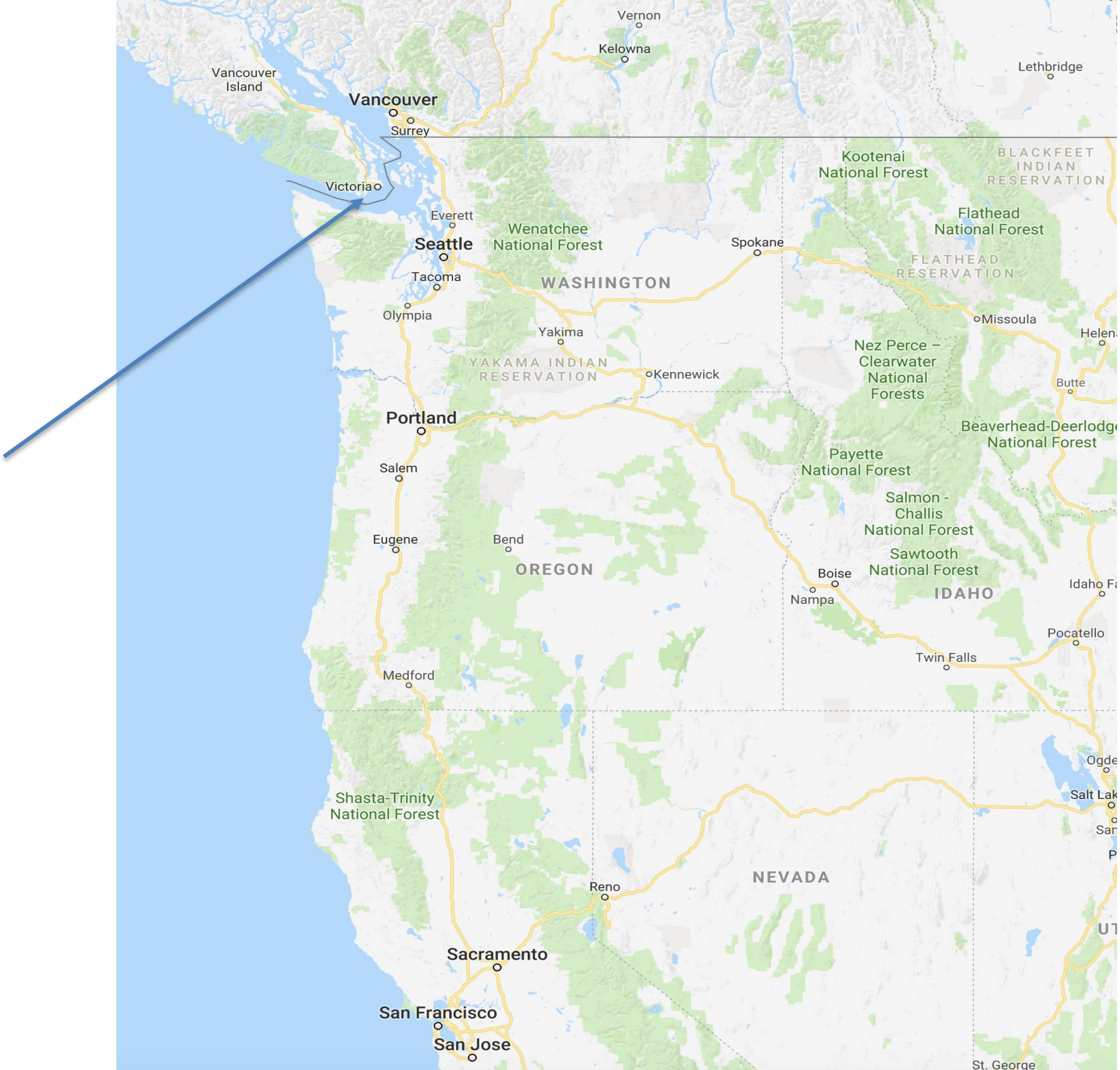
Data-driven elections and the micro-targeting of voters: key issues for privacy advocates

Professor Colin J. Bennett
Department of Political Science
University of Victoria
British Columbia, Canada
www.colinbennett.ca
cjb@uvic.ca

University of Victoria

Presentation to XI Brazilian Seminar on Privacy and Personal Data Protection (November 17, 2020)


Vernon
Kelowna
Lethbridge
Vancouver Island
Vancouver
Surrey
Victoria
Kootenai National Forest
BLACKFEET INDIAN RESERVATION
Everett
Wenatchee National Forest
Flathead National Forest
Seattle
Spokane
FLATHEAD RESERVATION
Tacoma
WASHINGTON
Olympia
Missoula
Yakima
Helena
Nez Perce – Clearwater National Forests
YAKAMA INDIAN RESERVATION
Kennewick
Butte
Portland
Beaverhead-Deerlodge National Forest
Payette National Forest
Salem
Salmon - Challis National Forest
Eugene
Bend
Sawtooth National Forest
OREGON
Boise
Idaho Fa
Nampa
IDAHO
Pocatello
Twin Falls
Medford
Ogde
Shasta-Trinity National Forest
Salt Lak
San
P
NEVADA
Reno
UT
Sacramento
San Francisco
San Jose
St. George

