Written evidence submitted by Dr Emma L Briant, American University, Washington, DC, USA. (OSB0155)

In 2018-19 I published testimony to several international inquiries on Cambridge Analytica and reports containing important recommendations. My contributions to the inquiries outlined new developments in influence, including how online activities have increasingly been monitored and monetized, and are being made successively more vulnerable to powerful actors abusing data for propaganda targeting as well as initial proposals on how to tackle these specific problems. Three years on, propaganda, data misuse, disinformation, and strategic influence present some of the most complex and rapidly evolving challenges for civil society and policymakers in our time. Though my proposals were included in the Digital Culture Media and Sport Committee's final report from their inquiry into disinformation, they were not acted upon – not only has the role of influence firms and 'disinformation for sale' not been properly addressed by this government but sub,itted bythe Information Commissioner's Office (ICO) in the UK, was halted at the discretion of the Commissioner without public announcement and without delivering on the report into Cambridge Analytica's servers that was promised to parliament in autumn 2019. Questions remained unanswered and there is much still to do. I write here to give my 2021 expert opinion and recommendations as the UK Parliament considers its Draft Online Safety Bill after a great deal of additional research.

Evidence in the second Impeachment of Donald Trump and subsequent investigations has highlighted the role a coordinated propaganda campaign played in inciting the disturbing violence of the January 6 attacks as well as the role of veterans who may have been targeted on social media. Disinformation and how to respond to it remains an important issue for governments worldwide. Many ideas have been proposed to tackle the problems of unintended misinformation, and intentional disinformation within wider influence operations. My statement here builds on an earlier report which details reforms needed to shape a more transparent and accountable influence architecture, incentivize more ethical behaviour among industries using data for persuasion. Many actors are engaged in influence activities – these might include democratic and authoritarian governments, NGO's, politicians, individuals and corporations, criminals and terrorists. This report considers influence broadly with an aim of making changes that could help enable a safer, more democratic information environment for citizens. It aims to inform policymakers, government, civil society and private organizations and my comments based on extensive research into systems of information warfare of western governments and the role of private 'influence industry'[1] contractors in this including lengthy interviews with those working in the field (also see Briant, 2015a, 2015b, 2018a, forthcoming 2020); submissions to numerous investigations and inquiries (2018b, 2018c, 2018d, 2018e, 2018f). I hope to address issues that I feel are overlooked by this Bill as well as a concerning general tendency for government not to enable transparent independent regulation but to shut down open

[1] I use term the 'influence industry' as we have seen an evolution and maturation of big data influence firms that no longer operate like traditional PR or advertising companies – these should not be normalized as the digital equivalent. A new industry has emerged transformed by surveillance capitalism which is marked by a hybridity between intelligence firms, commercial advertising firms and political campaign contractors and raises new problems for democracy.

government and anti-corruption measures and centralize control of information. I am concerned that this Bill will reinforce this.

Facebook and Trust

Against platforms such as Facebook we must act - I previously addressed the European Parliament in 2019 with the metaphor that "You make cars – you belch out fumes. …We legislate for cleaner air." – This holds true both for platforms and the influence industry which remails largely unregulated in the UK. The externalities of both categories of company are deeply damaging but need to be tackled separarely and differently. There is an assumption being made that trying to address Facebook and other major platforms will have a corresponding effect on influence firms which are social media companies' clients. But this does not necessarily follow. Influence firms often obscure, mislead and make it harder to tackle international problems.

Politicians and governments have incentivized this model by their own interests in working with such firms and international legislation is needed to change it beyond the UK.

