Mindf*ck

Inside Cambridge Analytica's Plot to Break the World

CHRISTOPHER WYLIE

PROFILE BOOKS

First published in Great Britain in 2019 by
Profile Books Ltd
29 Cloth Fair
London
EC1A 7NN

www.profilebooks.com

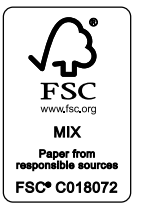
Published in the United States of America in 2019 by
Random House, an imprint and division of Penguin Random House LLC, New York

1 3 5 7 9 10 8 6 4 2

Printed and bound in Great Britain by
Clays Ltd, Elcograf S.p.A.

A CIP catalogue record for this book is available from the British Library.

ISBN 978 1 78816 499 3
Export edn 978 178816 506 8
eISBN 978 1 78283 677 3



On résiste à l'invasion des armées; on ne résiste pas à l'invasion des idées.

(One withstands the invasion of armies; one does not withstand the invasion of ideas.)

— VICTOR HUGO

CONTENTS

1

GENESIS

With each step, my new shoes dig into my heels. I clutch a dark-blue binder, filled with documents organised by coloured tabs. Awestruck by where I've found myself, and apprehensive of where I'm heading, I focus on the sounds of our footsteps. An aide reminds us to move quickly so we won't be seen. We walk past uniformed guards, into an atrium, and turn down a corridor. The aide pushes open a door and we rush down some stairs and into a hallway that looks exactly like the last one – marble floors, high ceilings, wooden doors with the occasional American flag. There are seven of us, and our footsteps echo through the hall. We are close; then I'm caught. A congressman spots me and waves hello. *Back again already?* A handful of journalists wander out of a press conference. They clock my electric pink hair and know who I am.

Two cameramen run in front of me and start filming, walking backward as they do. A scrum forms, the questions start coming – *Mr Wylie, a question from NBC! A question from CNN! Why are you here?* – and one of my lawyers reminds me to keep my mouth shut. The aide points me to a lift, warning the journalists to keep their distance, and we pile in. The cameras keep snapping as the doors close.

I'm jammed in the back of the lift, surrounded by people in suits. We start to descend, dropping deep underground. Everyone stays quiet on the way down. My mind is swimming with all of the prep

work I've done with my lawyers – what US laws were broken and by whom, what rights I do and don't have as a non-citizen visiting America, how to calmly respond to accusations, what happens if I am arrested afterward. I have no idea what to expect. No one does.

We come to a stop and the elevator doors glide open. There's nothing down here except another door, with a large red sign that reads RESTRICTED AREA in white lettering. NO PUBLIC OR MEDIA ACCESS. We're three floors beneath the US Capitol, in Washington, DC.

Beyond the door, the floors are covered in a plush maroon carpet. Uniformed guards confiscate our phones and other electronics, placing them on a numbered shelf behind the desk, one to a person, and giving us each a numbered ticket. They tell us we can have only pencils and paper beyond this point. And on the way out, they warn us, our papers could be confiscated if it's determined that we've taken notes on anything of a sensitive nature.

Two guards push open a massive steel door. One of them gestures us through, and one by one we step into a long hallway dimly illuminated by fluorescent lights. The walls are panelled in dark wood, and the corridor is lined with long rows of American flags on stands. It smells like an old building, stale and musty, with hints of cleaning fluid. The guards lead us down the hall, turning left and continuing to yet another door. Above, a wooden seal emblazoned with a giant eagle, arrows clutched in its talons, stares down at us. We have arrived at our destination: the Sensitive Compartmentalised Information Facility (SCIF) of the United States House Permanent Select Committee on Intelligence – the same room where classified congressional briefings are held.

Inside, hit by the glare of fluorescent lights, my eyes need time to adjust. The space is thoroughly nondescript, with blank beige walls and a conference table surrounded by chairs. It could be any room in any of the numerous bland federal buildings scattered across Washington, but I'm struck by the silence of the SCIF. It is soundproof, built with multilayer walls that make it impervious to surveillance. The architecture is said to be blast-proof. This is a secure space, a place for America's secrets.

Once we've taken our seats, the members of Congress begin filing in. Aides place tabulated binders on the table in front of each

committee member – the Democrats' ranking member, California congressman Adam Schiff, sits directly across from me, and to his left sits Congresswoman Terri Sewell, with Eric Swalwell and Joaquin Castro clustered together at the far end. I'm flanked by my lawyers and my friend Shahmir Sanni, a fellow whistleblower. We give the Republicans a few minutes to show up. They never do.

