Mindf*ck

Cambridge Analytica And The Plot To Break America

—

Christopher Wylie

CHAPTER 12

REVELATIONS

I WON'T TELL YOU WHERE I LIVE, EXACTLY. IT'S SOMEWHERE between Shoreditch and Dalston, in the East End of London. I am the pink-haired guy who lives on the top floor, but I don't really stand out much. The neighborhood is working class in its roots, and many buildings here were once factories in London's industrial age. Faded paint on smoke-stained brickwork advertises long-gone products from a century ago. There is a détente between the Indian, Pakistani, and Caribbean communities that moved here in the last wave of Commonwealth immigration and the new wave of artists, gays, students, and grungy weirdos who are being pushed out of central London by the cost of living. There are art deco cinemas, roof gardens, and the restless cacophony of intoxicated clubgoers drinking cans of Red Stripe until 4 A.M. every weekend. One often sees completely veiled Muslim women shopping in the same off-license greengrocer as tattoo-clad club kids with asymmetrical hair. It is still a place where I can walk outside in relative anonymity.

My building is old, built in a time before the Internet was even imaginable and when indoor plumbing was still a novelty. The floor is wooden and solid, but every so often it creaks as you take a step. There are extra bolts on the door, installed after a group of men kept coming to the door the week after I went public. My neighbors started complaining, until they realized who I was. Now they let me know anytime they see people loitering nearby.

There are many things missing where I live. In my living room, there's a stand in the far corner where there used to be a television. Wires still dangle from the walls there. It was a smart TV that connected to my Netflix and social media accounts, and it had a microphone and camera. In my room, there is a nightstand with a drawer that is lined with a special metallic fabric that prevents any devices in the drawer from sending or receiving electronic signals. As part of my bedtime ritual, I leave my devices in there. Across the room in my closet are my old electronics from my life before. An unplugged Amazon Alexa sits alone, buried among a pile of other electronic rubbish—tablets, phones, a smartwatch—that I have yet to dispose of properly. In another box sit the remnants of hard drives, degaussed, smashed up, or acid-bleached after the evidence on them was handed over to the authorities. The data is gone forever, and I might as well throw them out, but I feel oddly sentimental about them.

In the living room, I have an antique wooden desk from an old factory, and on it sits an air-gapped laptop that has never been connected to the Internet. I used it to work through evidence handed over to the House Intelligence Committee. In the drawer is the blank laptop I use for traveling, in case it is searched at the border. My personal computer sits in the living room, encrypted and locked down with a physical U2F key. The cameras are taped, although there is little you can do about the built-in microphone. On the floor, there is a private VPN server connected to the wall, which in turn connects onward onto other servers.

There is a security camera at the entrance of my building that relays data to a security company. I have no idea if any of it is encrypted, so who knows who is watching. When I leave my house, I bring a portable panic button, but I have not yet needed to use it. The NCA put me on a watch list connected to one of my phones. If I call, they will prioritize a response, even if I say nothing to the operator. My backpack always has a portable hardware VPN router in case I need to connect to insecure Wi-Fi, as well as several Faraday cases that I got in pink because it was cute. I often wear a hat, but people will still recognize me, even a year later. Almost daily, I get the question "Are you . . . *the whistleblower*?"

My life now looks like that of a paranoid man, but after being as-

saulted in the street, receiving threats from rogue private security firms, having my hotel room broken in to late at night as I was sleeping, and experiencing two hacking attempts on my email in the past twelve months, it is only sensible to be cautious. When I had my flat checked for security risks, the TV was deemed a risk, as it could be used to watch or listen to me without my ever knowing. As we dismantled it, I smiled at the irony of a TV that watches you.

In the days leading up to the story's publication, when Facebook began sending me legal threats and escalated my case up to its deputy general counsel and vice president, my lawyers realized that the company saw my whistleblowing as a major threat to its business. Having experience on other hacking cases, my lawyers knew what companies backed into a corner were willing to do. But Facebook was different. They did not need to hack me; they could simply track me everywhere because of the apps on my phone—where I was, who my contacts were, who I was meeting.

I disposed of my phone, and my lawyers bought new clean phones that have never touched Facebook, Instagram, or WhatsApp. The terms and conditions of Facebook's mobile app asked for microphone and camera access. Although the company is at pains to deny pulling user audio data *for targeted advertising*, there is nonetheless a technical permission sitting on our phones that allows access to audio capabilities. And I was not an average user: I was the company's biggest reputational threat at the time. At least in theory, audio could be activated, and my lawyers were concerned that the company could listen in on my conversations with them or the police. Facebook already had access to my photos and my camera, which put them in a position to not just listen to me but also to see where I was. Even if I was alone in the bathroom taking a shower, I wasn't *really* ever alone. If my phone was there, so was Facebook. There was no escape.

But getting rid of my phone was not going to be enough. My mom, dad, and sisters all had to remove Facebook, Instagram, and WhatsApp from their phones for the same reason. But Facebook also knew who all my friends were, they knew where we liked to go out, what we wrote about in messages, and they knew where we all lived. Even hanging out with my friends became a risk, as Facebook had access to their phones. If a friend took a photo, Facebook could access it, and

its facial recognition algorithms could, at least in theory, detect my face in the photos sitting on other people's phones, even if they were strangers to me.

As I was getting rid of my old electronics, my friends joked that it was as if I was exorcising the demons inside the machines, and one friend even brought over some sage to burn *just in case*. A funny gesture, of course, but in a way it really was an exorcism. We now live in a world where there are invisible spirits made of code and data that have the power to watch us, listen to us, and think about us. And I wanted these specters gone from my life.

ON MARCH 16, 2018, a day before *The Guardian* and *The New York Times* published my story, Facebook announced that it was banning me from not only Facebook but also Instagram. Facebook had refused to ban white supremacists, neo-Nazis, and other armies of hate, but it chose to ban me. The company demanded that I hand over my phone and personal computer and said that the only way for me to be reinstated was, in effect, to give them the same information I was providing the authorities. Facebook behaved as if it were a nation-state, rather than a company. The firm did not seem to understand that I was not the subject of investigation—*they were*. My lawyers advised me to refuse their demands, so as not to interfere with a lawful police and regulatory investigation. Later, when I was working with the authorities, the ban made it far more difficult to hand over evidence that was sitting in my Facebook account, and the investigation into what happened during the Brexit referendum suffered as a result.

They say you appreciate something only when it's gone, and it was only when I was erased from Facebook that I truly realized how frequently my life touched their platform. Several of my phone's apps stopped working—a dating app, a taxi app, a messaging app—because they used Facebook authentication. Subscriptions and accounts I had on websites failed for the same reason. People often talk about a dualism: the cyber world and our "real lives." But after having most of my digital identity confiscated, I can tell you they are not separate. When you are erased from social media, you lose touch with

people. I stopped getting invited to parties—not intentionally, but because those invites always happened on Facebook or were posted on Instagram. Friends who did not have my new phone number found it nearly impossible to get hold of me, except by trying to send an email to my lawyers. When I got through the thick of the whistleblowing, it would only be in coincidental encounters at clubs or bars that I would make contact with people I had not seen in months.

