ease of convenience and the disguise of benevolence provided by these systems keeps us lulled into complacency. Facebook is popular because it helps billions of people fill a void and connect with others in the otherwise vacuous online space. These seemingly benevolent technologies have become tightly integrated into the fabric of our societies – just as Orwell and Huxley predicted. Facebook, for its part, has become our online living room: it's the place where we chat with friends, hold forth about the news, organize events, grieve over things we've lost, celebrate babies, pets, engagements, new jobs, new shoes, and vacations.

Meanwhile, news-feed algorithms reinforce certain kinds of behavior and keep us in a feedback loop of positive and negative rewards. Positive feedback comes from friends who

'like' your posts; negative reinforcement comes when you only get a few responses to a personal disclosure, prompting you to question your self-worth and aim harder to please. Behavioral scientists call this 'intermittent reinforcement;' and, it's one of the most powerful performance-modifying techniques known to man (Doctorow, 2012, p. 66). For Facebook, there's nothing particularly clever or inventive about this business model – it's merely exploiting the dynamics of acceptance and rejection, buttressing deep-rooted insecurities and the sophomoric desire to be in the 'cool crowd (Wu, 2016, p. 291).'

III. A Wakeup Call

Facebook was recently plagued with controversy around the spreading of fake news, foreign agents acting as trolls, and a lot of other problems that emanate, in large part, from a scandal that originated in 2014. That year, Cambridge Analytica, a London-based firm that specializes in using online data to create voter personality profiles in order to target users with political messages, put out a request on Amazon's "Mechanical Turk" platform, a global Internet marketplace enabling individuals and businesses to meet and coordinate the performance of various tasks (Tufekci, 2018). Cambridge Analytica was seeking people who were Facebook users in the United States. It offered to pay them to download and use a personality quiz on Facebook called *"thisisyourdigitallife*" (Tufekci, 2018)."

About 270,000 Facebook users responded and downloaded the app (Tufekci, 2018). At the time, Facebook allowed app developers to access not only user data but the data of their friends. Thus, the app acquired information from these users' Facebook profiles, as well as detailed information from their friends' profiles, resulting in about 50 million Facebook profiles accessed (Tufekci, 2018). Most of those people had no inkling that their data was harvested - they hadn't installed the app themselves (Tufekci, 2018). Meanwhile, Cambridge Analytica began working for the Trump campaign in June 2016 and it promised that its "psychographic" profiles could predict the personality and political leanings of every adult in the United States (Dwoskin, 2018). It also used micro-targeting to serve up pro-Trump messages that resonated with specific voters (Galloway, 2017, p. 106).

In mid-March, 2018, this scandal was exposed by *The New York Times* and the London *Observer*. Facebook made a public announcement that it was suspending Cambridge Analytica and fervently denied that this was a "data breach." Paul Grewal, a vice president and deputy general counsel at Facebook, wrote that, "the claim that this is a data breach is completely false (Tufekci, 2018)." He insisted that Facebook users, "knowingly provided their information, no systems were infiltrated, and no passwords or sensitive pieces of information were stolen or hacked (Tufekci, 2018)." He also said that, "everyone involved gave their consent (Tufekci, 2018)."

In her *New York Times* opinion piece on this situation, Zeynep Tufekci, an Associate Professor at the School of Information and Library Science at the University of North Carolina, stated the following:

> This wasn't a breach in the *technical* sense. It is something even more troubling: an all-too-natural consequence of Facebook's business model, which involves having people go to the site for social interaction, only to be quietly subjected to an enormous level of

> surveillance. The results of that surveillance are used to fuel a sophisticated and opaque system for narrowly targeting advertisements and other wares to Facebook's users. Facebook makes money, in other words, by profiling us and then selling our attention to advertisers, political actors and others. These are Facebook's true customers, whom it works hard to please (Tufekci, 2018).

In 2015, Facebook removed the app and demanded guarantees from Cambridge Analytica that the information had been destroyed. The company certified to Facebook that they had done so, but Facebook said it received reports in March of 2018 that the data was not deleted (Tufekci, 2018).

In fact, Russian agents abused the company's networks to target millions of American voters with 'fake news' during 2016 presidential campaign. On May 10, 2018, House Intelligence Committee Democrats published downloadable files with more than 3,500 ads to their website (Wagner, 2018b). These are Facebook ads that were purchased by the Internet Research Agency (the "IRA"), a Kremlin-backed "online troll farm," both before and after the election. The Trump campaign also made significant use of Facebook and the social network has been criticized for having its employees connect with Trump campaign staffers.

In February 2018, Special Counsel Robert Mueller indicted 13 Russian individuals linked to the IRA (Kafka, 2018). The indictment blames Russia for starting a social media campaign aimed at disrupting "the lawful governmental functions of the United States (Kafka, 2018)." It claims the IRA "engaged in operations to interfere in elections and political processes," adding that the group, "posted derogatory information about a number of candidates (Wagner, 2018b)." In other words, the Russians set up bogus accounts and masqueraded as regular users who promoted Donald Trump or vilified Hillary Clinton (Kafka, 2018). What's more, the IRA bought thousands of ads and posted tens of thousands of other posts, promoting both sides of contentious political issues like gun control and race relations (Wagner, 2018b).

Mark Zuckerberg has openly acknowledged that his company has a strong view about what's best for you and how to get you there: "[t]o get people to this point where there's more openness – that's a big challenge. But I think we'll do it," Zuckerberg has said (Garber, 2012). With its power, size and influence over people worldwide, Facebook clearly has this power within its sites. And, indeed, Zuckerberg has stated that, "[i]n a lot of ways, Facebook is more like a government than a traditional company (Farrell, et. al., 2018)." With its vast influence and wealth, it's hard not to see that Facebook does, in fact, have much in common with a sovereign nation-state. It has long operated with absolute impunity, while abusing the immense trust vested in it, and it has the power to completely change the way businesses and individuals behave and relate to each other, on a universal scale.

Earlier this year, Facebook launched a 'petitions feature' called Community Actions. It will allow users to which will allow users to create, support and share petitions and notify their local officials of actions that they'd like to see happen (Liptak, 2019). Petition advocates will be able to discuss the topic with fellow supporters on the page, and will also be able to create events and fundraisers. Interestingly, this isn't the first time that the company has developed tools to get users more politically-involved.

Facebook already initiated a number of features designed to get people more involved in their communities, such as the Town Hall feature, which helps users access their local officials; as well as the Candidate feature, which allows political candidates to target their constituents with videos (Liptak, 2019). Facebook states that its Community Actions feature is a means by which "people [can] advocate for changes in their communities and partner with elected officials and government agencies on solutions (Liptak, 2019)" all within the safety and comfort of the Facebook site. Thus, the company has clearly decided to branch out into local markets and enable local communities to organize around sensitive topics and directly engage in the political process. This will no doubt provide vocal interest groups a podium from which to self-promote their ideas and pressure politicians with their agendas.

Why would Facebook want to do that, particularly when they've recently been the subject of so much condemnation for their involvement in the political process? First, controversy drives engagement, which benefits the platform. All Facebook needs to do is ensure that the Community Actions go viral and then sit back and wait for people to hit the "Support" button. The more debate there is around a topic, the more people get involved and share their views. This generates more data for Facebook, through the creation of micro-communities which both produce and attract new content, which translates to more power and influence for Facebook – in terms of its ability to understand us and shape our preferences and purchases – as well as more potential revenue for its privately owned-platform. Facebook can target those users with ads and glean new information about them. Thus, the motives behind Facebook's ever-expanding foray into local politics are not as altruistic as supporters might think.

As the Cambridge Analytica scandal demonstrated, bad actors can really misuse Facebook's features – in ways that may not have been intended by the developers from the outset, and which are largely hidden from the general public. Every tool that Facebook offers its users for cooperation, free expression and connectivity can be undermined for division, opposition and misinformation (Constine, 2019). Facebook's membership around the globe has also become an extremely valuable target for exploitation by trolls, extremist groups, and others. The question is whether Facebook puts in the appropriate safeguards to support its new tools, or whether they will continue to be used as mechanisms for disrupting democratic processes around the world. Thus, it is far more complex and far-reaching than Mr. Zuckerberg lets on.

We don't know what use Facebook will make of this information, or with whom it may be shared, and there's no reason to think that all this data about people's political beliefs and motivations won't be sold to third parties for nefarious uses. Clearly, it would be extremely valuable to political opponents to know the views of those who are rallying behind a particular candidate or platform. This could potentially undermine the very reason for those people to engage in the platform in the first place.