It's June 2018, and I'm in Washington to testify to the US Congress about Cambridge Analytica, a military contractor and psychological warfare firm where I used to work, and a complex web involving Facebook, Russia, WikiLeaks, the Trump campaign and the Brexit referendum. As the former director of research, I've brought with me evidence of how Facebook's data was weaponised by the firm, and how the systems they built left millions of Americans vulnerable to the propaganda operations of hostile foreign states. Schiff leads the questioning. A former federal prosecutor, he is sharp and precise with his lines of inquiry, and he wastes no time getting to the heart of the matter.

Did you work with Steve Bannon? *Yes.*
Did Cambridge Analytica have any contacts with potential Russian agents? *Yes.*
Do you believe that this data was used to sway the American electorate to elect the president of the United States? *Yes.*

An hour goes by, then two, then three. I chose to come here of my own accord and to answer these questions about how a liberal, gay twenty-four-year-old Canadian found himself part of a British military contractor developing psychological warfare tools for the American alt-right. Fresh out of university, I had taken a job at a London firm called SCL Group, which was supplying the UK Ministry of Defence and NATO armies with expertise in information operations. After western militaries were grappling with how to tackle radicalisation online, the firm wanted me to help build a team of data scientists to create new tools to identify and combat extremism online. It was fascinating, challenging and exciting all at once. We were about to break new ground for the cyber defences of Britain, America and their allies and confront bubbling insurgencies of radical extremism with

data, algorithms and targeted narratives online. But through a chain of events that unfolded in 2014, a billionaire acquired our project in order to build his own radicalised insurgency in America. Cambridge Analytica, a company few had ever heard of, a company that weaponised research in psychological profiling, managed to turn the world upside down.

In the military, when weapons fall into the wrong hands, they call it blowback. It looked as if this blowback had detonated in the White House itself. I could not continue working on something so corrosive to our societies, so I blew the whistle, reported the whole thing to the authorities, and worked with journalists to warn the public about what was going on. Sitting before this panel, jet-lagged from a transatlantic flight the day before, I still cannot help but feel on the spot as the questions grow more pointed. But several times, my attempts to explain the intricacies of the company's operations leave everyone with puzzled faces, so I simply pull out a binder and slide it to the congressmen. *What the hell,* I think. I've come this far, so I might as well give them everything I have with me. There is no break, and the door behind me remains closed the entire time. I'm locked in a stuffy, windowless room deep underground, with nowhere to look except straight into the eyes of these members of Congress as they all try to figure out what the hell just happened to their country.

THREE MONTHS BEFORE THIS, on 17 March, 2018, the *Guardian, The New York Times* and Channel 4 News had simultaneously published the results of a year-long joint investigation, spurred by my decision to reveal the truth about what was happening inside Cambridge Analytica and Facebook. My coming out as a whistleblower prompted the largest data crime investigation in history. In Britain, the National Crime Agency (NCA), MI5 (the UK's domestic intelligence agency), the Information Commissioner's Office, the Electoral Commission and London's Metropolitan Police Service all got involved. In the United States, the FBI, the Department of Justice, the Securities and Exchange Commission (SEC), and the Federal Trade Commission (FTC) jumped in.

In the weeks before that first story, the investigation by special counsel Robert Mueller had been heating up. In February, Mueller indicted thirteen Russian citizens and three Russian companies, charging them with two separate counts of conspiracy. A week later came indictments of former Trump campaign manager Paul Manafort and his deputy, Rick Gates. On 16 March, Attorney General Jeff Sessions fired FBI deputy director Andrew McCabe, just a little more than twenty-four hours before he was to retire with a pension. People were desperate for information about what had happened between the Trump campaign and Russia, but no one had been able to connect the dots. I provided evidence tying Cambridge Analytica to Donald Trump, Facebook, Russian intelligence, international hackers and Brexit. This evidence revealed how both an obscure foreign contractor engaged in illegal activity and the same foreign contractor had been used by the winning Trump and Brexit campaigns. The email chains, internal memos, invoices, bank transfer records and project documentation I brought demonstrated that Trump and Brexit had deployed the same strategies, powered by the same technologies, directed by many of the same people – all under the spectre of covert Russian involvement.

