The Mind Benders -- the Weaponization of Your Data by Big IT

by Roberto J. González via claire - Counterpunch *Monday, Mar 26 2018, 2:17am*
international / prose / post

How to Harvest Facebook Data, Brainwash Voters, and Swing Elections

> In the days and weeks following the 2016 presidential elections, reports surfaced about how a small British political consulting firm, Cambridge Analytica, might have played a pivotal role in Donald Trump's surprise victory. The company claimed to have formulated algorithms to influence American voters using individually targeted political advertisements. It reportedly generated personality profiles of millions of individual citizens by collecting up to 5000 data points on each person. Then Cambridge Analytica used these "psychographic" tools to send voters carefully crafted online messages about candidates or hot-button political issues.

Although political consultants have long used "microtargeting" techniques for zeroing in on particular ethnic, religious, age, or income groups, Cambridge Analytica's approach is unusual: The company relies upon individuals' personal data that is harvested from social media apps like Facebook. In the US, such activities are entirely legal. Some described Cambridge Analytica's tools as "mind-reading software" and a "weaponized AI [artificial intelligence] propaganda machine." However, corporate media outlets such as CNN and the Wall Street Journal often portrayed the company in glowing terms.

Cambridge Analytica is once again in the headlines–but under somewhat different circumstances. Late last week, whistleblower Christopher Wylie went public, explaining how he played an instrumental role in collecting millions of Facebook profiles for Cambridge Analytica. This revelation is significant because until investigative journalist Carole Cadwalladr published her exposé in The Guardian, Cambridge Analytica's then-CEO Alexander Nix had adamantly denied using Facebook data. And although Facebook officials knew that Cambridge Analytica had previously gathered data on millions of users, they did not prohibit the company from advertising until last Friday, as the scandal erupted. To make matters worse, the UK's Channel 4 released undercover footage early this week in which Cambridge Analytica executives boast about using dirty tricks–bribes, entrapment, and "beautiful girls" to mention a few.

The case of Cambridge Analytica brings into focus a brave new world of electoral politics in an algorithmic age–an era in which social media companies like Facebook and Twitter make money by selling ads, but also by selling users' data outright to third parties. Relatively few countries have laws that prevent such practices–and it turns out that the US does not have a comprehensive federal statute protecting individuals' data privacy. This story is significant not only because it demonstrates what can happen when an unorthodox company takes advantage of a lax regulatory environment, but also because it reveals how Internet companies like Facebook have played fast and loose with the personal data of literally billions of users.

From Public Relations to Psychological Warfare

In order to make sense of Cambridge Analytica it is helpful to understand its parent company, SCL Group, which was originally created as the PR firm Strategic Communications Laboratory. It was founded in the early 1990s by Nigel Oakes, a flamboyant UK businessman. By the late 1990s, the company was engaged almost exclusively in political projects. For example, SCL was hired to help burnish the image of Indonesian president Abdurrahman Wahid–but Oakes and SCL employees had to shut down their operations center when SCL's cover was blown by the Wall Street Journal .

In July 2005, SCL underwent a dramatic transformation. It very publicly rebranded itself as a psychological warfare company by taking part in the UK's largest military trade show. SCL's exhibit included a mock operations center featuring dramatic crisis scenarios–a smallpox outbreak in London, a bloody insurgency in a fictitious South Asian country–which were then resolved with the help of the company's psyops techniques. Oakes told a reporter: "We used to be in the business of mindbending for political purposes, but now we are in the business of saving lives." The company's efforts paid off. Over the next ten years, SCL won contracts with the US Defense Department's Combatant Commands, NATO, and Sandia National Labs.

Over the past few years SCL–now known as SCL Group–has transformed itself yet again. It no longer defines itself as a psyops specialist, nor as a political consultancy–now, it calls itself a data analytics company specializing in "behavioral change" programs.

Along the way it created Cambridge Analytica, a subsidiary firm which differs from SCL Group in that it focuses primarily on political campaigns. Its largest investors include billionaire Robert Mercer, co-CEO of hedge fund Renaissance Technologies, who is best known for his advocacy of far-right political causes and his financial support of Breitbart News. Steve Bannon briefly sat on Cambridge Analytica's board of directors.

