# WRITTEN STATEMENT TO THE UNITED STATES SENATE COMMITTEE ON THE JUDICIARY

# IN THE MATTER OF CAMBRIDGE ANALYTICA AND OTHER RELATED ISSUES

## OPENING REMARKS

1. Mr Chairman, Senators – Thank you for your invitation and opportunity to speak to your committee.

2. American democracy matters. It matters not just to the American citizens who vote, organise, protest, run for office or to those who just speak their minds. American democracy matters to the world which so often looks to the United States for leadership in defending and promoting democratic ideals. But to defend democracy around the world, the United States must defend its own at home. As Ronald Reagan cautioned, democracy is not a fragile flower, but still it needs cultivating.

3. Democracy is a bipartisan issue. I do not intend to make this a partisan testimony and I welcome questions from all members. Although Cambridge Analytica may have supported particular candidates in US elections, I am not here to point fingers. The firm's political leanings are far less relevant than the broader vulnerabilities this scandal has exposed. It should also be said that the actions of one rogue company are not necessarily reflective of the character of its past clients or candidates.

4. This should be about moving forward to protect democratic institutions from rogue actors and hostile foreign interference, as well as ensuring the safety of

Americans online, which is something I know both Democrats and Republicans care deeply about.

5. I am a Canadian citizen who is resident in the United Kingdom. I have come here today voluntarily as a witness and as a whistleblower. I reported these matters to the responsible UK authorities months before the stories were made public by the Guardian, New York Times and Channel 4, and it should be made clear that I am considered a witness by both the British and American authorities.

6. On 26 March 2018, the UK Information Commissioner personally confirmed in writing that I am *"not a subject of [their] investigation"*.

## COMPANY ORIGINS

7. I was the Director of Research for SCL and Cambridge Analytica from mid 2013 to late 2014. SCL Group was a UK based military contractor, which worked for the US and UK militaries and also worked at the NATO StratComm Centre in the Baltic region.

8. Cambridge Analytica ("CA") was created by SCL Group with funding from Robert Mercer, an American billionaire based in New York. Robert Mercer installed Steve Bannon as CA's Vice President with responsibilities to manage the company day-to-day. Mr Mercer's daughter, Rebekah Mercer, also played a role in the company.

9. Mr Bannon is a follower of the Breitbart Doctrine, which posits that politics flows downstream from culture. Therefore, Mr Bannon sees cultural warfare as the means to create enduring change in American politics. It was for this reason Mr Bannon engaged SCL, a foreign military contractor, to build an arsenal of informational weapons he could deploy on the American population. Mr Bannon wanted to use the same kinds of information

operations tactics used by the military for his political aims in the United States and elsewhere.

10. CA was created as the front-facing American brand to allow SCL to work in the USA. I was informed that this setup was largely to get around various electoral compliance and foreign agent restrictions in the USA. CA did not have any employed staff, only an intellectual property agreement and data assets it received from SCL. SCL assigned all its intellectual property ("IP") to CA and in return, CA licensed back this same IP and all CA clients would be handed to SCL staff.

11. SCL and Mr Mercer's lawyers decided upon the setup. I later learned that one advantage of this complicated setup was that funds invested by Mr Mercer and his investment vehicles would not necessarily be considered declarable campaign contributions. Rather, monies transferred for the firm's research and development ("R&D") would be classed investments not donations, even if that R&D ended up supporting political clients. This allowed the firm to develop IP worth far more than the value of each client contract it had with the campaigns it was supporting.

12. The majority of SCL staff were not American citizens. Although Mr Bannon was formally warned about the implications of using foreign citizens in US elections in a legal memorandum, the firm disregarded this advice and proceeded to install Alexander Nix, a British national resident in London, as CEO, and sent non-US citizens to play strategic roles embedded in American campaigns. To be clear, during my time at CA, I never directly worked in any of the firm's supported American campaigns, nor did I exert strategic or managerial influence on those campaigns, nor was I responsible for those SCL/CA staff hiring and deployment decisions.

13. The ethos of the firm was 'anything goes'. I witnessed some senior staff even going so far as attempting to

divert health ministry funds in a struggling African country to support a politician's re-election campaign. To be clear, I was not myself involved in inducing any public official to misuse their position.

14. By taking advantage of countries with still-developing civic institutions, the firm was a corrupting force in the world and became the face of what colonialism looks like in the 21st century.