Two days after the story's release, an urgent question was brought to the British Parliament. In a rare moment of solidarity, government ministers and senior opposition members of Parliament sang as a unified chorus about Facebook's negligence in failing to prevent its platform from becoming a hostile propaganda network for elections and the implications for western democracies. The next wave of stories focused on Brexit, with the integrity of the referendum vote called into question. A collection of documents I provided to law enforcement revealed that the Vote Leave campaign had used secret Cambridge Analytica subsidiaries to spend dark money to propagate disinformation on Facebook and Google ad networks. This was determined to be illegal by the UK's Electoral Commission, with the scheme ending up as one of the largest and most consequential breaches of campaign finance law in British history. The office of 10 Downing Street descended into communication crisis as the evidence of Vote Leave's cheating emerged. The NCA and MI5 were later handed

evidence of the Russian embassy's direct relationship with the largest funders of pro-Brexit campaigns during the referendum. A week later, Facebook's stock plummeted 18 per cent, amounting to an $80 billion loss in valuation. The turbulence would continue, culminating in what still stands as the largest single-day loss in share value in US corporate history.

On 27 March, 2018, I was called before Parliament for a live public hearing – something I'd get quite used to over the next several months. We covered everything from Cambridge Analytica's reliance on hackers and bribes to Facebook's data breach to Russian intelligence operations. After the hearing, the FBI, DOJ, SEC and FTC launched investigations. The US House Intelligence Committee, House Judiciary Committee, Senate Intelligence Committee and Senate Judiciary Committee all wanted to talk to me. Within weeks, the European Union and more than twenty countries had opened up inquiries into Facebook, social media and disinformation.

I told my story to the world, and now every screen was a mirror reflecting it back at me. For two weeks straight, my life was chaos. Days would start with appearances on British breakfast shows and European networks at 6 a.m. London time, continuing with interviews on US networks until midnight. Reporters followed me everywhere. I started to receive threats. Fearing for my safety, I had to hire bodyguards to protect me at public events. My parents, both physicians, had to temporarily close their medical clinic due to a frenzy of journalists asking questions and scaring patients. In the months that followed, my life became almost unmanageable, but I knew I had to keep sounding the alarm.

The story of Cambridge Analytica shows how our identities and behaviour have become commodities in the high-stakes data trade. The companies that control the flow of information are among the most powerful in the world; the algorithms they've designed in secret are shaping minds in ways previously unimaginable. No matter what issue you care about most – gun violence, immigration, free speech, religious freedom – you can't escape Silicon Valley, the new epicentre of our crisis of perception. My work with Cambridge Analytica exposed the dark side of tech innovation. We innovated. The alt-right innovated. Russia innovated. And Facebook, that same site where you

share your party invites and baby pictures, allowed those innovations to be unleashed.

I SUSPECT I WOULDN'T have been interested in technology, or ended up at Cambridge Analytica, had I been born into a different body. I defaulted to computers because there was not much else available to a kid like me. I grew up on Vancouver Island, on the west coast of British Columbia, surrounded by oceans, forests and farmland. My parents were both doctors, and I was their eldest, followed by my two baby sisters, Jaimie and Lauren. When I was eleven, I started to notice that my legs were becoming stiffer and stiffer. I couldn't run as fast as the other kids, and I started to walk funny, which of course made me a target for bullies. I was diagnosed with two relatively rare conditions, whose symptoms included severe neuropathic pain, muscle weakness and vision and hearing impairment. By twelve I was in a wheelchair – just in time for the onset of adolescence – and I used that chair for the rest of my school days.

When you are in a wheelchair, people treat you differently. You can sometimes feel more like an object than a person – your means of getting around is how people come to understand and define you. You have to approach buildings and structures differently – *What entrances can I go in? How do I reach my destination while avoiding stairs?* You learn to look for things that other people never notice.

Not long after I discovered the computer lab, it became the one room at school where I didn't feel alienated. Outside, there were either bullies or patronising staff. Even when teachers shepherded other kids to interact with me, it was always done out of obligation, which became even more annoying than being ignored. Instead I'd go to the computer lab.