Private third-parties would also find this information extremely valuable, particularly those who back a particular candidate or cause; or, those who may be impacted by the changes that users think they can bring about (e.g. if a group is advocating for a moratorium on oil and gas drilling by a large company, certainly that company and others invested in the project would want to have access to the petitioner's profiles and news feeds). Marketers would also find it useful to target the news feeds of petition supporters

with tailor-made advertisements based on the profile of these individuals (e.g. a twenty-something college graduate advocating for city bike lanes might be interested in purchasing bike gear, whole foods, and so on). The potential for misinformation and misuse by all sorts of agents and actors is virtually limitless.

IV. The Lack of Transparency and Accountability

It's apparent that we invested far too much trust in high-tech giants like Facebook. In reality, the whole idea that we can have a large profit-seeking entity solely in search of philanthropy and social justice is ludicrous and it's astonishing that we allowed ourselves to buy in to this myth for so long. However, while these companies have clearly been pushing the boundaries of the law – and there is a need to render their practices more transparent – it's not obvious that they've engaged in the kind of wholesale corruption that would put our society at risk, or is it?

Since the Cambridge Analytica revelations, the public and governments are finally waking up and talking about the fact that the consolidation of power in a few giant tech companies has gotten worse. Indeed, US House Speaker Nancy Pelosi avowed that it's a 'new era' for tech regulation: "…the era of self-regulation of these companies is over (Johnson, 2019)." And, in early April 2018, Facebook CEO Mark Zuckerberg appeared in front of almost half of the United States senate. He answered questions about Facebook's data protection and privacy practices from nearly 100 different politicians in nearly 10 hours of public testimony – the first real public debate about the rampant data sharing that has been allowed to continue unabated for more than a decade.

The idea that Facebook is a monopoly was raised multiple times that week. When asked who Facebook's biggest competition is, Zuckerberg didn't have much of an answer. Clearly, Google competes with Facebook for advertisement dollars, and there are other social services out there —primarily Twitter — but nobody comes anywhere close to matching the size and services that Facebook (which also owns Instagram, WhatsApp and Messenger) provides. On that note, some people think Facebook has grown so big that the government should break the company up. For example Democratic presidential candidate Elizabeth Warren has put forward a proposal to break up Amazon, Google, and Facebook (Warren, 2019).

Zuckerberg argued that breaking up Facebook would be bad for America because it would pave the way for Chinese tech companies — which don't have traditional American values — to step in and dominate: "there are plenty of other companies out there that are willing and able to take the place of the work that we're doing," he said, pointing to Chinese tech companies, "[a]nd they do not share the values that we have (Wagner, 2018a)." It's an outrageous assertion in response to allegations that Facebook permitted Russia to sway the 2016 US presidential election. Furthermore, Facebook doesn't even operate in China: the social network is banned there, and has been for years, which has enabled competitors — like WeChat — to thrive (Wagner, 2018a).

The FTC began investigating Facebook in March 2018 following reports that Cambridge Analytica had accessed the data of 87 million Facebook users. However, a central issue was whether Facebook's data-sharing practices violated an agreement it made with the FTC in 2011 to "better protect people's privacy (Wagner, 2019)." That agreement, which is known as a 'consent decree,' requires that Facebook receive

"affirmative express consent" from users before making any changes to its privacy policies. Facebook further agreed that it wouldn't make any "misrepresentations about the privacy or security of consumers' personal information (Wagner, 2019)." Yet, allowing third-party developers to access a user's personal information without their knowledge could certainly be perceived as a "misrepresentation" on Facebook's part (Wagner, 2019).

In 2011, in a case before the FTC by the name of *Facebook, Inc.*, Facebook agreed to settle charges that it "deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public," among other things. The complaint specifically referred to the fact that users' data could be obtained by third-party app developers in ways that could have caught those users unaware, which is clearly suggestive of Facebook's current debacle.

The final settlement in 2011 barred Facebook from making further deceptive privacy claims, required it obtain a user's explicit approval before changing the way it handles their data, and compelled it to receive periodic assessments of its privacy practices by third-party auditors for the next 20 years. It also demanded that users be notified explicitly if their data is shared beyond the privacy settings they have configured.

Facebook's 2011 consent decree says that the company could be fined as much as $16,000 per day for "each violation." In July 2019, the FTC approved a roughly $5 billion settlement with Facebook over the Cambridge Analytica scandal (Rodriguez, 2019). The fine represents the largest the agency has ever imposed on a technology company (Romm, 2019). Previously, the largest fine the FTC imposed on a tech giant for breaking an agreement with the government to safeguard consumers' data was a $22.5 million penalty that Google paid to settle a probe over in 2012 (Romm, 2019).