## USE OF HACKED MATERIALS

15. When I was at SCL and CA, I was made aware of the firm's "black ops" capacity, which I understood to include using hackers to break into computer systems to acquire kompromat or other intelligence for its clients. The firm referred to these operations as "special intelligence services" or "special IT services". I have been told about and seen documents relating to several instances where SCL or CA procured hacked material for the benefit of its clients. Some of the targets of these intelligence operations are currently heads of state in various countries. Of concern, some of the former CA staff who worked on these projects currently hold senior positions in the British government. I have also seen internal CA documents that make reference to using specialised technologies and intelligence gathering services from former members of Israeli and Russian state security services. Mr Bannon was Vice President at the time of some of these events.

16. Of further concern is CA's links to people closely associated with Wikileaks and Julian Assange. The firm hired two senior staff, both of whom were previously aides to John Jones QC in London. Mr Jones was the British lawyer who represented Julian Assange, Wikileaks and members of the Gaddafi regime. He later killed himself by walking in front of a train in 2016. I believe that part of the appeal of hiring these staff members was their pervious work with Mr Jones,

including the association with Mr Assange. At least one of these staff members was involved in a project that procured and used hacked materials on an election campaign. Although the firm claimed only brief contact with Mr Assange, recordings of SCL Group's former CEO suggest that contact with Wikileaks began 18 months prior to the US election.

17. I realise these are very serious allegations, and to be clear, I have already reported the matter to the UK National Crime Agency, which is co-ordinating a multi-jurisdictional investigation with their American colleagues in the Federal Bureau of Investigation ("FBI"). I have also been contacted directly by the FBI and the US Department of Justice, and I intend to fully co-operate with their investigations.

18. To be clear, I have never authorised, facilitated or otherwise procured the services of hackers for CA or anyone else. I have therefore been informed by both British and American authorities that I am not a target of these investigations.

## FACEBOOK DATA HARVESTING

19. Between 2013 and 2015, CA funded a multi-million dollar operation called Project Ripon. This project was overseen by Mr Bannon and was based upon research that was originally conducted by psychologists at the University of Cambridge.

20. It should be noted that some of the profiling research used as the basis of CA operations had declared funding from the US Defense Advanced Research Projects Agency ("DARPA").

21. The purpose of Ripon was to develop and scale psychological profiling algorithms for use in American political campaigns. To be clear, the work of CA and SCL is not equivalent to traditional marketing, as has

been claimed by some. This false equivalence is misleading. CA specialised in disinformation, spreading rumours, kompromat and propaganda. Using machine learning algorithms, CA worked on moving these tactics beyond its operations in Africa or Asia and into American cyberspace.

22. CA sought to identify mental and emotional vulnerabilities in certain subsets of the American population and worked to exploit those vulnerabilities by targeting information designed to activate some of the worst characteristics in people, such as neuroticism, paranoia and racial biases. This was targeted at narrow segments of the population.

23. For those who claim that profiling does not work, this contradicts copious amounts of peer-reviewed literature in top scientific journals, including the Proceedings of the National Academy of Science ("PNAS"), Psychological Science and the Journal of Personality and Individual Differences. Even Facebook itself has applied for a US patent on *"determining user personality characteristics from social networking system communications and characteristics"*.

24. The Russian-American researcher Dr Aleksandr Kogan was selected to lead the data harvesting operation, as he offered the use of Facebook apps which he had developed in his academic role to collect personal data about Facebook users and their friends. However, I later learned that Dr Kogan did not have permission from Facebook to exploit the app's privileged access for commercial or political activities. This has been confirmed to me in legal correspondence with Facebook.

25. Dr Kogan developed data harvesting applications that would capture not only the original app user but would harvest all the personal data of that user's Facebook friends and connections – without their knowledge or explicit consent.

26. CA did not conduct due diligence to ensure that Dr Kogan had authorisation before spending circa 1 million US dollars on this scheme. However, CA has a history of seeking out data with dubious provenance. For example, the company contracted a partner firm in an attempt to acquire live Internet service provider ("ISP") data to tacitly monitor the Internet browsing habits of voters in the Caribbean without their knowledge or consent.

27. As Facebook has now confirmed, over 80 million data subjects had their personal data misappropriated in the Ripon programme, many of whom were American citizens. Given this scale, Ripon could be one of the largest breaches of Facebook's data.