Research I recently contributed along with lead researcher Brent Allpress to the film People You May Know, includes evidence of US religious non-profits' misuse of data related to financial crisis, addiction, relationship stress and mental health for Republican political campaigns which in recent years have been advancing conspiracy theories. My research on Cambridge Analytica showed the company to be running extremely concerning experiments in 2016 on hundreds of thousands of US citizens testing fear messaging against neurotic people. These abuses occurred long before lists were uploaded to one of the major features unaddressed by recent policy, allowing influence operations to hide - Facebook's 'custom audiences' feature. This is a tool that allows advertisers to create and upload their own lists for targeting, and it is subject to abuse. Cambridge Analytica used it to upload a list of highly anxious neurotics they had experimented on, targeting fear-based and paranoid conspiracy messaging. Mental health data (lists exist online regardless of privacy restrictions) or other concerning datasets could be uploaded (persons with a propensity for violence, people interested in white nationalism, critics of authoritarian states...). How a 'custom audience' was compiled before uploading to Facebook is not volunteered by the advertiser or sought by Facebook. In the US Rep. Trahan's Social Media Data Transparency Bill asks platforms to seek "A description of the targeted audience for each advertisement" including audience demographics and interests, which could be used by researchers. However, Facebook would have no way of knowing how the lists have been compiled, checking the accuracy of descriptions, nor would researchers beyond the obvious demographics it would be hard to check. A list of candidate supporters could actually be a list of people with depression for example – how would one know? Some of these could be harvested online and while it is important to encourage people to be open about mental health, it is still important to bear in mind how publicly shared data could potentially be used as I pointed out in Congressional testimony.[2] Policymakers should insist that Facebook's upload custom audiences feature cease as it is easily abused and impossible for Facebook to properly ensure safety.

[2] Emma L Briant (June 2018) 'Evidence for the US Senate Judiciary Committee on Cambridge Analytica and SCL Group', published by US Senate Judiciary Committee, discussed at hearing on: Cambridge Analytica and the Future of Data Privacy.

It is not an exaggeration to say that some of the measures Facebook is introducing to respond to extremism are mirroring measures the Stasi and Soviet Union deployed in enabling mutual surveillance for social control. Getting people to monitor and report on each other is not the answer to disinformation and the spread of conspiracy theories. It is likely to fuel the paranoia that drives them. There is in fact a long history of failure too in this having negative counter-effects in counter-extremism... the UK's Prevent strategy is a case in point where educators were encouraged to flag small children and students as potentially exhibiting indicators for radicalization. This was shown to be subject to racial biases and cultural misunderstandings... Its new incarnation runs the risk of increasing suspicion within societies at a time when we need greater understanding and it can be extremely subjective what someone considers 'radical'. Reporting could be weaponized against the divisions in society by actors seeking to turn groups against each other making people suspicious of each other. The program gives certain messaging that might be based on 'othering' a sort of legitimacy. I see this as most likely to bolster paranoia around the platforms and increase divisions, distrust and partisanship in society with mutual suspicion. It also will have different effects among different cultural groups where some cultures have more concern and legacy memory around such snitching and its use by authorities. And it will be abused by people against those they dislike leading to a bulk of difficult and disputed cases that Facebook or any mediating scholars or NGO's will need to make subjective judgement upon. Finally the best answer to the very real issue of falsehood circulating on surveillant platforms is not more data for platforms farmed with our own paranoid snitching.

Explosive growth of social media like Facebook opened the door to big data analytics, psychographics, and the techniques of surveillant advertising. But the parent company of Cambridge Analytica, SCL Group, among more recent companies drew on *military and intelligence methodologies*, and growing access to social media data and the technology within our phones has developed mercenary surveillant and coercive influence capabilities. Policy has actually encouraged surveillant, data-driven propaganda for sale. It might be that taking ethical contracts SCL wouldn't have been able to offer as competitive a product and that's why Cambridge Analytica was set up – we need to disincentivize this and tweaks to Facebook won't achieve this. Transparency is a huge part of this but is not enough – as evidenced by SCL CEO Nigel Oakes comments in my evidence, notoriety can even drive up business and so professionalization that ensures regulation is necessary – blatant ethical breaches by influence-for-hire should be met with real penalties and fines that hurt.