And now, when guys on dating apps ask to check out my Instagram profile, it starts an awkward explanation about how I was banned—and that I'm not catfishing, I promise. It's as if my identity has been confiscated and people no longer believe that I am who I say I am. Sometimes I get recognized as *that guy,* and people worry that someone might start watching them if they decide to meet me. I always tell them that they needn't worry, because these companies are already tracking them 24/7. This ban was nothing more than a dick move by Facebook, and it felt like trolling by frightened bullies. For me, it created at most an annoying personal hassle and was not nearly as consequential to my life as the kinds of retaliation that other whistleblowers have experienced. (Not to mention the degree of damage to modern society that the platform had already aided and abetted.) But it showed me just how integral my online identity had become to so many facets of my life—and that my identity was afforded no due process rights or an impartial adjudication. Four days after my ban, during an emergency debate in Parliament, the British secretary of state for culture said that Facebook's ability to unilaterally ban whistleblowers was "shocking," because it raised serious questions about whether a company should be able to wield this kind of unchecked power.

Hundreds of millions of Americans have entered into Facebook's invisible architecture thinking it was an innocuous place to share pics and follow their favorite celebrities. They were drawn into the convenience of connecting with friends and the ability to fend off boredom with games and apps. Users were told by Facebook that the enterprise was about bringing people together. But Facebook's "community" was building separate neighborhoods just for *people who look like them.* As the platform watched them, read their posts, and studied how they interacted with their friends, its algorithms would then make decisions about how to classify users into digital neighborhoods

of *their kind*—what Facebook called their "Lookalikes." The reason for this, of course, was to allow advertisers to target these homogeneous Lookalikes with separate narratives just for people of their kind. Most users would not know their classification, as the other neighborhoods of people who did not look like them would remain unseen. The segmentation of Lookalikes, not surprisingly, pushed fellow citizens further and further apart. It created the atmosphere we are all living in now.

As the birthplace of social media, America was eased into the new digital commons of newsfeeds, followers, likes, and shares. And, as with the incremental effects of climate change on our shorelines, forests, and wildlife, it can be hard to fully picture the scale of change of something that envelops us. But there are cases where we can see the stark effects of social media, cases where it suddenly hits a country in full force. In the mid-2010s, Facebook entered into Myanmar and grew rapidly, quickly reaching 20 million users in a country of 53 million people. Facebook's app came preinstalled on many smartphones sold in the country, and market research identified the site as one of the primary sources of news for Burmese citizens.

In August 2017, hate speech surged on Facebook targeting the Rohingya, a predominantly Muslim minority group in Myanmar, with narratives of a "Muslim-free" Myanmar and calls for ethnic cleansing of the region going viral. Much of this was propaganda created and disseminated by military personnel conducting information operations. After Rohingya militants launched a coordinated attack on the police, the Burmese military capitalized on a surge in support they received online and proceeded to systematically kill, rape, and maim tens of thousands of Rohingya. Other groups joined in the slaughter, and calls to action to murder Rohingya continued to go out on Facebook. Rohingya villages were burned and more than 700,000 Rohingya refugees were forced across the border into Bangladesh. Facebook was warned repeatedly by international and local organizations about the situation in Myanmar. The company banned a Rohingya resistance group from the platform but left the military and pro-government groups on the site, which enabled them to continue spreading hate propaganda. This was despite what United Nations officials called a "textbook example of ethnic cleansing."

In March 2018, the U.N. concluded that Facebook had played a "determining role" in the ethnic cleansing of the Rohingya people. Violence was enabled by Facebook's frictionless architecture, propelling hate speech through a population at a velocity previously unimaginable. Facebook's apathetic response was positively Orwellian. "There is no place for hate speech or content that promotes violence on Facebook, and we work hard to keep it off our platform," read Facebook's statement about its facilitating role in the ethnic cleansing of forty thousand human beings. It seemed for all the world that if you wanted to maintain an oppressive regime, Facebook would be an excellent company to turn to.

What was supposed to be so brilliant about the Internet was that people would suddenly be able to erode all those barriers and talk to anyone, anywhere. But what actually happened was an amplification of the same trends that took hold of a country's physical spaces. People spend hours on social media, following people like them, reading news articles "curated" for them by algorithms whose only morality is click-through rates—articles that do nothing but reinforce a unidimensional point of view and take users to extremes to keep them clicking. What we're seeing is a *cognitive segregation,* where people exist in their own informational ghettos. We are seeing the segregation of our realities. If Facebook is a "community," it is a gated one.

Shared experience is the fundamental basis for solidarity among citizens in a modern pluralistic democracy, and the story of the civil rights movement is, in part, the story of being able to share space together: being in the same part of the movie theater or using the same water fountain or bathroom. Segregation in America has always manifested itself in insidiously mundane ways—through separate bus seats, water fountains, schools, theater tickets, and park benches. And perhaps now on social media. For Rosa Parks, being ordered to give up her bus seat was just one of the countless ways white America systematically ensured that her dark skin was separated and unseen—that she remained *the other,* not part of *their* America. And although we no longer allow buildings to segregate their entrances based on a guest's race, segregation rests at the heart of the architectures of the Internet.

From social isolation comes the raw material of both conspira-

cism and populism: *mistrust*. Cambridge Analytica was the inevitable product of this balkanized cyberspace. The company was able to get its targets addicted to rage only because there was nothing to prevent it from doing so—and so, unimpeded, the company drowned them in a maelstrom of disinformation, with predictably disastrous results. But simply stopping CA is not enough. America's newfound crisis of perception will only continue to worsen until we address the underlying architectures that got us here. And the consequences of inaction would be dire. The destruction of mutual experience is the essential first step to *othering*, to denying another perspective on what it means to be *one of us*.

Steve Bannon recognized that the "virtual" worlds of the Internet are so much more real than most people realize. Americans check their phones on average fifty-two times per day. Many now sleep with their phones charging beside them—they sleep with their phones more than they sleep with people. The first and last thing they see in their waking hours is a *screen*. And what people see on that screen can motivate them to commit acts of hatred and, in some cases, acts of extreme violence. There is no such thing as "just online" anymore, and online information—or disinformation—that engages its targets can lead to horrific tragedies. In response, Facebook, like the NRA, evades its moral responsibility by invoking the same kind of "Guns don't kill people" argument. They throw up their hands and claim they can't control how their users abuse their products, even when mass murder results. *If ethnic cleansing is not enough for them to act, what is?* When Facebook goes on yet another apology tour, loudly professing that "we will try harder," its empty rhetoric is nothing more than the *thoughts and prayers* of a technology company content to profit from a status quo of inaction. For Facebook, the lives of victims have become an externality of their continued quest to *move fast and break things*.

