25 February 2019

Artificial intelligence, Democracy and Your Election

Panelists

- Allan Rock – Commissioner, Transatlantic Commission on Electoral Integrity and President Emeritus, University of Ottawa.
- Kevin Chan – Global Director and Head of Public Policy Canada, Facebook.
- Merlyna Lim – Canada Research Chair in Digital Media and Global Network Society, Carleton University.
- Matthew Hindman – Associate Professor of Media and Public Affairs, George Washington University, author of *The Myth of Digital Democracy and The Internet Trap: How the Digital Economy Builds Monopolies and Undermines Democracy*.

Remarks

- Karina Gould, Minister of Democratic Institutions

Maureen Boyd offers introductory remarks and invites Merlyna Lim to deliver a primer.

Lim provides an overview of Artificial Intelligence (AI)

- AI will adapt our ability to learn, to reason, to use language, to form ideas, and to problem solve.
- AI stores concepts as chunks of data. It can perform complex updates automatically and frequently without requiring rest like humans do.
- Many different types of AI – machine learning, language processing, etc.
- AI bots can be used to perform automatic hacks or create fake accounts to spread propaganda. Of special concern is deep fake technology which is the ability for AI to create videos that frame a person to make it appear as if they are saying something that they are not.
- Types of actors: trolls (human), cyborg (half human, half bot), and bot (fully AI).
- As bots become smarter and smarter overtime, they may become more difficult to detect. Less intelligent bots are easier to detect because they do not interact randomly, they just spread.
- More than 80% of the accounts present during the 2016 U.S. election are still active and they publish more than one million tweets on a typical day.

Boyd mentions how the Canadian Security Establishment has warned that hacktivists will very likely try to influence our election; that Twitter trolls have tried to influence debate over issues such as pipelines and immigration; and that interfering is becoming cheaper and easier to use while becoming more difficult to detect. She invites Democratic Institutions Minister, the Honourable Karina Gould, to present the response from the government.

25 February 2019

Minister Gould comments

- When people think of social media, people think of the incredible opportunities to connect. It continues to be the great democratiser – it enables people to express an opinion and to engage with policy and thought leaders in a way they didn't have access to before. But the longstanding issue of foreign interference has found a new way to manipulate citizens by connecting directly with them over social media. Foreign interference aims to distort and polarize issues and ideas.
- There is a difference between foreign influence and foreign interference.
    - Influence: Legitimate diplomatic activities that are overt.
    - Interference: Covert activities to distort the facts and create chaos and confusion.
- We have a trusted election administration body and respected security agencies that work to protect Canada and democracy.
- In June 2017 the Minister asked the Canadian Security Establishment to publish a public report on cyber threats to Canada's democracy, identifying its strengths and vulnerabilities.
- On January 30, 2018, the Canadian government released its plan to protect the upcoming election which has four main pillars:
    1. Combat foreign interference
        - Ensure elections legislation was robust to deal with foreign threats and online manipulation and disinformation campaigns.
        - Created a security and intelligence threat to elections task force.
        - Activated rapid response mechanism from G7.
    2. Enhance public awareness
        - Strongest defence to cyber threats is an informed and engaged electorate.
        - Dedicated $7 million towards digital literacy campaign on how to spot fraud, disinformation and manipulation.
        - Announced a protocol to guarantee that a trusted messenger can relay honest information to the public.
    3. Improving government coordination
        - Canadian Centre for Cyber Security to have all the operational security experts at one point of contact.
    4. Pressure Media Platforms to Act Responsibly
        - Platforms have responsibility to control how information on their platform is shared and portrayed.
        - Analysis of how technology interfaces with democracy and what Canada needs to do to protect itself.
- There will be a continued dialogue between government, citizens, civil society organizations, media platforms to anticipate, recognize and respond to an ever-changing environment.

25 February 2019

Boyd asks Allan Rock: *Are the Canadian government's plans sufficient*?

Rock responds

- The Trans-Atlantic Commission of Election Integrity brings together policy leaders from 12 countries to focus on democratic elections taking place before 2020 and to evaluate their state's readiness to counter election interference, including cyber interference. The evaluation is based on the state's legislation, cybersecurity strategies, and actions they are taking. They will publish best practices as well as a checklist for states to evaluate their own readiness.
- Canada has solid infrastructure and a dedicated Minister to uphold Democratic Institutions. Canada's paper ballet system is an advantage to the system. However, central lists are vulnerable to hacking. Bill C-76 strengthens the legislated infrastructure.
- Canada demonstrates international coordination with the G7 rapid response framework.
- Social media cannot be taken at face value – the best response to foreign meddling is to laugh at it but unfortunately Canadians are a long way from being able to recognize it.
    - A good strategy to limit foreign meddling is to diversify media sources.
    - Canada could also express its expectations to social media platforms – potentially by introducing regulations or a code of conduct.

Maureen asks Matthew Hindman: *In* The Internet Trap: How the Digital Economy Builds Monopolies and Undermines Democracy*, you write that in mid-2016, Google and Facebook together combined for more than 73 percent of digital advertising in the United States –a lot of money in a $60 billion-a-year industry. The four largest internet firms—Google, Facebook, Microsoft, and Yahoo!— capture a third of all web visits. That's important because that shapes public life, including what content is produced, where audiences go, and ultimately which news and democratic information citizens see. Given that the top fake news outlets on Twitter during the 2016 U.S. election still operate today, should we have any cause for optimism in Canada?*

Hindman responds

- Matthew believes the case for optimism is mixed at best. On a positive note, the public in general is more sophisticated about this than they were previously. The case for pessimism rests with the largest platforms.
- It is deeply troubling how foreign states can use major platforms to spread misinformation. The concentration of web traffic on the major four sites (Google, Facebook, Microsoft and Yahoo) is extends beyond 1/3 of all web visits, considering that a huge fraction of the web visits outside of the major four originate from there.
- Disappointingly, Google recently failed to share information regarding videos that were seeded on YouTube by Russian intelligence.
- It seems there is currently disagreement within the major firms as to how they will respond to current challenges and what type of firm they will be going forward.

25 February 2019

Maureen asks Kevin Chan: *Facebook has announced its Canadian Election Integrity Initiative – 5 initiatives to help protect election integrity. Yet a Nanos/Globe poll earlier this month reported that over six in ten think Facebook will have a negative or somewhat negative impact on the election … and over seven in ten think Facebook does a poor or very poor job in monitoring how it is used to influence politics. Can you respond to that?*

Chan responds

- Kevin acknowledges that Facebook "clearly has more to do" but will explain what measures Facebook is undertaking and how well it is going thus far.
- Facebook is thinking about it as investments they're making in people, technology and partners.
- Security team has tripled. There is a dedicated team for the Canadian election to support the integrity of the information shared on the platform.
- AI is going to allow Facebook to tackle some challenges at scale. AI can quickly identify and disable fake accounts across the platform. This identification is made possible because fake accounts behave differently than real accounts. For example, Facebook took down approximately 1.6 billion accounts in the past six months. In general, approximately 3-4% of Facebook accounts are fake.
- Facebook has meaningful partnerships, such as its partnership with Media Smarts that focuses on digital literacy.
- Bill C-76 was a big step in the right direction as Canada is one of the few countries in the world to require there to be a political advertisement archive – accessible to anyone at any time – for all platforms with a certain amount of web traffic.
- Facebook is closely watching the action on their platform during election periods, such as the bi-elections taking place today.
- Kevin is happy to say that Facebook is still mainly a platform for people to connect.
- Facebook has established communication methods with appropriate government official to discuss if there is any kind of bad actor on the platform attempting to impact the election. Fortunately, Facebook has not yet found the kind of inauthentic behaviour in Canada that they saw in the 2016 United States election.

Boyd asks Lim: *There are a lot of politicians – especially in the United States - that are using bot accounts to make themselves appear more prominent on social media or to inflate support for certain issues. Is that a threat to democracy? Are bot accounts themselves a threat to democracy?*

Lim responds

- It is very inexpensive to buy followers on Twitter.
- Fundamental question is that this is sitting on a larger issue. There is a business model where any company, individual, or institution can target the user with advertising. Individuals without consent are being recorded 24/7. This raises the question, is it legal that a person's location, search history, etc. can be recoded 24/7? The potential for people to take advantage of this type of data is new.

- Data exploitation and manipulation are prominent issues and citizens should have the right to know when they are being recorded and how that information is used.

Boyd asks Hindman: *how concerned you are that technology firms, including Google and Facebook,actually shape political communication in showing clients, i.e. political parties and candidates, how to use their platform to best communicate their message?*

Hindman responds

- Matthew agrees that this is concerning but perhaps for different reasons that we may think.
- Looking forward, we should be most concerned about how roughly 40% of internet traffic is fake and the implications of this.
- Digital trace data taken from Facebook is very good at showing age, gender, location, partisanship, race or ethnicity and sexual orientation, which can be used to target adds. As it becomes easier to target people using unchosen identities, we end up with a political sphere that's more defined by these identities – which is deeply dangerous for democracy. It is dangerous to have political opinions designed by things that people do not choose.

Boyd asks Rock: *you raised the idea of regulation, can you comment on Facebook's response?*

Rock responds

- This is about more than just Facebook and other social media sites; it is ultimately about the kind of conversation we want to have regarding our elections.
- We should not assume that just because we have not yet had provincial meddling that we will continue to not have any in the future. Canada is a target for Russia in particular. Canada is a member of the G7, which was the G8 until Russia was kicked out, and Canada implemented a version of the Magnitsky Act. Canada needs to brace itself for interference.
- In terms of what can be done, Allan comments that he admires the steps that Facebook is undertaking. However, he recognizes that Facebook's board of directors will prioritize maximizing value for stakeholders which is not the same criteria as respecting Canadian democracy.
- The role of government is it protect the public interest from powerful businesses that can be used to undermine Canadian democracy.
- In terms of what can be done, Canada can learn from Germany and the European Union who are taking steps to regulate social media. Social media sites should be recognized as broadcasters that are obligated to perform due diligence to ensure foreign influencers are not buying advertisements.

Chan responds

- Kevin thinks that he and Allan agree on most things.
- First and foremost, Kevin mentions that Facebook is regulated in Canada. The platform is subject to hate speech laws, and regulated goods (Health Canada will ask Facebook to remove advertisements for prohibited goods).
- The way Facebook thinks about public discourse – they abide by the laws of constrained speech and set limitations on content (e.g. terrorism). Facebook must be careful to allow people to post things they want to share online, yet ensure that content does not conflict with Canadian law.
- Facebook hopes that by the end of 2019, they have an independent body that works in parallel with board of directors to rule on content policies and set precedent on what is allowed on their platform. This is an effort to externalize the responsibilities on entities outside of Facebook, instead of the onus being on Facebook to decide what remains online and what is taken down.

Questions from the audience

Question one: *People are trying to exacerbate vulnerabilities within Canada and we see this from a constant stream of manipulation from the outside. What do you do about it?*

Hindman responds: Facebook argues only 3-4% of accounts are fake, however he would like to see a large scale, peer reviewed audit of those numbers because that is the primary defence against interference and manipulation. Many new bots can behave more like real accounts and are therefore harder to identify. We celebrate social media and the internet because it reduces friction and allows a single person to spread an idea to potentially millions of people. However, it would be beneficial to our democracy to introduce some friction, and make it more difficult for bots to spread politically sensitive and polarized messaging, especially when it relates to political speech.

Question two: *Does focusing on the election result in us missing some of the activities that happen beforehand? Could you also comment on the use of data by parties and their exemption from the Privacy Act?*

Lim responds: AI is being used as an invasion of privacy and a method of manipulation. Online advertisement does not differentiate between whether you are Canadian or not.
Bots are becoming smarter overtime. We need to deal with these issues before elections, otherwise the damage will be done. We must improve transparency and uphold moral ethics. The problem is that political parties that benefit from bots have a direct incentive to be complacent.

Question three: *how do we deal with AI created by foreign actors versus domestic, because the country of origin may affect whether the freedom of speech law applies.*

Question four: *How did Russians interfere with the 2016 United States election? Was interference focused on pro-Trump or anti-Clinton rhetoric, voter suppression, dissention, or racial/immigrant animosity? What did they do and how did they use Facebook for this? How do we know if it's foreign interference and how do we catch them?*

Boyd invites the panelists to respond to final questions while providing closing remarks.

Hindman comments

- We know it was the Russians that meddled in the 2016 United States election because digital trace data can determine the origin of a sender. What did the Russians do? Everything! From all kinds of racist or inflammatory content to organizing real world events. To a striking degree, it leveraged existing domestic actors. Bots are worrisome because you see many conspiracy sites that coincidentally receive a ton of traffic when they talk about something that concerns the Russians.
- Ability of bots to create traction on sites allow them to be very good at setting the agenda.
- We should be encouraged by some of the changes that platforms have made, but the broader concern is that there's so much about the internet in general that allows for people's information to be collected by platforms that allow them to create blackmail.
- Dealing with the constellation of issues is the largest challenge for democracies.

Lim comments

- It is worrisome that entities that will deploy massive amounts of bots with marketing campaigns.
- Ultimately, the entities that we know, the companies know. Facebook did a great job by banning political foreign political messaging campaigns in Nigeria.

Chan comments

- Kevin is pressing his team to find something on Canadian interference, but it is a good thing that they have not found anything yet. In the event that there is even a minor issue, Kevin will brief appropriate Canadian ministers.
- In terms of a peer review of Facebook data, there is a process in place that allows for Facebook data to be turned over to academics for social science projects.
- Bill C-76 outlaws the ability for any company to sell advertisement to a foreign entity.
- To the extent that there have been issues reported (i.e. violations of the law) Facebook has made efforts to address it.
- In relation to how we determine whether accounts are Russian or domestic, some behaviours are consistent. Sometimes domestic actors will borrow from the playbook of foreign actors (called coordinated inauthentic behaviour). Facebook constantly tries to

identify accounts that engage in coordinated information operations and remove those accounts immediately.
- Kevin's most prominent concern is the inadvertent censorship of legitimate speech.

Rock comments
- Allan would like to see vigorous discussions and free speech without Russian bots inflaming debates on hot button issues.

Closing remarks by Dr. David Mendeloff
- Carleton Faculty of Public Affairs is honoured to support the Carleton Initiative for Parliamentary and Diplomatic Engagement.
- Dr. Mendeloff highlights how the core mission of the Carleton Initiative is to engage actively and directly with government and civil society.

The event was organized by the Carleton Initiative for Parliamentary and Diplomatic Engagement with the support of Member of Parliament co-sponsors: Anita Vandenbeld, Chair of the Democracy Caucus; Stephanie Kusie, Shadow Minister for Democratic Institutions; and Nathan Cullen, NDP Critic for Democratic Reform and with the generous support of GSK, the Insurance Bureau of Canada, Suncor, TD and Toyota.

Notes prepared by Claire Crawford, M.A. in International Relations with a specialization in International Economic Policy, Norman Paterson School of International Affairs, Carleton University