28. CA often stored or transmitted data in insecure formats, including files of hundreds of thousands of Americans' data being passed around via unencrypted e-mails. CA also allowed access to its American datasets to external contractors, including senior staff from the company Palantir, which is a contractor to the US National Security Agency ("NSA"). To be clear, Palantir denies having any formal relationship with CA and states this work was apparently done in a "personal capacity".

29. SCL has a documented history of poor handling of sensitive data. In 2014, SCL Group, the parent of CA, was criticised by the UK Defence Science and Technology Laboratory for its inability to properly handle sensitive Ministry of Defence information. This Ministry of Defence assessment was conducted the same year as the Facebook data harvesting scheme.

## RUSSIAN CONTACT

30. At the time, Dr Kogan was also working on Russian state-funded research projects. He was based at times in St Petersburg and also would fly to Moscow. The

Russian team at St Petersburg was also building similar algorithms using Facebook data for psychological profiling. The Russian project had a particular focus on the "dark triad" traits of narcissism, Machiavellianism and psychopathy. The Russian project also conducted behavioural research on online trolling.

31. It should be noted that CA was very much aware of this work going on in Russia and in fact sought to pitch *"the interesting work Alex Kogan has been doing for the Russians"* to its other clients.

32. Contemporaneous to Dr Kogan's data profiling work in Russia, CA was also in close contact with senior executives at Lukoil, one of Russia's largest oil companies. After receiving a request for information from Lukoil executives in the spring of 2014, CA discussed with Lukoil its experience with foreign disinformation, rumour campaigns, microtargeting and its American data assets. Mr Nix also emailed me to say that he was passing on a white paper I wrote outlining the US project to the CEO of Lukoil.

33. It should be noted that Lukoil has formal information sharing agreements with the Russian Federal Security Service ("FSB") and is known to conduct intelligence gathering on behalf of the FSB.

34. It should also be noted that CA's parent company, SCL Group, has managed information operations projects in Eastern Europe and the Baltic region and may have been an intelligence target at the time.

35. This means that in addition to Facebook data being accessed in Russia, there are reasonable grounds to suspect that *(1)* CA may have been an intelligence target of Russian security services at the time of Project Ripon, *(2)* that Russian security services may have been notified of the existence of CA's Facebook data and/or methods through CA's frequent contact with Russian

companies, and *(3)* that it was made known that certain data assets could have been accessed inside Russia or via accessing Dr Kogan's work and computers using something as simple as a keylogger device *(with or without his knowledge or consent).*

36. Other CA contractors have worked on pro-Russian political operations in Eastern Europe, including work in Ukraine with suspected Russian intelligence agents. This may have influenced some of CA's research in the USA. During its research projects in 2014, CA also set up focus groups, message testing and polling on Americans' views on the leadership of Vladimir Putin and Russian expansionism in Eastern Europe. Of note, Vladimir Putin was the only foreign leader tested by CA.

37. In short, Cambridge Analytica *(1)* used Russian researchers to gather its data, *(2)* openly shared information on "rumour campaigns" and "attitudinal inoculation" with FSB-linked Russian companies and executives, *(3)* pitched Russian-led profiling projects to its other clients, *(4)* contracted people who worked for pro-Russian parties in Eastern Europe with suspected Russian intelligence operatives, *(5)* referenced the use of former Russian intelligence agents in internal documents, and *(6)* went as far as to test Americans' views on Vladimir Putin's leadership.

38. CA's behaviour is more disconcerting given that its parent company SCL had extensive experience working in counter-extremism and military projects for the British and American governments. It should have known better.

39. To be clear, *no allegation* is being made that any CA personnel, including Mr Nix or Dr Kogan, knowingly colluded with the FSB, GRU or other Russian agencies. However, what is clear is the gross risk of data breaches and foreign intelligence gathering created by CA's

recklessness in the face of skilled intelligence and cyber operations.

## VOTER DISENGAGEMENT

40. CA did not operate in elections to promote democratic ideals. Oftentimes, CA worked to interfere with voter participation, including by weaponising fear. In one country, CA produced videos intended to suppress turnout by showing voters sadistic images of victims being burned alive, undergoing forced amputations with machetes and having their throats cut in a ditch. These videos also conveyed Islamophobic messages. It was created with a clear intent to intimidate certain communities, catalyse religious hatred, portray Muslims as terrorists and deny certain voters of their democratic rights. I have seen this video, but to be clear, I had no part in its creation, editing or deployment, and I left before the company made use of it in the field.