When I came out as a whistleblower, the alt-right's digital rage machine turned its sights to me. In London, enraged Brexiteers pushed me into oncoming traffic. I was followed around by alt-right stalkers and had photos of me at clubs with my friends published on alt-right websites with information about where to find me. When it came time to testify at the European Parliament, conspiracies about Facebook's

critics were beginning to percolate through forums of the alt-right. As I testified, there were chants of *"Soros, Soros, Soros"* in the back. As I was leaving the European Parliament, a man came up to me on the street, shouting *"Jew money!"* At the time, these narratives seemed to come out of nowhere. Later, it emerged that Facebook, in a panic about its PR crisis, had hired the secret communications firm Definers Public Affairs, which subsequently leaked out fake narratives filled with anti-Semitic tropes about its critics being part of a George Soros–funded conspiracy. Rumors were seeded on the Internet and, as I discovered personally, its targets took it as a cue to *take matters into their own hands*.

IN FEBRUARY 2013, a Russian military general named Valery Gerasimov wrote an article challenging the prevailing notions of warfare. Gerasimov, who was Russia's chief of the general staff (roughly equivalent to chairman of the U.S. Joint Chiefs of Staff), penned his thoughts in the *Military-Industrial Kurier* under the title "The Value of Science Is in the Foresight"—a set of ideas that some would later dub the Gerasimov Doctrine. Gerasimov wrote that the "'rules of war' have changed" and that "the role of nonmilitary means of achieving political and strategic goals has grown." He addressed the uses of artificial intelligence and information in warfare: "The information space," he wrote, "opens wide asymmetrical possibilities for reducing the fighting potential of the enemy." Essentially, Gerasimov took the lessons of the Arab Spring uprisings, which were propelled by information sharing on social media, and urged military strategists to adapt them. "It would be easiest of all to say that the events of the 'Arab Spring' are not war, and so there are no lessons for us—military men—to learn. But maybe the opposite is true—that precisely these events are typical of warfare in the twenty-first century."

Gerasimov's article was followed by another Russian military strategy paper, this one written by Colonel S. G. Chekinov and Lieutenant General S. A. Bogdanov. Their paper took Gerasimov's idea even further: The authors wrote that it would be possible to attack an adversary by "obtain[ing] information to engage in propaganda from servers of the Facebook and [T]witter public networks" and that, with

these "powerful information technologies at its disposal, the aggressor will make an effort to involve all public institutions in the country it intends to attack, primarily the mass media and religious organizations, cultural institutions, non-governmental organizations, public movements financed from abroad, and scholars engaged in research on foreign grants." At the time, it was a radical new idea. Read today, it is a precise blueprint for Russia's interference in the 2016 election.

The history of warfare is the history of new inventions and strategies, many of which were born out of necessity. By most metrics, Russia's military is significantly weaker than that of the United States. The U.S. military budget, at $716 billion, is more than ten times that of Russia. The United States has 1.28 million active military personnel, as compared with Russia's 1 million; has more than 13,000 total aircraft, as compared with Russia's 4,000; and has twenty aircraft carriers, whereas Russia has one. By all existing conventional measures, Moscow would never again be competitive with the United States in terms of "great powers" warfare, and Vladimir Putin knew it. So the Russians had to devise another way to regain the advantage—one that had nothing to do with the physical battlespace.

It's difficult for military strategists to envision new forms of battle when they're focused on those at hand. Before the advent of flight, military commanders cared only about how to wage combat on land or at sea. It wasn't until 1915, when the French pilot Roland Garros flew a plane jerry-rigged with a machine gun, that military strategists realized that war could actually be waged from the skies. Then, once aircraft began engaging in attacks, army units on the ground pivoted as well, creating compact, rapid-fire antiaircraft guns. And so the evolution of war continued.

Information warfare has evolved in similar fashion. At first, no one could have imagined that Facebook or Twitter could be battlefield tools; warfare was waged on the ground, in the air, at sea, and potentially in space. But the fifth domain—cyberspace—has proved to be a fruitful battleground for those who had the imagination and foresight to envision using social media for information warfare. You can draw a straight line from the groundwork laid by Gerasimov, Chekinov, and Bogdanov, right through the actions of Cambridge Analytica, to the victories of the Brexit and Trump campaigns. In

only five or so years, the Russian military and state have managed to develop the first devastatingly effective new weapon of the twenty-first century.

They knew it would work, because companies such as Facebook would never take the "un-American" step of reining in their users. So Russia didn't have to disseminate propaganda. They could just get the Americans to do it themselves, by clicking, liking, and sharing. Americans on Facebook did the Russians' work for them, laundering their propaganda through the First Amendment.

But this new era of scaled disinformation is not confined to the realm of politics. Companies like Starbucks, Nike, and other fashion brands have found themselves targets of Russian-sponsored disinformation operations. When brands make statements that wade into existing social or racial tensions, there have been several identified instances in which Russian-sponsored fake news sites, botnets, and social media operations have activated to weaponize these narratives and provoke social conflict. In August 2016, the football player Colin Kaepernick refused to stand for the American national anthem to protest systemic racism and police brutality toward African Americans and other minorities in the United States. The fashion brand Nike, Kaepernick's sponsor, stood behind the athlete, and a controversy ensued about Nike's response. But unknown to many at the time, Russian-linked social media accounts began to spread and amplify existing hashtags promoting a Nike boycott within hours of the scandal emerging. Some of this Russian-amplified content eventually made it into mainstream news, which helped legitimize the Nike boycott narrative as a purely homegrown protest. Cybersecurity firms also identified fake Nike coupons originating from alt-right groups that targeted African American social media users with offers like "75% off all shoes for people of color." The coupons were intended to create scenarios in which unwitting African American customers would try to use the coupons in a Nike store, where they would be refused. In the age of viral videos, this scenario could in turn create "real" footage showcasing a racist trope of an "angry black man" demanding free stuff in a store. So why would these disinformation operations target a fashion company and attempt to weaponize its brand? Because the objective of this hostile propaganda is not simply

to interfere with our politics, or even to damage our companies. The objective is to tear apart our social fabric. They want us to hate one another. And that division can hit so much harder when these narratives contaminate the things we care about in our everyday lives—the clothes we wear, the sports we watch, the music we listen to, or the even coffee we drink.

We are all vulnerable to manipulation. We make judgments based on the information available to us, but we are all susceptible to manipulation when our access to that information becomes mediated. Over time, our biases can become amplified without our even realizing it. Many of us forget that what we see in our newsfeeds and our search engines is already moderated by algorithms whose sole motivation is to select what will engage us, not inform us. With most reputable news sources now behind paywalls, we are already seeing information inch toward becoming a luxury product in a marketplace where fake news is always free.

In the last economic revolution, industrial capitalism sought to exploit the natural world around us. It is only with the advent of climate change that we are now coming to terms with its ecological externalities. But in this next iteration of capitalism, the raw materials are no longer oil or minerals but rather commodified attention and behavior. In this new economy of surveillance capitalism, *we are the raw materials*. What this means is that there is a new economic incentive to create substantial informational asymmetries between platforms and users. In order to be able to convert user behavior into profit, platforms need to know everything about their users' behavior, while their users know nothing of the platform's behavior. As Cambridge Analytica discovered, this becomes the perfect environment to incubate propaganda.