I started making webpages around age thirteen. My first website was a Flash animation of the Pink Panther being chased by a bumbling Inspector Clouseau. Soon after, I saw a video about programming Noughts and Crosses in JavaScript and thought it was the coolest thing ever. The game seems simple enough until you start having to break down all of the logic. You can't just let the computer randomly select a box, as that would be boring. You have to guide the computer

with rules, like putting an *X* in a box adjacent to another *X* – that is, unless there is an *O* already in that row or column. And what about diagonal *X*s – how do we explain them?

Eventually I strung together hundreds of lines of spaghetti code. I still remember the feeling of making a move and then watching my little creation play back. I felt like a conjurer. And the more I practiced my incantations, the more powerful my magic could become.

Outside of computer lab, school remained an education in what I wasn't able or allowed to do, and who I could not be. My parents encouraged me to keep trying to find a place where I could fit in, so when I was fifteen, I spent the summer of 2005 boarding at Lester B. Pearson United World College, an international school in Victoria named after the Nobel Peace Prize-winning Canadian prime minister who conceptualised the world's first UN peacekeeping force during the 1950s Suez Crisis. Spending so much time with students from every part of the world was enthralling, and for the first time, I was actually interested in the lessons and what my peers had to say. I became friends with a survivor of the Rwandan genocide, who told me one evening when we were up late in our residence hall about how his family was murdered and what it was like walking alone all the way to a refugee camp in Uganda when he was just a child.

But it was after sitting at a dinner one evening in the dining hall where Palestinian and Arab students sat directly across from Israeli students, forcefully debating the future of their homelands, that I really started to wake up to the world around me. I realised how much I didn't know about what was happening – but I wanted to – and so I very quickly developed an interest in politics. The following school year, I began skipping class to attend town hall events with local members of Parliament. At school, I rarely talked to anyone, but at these events I felt free to express myself. In a classroom, you sit in the back while the teacher tells you how and what to think. There is a curriculum, a prescription of thought. But in a town hall, I discovered the opposite. Sure, the politician stands up front, but it is the people in the audience – *us* – who get to tell him or her what *we* think. That inversion was so incredibly appealing to me, and whenever members of Parliament would announce an event, I'd show up, ask questions, and even tell them what I thought.

It was liberating to find my voice. Like any teenager, I was exploring who I was, but for someone gay and in a wheelchair, this was an even bigger challenge. When I started attending these public forums, I began to realise that many of the things I was living through were not simply personal issues – they were also political issues. *My challenges were political. My life was political. My mere existence was political.* And so I decided to become *political*. An adviser to one of the MPs, a former software engineer named Jeff Silvester, took notice of this outspoken kid who always showed up. He offered to help me find a role in the Liberal Party of Canada (LPC), which was looking for tech help. Soon it was agreed, at the end of that summer I would start my first real job, as a political assistant at Parliament in Ottawa.

I spent the summer of 2007 in Montréal, hanging out in hacker spaces frequented by French Canadian techno-anarchists. They tended to gather in converted industrial buildings with concrete floors and plywood walls, in rooms decorated with retro tech like Apple IIs and Commodore 64s. By then, with treatment, I could shuffle around without a wheelchair. (I have continued to improve, but my physical limits were tested by my experience as a whistleblower. Just before the first Cambridge Analytica story was published, I had a seizure and collapsed, unconscious, on a South London pavement before waking up at University College Hospital to the sharp pain of a nurse inserting an IV needle into my arm.) Most hackers couldn't care less what you look like or if you walk funny. They share your love of the craft and want to help you get better at it.

My brief exposure to hacking communities left a permanent impression. You learn that no system is absolute. Nothing is impenetrable, and barriers are a dare. The hacker philosophy taught me that if you shift your perspective on any system – a computer, a network, even society – you may discover flaws and vulnerabilities. As a gay kid in a wheelchair, I came to understand systems of power early on in life. But as a hacker, I learned that every system has weaknesses waiting to be exploited.

SHORTLY AFTER I STARTED my job at the Canadian Parliament, the Liberal Party took an interest in what was happening down south. At

that time, Facebook was just becoming mainstream and Twitter had just started gaining momentum; no one had any concept of how to use social media to campaign, because social media was in its infancy. But a rising star in US presidential politics was about to hit the accelerator.