VICTORIA, BRITISH COLUMBIA

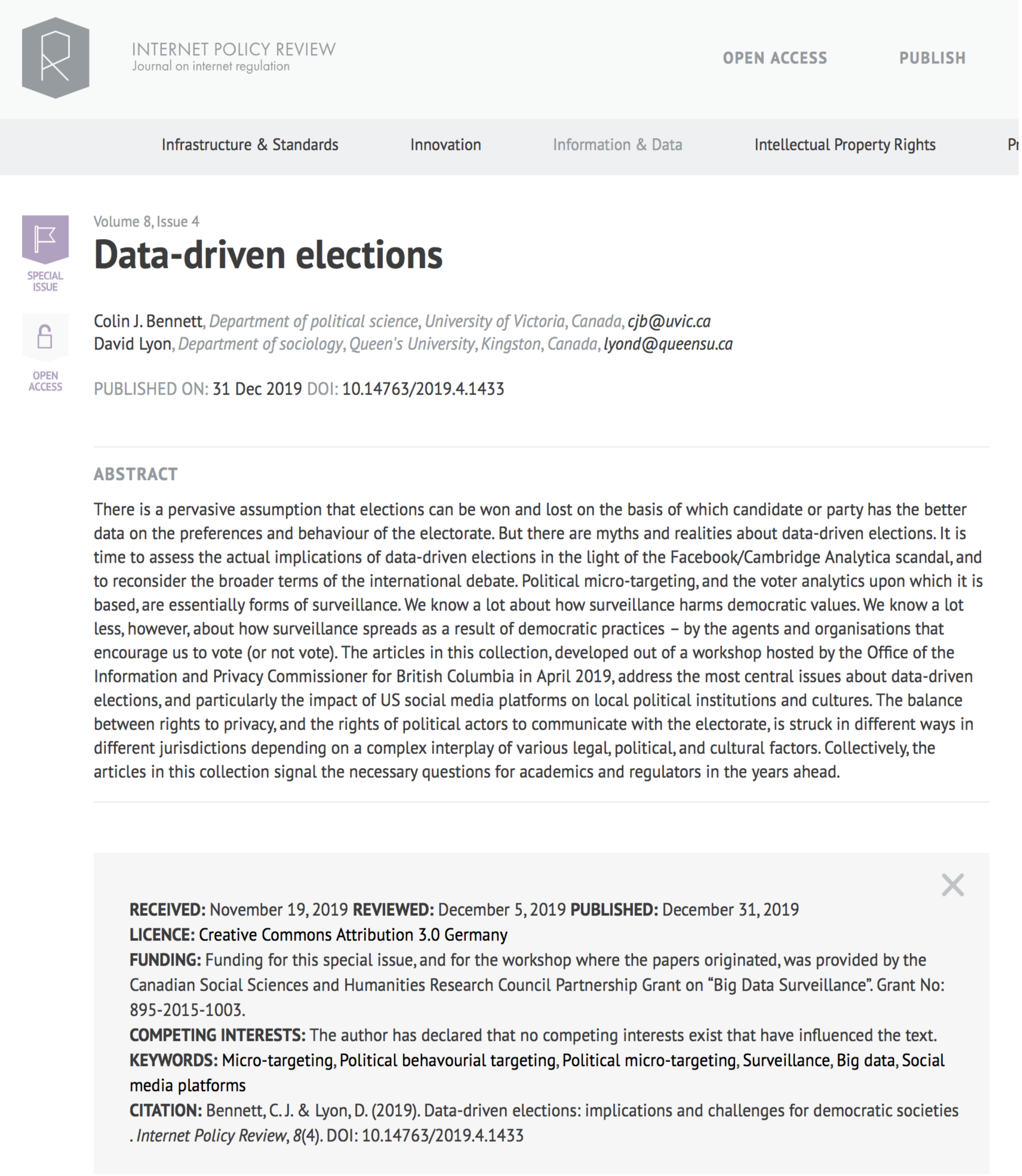
- HOME OF:
  - Legislature of British Columbia
  - Butchart Gardens
  - Killer Whales (Orcas)

AND….

- Aggregate IQ, Christopher Wylie and Elizabeth Denham

My Talk

- Voter surveillance and its effects on democracy
- Data-driven elections – the trends
- Factors that enable political micro-targeting
- Challenges for the protection of privacy
- Lessons for privacy advocates



Volume 8, Issue 4

Data-driven elections

Colin J. Bennett, *Department of political science, University of Victoria, Canada, cjb@uvic.ca*
David Lyon, *Department of sociology, Queen's University, Kingston, Canada, lyond@queensu.ca*

PUBLISHED ON: 31 Dec 2019 DOI: 10.14763/2019.4.1433

ABSTRACT

There is a pervasive assumption that elections can be won and lost on the basis of which candidate or party has the better data on the preferences and behaviour of the electorate. But there are myths and realities about data-driven elections. It is time to assess the actual implications of data-driven elections in the light of the Facebook/Cambridge Analytica scandal, and to reconsider the broader terms of the international debate. Political micro-targeting, and the voter analytics upon which it is based, are essentially forms of surveillance. We know a lot about how surveillance harms democratic values. We know a lot less, however, about how surveillance spreads as a result of democratic practices – by the agents and organisations that encourage us to vote (or not vote). The articles in this collection, developed out of a workshop hosted by the Office of the Information and Privacy Commissioner for British Columbia in April 2019, address the most central issues about data-driven elections, and particularly the impact of US social media platforms on local political institutions and cultures. The balance between rights to privacy, and the rights of political actors to communicate with the electorate, is struck in different ways in different jurisdictions depending on a complex interplay of various legal, political, and cultural factors. Collectively, the articles in this collection signal the necessary questions for academics and regulators in the years ahead.

RECEIVED: November 19, 2019 **REVIEWED:** December 5, 2019 **PUBLISHED:** December 31, 2019
LICENCE: Creative Commons Attribution 3.0 Germany
FUNDING: Funding for this special issue, and for the workshop where the papers originated, was provided by the Canadian Social Sciences and Humanities Research Council Partnership Grant on "Big Data Surveillance". Grant No: 895-2015-1003.
COMPETING INTERESTS: The author has declared that no competing interests exist that have influenced the text.
KEYWORDS: Micro-targeting, Political behavourial targeting, Political micro-targeting, Surveillance, Big data, Social media platforms
CITATION: Bennett, C. J. & Lyon, D. (2019). Data-driven elections: implications and challenges for democratic societies . *Internet Policy Review*, *8*(4). DOI: 10.14763/2019.4.1433

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Volume 8, Issue 4

WhatsApp and political instability in Brazil: targeted messages and political radicalisation

Rafael Evangelista, *Laboratory of Advanced Studies on Journalism (Labjor), State University of Campinas (Unicamp), Brazil, rae@unicamp.br*
Fernanda Bruno, *Communication and culture, Federal University of Rio de Janeiro (UFRJ), Brazil*

PUBLISHED ON: 31 Dec 2019 DOI: 10.14763/2019.4.1434

ABSTRACT

In the 2018 presidential election, Brazil elected a fringe congressman, Jair Bolsonaro, despite his radical rhetoric that would suffice to shake the public image of any candidate in the world and the lack of traditional resources of his campaign. One of the hypotheses for this electoral success is that his campaign built a specific communication strategy that used internet platforms to communicate directly with different groups of voters. We describe the Brazilian electoral scenario of 2018, focusing on the use of the messaging app WhatsApp. We discuss how Bolsonaro's campaign tapped into sentiments and perceptions spread by the legacy media, adding a stronger conservatism. We gather evidence of centralised management of WhatsApp chat groups by political actors that emerge from the work of computer scientists research, newspaper articles and our own ethnographic work. The radicalisation of Brazilian politics could be partially explained as an effect of the use of political micro-targeting in a highly concentrated news media ecosystem, and zero-rating policies that fuels WhatsApp popularity, a platform with affordances that favours the spread of misinformation.

RECEIVED: July 16, 2019 **REVIEWED:** November 21, 2019 **PUBLISHED:** December 31, 2019
LICENCE: Creative Commons Attribution 3.0 Germany
COMPETING INTERESTS: The author has declared that no competing interests exist that have influenced the text.
KEYWORDS: Political micro-targeting, Surveillance, Social media, Visibility, Brazil
CITATION: Evangelista, R. & Bruno, F. (2019). WhatsApp and political instability in Brazil: targeted messages and political radicalisation. *Internet Policy Review*, *8*(4). https://doi.org/10.14763/2019.4.1434

This paper is part of **Data-driven elections**, a special issue of *Internet Policy Review* guest-edited by Colin J. Bennett and David Lyon.

DEMOCRACY AND PRIVACY

- There is a rich tradition of trying to understand the role played by effective privacy protection within different forms of democracy.
  - For *liberal* democracy, privacy advances individual autonomy and self-fulfillment, and reinforces political competition.
  - For *participatory* democracy, privacy bolsters participation and engagement: voting freely, speaking out, engaging in interest groups, signing petitions, participating in civil society activism and protesting.
  - For *deliberative* democracy, privacy enhances the freedom to make choices under conditions of genuine reflection and equal respect for the preferences, values and interests of others.
- We know that privacy is important *for democracy*. Until recently, we have known relatively little about how privacy has been compromised *by democracy*, and by the agents that seek to mobilise, engage and encourage us to vote – or not to vote.

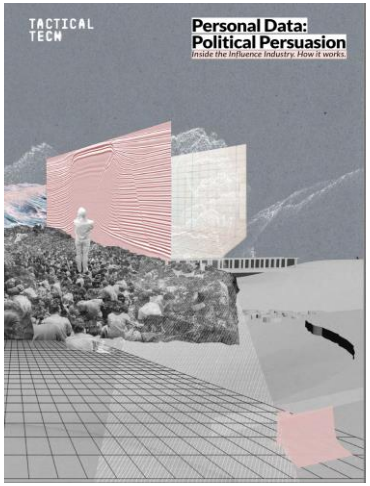
VOTER SURVEILLANCE AND DEMOCRACY

- Effects on divisiveness
- Effects on the “marketplace of ideas”
- Effects on political participation
- Effects on campaigning
- Effects on governance
- Effects on the party system and electoral competition

THE TRENDS

- Increasingly elections around the world are "data-driven" through a complex campaign "ecosystem"
- The entry of commercial behavioral marketing techniques into the world of political campaigning has produced a "political influence industry" where:
  - Personal data as a political asset through "voter relationship management systems"
  - Personal data as a political intelligence through testing and experimentation
  - Personal data as political influence – from mass messaging to micro-targeting

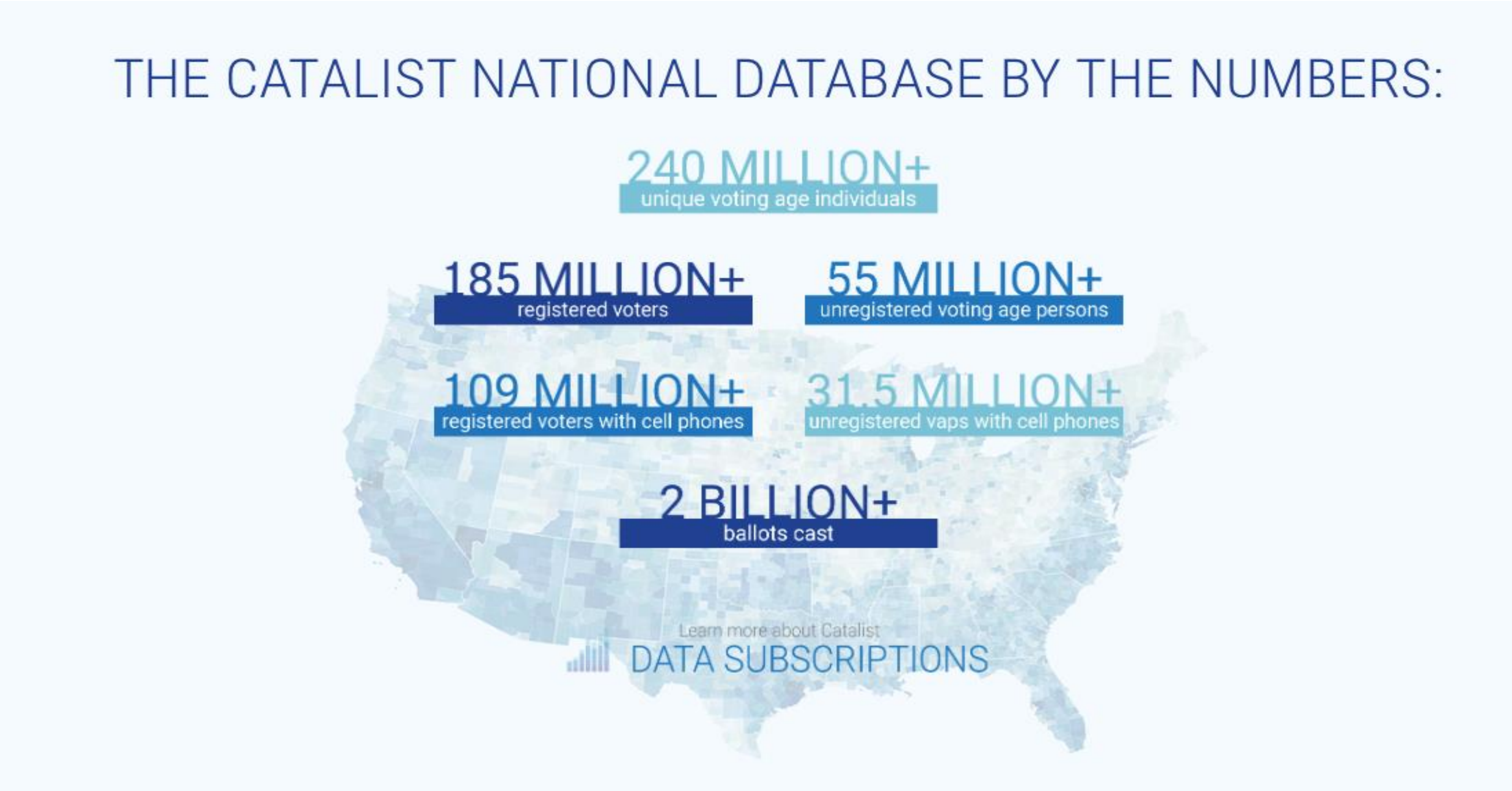
Tacticaltech.org


TACTICAL TECH
Personal Data: Political Persuasion