With the advent of home automation hubs such as Amazon Alexa and Google Home, we are seeing the first step toward the eventual integration of cyberspace with our temporal physical reality. Fifth-generation (5G) mobile and next-generation Wi-Fi are already being rolled out, laying the foundations for the "Internet of Things" (IoT) to become the new norm, where household appliances big and small will become connected to high-speed and ubiquitous Internet networks. These mundane devices, whether they are a refrigerator, a

toothbrush, or a mirror, are envisaged to use sensors to begin tracking users' behavior inside their own homes, relaying the data back to service providers. Amazon, Google, and Facebook have already applied for patents to create "networked homes" that integrate in-home IoT sensors with online marketplaces, ad networks, and social profiles. In this future, Amazon will know when you pop an aspirin, and Facebook will watch your kids play in the living room.

Fully integrated with intelligent information networks, this new environment will be able to watch us, think about us, judge us, and seek to influence us by mediating our access to information—where "it" can see us, but we cannot see "it." For the first time in human history, we will immerse ourselves in *motivated spaces* influenced by these silicon spirits of our making. No longer will our environment be passive or benign; it will have intentions, opinions, and agendas. No longer will our homes be a sanctuary from the outside world, for an ambient presence will persist throughout each connected room. We are creating a future where our homes will think about us. Where our cars and offices will judge us. Where doors become the doormen. Where we have created the demons and angels of the future.

This is the dream that Silicon Valley has for us all—to surround us at every minute and everywhere. In Cambridge Analytica's quest for informational dominance, it was never going to be satisfied with just social data sets and had already begun to build relationships with satellite and digital TV providers. After tapping into connected televisions, Cambridge Analytica planned to find a way to integrate with sensors and smart devices in people's homes. Imagine a future where a company like Cambridge Analytica could edit your television, talk to your children, and whisper to you in your sleep.

THE FOUNDATION OF OUR legal system is contingent upon the notion that our environment is passive and inanimate. The world surrounding us may *passively* influence our decisions, but such influence is *not motivated*. Nature or the heavens do not *choose* to influence us. Over centuries, the law has developed several fundamental presumptions about human nature. The most important of these is the notion of human agency as an irrefutable presumption in the law—that hu-

mans have the capacity to make rational and independent choices on their own accord. It follows that the world does not make decisions for humans, but that humans make decisions inside of that world.

This notion of human agency serves as the philosophical basis for criminal culpability, and we punish transgressors of the law on the grounds that they made a condemnable choice. A burning building may indeed harm people, but the law does not punish that building, as it has no agency. And so human laws regulate human acts, and not the motivations or behaviors of their surroundings. The corollaries to this are the fundamental rights we have. During the Enlightenment, the fundamental rights of people were articulated as core entitlements to protect the *exercise of human agency*. The rights to life, liberty, association, speech, vote, and conscience are all underpinned with a *presumption of agency,* as they are outputs of that agency. But agency itself has not been articulated as a right per se, as it has always been presumed to exist simply by virtue of our personhood. As such, we do not have an express *right to agency* that is *contra mundum*—that is, a right to agency that is exercisable *against the environment itself.* We do not have a right against the heavens or the undue influence of motivated and thinking spaces to mediate the exercise of our agency. At the time of America's founding, a situation where our agency could be manipulated by a motivated and thinking environment was never contemplated as a possibility. For the Founding Fathers, this would have been a power known only to God.

We can already see how algorithms competing to maximize our attention have the capacity to not only transform cultures but redefine the experience of existence. Algorithmically reinforced "engagement" lies at the heart of our outrage politics, call-out culture, selfie-induced vanity, tech addiction, and eroding mental well-being. Targeted users are soaked in content to keep them clicking. We like to think of ourselves as immune from influence or our cognitive biases, because we want to feel like we are in control, but industries like alcohol, tobacco, fast food, and gaming all know we are creatures that are subject to cognitive and emotional vulnerabilities. And tech has caught on to this with its research into "user experience," "gamification," "growth hacking," and "engagement" by activating ludic loops and reinforcement schedules in the same way slot machines do. So far, this

gamification has been contained to social media and digital platforms, but what will happen as we further integrate our lives with networked information architectures designed to exploit evolutionary flaws in our cognition? Do we really want to live in a "gamified" environment that engineers our obsessions and plays with our lives as if we are inside its game?

The underlying ideology within social media is not to enhance choice or agency, but rather to narrow, filter, and *reduce* choice to benefit creators and advertisers. Social media herds the citizenry into surveilled spaces where the architects can track and classify them and use this understanding to influence their behavior. If democracy and capitalism are based on accessible information and free choice, what we are witnessing is their subversion from the inside.

We risk creating a society obsessive about remembering, and we may have overlooked the value of forgetting, moving on, or being unknown. Human growth requires private sanctuaries and free spaces where we can experiment, play, dabble, keep secrets, transgress taboos, break our promises, and contemplate our future selves without consequence to our public lives until we decide to change in public. History shows us that personal and social liberation begins in private. We cannot move on from our childhoods, past relationships, mistakes, old perspectives, old bodies, or former prejudices if we are not in control of our privacy and personal development. We cannot be free to choose if our choices are monitored and filtered for us. We cannot grow and change if we are shackled to who we once were or who we thought we were or how we once presented ourselves. If we exist in an environment that always watches, remembers, and labels us, according to conditions or values outside our control or awareness, then our data selves may shackle us to histories that we prefer to move on from. Privacy is the very essence of our power to decide who and how we want to be. *Privacy is not about hiding—privacy is about human growth and agency.*

But this is not merely about privacy or consent. This is about who gets to influence our truths and the truths of those around us. This is about the architectures of manipulation we are constructing around our society. And herein lies the lesson of Cambridge Analytica. To understand the harms of social media, we have to first understand

what it is. Facebook may call itself a "community" to its users, or a "platform" to regulators, but it is not a service, in the same way a building is not a service. Even if you don't understand exactly how cyberspace works, it is important to understand that it now surrounds you. Every connected device and computer is part of an interconnected information architecture—and shapes your experience of the world. The most common job titles in most Silicon Valley companies are *engineer* and *architect,* not *service manager* or *client relations.* But unlike engineering in other sectors, tech companies do not have to perform safety tests to conform to any building codes before releasing their products. Instead, platforms are allowed to adopt *dark pattern designs* that deliberately mislead users into continual use and giving up more data. Tech engineers intentionally design confounding mazes on their platforms that keep people moving deeper and deeper into these architectures, without any clear exit. And when people keep clicking their way through their maze, these architects delight in the increase in "engagement."

Social media and Internet platforms are not services; they are architectures and infrastructures. By labeling their architectures as "services," they are trying to make responsibility lie with the consumer, through their "consent." But in no other sector do we burden consumers in this way. Airline passengers are not asked to "accept" the engineering of planes, hotel guests are not asked to "accept" the number of exits in the building, and people are not asked to "accept" the purity levels of their drinking water. And as a former club kid, I can tell you that when bars or concerts are over capacity and heaving with ravers, fire inspectors will order those *consenting customers* to leave a building if the conditions become manifestly unsafe.

Facebook may say: If you don't like it, don't use it. But there are no comparable alternatives to the dominant players on the Internet, just as there are no alternatives to electric, telecommunications, or water companies. To reject the use of platforms like Google, Facebook, LinkedIn, and Amazon would be to remove oneself from modern society. How are you going to get a job? How are you going to get information? How are you going to socialize with people? These companies love to talk about consumer choice, when they know that they have

done everything in their power to become a necessary part of most people's lives. Getting users to click "accept" after presenting them with a novella's worth of dense legalese (almost twelve thousand words in Facebook's case) is nothing but *consent-washing*. These platforms are purpose-built to run user consent through a blender. No one opts out of these platforms, because users have no other choice but to accept.

When Facebook banned me, they did not simply deactivate my account; they erased my entire presence on Facebook and Instagram. When my friends tried to look up old messages I had sent, nothing came up: My name, my words—everything—had disappeared. I became a shadow. Banishment is an ancient punishment to rid a society of its criminals, heretics, and political radicals who jeopardized the power of the state or church. In ancient Athens, people could be banished from society for ten years for any reason with no opportunity for appeal. In the Stalinist period of the Soviet Union, *enemies of the state* would not just disappear; all remnants of their existence—photos, letters, news references—would be erased and cleansed from the annals of official history. Throughout history, the powerful have used social memory and collective forgetting as a powerful weapon to crush dissent and correct their preferred histories to shape the realities of the present. And if we want to understand why these technology companies behave this way, we should listen to the words of those who built them. Peter Thiel, the venture capitalist behind Facebook, Palantir, and PayPal, spoke at length about how he no longer believes "that freedom and democracy are compatible." And in elaborating his views on technology companies, he expounded on how CEOs are the new monarchs in a techno-feudal system of governance. We just don't call them monarchies in public, he said, because "anything that's not democracy makes people uncomfortable."

The philosophical basis of authoritarianism rests in the creation of total certainty within society. The politics of certainty repositions the notion of freedom, where *freedoms from* replace *freedoms to*. Strict rules and laws are coercively enforced to govern and shape the behavior, thoughts, and actions of the polity. And the first tool of authoritarian regimes is always informational control—both in the

gathering of information on the public through surveillance and the filtration of information to the public through owned media. In its early days, the Internet seemed to pose a challenge to authoritarian regimes, but with the advent of social media, we are watching the construction of architectures that fulfill the needs of every authoritarian regime: surveillance and information control. Authoritarian movements are possible only when the general public becomes habituated to—and numbed by—a new normal.

THE INTERNET HAS FRUSTRATED these old assumptions about the law and the polity that it governs. The Internet is both everywhere and nowhere—it is physically dependent on servers and cables, but it exists without a single location of primary residence. This means that a single digital act could partially occur in countless physical locations simultaneously, or an action in one place could result in effects in another place. This is because the Internet is a type of *hyperobject*—like our climate and biosphere, the Internet surrounds us and we live within it. The tech community often call their platforms "digital ecosystems," with an implicit recognition that their construction is a digital container or realm for at least part of our lives to exist within. We cannot see it or touch it, but we know it exists around us by its effects.

Often I encountered police investigators unfamiliar with data crime using false analogies about finding the "murder weapon," the "location of the body," and linear "chains of causation." But data crimes are crimes that usually don't happen in one specific place. Data crime can often behave like pollution—it's everywhere generally, but nowhere specifically. Data is completely fungible and intangible, as it is merely a representation of information. It can be stored simultaneously in distributed servers around the world; where even when it's in a place, it's never entirely in that place. Servers based in country A handling data subjects in country B could be accessed by a person in country C and deployed on a platform in country D after receiving instructions from a company in country E with financing from country F. This was the nature of Cambridge Analytica's complex setup.

Even if serious harms were clearly incurred, such as hacking, data theft, menacing threats, or deception, it would be unclear who could be held responsible, and our known systems for assessing culpability were entirely incapable of the job.

We like to imagine our government as the captain of the ship, but when the ocean itself changes, our captains may find themselves unprepared and unable to navigate. In July 2018, Britain's Electoral Commission found that the Vote Leave campaign had broken the law, illegally coordinating with BeLeave. On March 30, 2019—one year after the Brexit whistleblowing stories broke—the Vote Leave campaign officially dropped its appeal of the EC's findings and fines, essentially admitting to what it had done. Some have asked: Why should we care so much about a mere £700,000? Let's be clear on this point: *Vote Leave's scheme was the largest known breach of campaign finance law in British history.* But even if it wasn't, elections, like a 100-meter sprint in the Olympics, are zero-sum games, where the winner takes all. Whoever comes first, even if it's by just a few votes or milliseconds, wins the whole race: They get to sit in the public office. They get the gold medal. They get to name your Supreme Court justices. They get to take your country out of the European Union.

The only difference, of course, is that if you are caught cheating in the Olympics, you get disqualified and lose your medal. There are no discussions of whether the doped athlete "would have won anyway"—the integrity of the sport demands a clean race. But in politics, we do not presume integrity as a necessary prerequisite to our democracy. There are harsher punishments for athletes who cheat in sport than for campaigns that cheat in elections. Though they won by only 3.78 percent, the Brexiteers claimed the entire "will of the people" for themselves—and even when Trump *lost* the popular vote by 2.1 percent, he too claimed victory. Despite proven cheating, Vote Leave did not have its Brexit medal taken away. No one was disqualified from running in future campaigns, and Vote Leave's two leaders, Boris Johnson and Michael Gove, were both allowed to run for prime minister. Crimes waged against our democracy were not considered by the political class to be "real crime." Many framed these transgressions as being on par with a parking fine, despite the very real harm

we face when our civic institutions can be so easily undermined by criminals and hostile foreign states seeking to wage electoral terrorism on our society. And, of course, the most powerful people in Britain and America took the position that these crimes didn't even happen—rather, they were a "hoax," the invention of the bitter opponents they had vanquished. This, in the face of what were once known as "facts" and "reality."

You'd think that after pulling off a conspiracy to hack a world leader's private emails and medical records, bribe ministers, blackmail targets, and shower voters with menacing videos of gruesome murders and threats, there would be some kind of legal consequence. But there were no consequences for anyone involved in Cambridge Analytica's African projects. It was too difficult to establish *jurisdictionality*—whether or not "enough" of the crime happened in Britain to warrant prosecution in the English courts. Their servers were all over the world, the meetings happened in different countries, the hackers were based in yet another country, and Cambridge Analytica only *received* the hacked material in London but did not *request* the hacked material in the U.K. Even though there were several witnesses to what happened, Cambridge Analytica simply got away with it. In fact, one of the managers from the Nigeria project eventually moved on to work in a senior position at the U.K. Cabinet Office on foreign affairs projects, sitting in the highest levels of the British government.