Facebook's revenue in 2018 is estimated at more than $50 billion USD; accordingly, the fine represents only about 9% of its profits for that year (Rodriguez, 2019). The settlement drew criticism from a number of senators and Congress members, who argued that this was little more than a 'slap on the wrist' (Rodriguez, 2019). Given the company's repeated privacy violations, it may be that significant structural reforms are needed (Rodriguez, 2019).

Other than the FTC's involvement in the matter, though, there is little else that can be done at the moment to hold Facebook accountable for its misdeeds. Unlike in the EU and Canada, the United States has no general data protection laws. In fact, the US has long been the great exception when it comes to the global predilection for this sort of omnibus legislation. The 1974 *Privacy Act* only addresses the personal information practices of federal entities, not state and local governments or private entities (Donohue, 468). What's more, Silicon Valley has long been immune to the *Communications Decency Act* (47 U.S.C.) by virtue of section 230 which says that Internet companies are not responsible for what is posted on their platforms.

Section 230 says that *"No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."* Thus, online intermediaries that host or republish speech are protected against laws that could otherwise be used to hold them accountable for what others say and do. The protected intermediaries include not only Internet Service Providers (ISPs), but also a range of "interactive computer service providers," or any online service that

publishes third-party content, including Facebook and Twitter. In theory, this makes good sense: it would be nearly impossible for online intermediaries to stop offensive content from making its way onto their site; and, rather than face potential liability for their users' actions, most would prefer to not host any user content at all or would be actively engaged in an online cat-and-mouse game of censoring what we see, do and say online.

Yet, in Europe, policy-makers have recently adopted an entirely different approach. Of course, it's much easier to impose weak laws, or no laws altogether, and then try to strengthen them, rather than the other way around. This is particularly significant given that time was needed for the Internet to flourish as a generative medium and an instrument of free speech. Now, with the benefit of hindsight and experience, we can subject it to far more rigorous scrutiny than if we had come in heavy-handed right from the start.

As of May 25, 2018, the *European Union General Data Protection Regulation* ("GDPR") - a series of laws that were approved by the European Union Parliament and the Council of the European Union in 2016 - replaced the *EU Data Protection Directive of 1995*. It is a comprehensive legal framework aimed at the protection of persons from the processing of personal data and their right to informational privacy. The GDPR affects all companies, individuals, corporations, public authorities or other entities that offer goods or services to individuals in the EU or that monitor their behaviour there (Harris, 2018).

The new *GDPR* regulations will give users greater control over their data, including the ability to export it, withdraw consent, and request access to it. The new regulations are far stricter than their predecessors in Europe, as well as the rules in many other countries. Indeed, the law will set a new global benchmark around the importance of personal information ownership and consumer protection (Harris, 2018). Any advertising agencies doing business with clients in the EU, or companies targeting ads to potential customers there, will have to comply with the new rules. Penalties for non-compliance could be up to €20-million or four percent of a company's total global revenue, whichever is greater.

In the US senate hearings discussed above, Mark Zuckerberg said he thought the *GDPR* was a good idea: "I think the GDPR, in general, is going to be a very positive step for the Internet (Wagner, 2018d)." However, Zuckerberg made swift changes to ensure that the number of Facebook users protected by it will be considerably less. Facebook members outside the United States and Canada were historically governed by terms of service agreed with the company's international headquarters in Ireland. Yet, before the *GDPR* came into force, Facebook deliberately moved 1.5 billion of its users out of reach of the new European privacy law by "shifting the responsibility…from its international HQ in Ireland to its main offices in California (Hern, 2018)." This means that users in North America, Africa, Asia, Australia and Latin America will now be on a site governed by much weaker US privacy laws. That removes a massive potential liability for Facebook, which could have meant billions of dollars.

In April 2018, Zuckerberg told *Reuters* in an interview that his company would apply the EU law globally "in spirit," but stopped short of committing to it as the standard for the social network across the world (Reuters, 2018). In practice, the change means that 1.5 billion affected users will not be able to avail themselves of the robust protections

provided by the *GDPR*. They also won't be able to file complaints with Ireland's Data Protection Commissioner or in Irish courts.

The challenge of effective regulatory enforcement in cyberspace has been a persistent problem for decades. Traditionally, crime tends to be perpetrated on a local level; and, it would be very difficult for a real-world criminal to simply pack-up and relocate to another country where the laws happen to be more lenient and hospitable. Yet, the lack of an international consensus around cybercrime, in particular, led to inconsistent standards and practices around the world, creating a large number of "safe havens" for criminals to exploit.

Another problem is that the Internet's reach is so vast that law enforcement agents in only a handful of countries cannot possibly investigate and prosecute offenders on their own, particularly if they are faced with conflicting regulations in multiple jurisdictions worldwide. This provided great impetus globally for the creation of international treaties – like the *Budapest Convention* – to facilitate international cooperation and investigation in this area. Fortunately, these and other international efforts toward increased interjurisdictional harmonization and cooperation have made it easier to combat cybercrime in recent years.

Yet, we are also seeing that the large, private corporations that dominate the Internet are equally eager to evade the law by simply relocating their headquarters elsewhere. It's noteworthy that the most prominent online services are based in the United States. This is in part because the lax privacy and data protection laws have made the US a safe haven for those who want to provide a platform for controversial or political speech and a legal environment favorable to free expression. They have also nourished a culture of rampant Internet entrepreneurship that many now believe has grown beyond our public interest. If targeting these entities directly is ineffective, due to the ease with which they can relocate to a jurisdiction outside the regulatory influence of the state, policymakers must decide between allowing the harm to continue and looking for other regulatory solutions (Mann & Belzley, 256).

Conclusion

It seems impractical, if not impossible, that Facebook and Google would completely overhaul their businesses, tossing aside their winning advertising engines to start afresh. But, it's increasingly clear that something is going to have to change. We've seen that from the beginning, there has been an astonishing inattentiveness about what could happen if global tech giants were left alone to accumulate enormous amounts of power. The world is finally waking up to the fact that they have been given too much power over our economy, our way of life and our democracy. They've bulldozed their competition, used our private information for their own profit, annihilated small businesses and flaunted their political power.

Recognition of this has prompted calls to reform existing policies and practices to ensure stronger protection of privacy. The suggestion of changing Facebook's default privacy settings from opt-out to opt-in, meaning the company would need to ask for permission to collect data right away instead of collecting it by default, seems like it would be the most dangerous to Facebook. It would severely limit the amount of data they can collect about people, thus hurting their business model.

Lawmakers in the United States are increasingly calling for the FTC to crack down on Facebook. They have also recommended that the FTC lay out what Facebook can do with private information, such as demanding that tracking data be deleted, as well as placing limits on the collection of private information and advertising practices. It may be nearly impossible for Facebook to transform its own practices, given its longstanding business model. However, it is certain to face some significant challenges in re-building trust and credibility with regulators.

References

Amoore, L. (2008). Governing by Identity. In C. J. Bennett & D. Lyon (Eds.), *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective.* New York: Routledge.

Bennett, C. J. (2008). Unsafe at Any Altitude: The Comparative Politics of No-Fly Lists in the United States and Canada. In M. B. Salter (Ed.), *Politics at the Airport* (P.51). Minneapolis: University of Minnesota Press.

Borchers, C. (2018). Would you Pay $18.75 for Ad-Free Facebook? *The Washington Post*, April 14, 2018.

Brand, S. (1989). *The Media Lab: Inventing the Future at M. I. T.* London: Penguin Books.

Cohen, J. E. (2013). What Privacy is For. *Harvard Law Review*, *126*(7), 1904.

Constine, J. (2019). Facebook Launches Petitions Feature – Its Next Battlefield. *TechCrunch*, January 20, 2019.

Doctorow, C. (2012). The Curious Case of Internet Privacy. *Technology Review*, July/August 2012.

Donohue, L. K. (2012). Technological Leap, Statutory Gap. *Minn. L. Rev, 97*, 407.

Dwoskin, E. (2018). Facebook bans Trump campaign's data analytics firm for taking user data. *The Washington Post*, March 16, 2018.

Farrell, H., Levi, M., & O'Reilly, T. (2018). Mark Zuckerberg runs a Nation-state, and he's the King. *Vox*, April 10, 2018.

Foer, F. (2017). *World Without Mind – The Existential Threat of Big Tech.* New York: Penguin Press.

Galloway, S. (2017). *The Four: The Hidden DNA of Amazon, Apple, Facebook and Google.* London: Transworld Publishers.