Cambridge Analytica first received significant media attention in November 2015, shortly after the firm was hired by Republican presidential nominee Ted Cruz's campaign. Although Cruz ultimately failed, Cambridge Analytica's CEO, Alexander Nix, claimed that Cruz's popularity grew largely due to the company's skillful use of aggregated voter data and personality profiling methods. In August 2016, the Trump campaign hired Cambridge Analytica as part of a desperate effort to challenge Hillary Clinton's formidable campaign machine. Just a few months later, reports revealed that Cambridge Analytica had also played a role in the UK's successful pro-Brexit "Leave.EU" campaign.

Hacking the Citizenry

Cambridge Analytica relies upon "psychographic" techniques that measure the Big Five personality traits borrowed from social psychology: openness, conscientiousness, extroversion, agreeableness and neuroticism.

In the US, Cambridge Analytica developed psychological profiles of millions of Americans by hiring a company called Global Science Research (GSR) to plant free personality quizzes. Users were lured by the prospect of obtaining free personality scores, while Cambridge Analytica collected data–and access to users' Facebook profiles. Last week, The Guardian reported that Cambridge Analytica collected data from more than 300,000 Facebook users in this way. By agreeing to the terms and conditions of the app, those users also agreed to grant GSR (and by extension, Cambridge Analytica) access to the profiles of their Facebook "friends"–totalling approximately 50 million people.

Psychographics uses algorithms to scour voters' Facebook "likes," retweets and other social media data which are aggregated with commercially available information: land registries, automotive data, shopping preferences, club memberships, magazine subscriptions, and religious affiliation. When combined with public records, electoral rolls, and additional information purchased from data brokers such as Acxiom and Experian, Cambridge Analytica has raw material for shaping personality profiles. Digital footprints can be transformed into real people. This is the essence of psychographics: Using software algorithms to scour individual voters' Facebook "likes," retweets and other bits of data gleaned from social media and then combine them with commercially available personal information. Data mining is relatively easy in the US, since it has relatively weak privacy laws compared to South Korea, Singapore, and many EU countries.

In a 2016 presentation, Nix described how such information might be used to influence voter opinions on gun ownership and gun rights. Individual people can be addressed differently according to their personality profiles: "For a highly neurotic and conscientious audinece, the threat of a burglary–and the insurance policy of a gun. . .Conversely, for a closed and agreeable audience: people who care about tradition, and habits, and family."

Despite the ominous sounding nature of psychographics, it is not at all clear that Cambridge Analytica played a decisive role in the 2016 US presidential election. Some charge that the company and its former CEO Alexander Nix, exaggerated Cambridge Analytica's effect on the election's outcome. In February 2017, investigative journalist Kendall Taggart wrote an exposé claiming that more than a dozen former employees of Cambridge Analytica, Trump campaign staffers, and executives at Republican consulting firms denied that psychographics was used at all by the Trump campaign. Taggart concluded: "Rather than a sinister breakthrough in political technology, the Cambridge Analytica story appears to be part of the traditional contest among consultants on a winning political campaign to get their share of the credit–and win future clients." Not a single critic was willing to be identified in the report, apparently fearing retaliation from Robert Mercer and his daughter Rebekah, who is also an investor in the firm.

Not-So-Innocents Abroad

By no means has Cambridge Analytica limited its work to the US. In fact, it has conducted "influence operations" in several countries around the world.

For example, Cambridge Analytica played a major role in last year's presidential elections in Kenya, which pitted incumbent Uhuru Kenyatta of the right-wing Jubilee Party against Raila Odinga of the opposition Orange Democratic Movement. The Jubilee Party hired Cambridge Analytica in May 2017. Although the company claims to have limited its activities to data collection, earlier this week Mark Turnbull, a managing director for Cambridge Analytica, told undercover reporters a different story. He admitted that the firm secretly managed Kenyatta's entire campaign: "We have rebranded the party twice, written the manifesto, done research, analysis, messaging. I think we wrote all the speeches and we staged the whole thing–so just about every element of this candidate," said Turnbull.

Given the most recent revelations about Cambridge Analytica's planting of fake news stories, it seems likely that the company created persuasive personalized ads based on Kenyans' social media data. Fake Whatsapp and Twitter posts exploded days before the Kenyan elections. It is worth remembering that SCL Group has employed disinformation campaigns for military clients for 25 years, and it seems that Cambridge Analytica has continued this pattern of deception.