In America there were no consequences for Cambridge Analytica, either. The company knowingly and willfully violated the Foreign Agents Registration Act. It conducted operations to suppress African American voters. It defrauded Facebook users and menaced them with disgusting content. It exposed hundreds of millions of private records of American citizens to hostile foreign states. And yet nothing happened, because Cambridge Analytica was set up for jurisdictional arbitrage. Tax evasion frequently involves setting up shell companies on tropical islands all around the world in an attempt to launder money through a complex enough chain of countries and companies, each with its own unique rules, that authorities lose track of where the money is. This is possible because money, like data, is a completely fungible asset and can be instantly moved through a global finance system. What Cambridge Analytica did was use complex

Canadian Parliament opened its own inquiry into AIQ's role in Brexit, to help the U.K. authorities compel answers from AIQ after the firm had successfully avoided its jurisdiction by remaining in Canada.

It turns out cheating is a pretty good strategy to win, as there are very few consequences. The Electoral Commission later conceded that even if the vote was won with the benefit of illegal data or illegal financing, the result still stands. Facebook refused to hand over the full details of what happened on its platform during Brexit or the number or types of voters who were profiled and targeted by illegal campaigns. Mark Zuckerberg defied three requests to testify before the British Parliament, and when fifteen national parliaments, collectively representing almost one billion citizens across six continents, banded together in a joint request to interview Zuckerberg, even over the phone, he still turned them down—twice. It seemed that Zuckerberg's time was more valuable than that of legislatures representing almost one seventh of the human race. Facebook learned that, despite the wrath of the media storm, there were actually very few consequences for simply ignoring the parliaments of the world—the company learned that it could behave like a sovereign state, immune from their scrutiny. Facebook eventually sent its chief technology officer, Mike Schroepfer, to the British parliamentary inquiry, but he failed to fully answer forty questions according to a subsequent statement by the committee. But what was perhaps most revealing about the performance was the lack of contrition on the part of the company. When Schroepfer was asked if Facebook's first instinct to send journalists legal threats was bullying behavior, the Facebook CTO replied that "my understanding is that this is common practice in the U.K." After being pressed by the incredulous MPs, Schroepfer acquiesced and finally apologized, saying that he was "sorry that journalists feel we are attempting to prevent the truth coming out."

Of all the individuals who could have been formally punished in this saga, it was sad for me to see that one of the only people to face a sanction was Darren Grimes, the twenty-two-year old Vote Leave intern. As frustrating as his situation was, the archaic legislation meant that he was personally liable for electoral offenses. The commission levied a £20,000 fine against him personally and referred his case to the police. He subsequently succeeded in an appeal against

that finding, although further appeals may yet be brought by the Electoral Commission. The campaign, Vote Leave, was fined £61,000, part of which reflected their refusal to cooperate with the regulator. Vote Leave dropped their appeal and that sanction, at least, remains.

It was incredibly hard to watch what happened to Grimes, who had his life torn up over a scheme that others had orchestrated. We had hoped that he would come forward with Sanni, Gettleson, and me, but Grimes defended the scheme until the very end. He panicked and broke down every time Sanni broached the topic, and did not want to accept that he had been used by the people he trusted. Grimes was set up to become their fall guy, and Vote Leave could not have asked for a better candidate. As much as he defended his old bosses' actions, Grimes was their captive victim. They transformed him from a talented, liberal, and artistic student into a public shill for their alt-right causes, in exchange for help with legal fees.

Several weeks after the story went public, Shahmir Sanni was terminated from his job at the TaxPayers' Alliance, a think tank, after pressure from Conservative Party advisers. The alliance later admitted to his lawyers that they unlawfully fired Sanni in retaliation for what they called his "philosophical belief in the sanctity of British democracy." Although the question of Parkinson's job at 10 Downing Street was raised several times in Parliament, Parkinson kept his job and faced no consequences for using the press office of the prime minister to out his former intern as being gay. And Mark Gettleson, who provided evidence to authorities on both sides of the Atlantic, was pushed out of his new job at a mobile app company over reputational concerns about his whistleblowing.

In March 2018, just before the staff at Cambridge Analytica learned about the impending demise of their firm, Alexander Nix allegedly emptied £6 million from company accounts, preventing severance pay from being issued to its former staff. He later denied this at Parliament, saying that the withdrawn money was "in exchange for unbooked services" and that he intended on paying some of it back. Nix was shunned by many of his former business partners and peers in the private clubs of Pall Mall, but, as a man of exceptional wealth, he could continue living off his inheritance in his mansion in London's Holland Park. Nothing much happened to him beyond some cringe-

worthy public hearings in Parliament in which he blamed the "global liberal media" for his company's demise.

After I came forward with the Cambridge Analytica story, Brittany Kaiser rebranded herself as a whistleblower and hired a PR manager to start booking interviews. She attended a parliamentary hearing in which she admitted to being involved in the Nigeria project, said that Cambridge Analytica likely retained Facebook data, and outlined her relationship with Julian Assange. (Later, it would emerge that she visited Assange in the Ecuadorian embassy in London.) Immediately after Kaiser's testimony concluded, Nix texted her, "Well done Britt, it looked quite tough and you did ok. ;-)." The next day, she flew to New York and held a press conference to plug her new data project, which launched something called the Internet of Value Omniledger, apparently intended to unleash our "data freedom."

Like Kaiser, several other former executives from Cambridge Analytica went on to found their own data companies. CA's former head of product Matt Oczkowski founded a firm called Data Propria (Latin for "Personal Data") and brought CA's chief data scientist David Wilkinson with him. The firm has stated that it will focus on targeting "motivational behavioral triggers" and had already started work for the 2020 U.S. presidential campaign of Donald Trump. Mark Turnbull, the former managing director of Cambridge Analytica, joined up with one of the firm's former associates, Ahmad Al-Khatib, to set up Auspex International, which they described as an "ethically based" and "boutique geopolitical consultancy."

My biggest regret was Jeff Silvester. I can't even begin to put into words how maddening and disheartening it was for me to sit with the knowledge about what he and AIQ had done. He was my mentor when I was a teenager and the man who helped me enter politics in the first place. He had supported me, encouraged me, and nurtured my talents so I could grow. And I just still cannot understand how he could have let himself continue working for something so wrong, so colonial, so illegal, and so evil. I tried to talk to him, and I told him to be open with *The Guardian,* but I failed. He could have come clean. He could have cooperated with the investigations. He knew what AIQ had done was wrong. He knew that the effects of his work had profound

consequences for the future of an entire nation and the rights of millions of people. Having to choose between a deep friendship and reporting a crime is torture, because no matter what you choose, you'll feel profound regret. But I had no choice but to betray him. On the day *The Guardian* sent out the right-to-reply letters to all of the accused parties, I agonized over what was happening the entire day, waiting to hear anything. When he received his letter, Silvester finally learned of the choice I had made, and he began to realize what was about to happen to him. His final text message to me was simply "Wow."

Walking into my first parliamentary hearing, to the sound of rapidly clicking cameras and shouted questions, I felt unexpectedly at ease. Allen sat behind me, occasionally passing me notes of legal advice. We had prepared for hours, going through the evidence, and I had the special protection of parliamentary privilege—meaning that nothing I said could be used in civil or criminal proceedings. The hearing caused a wave of legislative attention around the world, and the DCMS committee chair, Damian Collins, began organizing international joint hearings among fifteen national parliaments. There were debates on the floor of the House of Commons and cross-party support for regulating social media. For a couple of months, it seemed as if Britain was leading the way in challenging the power of Silicon Valley.