Garber, M. (2012). The Ballad of Mark Zuckerberg. *The Atlantic*, February 1, 2012.

Harris, N. (2018). A practical guide to the European Union's GDPR for American businesses. *Recode*, May 16, 2018.

Hern, A. (2018). Facebook moves 1.5bn users out of reach of new European privacy law. *The Guardian*, April 19, 2018.

Johnson, E. (2019). "Silicon Valley's self-regulating Days "probably should be" over, Nancy Pelosi says." *Vox*, Apr 11, 2019.

Kafka, P. (2018). The U.S. government says Russia infiltrated Facebook with fake users, accounts and groups supporting Donald Trump. *Recode*, February 16, 2018.

Liptak, A. (2019). Facebook is Launching a Petitions Feature. *The Verge*, January 20, 2019.

Lyon, D. (2008a). Filtering Flows, Friends and Foes. In M. B. Salter (Ed.), *Politics at the Airport* (P.29). Minneapolis: University of Minnesota Press.

Lyon, D. (2008b). Biometrics, Identification and Surveillance. *Bioethics, 22*(9) 499.

Mann R. J., & Belzley, S. R. (2005). The Promise of Internet Intermediary Liability. *Wm. & Mary L. Rev*, *47*, 239.

McMillan, R. (2015). A 125-Year-Old Letter Dives into the True Meaning of the Word *Hack. Slate,* January 29, 2015.

Mitchell, W. J. (2004). *ME ++.* Cambridge, MA: MIT Press.

Nissenbaum, H. (1998). Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy, 17*, 559.

Regan, P. (2003). Privacy and Commercial Use of Personal Data: Policy Developments in the United States. *Journal of Contingencies and Crisis Management, 11*(1), 12.

Reuters. (2018). Facebook is Ensuring that GDPR Protection is Limited to EU Residents, the Privacy of Everyone Else is Still at its Mercy. April 19, 2018.

Rheingold, H. (2000). *Virtual Communities – Homesteading on the Electronic Frontier*, Cambridge, MA: MIT Press.

Rifkin, J. (2000). *The Age of Access: The New Culture of Hypercapitalism, Where all of Life is a Paid-For Experience.* New York: Penguin Putnam.

Rodriguez, S. (2019). "Facebook to be slapped with $5 billion fine for privacy lapses, say reports." *CNBC*, July 12, 2019.

Romm, T. (2004). The U.S. government and Facebook are negotiating a record, multibillion-dollar fine for the company's privacy lapses. *The Washington Post*, February 14, 2019.

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (New York: W.W. Norton & Co.).

Schneier, B. (2015). How We Sold Our Souls—and More—to the Internet Giants. *The Guardian*, May 17, 2015.

Selk, A. (2018). Apple's Tim Cook: I would have avoided Facebook's privacy mess. *The Washington Post*, March 29, 2018.

Stewart, E. (2019). Senators on Facebook's potential $5 billion fine: not good enough. *Recode*, May 17, 2019.

Tufekci, Z. (2012). Data Dystopia. *Technology Review*, July/August, 2012.

Tufekci, Z. (2018). Facebook's Surveillance Machine. *The New York Times*, March 19, 2018.

Wagner, K. (2018a) "Mark Zuckerberg says Breaking up Facebook Would Pave the way for China's Tech Companies to Dominate," *Recode*, July 18, 2018a.

Wagner, K. (2018b). Congress just Published all the Russian Facebook Ads Used to Try and Influence the 2016 Election. *Recode*, May 10, 2018b.

Wagner, K. (2018c). This is How Facebook Collects Data on You Even if You Don't Have an Account. *Recode*, April 20, 2018c.

Wagner, K. (2018d). Facebook is taking its first steps to comply with Europe's strict data privacy rules. *Recode*, April 18, 2018d.

Wagner, K. (2019). Facebook may be facing a "multibillion-dollar" fine from the FTC. Here's why. *Recode*, February 14, 2019.

Warren, E. (2019). Here's How We Can Break Up Big Tech. *Medium*, March 8, 2019.

West, S. M. (2017). Data Capitalism: Redefining the Logics of Surveillance and Privacy. (2017) *Business & Society, 00*(0), 1.

Wu, T. (2016). *The Attention Merchants – The Epic Scramble to Get Inside Our Heads.* New York: Vintage Books.

Case Law

Facebook, Inc., No. 092 3184 (Fed. Trade Comm'n Nov. 29, 2011).