The August elections were fraught with accusations of vote tampering, the inclusion of dead people as registered voters, and the murder of Chris Msando, the election commission's technology manager, days before the election. When the dust settled, up to 67 people died in post-election violence–and Kenyatta ultimately emerged victorious. Weeks later, the Kenyan Supreme Court annulled the elections, but when new elections were scheduled for October, Odinga declared that he would boycott.

Given Kenya's recent history of electoral fraud, it is unlikely that Cambridge had much impact on the results. Anthropologist Paul Goldsmith, who has lived in Kenya for 40 years, notes that elections still tend to follow the principle of "who counts the votes," not "who influences the voters."

But the significance of Cambridge Analytica's efforts extends beyond their contribution to electoral outcomes. Kenya is no technological backwater. The world's first mobile money service was launched there in 2007, allowing users to transfer cash and make payments by phone. Homegrown tech firms are creating a "Silicon Savannah" near Nairobi. Two-thirds of Kenya's 48 million people have Internet access. Ten million use Whatsapp; six million use Facebook; two million use Twitter. As Kenyans spend more time in the virtual world, their personal data will become even more widely available since Kenya has no data protection laws.

Goldsmith summarizes the situation nicely:

Cambridge Analytica doesn't need to deliver votes so much as to create the perception that they can produce results. . .Kenya provides an ideal entry point into [Africa]. . .Embedding themselves with ruling elites presents a pivot for exploiting emergent commercial opportunities. . .with an eye on the region's resources and its growing numbers of persuadable youth.

Recent reports reveal that Cambridge Analytica has ongoing operations in Mexico and Brazil (which have general elections scheduled this July and October, respectively). India (which has general elections in about a year) has also been courted by the company, and it is easy to understand why: the country has 400 million smartphone users with more than 250 million on either Facebook or Whatsapp. India's elections are also a potential gold mine. More than half a billion people vote in parliamentary elections, and the expenditures are astonishing: Political parties spent $5 billion in 2014, compared to $6.5 billion in last year's US elections. India also has a massive mandatory ID program based on biometric and demographic data, the largest of its kind in the world.

Cambridge Analytica's global strategy appears focused on expanding its market share in promising markets. Although many people might describe Kenya, Mexico, Brazil, and India as developing countries, each in fact has a rapidly growing high-tech infrastructure, relatively high levels of Internet penetration, and large numbers of social media users. They all have weak or nonexistent Internet privacy laws. Though nominally democratic, each country is politically volatile and has experienced episodic outbursts of extreme political, sectarian, or criminal violence. Finally, these countries have relatively young populations, reflecting perhaps a long-term strategy to normalize a form of political communication that will reap long-term benefits in politically sensitive regions.

The capacity for saturating global voters with charged political messages is growing across much of the world, since the cost of buying Facebook ads, Twitterbots and trolls, bots for Whatsapp and other apps is cheap–and since more people than ever are spending time on social media. Such systems can be managed efficiently by remote control. Unlike the CIA's psyops efforts in the mid-20th century, which required extensive on-the-ground efforts–dropping leaflets from airplanes, bribing local journalists, broadcasting propaganda on megaphones mounted on cars–the new techniques can be deployed from a distance, with minimal cost. Cambridge Analytica relies upon small ground teams to do business with political parties, and partnerships with local business intelligence firms to scope out the competition or provide marketing advice, but most of the work is done from London and New York.

Weaponizing Big Data?

From its beginnings, Cambridge Analytica has declared itself to be a "data-driven" group of analytics experts practicing an improved form of political microtargeting, but there are indications that the firm has broader ambitions.

In March 2017, reports emerged that top executives from SCL Group met with Pentagon officials, including Hriar Cabayan, head of a branch which conducts DoD research and cultural analysis. A decade ago, Cabayan played an instrumental role in launching the precursor to the Human Terrain System, a US Army counterinsurgency effort which embedded anthropologists and other social scientists with US combat brigades in Iraq and Afghanistan.

A few months later, in August 2017, the Associated Press reported that retired US Army General Michael Flynn, who briefly served as National Security Director in the Trump administration, had signed a work agreement with Cambridge Analytica in late 2016, though it is unclear whether he actually did any work for the firm. Flynn pleaded guilty to lying to the FBI about his contacts with Russian operatives in late 2017, when he was working with Trump's transition team. Given his spot in the media limelight, it is easy to forget that he once headed US intelligence operations in Afghanistan, advocating for a big data approach to counterinsurgency that would, among other things, include data collected by Human Terrain Teams.