Inside the Influence Industry. How it works.

Data-Driven Elections in the US

- Massive accumulation of personal data on political affiliation in integrated Voter Relationship Managemen (VRM) systems
- Close alliances between political data brokers, digital advertising firms, and political parties
- Sophisticated personalization techniques using behavioral data, AI and machine-learning to produce highly granular ad-campaigns
- Use of commercial geo-spatial, mobile and geo-targeting strategies

Commercial Voter Analytics: Catalist.US



THE CATALIST NATIONAL DATABASE BY THE NUMBERS:

240 MILLION+
unique voting age individuals

185 MILLION+
registered voters

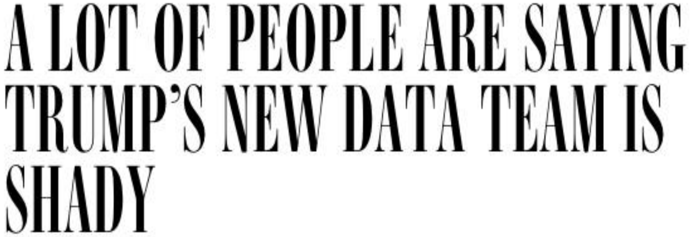
55 MILLION+
unregistered voting age persons

109 MILLION+
registered voters with cell phones

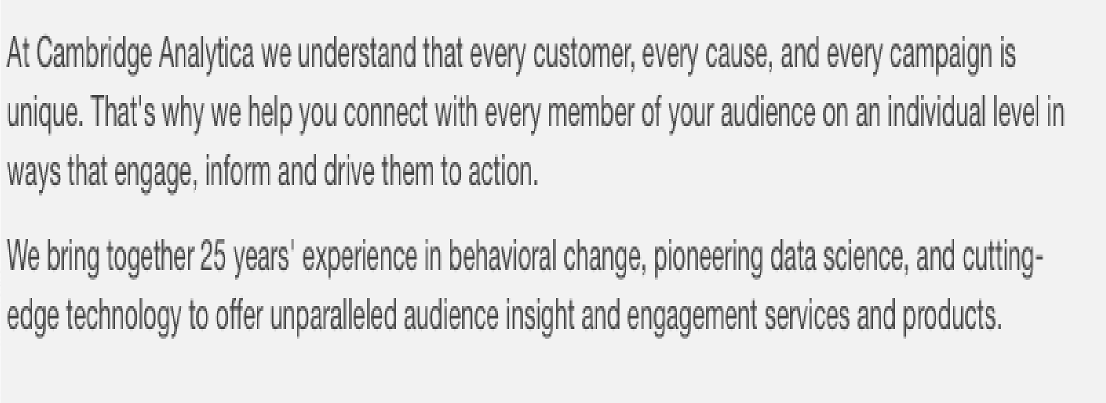
31.5 MILLION+
unregistered vaps with cell phones