But then, in October 2018, seven months after the Cambridge Analytica scandal rocked Facebook, the company announced that it was making a major hire: a new apologist in chief to world governments. Facebook's new global spin doctor was going to be Nick Clegg, the former leader of the Liberal Democrats and deputy prime minister of the United Kingdom—the same man I used to work for in my days at LDHQ. Ironically, it was Clegg who had once vowed that he would go to prison before registering in a pilot national identity database. But he was also the guy whose tenure as deputy prime minister became in effect a five-year apology tour after he broke a host of key promises in the coalition government. And the more I thought about it, the more the pairing seemed to be a match made in heaven. Both Zuckerberg and Clegg had built their careers on compromising their principles, both suffered catastrophic blows of public confidence after they ig-

nored their promises to users or voters, and both stopped being cool in 2010. When Channel 4 asked me for comment on camera after Clegg's appointment was announced, all I could think to say was "This is bullshit." They aired the comment, albeit with a bleep.

On May 24, 2019, Prime Minister Theresa May announced her intention to resign, triggering an internal leadership race within the Conservative Party. In the United Kingdom, if a prime minister resigns mid-term, the convention is that Her Majesty the Queen appoints the new leader of the governing party as the new prime minister without a general election. This means that the internal party back-roomers, donors, and paid members of the party can bypass an election and choose among themselves who shall lead Britain. On July 23, the members of the Conservative Party decided that the new prime minister would be Boris Johnson, the former foreign secretary and lead advocate for leaving the European Union without any negotiated exit deal (often referred to as a "hard Brexit"). When forming his new government, Johnson appointed Dom Cummings, his former colleague from Vote Leave, to become one of his new senior advisers in 10 Downing Street. It did not seem to matter that Cummings was the director of a campaign that cheated during the very referendum Johnson was now using as the "democratic" basis for leaving the European Union at almost any cost. Only a few months prior to his appointment, Cummings was found to be in contempt of Parliament after ignoring an order to appear before Parliament to answer questions about cheating and the dissemination of fake news in the EU referendum. Although Cummings is one of only a handful of people ever to be formally admonished by a unanimous vote of the House of Commons, the limits of parliamentary authority were tested, at it appears there were very few consequences for Cummings. And slated to join Cummings in the new Johnson government as a new special adviser to Her Majesty's Treasury was Matthew Elliott, the former chief executive of Vote Leave and co-founder of the TaxPayers' Alliance, the lobbying group that fired Sanni in retaliation for his whistleblowing. It looked like a Vote Leave takeover of the British government. During his first Prime Minister's Questions session in the House of Commons, Johnson was asked by opposition members about what was discussed in December 2016, when he met with Cam-

bridge Analytica's CEO, Alexander Nix, when he was Britain's foreign secretary. His response was simply "I have no idea."

Inside Cambridge Analytica, I saw what greed, power, racism, and colonialism looks like up close. I saw how billionaires behave when they want to shape the world in their image. I saw the most bizarre, dark niches of our society. As a whistleblower, I saw what big companies will do to protect their profits. I saw the lengths to which people will go to cover up crimes that others committed for the sake of a convenient narrative. I saw flag-waving "patriots" turn a blind eye to the defacement of the rule of law on the most important constitutional question of a generation. But I also saw all the people who cared and who fought back against a failing system. I saw journalists at *The Guardian, The New York Times,* and Channel 4 all working to bear witness to the crimes committed by Cambridge Analytica and the incompetence of Facebook. I saw my brilliant lawyers outmaneuver every threat that was thrown my way. I saw the kindness of people who came to support me and asked for nothing in return. I saw the tiny Information Commissioner's Office, based in the parish town of Wilmslow, England, use what powers it could to take on an American technology giant—eventually issuing Facebook the maximum fine allowable in law for data breaches.

And I saw members of Congress who were concerned and eager to learn about the brave new world we now find ourselves in. As I left the House Intelligence Committee hearing, emerging from the SCIF with my lawyers and Sanni, I shook hands with the members of the committee and was walked to the security entrance by Congressman Adam Schiff and his aides. They were gracious, and they thanked me for flying to America to help them understand not only Cambridge Analytica but the emerging risks to American elections posed by social media platforms. It would be the last of my testimonies in the United States, but everything felt far from resolved.

On July 24, 2019, the Federal Trade Commission levied a record $5 billion civil penalty against Facebook, and the same day the Securities and Exchange Commission issued notice of an additional $100 million fine. The regulators found that not only did Facebook fail to protect users' privacy, the company misled the public and journalists by issuing false statements that it had seen no evidence of wrongdoing

when it in fact had. The fine was one of the largest imposed by the U.S. government for any violation. In fact, this was the largest ever fine issued to an American company for violating consumers' privacy rights, and was twenty times greater than the largest privacy or data security penalty ever imposed worldwide. However, it was nonetheless seen by investors as good news. The news actually increased Facebook's share value by 3.6 percent, with the market tacitly recognizing that even the law cannot stop the growth of these technology giants.

I would be lying if I didn't admit that I am far more cynical now than before I started this journey. But it hasn't made me more resigned. If anything, it has made me even more radical. I used to believe that the systems we have broadly work. I used to think that there was someone waiting with a plan who could solve a problem like Cambridge Analytica. I was wrong. Our system is broken, our laws don't work, our regulators are weak, our governments don't understand what's happening, and our technology is usurping our democracy.

So I had to learn to find my voice in order to speak up about what I saw was happening. I am hopeful, because I have seen what happens when we find our voices. When *The Guardian* took on this story, many journalists saw it as a series of conspiracy theories. The tech bros of Silicon Valley laughed at the notion that they should be subjected to any scrutiny. Politicos in D.C. and Westminster called the story *niche*. It took the persistence of a team of women at *The Guardian*'s Arts & Culture section and its Sunday paper, *The Observer,* where the blockbuster story appeared. It took the attention of the women who led the investigations at the Information Commissioner's Office and the Electoral Commission. And it took two immigrant queer whistleblowers backed by a steadfast woman lawyer. This story took the leadership of dedicated women, immigrants, and queers to ignite a public awakening about the discreet colonizing power of Silicon Valley and the digital technologies they have created to surround us. We all persisted in raising our voices until the world could finally see what we saw.

Growing up queer, you learn early in life that your existence is outside the norm. We incubate ourselves inside a closet, remaining unknown, and hide our truth until it becomes unbearable. Living in a

closet is painful. It is an act of emotional violence we inflict upon ourselves so as not to discomfort those around us. Queers understand systems of power intimately, and coming out is our transformative act of truth telling. In coming out, we realize the power of speaking our truth to those who may not want to hear it. We reject their comfort and make them listen. Why do so many gays blow whistles at Pride? To get your attention. To announce that we will no longer hide ourselves. To defy hegemonies of the powerful. And, like so many queers who came before me, I had to accept my own truth and come to terms with my inevitable failure to ever become society's notion of a perfect man.

