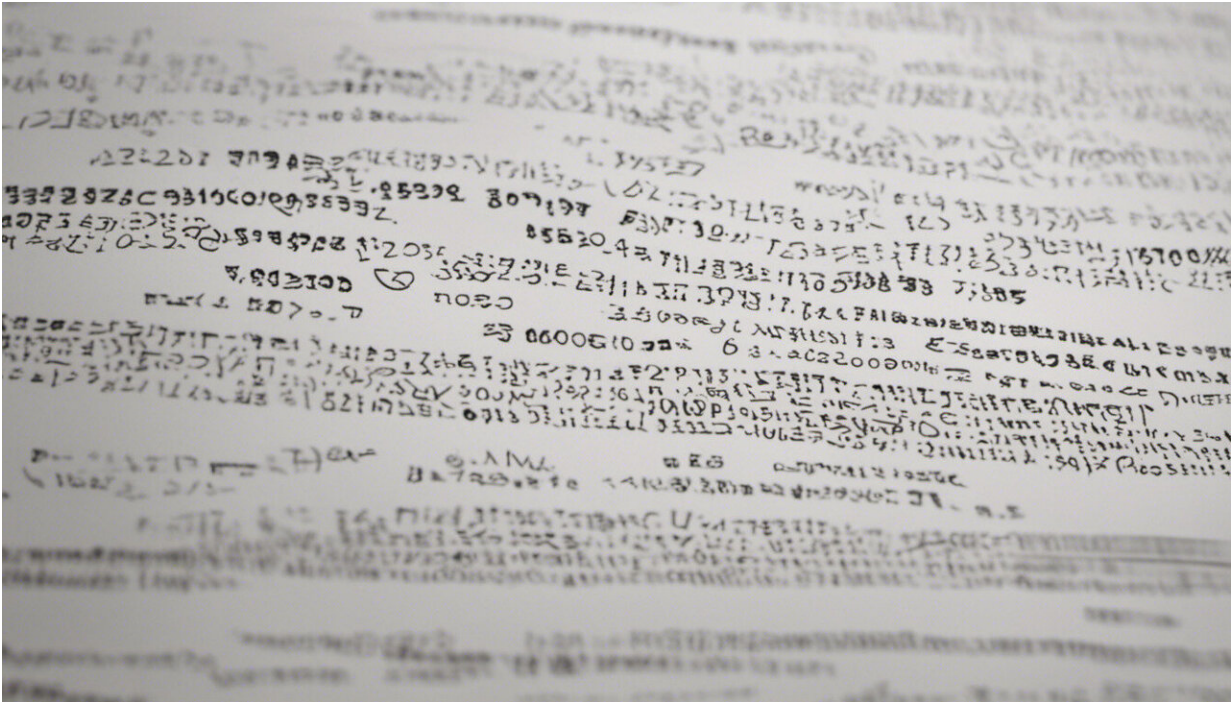# Data-driven elections and the key questions about voter surveillance

August 6 2019, by David Lyon And Colin Bennett

Credit: AI-generated image ([disclaimer](#))

The upcoming Canadian federal election once again raises the spectre of interference and disruption through the misuse and abuse of personal data.

This is a surveillance issue, because as experts who study surveillance,

we know political consultancy companies are collecting, analyzing and using data in order to powerfully influence populations who are [generally unaware of how their data is being processed](). Opacity and complexity are [common features of contemporary surveillance issues]().

These questions have come to global public attention as a result of the [Cambridge Analytica and Facebook scandals]().

The now-defunct Cambridge Analytica has become a symbol of all that is intrusive and manipulative about data-driven elections.

Nonetheless, data and [data analytics]() have played a role in elections for years. All modern campaigns in all democracies use data—even if it's simply polling data.

But today's massive voter relationship management platforms use digital campaigning practices that leverage the power of social media, mobile apps, geo-targeting and artificial intelligence to take it to another level.

A recent workshop organized through the [Big Data Surveillance]() project and hosted by the [Office of the Information and Privacy Commissioner of British Columbia](), brought together international scholars, civil society advocates and regulators to take stock in the wake of the Cambridge Analytica scandal.

How can we understand the nature and effects of data-driven elections in different countries? What issues will tax our regulators in the years ahead?