While other candidates were twiddling their thumbs trying to figure out the internet, Barack Obama's team set up My.BarackObama.com and started a grassroots revolution. While other sites (like Hillary Clinton's) focused on putting up standard political advertisements, Obama's website centered on providing a platform for grassroots organisations to organise and execute get-out-the-vote campaigns. His website ratcheted up excitement around the Illinois senator, who was much younger and more tech savvy than his opponents. Obama felt like what a leader is supposed to be. And after spending my formative years being told about my limits, the defiant optimism he instilled in that simple message of *Yes, we can!* spoke to me. Obama and his team were transforming politics, so when I was eighteen, I was among several people sent to the United States by the Liberal Party to observe different facets of his campaign and identify new tactics that could be transported back for progressive campaigns in Canada.

At first, I toured a couple of early primary states, starting with New Hampshire, where I spent time talking to voters and seeing up close what American culture was really like. This was both fun and eye-opening; coming from Canada, I was struck by how different our sensibilities were. The first time an American told me he was dead set against 'socialised medicine', the same kind of public healthcare I accessed almost every month back home, I was shocked that someone could even think this way. The hundredth time, not so much.

I liked roaming around and talking with people, so when it was time to switch focus to the data group, I wasn't terribly excited to do it. But then I was introduced to Obama's national director of targeting, Ken Strasma, who quickly changed my mind.

The sexy part of the Obama campaign was its branding and use of new media like YouTube. This was the cool stuff, the visual strategy nobody had used before because YouTube was still so new. That was what I wanted to see, until Ken stopped me short. *Forget the videos,*

he told me. I needed to go deeper, into the heart of the campaign's tech strategy. *Everything we do,* he said, *is predicated on understanding exactly who we need to talk to, and on which issues.*

In other words, the backbone of the Obama campaign was data. And the most important work Strasma's team produced was the modelling they used to analyse and understand that data, which allowed them to translate it into an applied fit – to determine a real-world communications strategy through … artificial intelligence. *Wait – AI for campaigns?* It seemed vividly futuristic, as if they were building a robot that could devour reams of information about voters, then spit out targeting criteria. That information then travelled all the way up to the senior levels of the campaign, where it was used to determine key messages and branding for Obama.

The infrastructure for processing all this data came from a company then called the Voter Activation Network, Inc. (VAN), which was run by a fabulous gay couple from the Boston area, Mark Sullivan and Jim St George. By the end of the 2008 campaign, thanks to VAN, the Democratic National Committee would have ten times more data on voters than it had after the 2004 campaign. This volume of data, and the tools to organise and manipulate it, gave Democrats a clear advantage in driving voters to the polls.

The more I learned about the Obama machine, the more fascinated I was. And I later got to ask all the questions I wanted of Mark and Jim, as they seemed to find it amusing that this young Canadian had come to America to learn about data and politics. Before I saw what Ken, Mark and Jim were doing, I hadn't thought about using maths and AI to power a political campaign. In fact, when I first saw people lined up at computers at the Obama headquarters, I thought, *Messages and emotions, not computers and numbers, are what create a winning campaign.* But I learned that it was those numbers – and the predictive algorithms they created – that separated Obama from anyone who had ever run for president before.

As soon as I realised how effectively the Obama campaign was using algorithms to deliver its messages, I started studying how to create them on my own. I taught myself how to use basic software packages like MATLAB and SPSS, which let me mess around with data. Instead of relying on a textbook, I started by playing with the

Iris data set – the classic data set for learning statistics – and learned by trial and error. Being able to manipulate the data, which involved using the different features of irises, like petal length and colour, to predict species of flowers, was absolutely absorbing.

Once I understood the basics, I switched from petals to people. VAN was filled with information on age, gender, income, race, home-ownership – even magazine subscriptions and airline miles. With the right data inputs, you could start to predict whether people would vote for Democrats or Republicans. You could identify and isolate the issues that were likely to be most important to them. You could begin to craft messages that would have a greater chance of swaying their opinions.

For me, this was a wholly new way of understanding elections. Data was a force for good, powering this campaign of change. It was being used to produce first-time voters, to reach people who felt left out. The deeper I got into it, the more I thought that data would be the saviour of politics. I couldn't wait to get back to Canada and share with the Liberal Party what I'd learned from the next president of the United States.

In November, Obama achieved a decisive victory over John McCain. Two months later, after friends in the campaign extended an invitation to the inauguration, I flew to Washington to party with the Democratic victors. (First came a slight kerfuffle at the door, when staff freaked out about letting the under-twenty-one me into the open-bar event.) I had an incredible evening, chatting with Jennifer Lopez and Marc Anthony, watching Barack and Michelle Obama enjoy their first dance as the First Couple. A new era had dawned, and now came a chance to celebrate what could happen when the right people understood how to use data to win modern elections.

BUT BY DIRECTLY COMMUNICATING select messages to select voters, the microtargeting of the Obama campaign had started a journey toward the privatisation of public discourse in America. Although direct mail had long been part of American campaigns, data-driven microtargeting allowed campaigns to match a myriad of granular narratives to granular universes of voters – your neighbour

might receive a wholly different message than you did, with neither of you being the wiser. When campaigns were conducted in private, the scrutiny of debate and publicity could be avoided. The town square, the very foundation of American democracy, was incrementally being replaced by online ad networks. And without any scrutiny, campaign messages no longer even had to look like campaign messages. Social media created a new environment where campaigns could now appear, as Obama's campaign piloted, as if your friend was sending you a message, without your realising the source or calculated intent of that contact. A campaign could look like a news site, university or public agency. With the ascendancy of social media, we have been forced to place our trust in political campaigns to be honest, because if lies are told, we may never notice. There is no one there to correct the record inside of a private ad network.

In the years leading up to the first Obama campaign, a new logic of accumulation emerged in the boardrooms of Silicon Valley: Tech companies began making money from their ability to map out and organise information. At the core of this model was an essential asymmetry in knowledge – the machines knew a lot about our behaviour, but we knew very little about theirs. In a trade-off for convenience, these companies offered people information services in exchange for more information – data. The data has become more and more valuable, with Facebook making on average $30 from each of its 170 million American users. At the same time, we have fallen for the idea that these services are 'free'. In reality, we pay with our data into a business model of extracting human attention.

More data led to more profits, and so design patterns were implemented to encourage users to share more and more about themselves. Platforms started to mimic casinos, with innovations like the infinite scroll and addictive features aimed at the brain's reward systems. Services such as Gmail began trawling through our correspondence in a way that would land a traditional postal worker in prison. Live geotracking, once reserved for convicts' ankle bracelets, was added to our phones, and what would have been called wiretapping in years past became a standard feature of countless applications.

Soon we were sharing personal information without the slightest hesitation. This was encouraged, in part, by a new vocabulary. What

were in effect privately owned surveillance networks became 'communities', the people these networks used for profit were 'users', and addictive design was promoted as 'user experience' or 'engagement'. People's identities began to be profiled from their 'data exhaust' or 'digital breadcrumbs'. For thousands of years, dominant economic models had focused on the extraction of natural resources and the conversion of these raw materials into commodities. Cotton was spun into fabric. Iron ore was smelted into steel. Forests were cut into timber. But with the advent of the internet, it became possible to create commodities out of our lives – our behaviour, our attention, our identity. People were processed into data. We would serve as the raw material of this new data-industrial complex.

One of the first people to spot the political potential of this new reality was Steve Bannon, the relatively unknown editor of right-wing website Breitbart News, which was founded to reframe American culture according to the nationalist vision of Andrew Breitbart. Bannon saw his mission as nothing short of cultural warfare, but when I first encountered him, Bannon knew that something was missing, that he didn't have the right weapons. Whereas field generals focused on artillery power and air dominance, Bannon needed to gain *cultural power* and *informational dominance* – a data-powered arsenal suited to conquer hearts and minds in this new battlespace. The newly formed Cambridge Analytica became that arsenal. Refining techniques from military psychological operations (PSYOPS), Cambridge Analytica propelled Steve Bannon's alt-right insurgency into its ascendancy. In this new war, the American voter became a target of confusion, manipulation and deception. Truth was replaced by alternative narratives and virtual realities.

Cambridge Analytica (CA) first piloted this new warfare in Africa and tropical islands around the world. The firm experimented with scaled online disinformation, fake news and mass profiling. It worked with Russian agents and employed hackers to break into opposition candidates' email accounts. Soon enough, having perfected its methods far from the attention of western media, CA shifted from instigating tribal conflict in Africa to instigating tribal conflict in America. Seemingly out of nowhere, an uprising erupted in America with manic cries of *MAGA!* and *Build the wall!* Presidential debates

suddenly shifted from policy positions into bizarre arguments about what was *real news* and what was *fake news*. America is now living in the aftermath of the first scaled deployment of a psychological weapon of mass destruction.