2 BILLION+
ballots cast

Learn more about Catalist
DATA SUBSCRIPTIONS

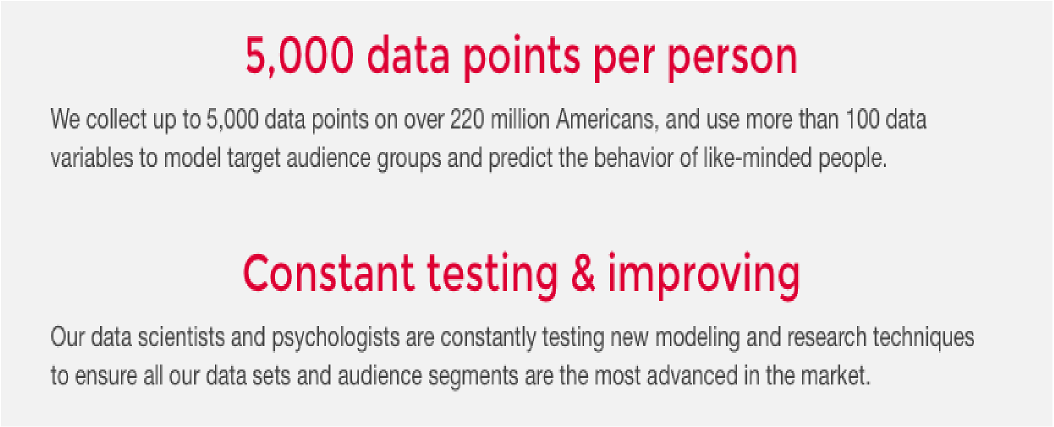


A LOT OF PEOPLE ARE SAYING TRUMP'S NEW DATA TEAM IS SHADY



At Cambridge Analytica we understand that every customer, every cause, and every campaign is unique. That's why we help you connect with every member of your audience on an individual level in ways that engage, inform and drive them to action.

We bring together 25 years' experience in behavioral change, pioneering data science, and cutting-edge technology to offer unparalleled audience insight and engagement services and products.



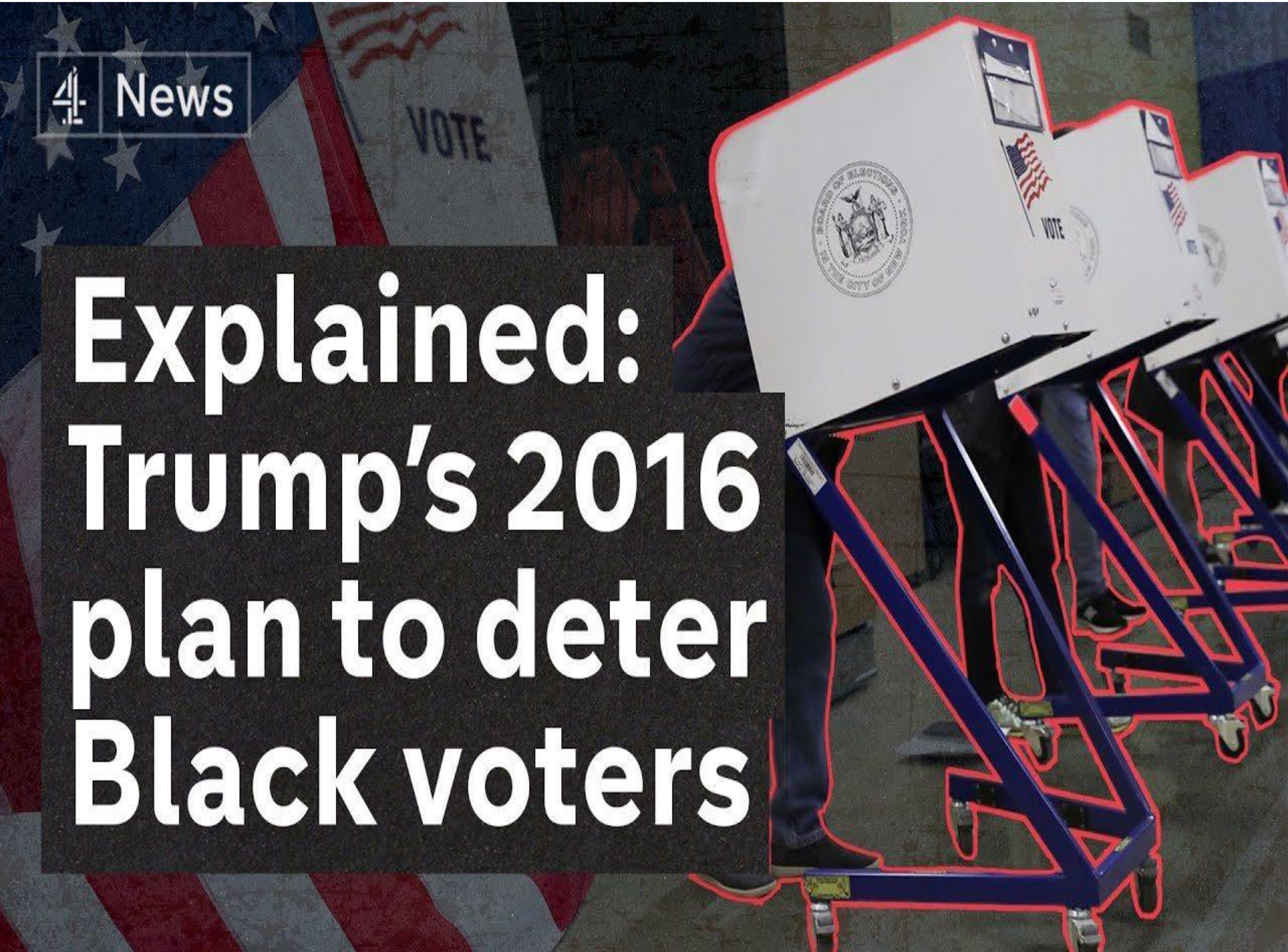
5,000 data points per person

We collect up to 5,000 data points on over 220 million Americans, and use more than 100 data variables to model target audience groups and predict the behavior of like-minded people.