Protecting Journalism and Ensuring Government Transparency

So what is the answer? The primary problem in our society is not just falsehood but highly targeted and algorithmically amplified systems advancing fear, anxiety and distrust. This, particularly backed with personal data enabling measurement of our propensity to such motivators encourages and facilitates the sharing of propaganda - both truthful information used to mislead and falsehood. Governments need to invest in privacy and build trust. It is vital, particularly given the centrality of anti-government conspiracies that the UK prioritize transparency and openness in how it handles information. This Online Safety Bill and accompanying measures such as 'Legislation to Counter State Threats (Hostile State

Activity)' that are extremely counter-productive to tackling the spread of propaganda by foreign and domestic entities.

The 6 January coup attempt in the US shifted debates around tackling disinformation from public health concerns to white nationalist extremism – quite reasonably 'securitizing' the policy debate. Government must play a vital role in tackling influence operations, but caution should be heeded because the wrong kinds of responses could produce unintended effects, increased distrust and threaten human rights. In the wake of the January 6th insurrection in the United States, the Stanford Internet Observatory researcher Renee DiResta has proposed a "centralized task force" for the Biden administration to respond to misinformation and conspiracy theories. This entity led by a "reality czar" would "meet regularly with tech platforms, and push for structural changes that could help those companies tackle their own extremism and misinformation problems" and create "exemptions" to privacy laws for "platforms to share data" about conspiracy theory communities with the US Government. The last thing governments should create would be perceived as a surveillant propaganda unit pressuring the platforms which will feed the paranoia that these threats thrive on.

The UK needs to learn from this by making the OFCOM regulator transparent. Misinformation is best tackled with transparent government that builds trust, strong journalism and supports digital and media literacy and a strong public service media protected from political influence. The proposed extension of an Official Secrets Act - which was always out of step with allies such as the US – will criminalize whistleblowing and journalism that are essential to building public trust in government and preventing Russian and misleading ideological outlets filling a void left by strong, critical national security reporting. This is happening at a time when journalists have been unfairly blacklisted and singled out for inconsistent refusals of FOIA and press inquiries resulting in their profiling.UK is running the risk Transparency and open government has become increasingly restricted in the UK – see my recent evidence to the Home Office.

Governments worldwide seek to respond to foreign and domestic influence threats. It is crucial for democracies to strike the right balance, ensuring their activities are limited and build trust through transparency and restraint. Democratic governments over-reach not only undermines trust in their message but can be used to justify repressive tactics by authoritarian regimes. Some recent efforts in the information domain have fuelled the crisis of trust that currently embattles us. Most memorably, in 2018 SCL Group were revealed to have sold in political campaigns worldwide the behavioral influence methods developed for defence which they had drawn on research by DARPA and DSTL. Wider concern about the lack of restrictions to prevent military tactics being redeployed by veterans commercially include recent concerns over the origins and spread of QAnon. There have been several over examples where influence by western governments has raised issues over process, transparency or domestic influence concerns:

- Procurement processes and hiring companies also working for unethical clients,
- The 2018 exposure of the 'Integrity Initiative' which misrepresented itself as a charity and was caught putting out political messaging against the opposition Labour Party,

- The US public diplomacy found targeting US based audiences with pro-Trump political messaging,
- The misleading Home Office website 'On The Move' set up to deter asylum seekers
- In Canada a rash of domestic targeting and training 'accidents' revealing weak governance.

Secrecy is not the answer as I have explained elsewhere - the truth and indeed damaging information will come out. It's better to have strong, truthful public affairs.

It is not good enough for governments to argue that further secrecy is needed because of public criticism – we need more robust oversight and governance in place. Despite my recommendation being taken up in the final report of the DCMS Inquiry into Fake News and Disinformation, there seems to be little effort to respond to the problem of conflicts of interest and security risks concerning influence companies working across commercial, political and national security domains – a concern I highlighted to investigations in 2018.

Over-classification must be addressed in the UK and given the increasing role of the private sector in recent decades, it is essential private contractors for government are made subject to FOIA in the US and UK - something which the UK Government refused to do in 2016. The argument that it is too onerous is increasingly flimsy.