The connections between Cambridge Analytica/SCL Group and the Pentagon's champions of data-driven counterinsurgency and cyberwarfare may be entirely coincidental, but they do raise several questions: As Cambridge Analytica embarks on its global ventures, is it undertaking projects that are in fact more sinister than its benign-sounding mission of "behavioral change"? And are the company's recent projects in Kenya, India, Mexico, and Brazil simply examples of global market expansion, or are these countries serving as laboratories to test new methods of propaganda dissemination and political polarization for eventual deployment here at home?

Here the lines between military and civilian applications become blurred, not only because ARPANET–the Internet's immediate precursor–was developed by the Pentagon's Advanced Research Projects Agency, but also because the technology can be used for surveillance on a scale that authoritarian regimes of the 20th century could only have dreamed about. As Yasha Levine convincingly argues in his book Surveillance Valley: The Secret Military History of the Internet, the Internet was originally conceived as a counterinsurgency surveillance program.

Neutralizing Facebook's Surveillance Machine

It appears that many people are finally taking note of the digital elephant in the room: Facebook's role in enabling Cambridge Analytica and other propagandists, publicists, and mind-benders to carry out their work–legally and discreetly. As recently noted by Lorenzo Franceschi-Bicchierai in the online journal Motherboard, Cambridge Analytica's data harvesting practices weren't security breaches, they were "par for the course. . .It was a feature, not a bug. Facebook still collects—and then sells—massive amounts of data on its users." In other words, every Facebook post or tweet, every g-mail message sent or received, renders citizens vulnerable to forms of digital data collection that can be bought and sold to the highest bidder. The information can be used for all kinds of purposes in an unregulated market: monitoring users' emotional states, manipulating their attitiudes, or disseminating tailor-made propaganda designed to polarize people.

It is telling that Facebook stubbornly refuses to call Cambridge Analytica's actions a "data breach." As Zeynep Tufekci, author of the book Twitter And Tear Gas: The Power and Fragility of Networked Protest puts it, the company's defensive posture reveals much about the social costs of social media. She recently wrote:

“If your business is building a massive surveillance machinery, the data will eventually be used and misused. Hacked, breached, leaked, pilfered, conned, targeted, engaged, profiled, sold. There is no informed consent because it’s not possible to reasonably inform or consent.”

Cambridge Analytica is significant to the extent that it illuminates new technological controlling processes under construction. In a supercharged media environment in which Facebook, Twitter, and WhatsApp (owned by Facebook) have become the primary means by which literally billions of people consume news, mass producing propaganda has never been easier. With so many people posting so much information about the intimate details of their lives on the Web, coordinated attempts at mass persuasion will almost certainly become more widespread in the future.

In the meantime, there are concrete measures that we can take to rein in Facebook, Amazon, Google, Twitter, and other technology giants. Some of the most lucid suggestions have been articulated by Roger McNamee, a venture capitalist and early Facebook investor. He recommends a multi-pronged approach: demanding that the social media companies’ CEOs testify before congressional and parliamentary committees in open sessions; imposing strict regulations on how Internet platforms are used and commercialized; requiring social media companies to report who is sponsoring political and issues-based advertisements; mandating transparency about algorithms (“users deserve to know why they see what they see in their news feeds and search results,” says McNamee); requiring social media apps to offer an “opt out” to users; banning digital “bots” that impersonate humans; and creating rules that allow consumers (not corporations) to own their own data.

In a world of diminishing privacy, our vulnerabilities are easily magnified. Experimental psychologists specializing in what they euphemistically call “behavior design” have largely ignored ethics and morality in order to help Silicon Valley companies create digital devices, apps, and other technologies that are literally irresistible to their users. As the fallout from Cambridge Analytica’s activities descends upon the American political landscape, we should take advantage of the opportunity to impose meaningful controls on Facebook, Google, Twitter, and other firms that have run roughshod over democratic norms–and notions of individual privacy–in the relentless pursuit of profit.

Follow link below for additional embedded information:

https://tinyurl.com/ydbctatf