Constant testing & improving

Our data scientists and psychologists are constantly testing new modeling and research techniques to ensure all our data sets and audience segments are the most advanced in the market.

CAMBRIDGE ANALYTICA – ALSO WORKED FOR LEAVE CAMPAIGN



4 News

Explained: Trump’s 2016 plan to deter Black voters

CAMPAIGN CHRONICLES

HOW THE TRUMP CAMPAIGN'S MOBILE APP IS COLLECTING HUGE AMOUNTS OF VOTER DATA

By Sue Halpern

September 13, 2020

[illegible]

Pro-Trump group targets Catholic voters using cellphone technology

'Geofencing' captures cellphone data of Mass-goers

Jan 2, 2020

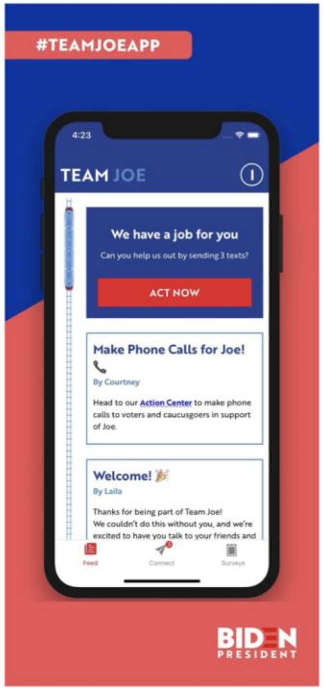
by **Heidi Schlumpf** | **Parish** | **Politics**

“Relational Organizing”

BIDEN
PRESIDENT

Step 2: Getting Ready to Take Action for Joe

When you first log in to your Team Joe App account, you will see your newsfeed and updates that will prepare you to take action for Joe! The red “Act Now” button at the top of the homepage and the bottom center “Connect” button will navigate you to action items.



We have a job for you

Can you help us out by sending 3 texts?

Make Phone Calls for Joe! ☎

By Courtney

Head to our Action Center to make phone calls to voters and caucusgoers in support of Joe.