There is a myth that secrecy makes us safer – the reality is it often allows continuing poor work to remain hidden and unevaluated while rhetoric of 'innovation' is touted. My own research indicates the level of plausible deniability and cutaways necessary to remove British fingerprints, actually reduce oversight and leave us vulnerable to subversion and corporate and state attempts to undermine national security. Governments must cooperate with informing platforms and allowing transparency over accounts they are responsible for, whether or not these are paid for by an intermediary, and these should be labelled online as long as this does not conflict with safety.

Global Internet Forum to Counter Terrorism

A body was established by Facebook, Microsoft, Twitter and YouTube in 2017 called the Global Internet Forum to Counter Terrorism. Its goals were to establish norms and coordinate content removal across different platforms. Evelyn Douek from Harvard has called it "the most underrated project in the future of free speech" and I would agree – it is essentially hosting a form of 'blacklist'. Some information sharing and coordination is essential – but so is transparency over the organization and its processes. The GIFCT website states that "the Global Network on Extremism and Technology will be folded into three strategic pillars designed to house and foster additional work programs and maximize transparency". Its 'Independent Advisory Committee', includes members from civil society, governments, and intergovernmental bodies – but government representatives are not made transparent. When I asked the UK Government to disclose who is on this committee and their role in government, I learned this was someone from the UK Home Office, but further information was denied as "exempt from disclosure under Section 38(1) of the Freedom of Information Act 2000. It is vital that the UK's involvement in this body be transparent. This section of the Act pertains to health and safety and is a qualified exemption, which requires consideration of the Public Interest Test." As Richard Norton

Taylor points out, the definition of "terrorism" is loosely defined and too often interpreted in ways that curb civil liberties. Government influences on content removal MUST be transparent – this is the epitome of unaccountable censorship and – who by? One must question whether the UK representative on GIFCT is from the Research, Information and Communications Unit (RICU) – a Home Office body that has been embroiled in domestic propaganda scandals with some critics accusing it of domestic surveillance of Muslims in relation to its 'prevent' counter-extremism efforts. FOIA is no longer fit for purpose in an age when giant companies like Facebook act together to make policy decisions in opaque ways in coordination with government and as powerful as a government with no transparency. FOIA should be extended to encompass private companies working on contracts with government.

The UK must introduce FOIA for intelligence agencies to bring it in line with other democracies such as the US. Further, my own FOIA experience has also revealed a major concern with respect to Information Commissioners' Office oversight of FOI requests and complaints concerning security and the UK Ministry of Defence. The ICO does not have an ability to access relevant information held by the Ministry of Defence in the case of a complaint to review whether a decision really was 'public interest'. It instead of reviewing the actual documents is forced to evaluate security-related complaints based on an opaque process of reviewing hand-selected partial information that ministry provides to justify that its own decision. This is not accountable. The ICO cannot evaluate the MoD decision without seeing the documents, which means there can be no public confidence in the process.

Government Strategic Communication and Contemporary Information Warfare

Strong oversight and more transparency of intelligence and information warfare would improve trust. The former head of UK's MI6 Sir Richard Dearlove has also recommended an independent panel meeting privately to give scrutiny and oversight of security and intelligence comprised of NGO's, experts and citizens group – a measure which would provide essential oversight and build trust in any democracy. Additionally there needs to be clear information about the status of UK Government online communications and these also need to be available to researchers. Often even the overt state-linked Western media and propaganda are not labelled transparently enough requiring researchers and citizens to dig through externally facing websites or accounts to find how a regional 'news' page is funded. Social media accounts by affiliates should include clearer transparency information declaring they have received funding or other support. Non-attribution is often used for reasons of effectiveness when targeting enemies, for example in deception operations (or through the Pentagon's Regional Web Interaction Program).