I am a queer whistleblower, and this was my second coming out. Subjecting me to covenants of nondisclosure, I was forced into a new closet, to live in hiding with my uncomfortable knowledge and objectionable truths. I lived my life for two years with a personalized *don't ask, don't tell* policy imposed upon me by powerful companies. If I hoped to avoid any consequences, I was forbidden to reveal myself to others, and I became their little secret. But like other out queers, I am a truth teller, and I chose to be indiscreet with those uncomfortable truths, to stop hiding, to stop being their secret, to face the consequences before me, and to shout out to the world what I know.

The closet is not a literal space; it is a social structure that we as queer people internalize and conform to. The closet is a container whose boundaries are imposed by others who want to control how you behave and present yourself. The closet is invisible, and it is placed upon you by default, never by choice, for others to create a more palatable version of who you are—for *their* benefit, *not yours*. Growing up in a closet means incrementally learning how to *pass* in society—which movements, tones, expressions, perspectives, or uttered desires transgress the norms of those social boundaries imposed upon you. Queer kids learn, little by little, how to restrain their behavior until it becomes almost second nature, until they pass. So incremental are these changes that sometimes you do not even notice how much you have changed your behavior until, one day, you decide to leave that closet. And part of coming out is coming to terms with how much of you has been constructed for you inside that closet, and it can be pain-

ful to realize how much of who you once were was imposed upon you without your awareness or consent. The closet is a place of acquiescing to society in exchange for *passing*, but it is also a place where rage builds as those boundaries and definitions slowly suffocate you until you cannot bear to remain inside that prison.

Coming out is our rejection of the definitions that have been imposed upon us by someone else. The ability to define our identities is extremely powerful, and whether the threats to that power take the form of a social closet or an algorithmic one, we must resist anyone or anything that seeks the power to define or classify who we are for their benefit. Silicon Valley risks creating a new hegemony of identity through its construction of these personalized spaces for each person. And these spaces are nothing but a new closet to define our identities, expressions, and behaviors. In harvesting and processing your data self, algorithms make decisions on how to define you, how to classify you, what you should notice, and who should notice you. But there is a fine line between an algorithm defining you in order to represent *who you really are* and an algorithm defining you to create a self-fulfilling prophecy of *who it thinks you should become.*

People are *already* morphing themselves to fit a machine's idea of who they should be. Some of us are curating ourselves on social media to increase our follower engagement, to the point that who we really are and how we present online become confused and conflated. And when those followers see enough of these curated identities, some of them begin to hate who they are or how they look, and they starve their bodies to conform to a new standard that now surrounds them. Others click on links recommended to them by algorithms, engaging with that content, and get drawn further and further down the rabbit hole of personalization until their worldview changes without their realizing it. What we buy online is now curated based on a profile of us, *defined by something else.* Our worthiness as job, insurance, credit, or mortgage applicants is now based on a profile of us, *defined by something else.* The shows we watch and the music we discover are now preselected based on a profile of us, *defined by something else.* As we move toward the inevitable merger of our physical and digital worlds, more and more of our lives will start to become defined not

by us but *by something else*. And so, if we are ever to resist our future lives being *defined by something else,* we may all need to come out of our closets before someone or something locks us inside.

ON MAY 23, 2019, I woke up at 6 A.M., unusually early for me. My room was bright and warming up, the sunrise peeking through my curtains. I hate getting up early, so I stared at the ceiling for a bit before glancing out the window to see life emerging on the street. A guy I had been seeing stayed the night, so I had to slip out of bed carefully in order not to make a sound. It was polling day in Britain, in what was potentially the last-ever European Parliament election. My polling card said polls would open at 7 A.M., so I wanted to sneak out to run to the local community center where voting in my local ward was taking place.

Taking slightly exaggerated steps to silently glide over to my dresser, I grabbed my jeans and a T-shirt, lying in a heap on the floor. The shirt was a gift from the English designer Katharine Hamnett. Soft black cotton with bold white letters, it simply read, SECOND REFERENDUM NOW! *If I wear anything today, it should be this T-shirt,* I thought. I reached over into my drawer to pull out my phone, and once it regained signal, it began buzzing with messages.

Oh shit, I thought. I turned back to see I had woken him up. Groaning into a pillow, he asked why I was up so early and I simply said because I want to go vote. He sat up and smirked, rolling his eyes, asking if today was like Christmas for *people like me*. I told him no, that I wanted to go early, before the party poll watchers show up and start tallying who is voting. I didn't want to get into another fight with UKIP or Brexiteers. I have been called a traitor and pushed into the streets, but I did not want to be stopped from voting.

It did not feel like Christmas, and it wasn't exciting at all. It was a sad day, because I knew in my heart that I wasn't going to be taking part in a *real* election—it was all part of a final performance before Britain was scheduled to leave the European Union. Despite the Electoral Commission's ruling against Vote Leave, an ongoing National Crime Agency investigation, testimonies at Parliament, and a weeks-

long exposé in *The Guardian* about the cover-up inside Downing Street, the government was nonetheless determined to exit the European Union with a mandate won through cheating and fraud.

My postbox was filled with leaflets and literature. I was half expecting to receive something mad from Arron Banks or Leave.EU, like a Brexit leaflet rolled into a Russian vodka bottle, as they were so fond of trolling me and *Guardian* journalist Carole Cadwalladr. But no, it was just regular leaflets. Greens. Lib Dems. UKIP. Nothing from the Tories or Labour, for some reason. I opened up the Lib Dem one and I thought about what data they were using now and whether they had targeted me with a message. It didn't look like it. It was just another crap leaflet.

I looked up at the security camera watching me in the lobby and left. I set out, walking through a couple of streets in my neighborhood. Old Georgian row houses interspersed with the occasional block of flats. It was extremely bright and sunny. The morning air was fresh and invigorating. I turned onto a high street, where the shops were not yet open, save for a local coffee shop. I walked in and ordered a coffee with a splash of soy milk. As I waited, I looked at everyone in the café, standing and looking at their phones, all scrolling, following and engaging with content. I stood beside them, but they were all off in their own digital worlds. To be honest, I used to do the same thing before my ban. But without social media, aside from a Twitter account I barely use, I have found myself scrolling less, posting less, and taking fewer photos of things. I no longer spend hours being alone together with other people through my screen. I may live outside these digital worlds, but at least I have come to be more present in this world. After grabbing my coffee, I left and walked down a tree-lined street before reaching the community center. Tied to the trees were large white placards with black letters that read POLLING STATION. I kept my distance and peered around, but no one from any of the parties was loitering outside yet. So I walked inside and followed the signs down a corridor and into a simple, unadorned room scattered with cardboard voting booths and tiny pencils without erasers.

The polling station clerk looked at me and asked for my name. She flipped through the paper list and took a pencil to cross it out. That was it—no IDs, no electronics. She handed me what seemed like a

meter-long ballot for the election of London's delegation of members of the European Parliament. The paper was only slightly thicker than newspaper, but as I held it, I thought about how physical the act of voting seems, and yet so much sophisticated activity online leads up to this simple act of crossing an *X* on a thin piece of paper. I dropped the ballot into the ballot box and hoped it would not be the last time.