Welcome! 🎉

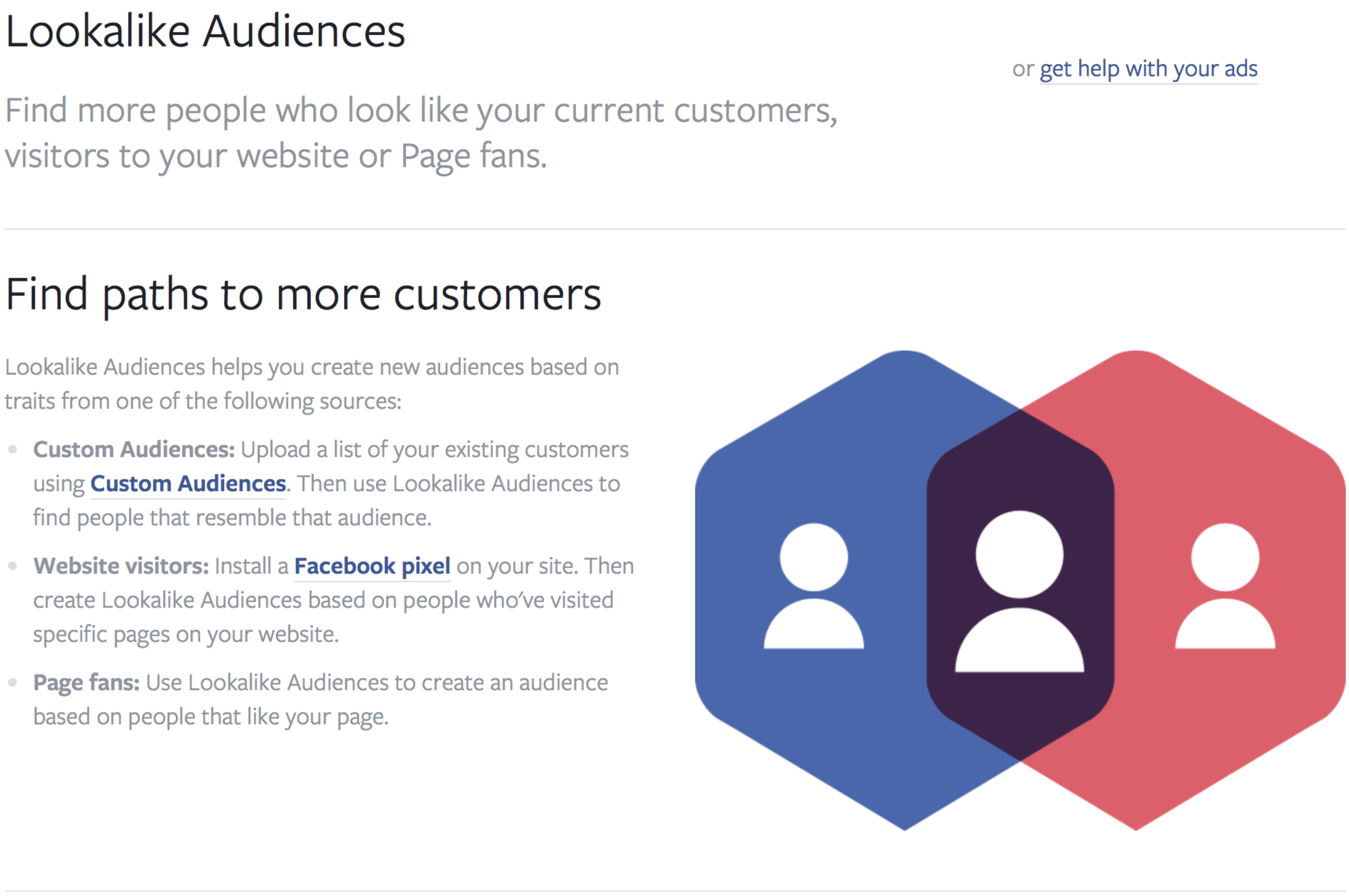
By Laila

Thanks for being part of Team Joe!
We couldn’t do this without you, and we’re excited to have you talk to your friends and

Step 3: Connecting with Your Friends & Family

Sending a Text: After clicking on “Act Now” from the homepage, you will be redirected to your list of contacts that match our campaign’s targets. Pick a person you would like to reach out to and press the red “Send Text” button.

From there, you will be redirected to iMessage where a scripted text will populate. You can tweak this language to reflect your relationship with the person and how you would typically talk to them. Press send and wait for a reply!



Lookalike Audiences

or get help with your ads

Find more people who look like your current customers, visitors to your website or Page fans.

Find paths to more customers

Lookalike Audiences helps you create new audiences based on traits from one of the following sources:

- **Custom Audiences:** Upload a list of your existing customers using **Custom Audiences**. Then use Lookalike Audiences to find people that resemble that audience.
- **Website visitors:** Install a **Facebook pixel** on your site. Then create Lookalike Audiences based on people who've visited specific pages on your website.
- **Page fans:** Use Lookalike Audiences to create an audience based on people that like your page.

FACTORS THAT ENABLE POLITICAL MICRO-TARGETING

Legal

- Constitutional provisions on freedom of communication/speech
- Statutory: Data protection, election law, campaign financing law
- Telemarketing rules, anti-spam rules, election advertising codes

Political

- The party and electoral system
- Mandatory or non-mandatory voting
- Existence of primary elections
- Frequency of referendums

Cultural

- General acceptability of direct candidate to voter campaigning
- Legacies of authoritarian rule
- Trust in political elites

IT IS NOT JUST ABOUT THE TECHNOLOGY!

CHALLENGES FOR THE PROTECTION OF PRIVACY IN POLITICAL CAMPAIGNS

- What is a political campaign – and when do they start and end?
- Voter surveillance is a global phenomenon, requiring high degree of international harmonization
- A large, secret and shifting ecosystem of global actors – data controllers and processors within the "political influence" industry
- The interests on the other side of the debate are compelling – the need for democratic engagement and mobilization
- It is difficult to convince politicians to regulate themselves
- Different regulatory authorities are involved besides data protection agencies, including elections regulators
- Many legal, institutional and cultural factors affect the processing of personal data in political campaigns

LESSONS FOR PRIVACY ADVOCATES

- The need to understand the increasingly complex political campaigning network in their respective societies

- The need to grasp of the regulatory conditions that permit, or prohibit, the processing of personal data for purposes of democratic engagement including the rules for campaign financing

- The need to cooperate with, or challenge, relevant regulators including elections and telecommunications regulators

- The opportunity for leverage through global initiatives against fake news and proposals for ad transparency

- The opportunity to work within political parties in the detailed and practical work of data protection and security implementation

- The need for international collaboration through your international and regional associations, as well as from the wider network of international privacy advocates and experts.

CONCLUSIONS

- Familiar privacy questions on transparency, fair processing, consent, security, and accountability, are now at the center of an international debate about democratic practice
- Privacy advocates and regulators now find themselves at the center of this global conversation
- Elected officials over the world have gradually come to realise that the inappropriate processing of personal data within elections can hurt them where it hurts most – at the ballot box.
- Privacy and data protection have rarely in the past been “Big P” political questions …they are now!

Muito obrigado pela atenção.
Ficarei muito feliz em responder suas perguntas e ouvir seus comentários

www.colinbennett.ca
cjb@uvic.ca