During a public information crisis, building public trust through accountability and transparency is vital. It is the best way to anticipate and deflate the efforts of attackers who will continue to seek ways to leak and misrepresent those activities. At minimum, as Prof Grygiel of Syracuse University has argued political state media ads such as those disseminated by VOA should be added to Facebook's archive of political ad posts for which they display a 'paid for by' disclosure. Political ad databases must contain information about the targeting of ads and companies who created them. Currently Twitter has been unveiling

new labelling for state-associated media – however this has been done very inconsistently. All state-linked accounts should be marked, including those of Western Governments propaganda and public diplomacy accounts like Voice of America. Not to do so fuels very reasonable accusations of hypocrisy and bias, it is counter-productive and fuels related conspiracy theories - undermining credibility and trust at a time when 'fake news' attacks on media have left many unable to know who to trust. Platforms should be making clear all state funding and this should include accounts run by organizations funded by state funded organizations like the National Endowment for Democracy and those run by government contractors. Government contractors or other intermediaries who are managing attributable accounts should also be identified in transparency information.

In public diplomacy it is preferable to provide grants that support credible local independent journalism and NGOs, funding or other relationships should be declared more clearly in all but the rarest circumstances such as to guarantee safety in high risk environments. In democracies, Public Affairs, Public Diplomacy and PSYOP activities – which are intended to be 'white' and truthful operations - are increasingly deconflicted and coordinated with other information activities, a process which needs more scrutiny and transparency in the UK.

Transparency and the Influence Industry

It is unsurprising that the Cambridge Analytica scandal emerged from a British defense contractor, SCL; Britain, despite its size, is a world centre for private military contractors and the EU's primary centre for intelligence firms partly because it is a more opaque environment to do business - weaker lobbying laws than the United States for example. Post-9/11 counter-terror wars placed Israel as another world center for private intelligence firms, and US provides a huge market, it headquartered 122 intelligence firms in 2016. The intelligence and the inter-connected 'influence industry'[3] are both mutually dependent upon the largescale amassing of data 'surveillance capitalism' creates and surged worldwide in the 2000's as powerful clients have increasingly bought the promise data-driven surveillance and manipulation. Companies work across multiple domains, and despite the final Digital, Culture, Media and Sport committee highlighting my comments about the conflicts of interest posed by this. I argued for strict regulation of the industry but there has been little done to address problems in the influence industry in the wake of the CA scandal.

Influence firms appear and disappear, often having no website, occasionally with vaguely worded services offered – a transparency issue common in defense. A regulator or license could require UK or US registration, a clear statement of all a companies' services, countries it has worked in, senior directors and staff. Regulating and imposing better standards of online and offline behaviour for the influence industry would – along with measures to address transparent funding – be the longer-term solution reducing the need for reactive measures and censorship of platforms in many cases. It would address a failure here to

[3] I use term the 'influence industry' as we have seen an evolution and maturation of big data influence firms that no longer operate like traditional PR or advertising companies – these should not be normalized as the digital equivalent. A new industry has emerged transformed by surveillance capitalism which is marked by a hybridity between intelligence firms, commercial advertising firms and political campaign contractors and raises new problems for democracy.

consider the offline components of UK influence industry harms, alongside online disinformation campaigns. We also must impose codes of practice to ensure human rights based policy and companies operating abroad including their 'partners' and networks are held to domestic legal standards even when working abroad and fines and revocation of licenses/kite mark could be a possible penalty clear violations. UK-based influence and traditional private security companies have been observed to operate under a system of 'self-regulation' and national laws or working with partners to navigate the international legal space. If a company works in Human Rights Priority countries, the clients must be declared. Transparency and accountability databases can also be used to force greater transparency over these transactions and clients. Industries presently see unethical work as negative externalities of keeping your business going in the industry but this must not be standard in democracies like the US and UK – it is essential to find ways to require or incentivize through transparency a more ethical business standard as I argued in 2018.

Perhaps no-one appreciated just *how* bad this influence operations crisis was in 2016. But they should have and the last four years have not achieved a resolution. If we don't change policy, ensuring transparency and both strong oversight in government contracting and licensing or regulation in the private influence industry working in politics and commercial influence internationally we will perpetually reproduce an unethical model. The UK can play a leading role in incentivising an ethical industry.

As a British citizen I hope my representatives take my recommendations seriously.

28 September 2021