As one of the creators of Cambridge Analytica, I share responsibility for what happened, and I know that I have a profound obligation to right the wrongs of my past. Like so many people in technology, I stupidly fell for the hubristic allure of Facebook's call to '*move fast and break things*'. I've never regretted something so much. I moved fast, I built things of immense power, and I never fully appreciated what I was breaking until it was too late.

AS I MADE MY WAY to the secure facility deep under the Capitol that day in the early summer of 2018, I felt numbed to what was happening around me. Republicans were already conducting opposition research on me. Facebook was using PR firms to smear its critics, and its lawyers had threatened to report me to the FBI for an unspecified cybercrime. The DOJ was now under the control of a Trump administration that was publicly ignoring long-held legal conventions. I had enraged so many interests that my lawyers were genuinely concerned the FBI might arrest me after I was finished. One of my lawyers told me the safest thing to do was stay in Europe.

I cannot, for security and legal reasons, quote directly from my testimony in Washington. But I can tell you that I walked into that room with two large binders, each containing several hundred pages of documents. The first binder contained emails, memos and documents showing the extent of Cambridge Analytica's data-harvesting operation. This material demonstrated that the company had recruited hackers, hired personnel with known links to Russian intelligence, and engaged in bribery, extortion and disinformation campaigns in elections around the world. There were confidential legal memos from lawyers warning Steve Bannon about Cambridge Analytica's violations of the Foreign Agents Registration Act, as well as a cache of documents describing how the firm exploited Facebook to access more than eighty-seven million private accounts and used that data in efforts to suppress the votes of African Americans.

The second binder was more sensitive. It contained hundreds of pages of emails, financial documents and transcripts of audio recordings and text messages that I had covertly procured in London earlier that year. These files had been sought by US intelligence and detailed the close relationships between the Russian embassy in London and both Trump associates and leading Brexit campaigners. This file showed that leading British alt-right figures met with the Russian embassy before and after they flew to meet the Trump campaign, and that at least three of them were receiving offers of preferential investment opportunities in Russian mining companies potentially worth millions. What became clear in these communications was how early the Russian government had identified the Anglo-American alt-right network, and that it may have groomed figures within it to become access agents to Donald Trump. It showed the connections among the major events of 2016: the rise of the alt-right, the surprise passage of Brexit, and the election of Trump.

Four hours went by. Five. I was deep into describing Facebook's role in – and culpability for – what had happened.

Did the data used by Cambridge Analytica ever get into the hands of potential Russian agents? *Yes.*

Do you believe there was a nexus of Russian state-sponsored activity in London during the 2016 presidential election and Brexit campaigns? *Yes.*

Was there communication between Cambridge Analytica and WikiLeaks? *Yes.*

I finally saw glimmers of understanding coming into the committee members' eyes. Facebook is no longer just a company, I told them. It's a doorway into the minds of the American people, and Mark Zuckerberg left that door wide open for Cambridge Analytica, the Russians, and who knows how many others. Facebook is a monopoly, but its behaviour is more than a regulatory issue – it's a threat to national security. The concentration of power that Facebook enjoys is a danger to American democracy.

Dancing a delicate ballet among multiple jurisdictions, intelligence agencies, legislative hearings and police authorities, I have given more

than two hundred hours of sworn testimony and handed over at least ten thousand pages of documents. I found myself travelling around the world, from Washington to Brussels, to help leaders unpack not only Cambridge Analytica but also the threats social media poses to the integrity of our elections.

Yet, in my many hours of giving testimony and evidence, I came to realise that the police, the legislators, the regulators and the media were all having a difficult time figuring out what to do with this information. Because the crimes happened online, rather than in any physical location, the police could not agree on who had jurisdiction. Because the story involved software and algorithms, many people threw up their hands in confusion. Once, when one of the law enforcement agencies I was dealing with called me in for questioning, I had to explain a fundamental computer science concept to agents who were supposedly specialists in technology crime. I scribbled a diagram on a piece of paper, and they confiscated it. Technically, it was evidence. But they joked that they needed it as a crib sheet to understand what they were investigating. *LOL, so funny, guys*.

We are socialised to place trust in our institutions – our government, our police, our schools, our regulators. It's as if we assume there's some guy with a secret team of experts sitting in an office with a plan, and if that plan doesn't work, don't worry, he's got a plan B and a plan C – someone in charge will take care of it. But in truth, that guy doesn't exist. If we choose to wait, nobody will come.