41. If it suited the client's objective, the firm was eager to capitalise on discontent and to stoke ethnic tensions. This was not just on its projects in Africa. As the CEO of SCL said in a recorded conversation about the firm's work in the USA in 2016:

> *"It's the things that resonate, sometimes to attack the other group and know that you are going to lose them is going to reinforce and resonate your group. Which is why […] Hitler attacked the Jews, because he didn't have a problem with the Jews at all, but the people didn't like the Jews […] So he just leveraged an artificial enemy. Well that's exactly what Trump did. He leveraged a Muslim […] Trump had the balls, and I mean, really the balls, to say what people wanted to hear."*

42. I am aware that CA clients requested voter suppression as part of their contracts. CA offered "voter disengagement" as a service in the United States and

there are internal documents that I have seen that make reference to this tactic. My understanding of these projects, which I did not personally participate in, was that the firm would target African American voters and discourage them from participating in elections. Mr Bannon was Vice President of the company at the time of these voter disengagement projects.

## FACEBOOK'S RESPONSE

43. Facebook was first notified of CA's harvesting scheme in 2015. It did not warn users then, and it only took action to warn affected users three weeks after the Guardian, New York Times and Channel 4 made the story public.

44. Facebook's behaviour before the story broke was to threaten to sue the Guardian. Facebook's lawyers also tried to intimidate me with aggressive legal notices. Facebook tried to shut down this story from going public when it knew it was true. At the British parliamentary inquiry, the CTO of Facebook recently explained, to the surprise of many in the inquiry, that the company had assumed *"that this is common practice in the UK"*.

45. Credit should therefore be given to the international team of journalists who supported me as a whistleblower, stood up to these threats and nonetheless dared to publish: *Carole Cadwalladr, Sarah Donaldson, Emma Graham-Harrison, Paul Webster, John Mulholland* and *Gill Phillips* at the Guardian; *Matt Rosenberg, Nick Confessore, Gabriel Dance* and *Danny Hakim* at the New York Times; *Job Rabkin* and *Ben de Pear* at Channel 4.

46. I am disappointed that Facebook has not acted constructively in the wake of this scandal. Before the story broke, I offered to help Facebook. One of Facebook's Vice Presidents explicitly told my lawyer that they would welcome a collaborative engagement, but at the last minute, they instead announced in a press

release that they had banned me from their platform. I believe I was banned in a bungled attempt to re-frame the story and cast Facebook as the victim.

47. But it did not work. Facebook's decision to ban me from their platform was recently debated in the UK Parliament. Responding on behalf of the British Government, the UK Secretary of State for Culture, Media and Sport said on the floor of Parliament that:

> *"Of all the different things that have surprised me and shocked me in this revelation, the decision by Facebook to take down the whistleblower's Facebook account, and the removal of their WhatsApp account and the Instagram account, was the most surprising".*

48. The Secretary of State went further to call the ban *"outrageous"* – because the ban is outrageous. It reveals the unrestrained power technology companies have over users when a person's entire online presence can be so quickly and so thoroughly eliminated from existence. There is no due process or check on this power and my ban raises a serious question for Republicans and Democrats alike: *what happens to our democracy when these companies can delete people at will who dissent, scrutinise or speak out?*

49. Silicon Valley has this power now. I know because Facebook used it on me. They sought to make me a digital pariah.

50. Facebook's actions against me also show the serious consequences of Silicon Valley's rush to consolidate the ownership of different platforms. Although this scandal had nothing to do with Instagram, my account on Instagram was also eliminated in what I can only assume was a punitive move by Facebook, which now owns Instagram. This unchecked monopoly on digital space presents a serious risk to people's rights.

51. Facebook also demanded that I hand over my personal computer and phone after the story broke. The company disregarded that I had already handed over evidence to the responsible British authorities with jurisdiction over the investigation. In effect, Facebook was demanding that I let them acquire and handle evidence relevant to an ongoing investigation it was a party to. The company did not seem to understand or care about due process or respecting the integrity of an ongoing investigation by a competent legal authority.

52. I remain banned from Facebook despite the UK Information Commissioner's Office confirming in writing that I am *"not a subject of [their] investigation"*.

53. I would like to be able to discuss the data security and digital privacy issues raised by my evidence with Facebook in a non-confrontational manner and help it figure out how to move forward. I came out as a whistleblower to help the authorities uncover what happened. But I also want to work towards finding solutions and Facebook is a key player in finding those solutions. Platforms like Facebook are still huge public assets that do a lot of amazing work, but we should not shy away from the real problems that exist.

