Building a stronger and more secure democracy in a digital age
A Response to Recent Interim Reports and Proposals by: U.S. Senate Select Committee on Intelligence; & U.K. Parliament Digital, Culture, Media and Sport Select Committee Inquiry into Fake News.

Responses to the Problem of ‘Fake News’ and Digital Propaganda in Democracies
This year, a series of whistleblowers, journalistic investigations and public inquiries exposed systems in which the public, as their online activities have increasingly been monitored and monetized, are being made successively more vulnerable to powerful actors abusing data for propaganda targeting.\(^1\) This is enabled by digital platforms and influence industry applications that consumers trust, and which obscure their central purpose as part of their business model. Inquiries interrogated the respective roles of: the campaigns themselves; foreign actors such as Russia; digital media platforms; influence industry companies and their business models and methodologies. As the inquiries mature, policymakers are suggesting solutions for the problem of ‘fake news’ and digital campaign practices that may undermine democracy. For the Digital, Culture, Media and Sport [DCMS] Select Committee (July 2018) Fake News Inquiry and Sen. Mark Warner (U.S. Senate Select Committee on Intelligence), proposals largely focus on: Information Operations (IO) and coordinated responses to Russia; privacy and transparency measures largely focused on encouraging better behavior from digital platforms like Facebook; and providing public media education. Central to debates has been the extent to which platforms like Facebook are complicit, enabling mis- or dis-information and misuse of data, or failing to act. Scholarly proposals rightly emphasize a need to address the monopoly of these platforms by forcing data portability and allowing competition and plurality (Baron et al 2017; Freedman, 2018; Tambini, 2017, for example). However, a central question remains about the influence industry itself. As democratic governments sought extended powers of surveillance and information warfare to enable them to counter threats post-9/11, they also helped to build a digital infrastructure and a corresponding influence industry that advantaged their range of action at home and abroad (Bakir, 2018; Briant, 2015). My own research focuses on propaganda and my submission helped expose the role of Cambridge Analytica (CA) and SCL Group (their parent company) and indicated problems which seem to be largely unaddressed by recent proposals.\(^2\) Importantly, if UK and US responses are likely to include more IO, targeting Russia, it is unfortunate that both reports fail to address the fact the company central to the scandal emerged out of IO contracting for US and UK governments and NATO. Policymakers must consider whether oversight and intelligence mechanisms were adequate as they failed to identify or prevent a developing problem, the public must see changes that will ensure there can be no recurring issues with another contractor.

Key Recommendations:

US and UK inquiries examining the intelligence and oversight mechanisms in IO contracting, strengthening these systems.
1. The adequacy of oversight of networks of companies that could be designed to obscure their activities;
2. How to ensure defense-derived expertise and techniques are not:
   a. used in electoral campaigns,

---

1 The scope was far reaching, including the UK’s EU Referendum, 2016 US election and other international elections such as those in Nigeria (2014) and Kenya (2013/2017).
2 See the Fake News Inquiry in April and June (Briant, 2018a; 2018b).
b. pitched to organisations with risk factors for national security.

The following proposals should be considered as possible solutions:

a. Monitoring and restriction of technologies and methods developed by contractors with defense collaboration/funding being used in elections or pitched for any work abroad
b. Restriction of former information operations/intelligence/psychological operations personnel from working subsequently in political campaigns
c. Greater transparency in government contracting, reporting mechanisms, substantial penalties for defense contractors found obscuring overlaps and company relationships from government

A dual strategy ensuring both plurality of platforms and regulation of influence industry to protect media users.

1. Data portability for platforms like Facebook essential to ensure competition and reduce monopoly power.
2. Regulation or professional licensing in the influence industry as in other professions. Professional industry licensing could be revoked on evidence of serious violations of codes of conduct.

Unaddressed Problems in the Influence Industry

Many of those who best anticipated how powerfully ‘big data’ would transform ‘influence’, were those who saw it as an opportunity to be exploited for profit. The opaque and monopolistic business models of digital platforms have recently been scrutinized, highlighting the implications of data harvesting and misuse as well as consent and privacy issues. To solve this, is vital to enable data portability (Cyphers and O’Brien, 2018), something unlikely to be successfully achieved if left to the goodwill of profit-orientated companies like Facebook (Freedman, 2018). Yet if we enable consumers to ‘be in control of’ their data, we need to protect them too, to ensure we are not making them vulnerable to other companies like Cambridge Analytica, who may be keen to obtain and exploit their data in further unethical ways. We must address a problem not just of social media companies, but of an influence industry with deeply concerning norms.

These companies grew not just from political campaigning and commercial advertising, but some via our own governments’ information warfare expertise (Bakir, 2018; Briant, 2015; 2018a; 2018c; 2018d; Wylie, 2018a). There has long been a revolving door between military and intelligence and private influence industries (Bakir, 2018 12-13; Briant, 2015: 93; 69-73). PR companies, and wider cultural industries have frequently been involved in wartime propaganda (see for example Bakir, 2018; Stonor-Saunders, 2000). It is fair that government employees want jobs after they leave public service, but particularly as defense and intelligence methodologies increase in sophistication, we must take more seriously the risk of knowledge migrating into commercial and electoral campaigning (Briant, 2015; 2017; 2018a). Specific training and/or knowledge formally or informally acquired in a military or intelligence context could include: disinformation and deception techniques; methods used to demoralize an enemy; methods of harnessing psychological weaknesses or violent tendencies within a population or group; methods for influencing extremists, or increasing or decreasing inter- and intra-group tensions; techniques and specialist knowledge about surveillance and hacking; all of which many would recognize would be inappropriate knowledge to risk having among teams handling election campaigns if we wish to prioritize the protection of democracy. The inquiries and journalistic investigations have raised concerns about relationships between a defense contractor, SCL, and Cambridge Analytica, who ran political campaigns; concerns included possible data, financial and staffing overlaps with some staff on defense projects working on political campaigns (Briant, 2018a; Wylie, 2018a; Wylie, 2018b pp6-7;
Vickery, 2018), and questions of whether defense-derived methodologies or possible hacking\(^3\) may have been used in political campaigns (Wylie, 2018a; Kaiser, 2018; Briant, 2018a; Cadwalladr, 2018). It cannot be a question of personal integrity, it raises too great a level of risk. And it can be hard for people to speak out, particularly in the light of silencing strategies deployed by governments in the national security domain (Bakir, 2018: 57; Briant & Wanlass, In Print 2018).

Strict regulation of the influence industry, or perhaps professional licensing that can be revoked on evidence of abuse, would not only protect citizens, it would give substance to a truthful narrative that would undermine Russian and other hostile narratives directed at democracies. And it would commercially protect the industry itself, creating a resulting ‘soft power’ economic benefit for industry and Western governments.

It is vital governments not shy away from considering how companies seek to adapt services developed for defense beyond that domain, for example by adapting a business model or company structure to obscure what they do in lucrative political campaigns. SCL were a government contractor who developed their methodology through their own research facility, the ‘Behavioural Dynamics Institute’ (BDI), including through collaboration with US government’s Defense Advanced Research Projects Agency (DARPA) (Briant, 2018; Wylie, 2018a). All SCL Group companies could draw on the methodologies developed. If these may have been able to inform tactics deployed in democratic elections this is very serious.

In her Fake News Inquiry testimony Brittany Kaiser, former Development Manager for Cambridge Analytica revealed that:

“I found documents from Nigel Oakes, the co-founder of the SCL Group, who was in charge of our defence division, stating that the target audience analysis methodology, TAA, used to be export controlled by the British Government. That would mean that the methodology was considered a weapon—weapons grade communications tactics—which means that we had to tell the British Government if that was going to be deployed in another country outside the United Kingdom. I understand that designation was removed in 2015.” (Kaiser, 2018).

The potential for defense-derived methods and knowledge to be commercially sold in other industries raises further risks to national security, as techniques could migrate abroad. Concern was raised by whistleblowers over Cambridge Analytica’s pitches to Lukoil, a Russian FSB-connected oil company, while SCL Group were delivering counter-Russian propaganda training for NATO, that methods for both might be based on a similar methodological core and could be utilized by Russia (Briant, 2018c; Wylie, 2018a; Kaiser, 2018). My own evidence indicates around the same time, Alexander Nix from CA contacted Julian Assange at Wikileaks about amplifying the release of damaging emails; Russia has been accused of the hacking of these, which it denies (Briant, 2018a; Shane & Mazzetti, 2018).

The Role of Government Planning and Oversight

CA and many SCL Group companies may have gone bankrupt now, but SCL Insight appears to remain (Siegelman, 2018a) and new companies are growing from their ashes (Auspex International, Emerdata and Datapropria for example – Datapropria, 2018; Murdock, 2018; Siegelman, 2018b). These companies are part of a wider industry (Briant, 2015). Proposals from the inquiries emphasize IO or defense responses to Russia, but do not fully consider how to address the concerns raised about that industry, or how intelligence and oversight might be strengthened to prevent future recurrence. It is important to ensure potential vulnerabilities that might have contributed to the crisis are addressed (see Bakir, 2018 on the persistent challenges of oversight). As I stated in my evidence, Nigel Oakes, the CEO of defense contractor SCL Group told me in interview that, ‘

\(^3\) Something denied by Former Cambridge Analytica Business Development Director Brittany Kaiser (2018).
defense people can’t be seen to be getting involved in politics, and the State Department, they get very upset so Oakes stated that they imposed ‘strong lines’ between the companies (Briant, 2018a). If the State Department had expressed concern, one might wonder if this could be due to the troublingly anti-democratic and potentially destabilizing roles CA played in international elections in Nigeria, Kenya and beyond (Cadwalladr, 2018; Wylie, 2018a; Wylie, 2018b). Oakes’ comments imply that the State Department may have been concerned that there was something to be ‘upset’ about in the conduct of, or relationships between, the companies. Oakes, the defense contractor, stressed his importance to the methods underpinning what CA did, saying that if Alexander Nix was ‘the Steve Jobs, I’m the Steve Wozniak. I’m sort of the guy who wants to get the engineering right and he’s the guy who wants to sell the flashy box. And he’s very good at it. And I admire him enormously for doing it. But I’m the guy who say, yeh, but without this you couldn’t do any of that!’ (Briant, 2018a). It is vital that US and UK governments, including research entities like DARPA who worked with BDI, build into private contracts more control over tools and weapons they help to create for information warfare.

The public also to know that networks of companies cannot obscure unethical practices, flows of data, financial interests or possible conflicts of interest with foreign powers – all concerns raised in the Cambridge Analytica scandal. On the question of related companies the UK report states:

“SCL’s alleged undermining of democracies in many countries, by the active manipulation of the facts and events, was happening alongside work done by the SCL Group on behalf of the UK Government, the US Government, and other allied governments. We do not have the remit or the capacity to investigate these claims ourselves, but we urge the Government to ensure that the National Crime Agency thoroughly investigates these allegations.” (Paragraph 231 DCMS Committee, July 2018)

However, this seems to be beyond the current scope of the UK National Crime Agency and a UK Defence Select Committee Inquiry is needed to review this and why UK export control restrictions were removed.

Investigations in both countries should ensure oversight is fully reviewed, particularly in relation to oversight of groups of companies, protection against commercial exposure of IO practices and migration into elections. Transparency in government contracting, stronger oversight and reporting mechanisms, and reforms in the industry such as licensing that could be revoked or fines set at a deterrent level that can prevent future scandals are essential in both countries. Transparency in the US could be improved by a reporting system for private companies equivalent to Companies House in the UK. There could also be penalties for defense contractors in each country found obscuring overlaps and company relationships. Digital ‘whack-a-mole’ banning of particular techniques, or dropping of companies as they are exposed in the media would leave us falling short of responding to complex multi-layered adaptive manipulation and or preventing problems as a fast-moving industry develops.

While Damian Collins MP of the UK Fake News Inquiry and Sen. Mark Warner are rightly cautious about government interventions regulating the media, improved oversight in the national security

---

4 Parkinson & Parkinson (2003) consider arguments for and against licensing in PR. The Public Relations Society of America for example has a voluntary code of ethics intended to ‘inspire’ companies’ good behaviour and explains why it stopped enforcing this: ‘Organizations that have enforceable regulations, rules and procedures are empowered by higher authorities often government or quasi-government organizations who can license or delegate the power to enforce and sanction.’ - this is absent in the US context (PRSA, 2018).

5 See: https://www.gov.uk/government/organisations/companies-house

6 However, recent legal cases in the US are challenging whether lies are protected free speech, for example in a recent legal case concerning Alex Jones it was argued that “False speech does not serve the public interest
realm, electoral protections and licensing in the influence industry provide little threat to free speech, indeed unethical conduct in the influence industry could be argued to threaten free speech and democratic debate. Policymakers should ensure a) competition is enabled via data portability and b) influence industries are properly regulated, with enforced codes of conduct, professional licensing we see in other professions, and robust monitoring of companies and individuals beyond their contracts to ensure defense technologies are restricted and elections are protected. Preconditions for resolving this are of course greater transparency in the industry and may include dedicated monitoring by expert-led independent regulators. This would actually strengthen an industry in which the absence of regulation has become unsustainable, threatening democracy and national security in this case. Current unethical practices can also be exploited by those wishing to spread narratives about the ‘corrupt West’ and weakness of democracy. The measures proposed above will together ensure that data portability produces competition and therefore innovation, and concurrently ensure that media consumers are not vulnerable to the actions of unethical companies. Democratic controls would strengthen public trust in democracy, help to protect and secure our elections and have a long term ‘soft power’ benefit for both countries.

Bibliography
Cyphers, B & O'Brien, D (2018) 'Facing Facebook: Data Portability and Interoperability Are Anti-Monopoly Medicine' in Electronic Frontier Foundation:

the way that true speech does,” … “And indeed, there is no constitutional value in false statements of fact.” (Feuer, 2018).
Datapropria (2018) 'Data and Behavioral Science Experts' Datapropria.com
Siegelman, W (2018b) 'They're Back: Ex-Cambridge Analytica employees launch Auspex International to focus on social and political campaigns in the Middle East and Africa' in Medium: https://medium.com/@wsiegelman/theyre-back-ex-cambridge-analytica-employees-launch-auspex-international-to-focus-on-social-and-aa51a0ab6fca

August 2018