Myths versus realities

Digital campaigning and harnessing the power of Big Data [has long been considered a key to electoral success in the United States and]()

[increasingly in other countries](#).

Politicians the world over now believe they can win elections if they just have better, more refined and more accurate data on the electorate.

At one stage, Cambridge Analytica claimed to have about 5,000 different data points on the American electorate. They were not alone. The voter analytics industry in the U.S. —including companies like [Catalist](#), [i360](#) and [HaystaqDNA](#)—boasts an extraordinary volume of personal data under their control. The data is both free and purchased, and from public and commercial sources.

A recent report by the [Tactical Tech collective](#) in Germany documents the range of companies, consultancies, agencies and marketing firms—from local startups to global strategists —that aggressively target parties and campaigns across the political spectrum. Data is used as an asset, as intelligence and as influence.

At the same time, the power of data-driven elections is exaggerated. Evidence on how and whether Big Data actually does win elections is difficult to determine empirically. Research by U.S. communications expert Jessica Baldwin-Philippi suggests that [data-driven campaign strategies are far more effective at mobilizing adherents and donors than in persuading voters](#). Emphasis on size and scale often is conflated as claims of effectiveness.

The U.S. versus the rest

Generally, voter analytics have been pioneered in the U.S. and exported to other democratic countries. A startling recent illustration is the pernicious use of WhatsApp in Brazil for the [spread of racist, misogynistic and homophobic messages by Jair Bolsonaro's campaign when he successfully ran for president](#).

In other countries, the field of voter analytics faces constraints that temper and perhaps twist its impact.

These include campaign finance restrictions, varying party and electoral systems and many different electoral laws and data protection rules.

How are local political party workers and volunteers to navigate the terrain, especially when the actual methods and alleged impacts of voter analytics are so unclear?

No political party wants to appear dated in its methods or fall behind its rivals for failing to recognize the supposed benefits of data analysis for success.

But as researchers, we know too little about how data-driven campaigning interacts with different institutional and cultural practices. Nor do we know how data is assessed by professionals and volunteers at local and central levels of campaigns around the world.

It's also clear that the major platforms of Google and Facebook perform differently in different countries. University of North Carolina journalism and media professor Daniel Kreiss [compares Google and Facebook as "democratic infrastructures"](#) in terms of the services offered.

Even platforms claiming to be non-ideological, like the prominent voter-tracker [Nationbuilder](#), are hardly apolitical, as Concordia University's Fenwick McKelvey [has shown](#). Google algorithms also demonstrate [the inherent political biases built into its search functions](#).

New practices versus dated laws

Outdated laws govern the voter analytics industry and digital

campaigning. These include elections laws that control the circulation of lists, and data protection laws that, until recently, [have not been used to regulate the capture, use and dissemination of personal data by political campaigns](#).

Data protection laws, such as the [European Union's General Data Protection Regulation (GDPR)](#), constrain thecapture and processing of sensitive personal data on political opinions.

But the problems don't just involve privacy and intrusiveness —they also include data governance, freedom of speech, disinformation and democracy itself. Data-driven elections require new thinking about the balance between the democratic interest of an informed and mobilized public on one side and the dangers of excessive voter surveillance on the other.

Transparency versus secrecy

A related key issue, not limited to data-driven elections but illustrated acutely by them, is the question of transparency.

There is a divide between how little is publicly known about what actually goes on in platform businesses that create online networks, like Facebook or Twitter, and what supporters of proper democratic practices argue should be known.

After all, when it comes to elections, the open sharing of relevant information is critical. Voter management platforms such as Cambridge Analytica are inherently secretive, both about their political paymasters and their actual practices. Few know who pays for political ads, for instance.

Those running and participating in elections, on the other hand, have a

vital interest in the transparency of all parties as the prerequisite of accountability. Because the use of data to influence election outcomes is fundamentally opaque, the tension is palpable.

It's therefore difficult to know what actually transpires within data-driven electioneering.

University of Wisconsin professor Young Mie Kim runs a stealth media project: a user-based, real-time digital ad tracking app that enables researchers to trace the sponsors of political campaigns in the U.S., identify suspicious sources and assess the patterns of voter-targeting.

The officials responsible for the conduct of elections should be paying close attention to this kind of information in Canada as the federal election approaches —and around the world.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation