Freedom On The Internet

Isha S Terdal

Fall 2019 Information Policy

The George Washington University

School of Engineering and Applied Science

Master of Science in Computer Science

(This research paper is prepared for the course of CSCI 6532. As instructed, this paper is based on all of the research, group interaction, and learning I have completed for the class.)

Introduction

Since the dot com bubble in the late twentieth century, the Internet has permeated through almost every sphere of human life. From personal relationships to organizations conducting their entire business on a global scale via the network, the Internet has become an indispensable part of our lives. Such an interconnection, however, brings enormous power to any entity that can control and/or regulate it – including the ability to decide how much freedom and access a citizen of the globe gets. In today's world, national governments and social media companies are the two major forces at the crux of freedom on the internet, and it is essential to find ways in which these entities can wield their power in an ethical and transparent manner.

Forces disrupting freedom on the internet

According to the Freedom on the Net Report 2019, free speech and privacy on the Internet is in decline globally. This can be attributed to two main causes – 1) increased online election interference and 2) increased government surveillance. The report outlines that out of 65 countries surveyed, 40 countries had already implemented advanced social media surveillance, and a record 47 countries have had cases of law enforcement arresting people for posting political or religious opinions online (Molla, 2019). Possibly the worst-case scenario for internet freedom is in China, with its Great Firewall policing the digital lives of its citizens through constant surveillance and censorship (Marvin, 2019). Another infamous example would be the misuse of Facebook data for influencing the US Presidential Election in 2016, with foreign actors harnessing users' personal data for spreading propaganda.

Governments all over the world have been using the online space to promote propaganda and sway public opinion [See Appendix 1], with measures such as regulating access to Internet sources, or arresting citizens for expressing a political opinion against the ruling party. Social media surveillance has been constantly justified by security authorities as a tool for combating terrorism, human trafficking, child sexual abuse, and other atrocities, but the boundaries for such surveillance are being constantly pushed to track political views of travelers or monitoring activists and protestors.

Solutions being implemented by countries globally

One of the first effective steps taken towards protecting user privacy on the Internet was the EU's General Data Protection Regulation (GDPR) framework, implemented in May 2018. The framework mandated organizations to be completely transparent about their data collection practices by clearly asking for user consent and providing a way to access and delete the information collected. Another innovative model has been implemented in Estonia, with its X-Road platform encrypting transaction information via blockchain technology. Citizens are notified if government or any other entities access their information (Shahbaz, 2018).

Within the US, Section 230 of the Communications Decency Act has been the champion for protecting internet freedom and innovation, providing online platforms immunity against user content. On the other hand, the Stop Enabling Sex Trafficking Act (SESTA) holds technology platforms accountable for prostitution or sex trafficking content being posted on their platform. Major technology companies centered in the US are implementing methods that allow them to be transparent about data they are collecting, while allowing the user to review and delete any data collected about them. Nevertheless, such efforts are nation-centered and there is still a long way to go in terms of ensuring internet freedom that spans across borders.

Conclusion

In the twenty-first century, it is pretty much impossible to prevent personal data from being collected by various agencies around the globe. Obtaining true freedom on the net will have to be a mutual effort i.e. while data-collecting organizations need to be more vigilant about getting consent from the user, along with providing transparency and control over its use, the citizens must be made aware of how to exercise these rights provided to them. In the end, our security and privacy start with us, the individual himself/herself and the measures we take to protect ourselves online, irrespective of any privacy laws and regulations.

References

1) Molla, R. (Nov 5, 2019). The internet is getting less free. Retrieved from https://www.vox.com/recode/2019/11/5/20947419/internet-freedom-report-2019-social-media-election-interference-surveillance

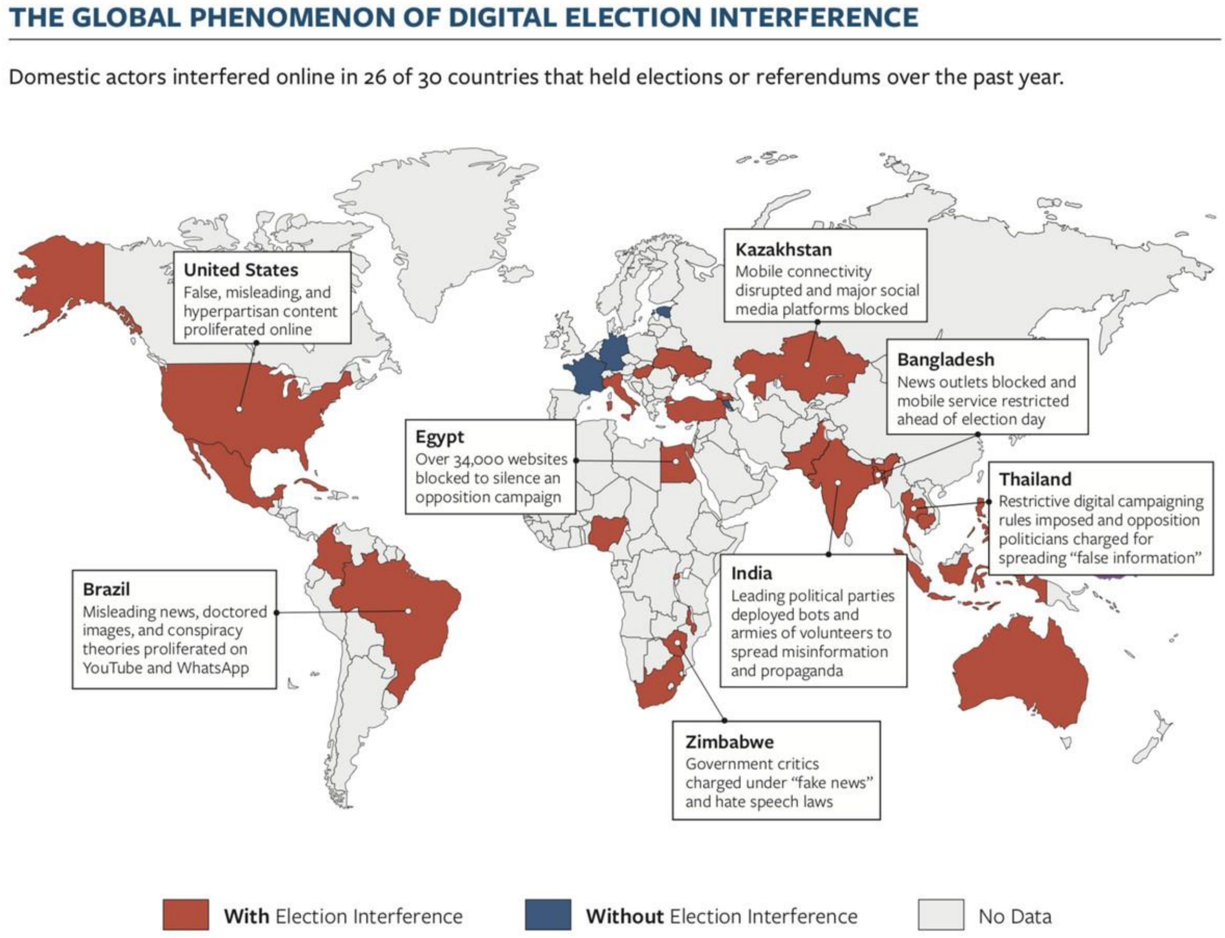
2) Marvin R. (March 22, 2019). The State of Internet Freedom Around The World. Retrieved from https://www.pcmag.com/news/367266/the-state-of-internet-freedom-around-the-world

3) Shahbaz A. (October 2018). Freedom On The Net 2018. Retrieved from https://freedomhouse.org/report-types/freedom-net

4) Goldsmith J. (June 13, 2018). The Failure of Internet Freedom. Retrieved from https://knightcolumbia.org/content/failure-internet-freedom

Appendix

1. **Election Interference, surveyed by Freedom House, 2018**



THE GLOBAL PHENOMENON OF DIGITAL ELECTION INTERFERENCE

Domestic actors interfered online in 26 of 30 countries that held elections or referendums over the past year.

United States
False, misleading, and hyperpartisan content proliferated online

Kazakhstan
Mobile connectivity disrupted and major social media platforms blocked

Bangladesh
News outlets blocked and mobile service restricted ahead of election day

Egypt
Over 34,000 websites blocked to silence an opposition campaign

Thailand
Restrictive digital campaigning rules imposed and opposition politicians charged for spreading “false information”

Brazil
Misleading news, doctored images, and conspiracy theories proliferated on YouTube and WhatsApp

India
Leading political parties deployed bots and armies of volunteers to spread misinformation and propaganda

Zimbabwe
Government critics charged under “fake news” and hate speech laws

🟥 **With** Election Interference
🟦 **Without** Election Interference
⬜ No Data

(**Source:** https://www.vox.com/recode/2019/11/5/20947419/internet-freedom-report-2019-social-media-election-interference-surveillance)