54. The Cambridge Analytica scandal has exposed that social platforms are no longer safe for users. We have to face up to this fact. These platforms are critical parts of American cyberspace in desperate need of protection and oversight.

55. In the context of information operations from hostile foreign actors, we cannot keep relying on the promises, apologies or good intentions of these firms to protect American citizens. We protect our borders at land, sea and air with dedicated public agencies. We do not leave this critical public service to private companies or land

owners. We should protect our digital spaces with the same level of care.

56. The security of American communities online is one of the most pressing national security issues in the 21st century. This is not an emerging problem on the horizon. This is not a niche issue. This is a problem today, in the here and now, affecting the 260 million Americans who use social media.

57. But it is not just Americans who have been affected. The rest of the world uses and often depends on American technology. But as we have seen with Mark Zuckerberg's continual refusal to attend the British Parliament's inquiry, it is impossible for other countries like the UK to hold these companies to account. To highlight the seriousness of the matter, the British parliamentary inquiry is now considering issuing a standing summons on Mark Zuckerberg after the company failed to answer 40 of the inquiry's questions.

## MOVING FORWARD

58. What I bore witness to at Cambridge Analytica should alarm everyone. Cambridge Analytica is the canary in the coal mine to a new Cold War emerging online.

59. If a foreign actor dropped propaganda leaflets by aeroplane over Florida or Michigan, that would universally be condemned a hostile act. But this is what is happening online. We must address these issues before disinformation and information warfare become pervasive in American cyberspace.

60. We also must address the digital echo chambers that are being exploited to algorithmically segregate American society. Online communities should unite us, not divide us.

61. But we cannot keep deferring to the technology sector with the defeatist mantra that *'the law cannot keep up with technology'*. We need a different mentality. Technology should not be exempt from public oversight or debate simply because it relates to software. If we can regulate the safety standards of aeroplanes, medicines or nuclear power plants, we can create safety standards for software.

62. Every year, Americans are buying more and more Internet-enabled devices and appliances. Soon the so-called 'Internet of Things' will become the norm in American households. Algorithms will soon be driving our cars and organising our lives.

63. This is not just about technology today, we have to seriously consider the implications for tomorrow. To put it bluntly, we risk walking into the future blind and unprepared.

64. What happens when your cousin's DNA profile affects your insurance because an algorithm has used someone else's data to infer risks about you? What happens when an algorithm targets ads that provoke your daughter's body image issues because it has inferred this is the optimal way to sell her a product? What happens when our appliances and physical spaces are influenced by algorithms that start to make decisions about what you can eat, see or experience? What happens when an innocent person is stopped on the street because the police used a biased dataset? What happens when monolithic technology platforms start taking sides and distort our elections?

65. Some of us worry about big government robbing us of our freedom – but what about big data?

66. Data is the new electricity of our digital economy. And just like electricity, we cannot escape data. It is nearly impossible for the average American to stop using social

media, search engines, apps and e-mail, but still be functional in the workplace and in society. We should therefore be wary of any company that presents a false dichotomy between our privacy rights and living in a modern digitised society. Online platforms' terms and conditions present users with a false choice because using the Internet is no longer a choice. Americans cannot opt out of the 21st century.

67. Data protection is a consumer safety issue and we cannot continue putting the burden on consumers by using this false narrative of choice. We don't allow buildings to lack fire exits as long as there are terms and conditions posted on the wall. We do not allow automotive companies to build unsafe cars as long as they include warning labels. In every other sector, we empower public regulators to create safety standards. Because safety matters. So why should software and online platforms be any different?

68. Legislators have an opportunity to create expert-led technology safety authorities to enforce standards for user safety, just as we already do for everything else we value: our cars, electricity, appliances, medicines, buildings and food. Regulators do not need to be the adversaries of innovation, but innovation must always put the safety of people first.

69. Technology companies may claim that rules inhibit growth in the sector. But car safety standards have not inhibited innovation or demand, nor have they unreasonably inhibited profit. Seat belts do not stop people from buying cars and privacy engineered software will not stop people from using online platforms.

70. Technology is a social issue. Technology is a national security issue. Technology is a consumer rights issue. Everyone has a stake in this, not just engineers. My generation's future will involve technology in almost every space and part of our lives.

71. I am still optimistic about the future of technology. But we should not walk into the future blind, and it is the job of lawmakers to ensure that technology serves citizens and not the other way around.

**CHRISTOPHER WYLIE**

**16 MAY 2018**