Addressing the Issue of Global Data Corruption

General Assembly 4

Enya Yuniarta, Deputy Chair

Introduction

The rising digitalization and the world's increasing convergence to artificial intelligence (AI) raise issues concerning cyber threats. Namely, the collection of personal data from various technologies or platforms can be misused and more specifically can play a major role in electoral fraud. Including biasedly discrediting electoral institutions, influencing individuals' behaviors, or weakening citizens' confidence in a political group. Particularly, user's private information from media platforms could unethically be recorded without permission and used to influence the user's views including political opinions. This has serious implications on the principles of democracy, as citizens are misinformed regarding political disputes or candidates, therefore unable to form their own objective opinions on the situation and votes do not represent citizens' personal views without manipulation from the malicious party.

Previously suggested solutions included strengthening the information security itself to maximize elections defense. While it is important to maintain high defense on cybersecurity, elections since the 2010s were considered highly robust and virtually no data breeches were performed to the presidential election administrative itself, rather data corruptions occurred through online political advertising. Malicious actors can widespread public doubt, weaponizing the polarization of society and giving distrust on the targeted party. Thus, vast collections of personal data from large data vaults such as Google or Facebook, in combination with precise algorithmic content targeting can easily direct misinformation to registered national voters. Therefore, methods to enable greater transparency regarding tech platform's data collection and advertisement's algorithms should further be investigated to address these dangers for greater integrity in nations' electoral systems.

Definition of Key Terms

Electoral Fraud
This is a type of election manipulation, referring to voter fraud or vote-rigging. This involves illegal interference during or before the process of an election, either to increase votes and preference of a favored candidate or by deteriorating the rival candidate's image.

Data Privacy
Data privacy refers to the protection of personal data. This concerns which individuals or parties are authorized to access the personal information. Data privacy determines who has access to the data, while data protection is a tool and policy to restrict entry to the data.

Data Protection
Refers to tools and policies that protect individuals against the misuse of personal information by data processors. Data protection's purpose is to reduce privacy risks from potential control and loss over sensitive information.

Information Security
The prevention and protocols to prevent unauthorized access for usage, disclosure, modification, transmission to another recipient, recording/ storing or destruction of both physical and digital information without permission from the owner.

Psychographic Profile
Psychographics is the study of consumers based on their activities, interests, and opinions (AIOs). AIOs are individuals' characteristics used to construct their psychographic profile or personality types. An individual's AIO is deciphered by for example their responses to statements/ questions in a survey. The psychographic profile is the conclusions from AIOs e.g., the user's personality type.

Social Engineering
This is the psychological manipulation of people into performing actions or revealing confidential information.

Phishing
Type of social engineering attack often used to steal user data, masquerading as a trusted entity, manipulating the victim into e.g., opening an email, text message, URL links to install malware into the user's system.

Political Advertising
Advertising campaigns to the public through communications media (social media platforms, radio, TVs, satellite etc.) to influence a political debate, voter's impression on the presidential candidates etc.

Malware
A short term for "Malicious Software". Is a software designed to damage, disrupt, or gain unauthorized access to the targeted digital system, usually conducted by malicious actors. Malware is a file or code, usually delivered via a network, allowing the attacker to infect the targeted computer system.

Domain

An identification string that defines a server within internet networking. Whether an address is registered under organization's administration DNS (Domain Name System) records can determine whether the browser, sender address, URL links etc. are authorized to enter the organization's server, ultimately can be used to determine any cyber-attack attempts.

DKIM

"Domain Keys Identified Mail" an email authentication method, with purpose to detect illegitimate sender addresses in email, enable to prevent phishing or email spam. DKIM allows the recipient to verify whether the email received have come from specific domain which was indeed authorized by the domain's owner or the official organization the email might be replicating.

SPF

"Sender Policy Framework", another method of mail authentication. When the receiver receives an email, their email provider (Outlook, Gmail etc.) verifies the SPF records by searching the received email's domain name, checking if their return address is indeed in the DNS records. If the email's IP address is not on the records list, the email would be categorized as spam and failed the SPF authentication check.

DMARC

"Domain-Based Message Authentication, Reporting and Conformance". A DMARC record notifies the receiver on what to do if the received email fails the SPF or DKIM authentication methods. DMARC could flag it as spam, eliminate it to junk or reject the message, limiting the user's exposure to potentially fraudulent messages. DMARC also allows the email receiver to report to the sender regarding if their email passed or failed the DMARC evaluation.

General Overview

In some nations such as the United States, there is a lack of a well-enforced federal privacy law, where companies have limited obligations to protect user privacy and users have minimal control regarding their personal data. If no strategies of improving these laws are conducted, this can allow further implications to occur. For example, by advertisers, including political campaigns, where media platforms or search engines can act as large data vaults for malicious actors to collect online user's data, enabling to build detailed profiles from their viewed interest for ad micro-targeting.

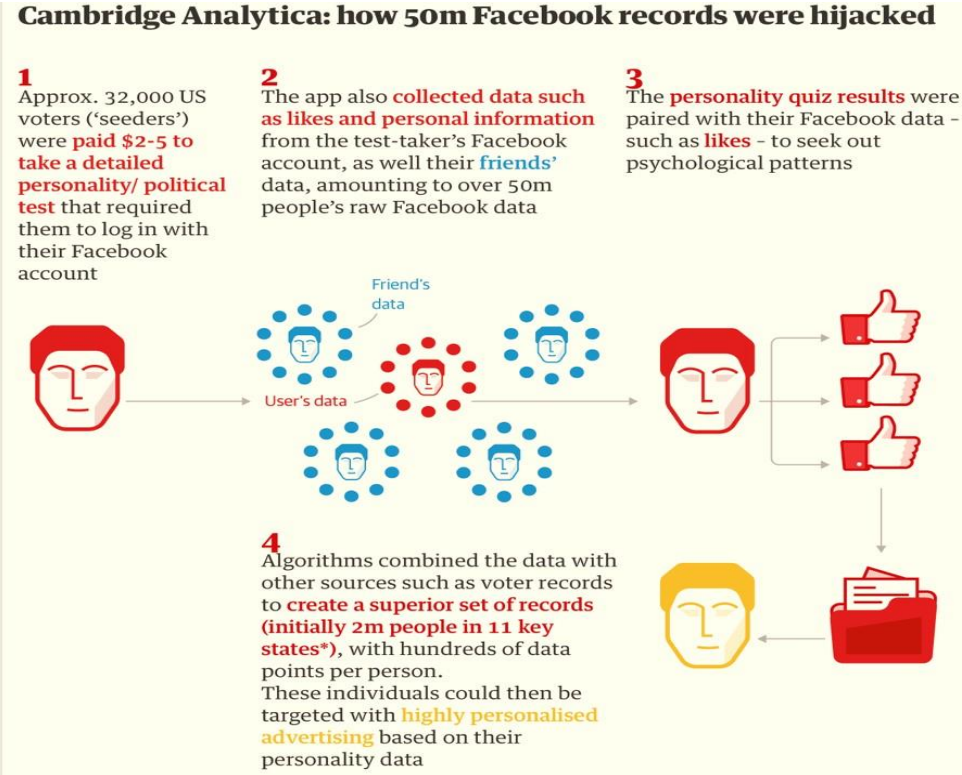
Cambridge Analytica and Facebook Scandal

Digital platforms such as Facebook and Google have cumulated vast data vaults with volumes of information on various users e.g., from tracking your search inputs and user online activity. These were therefore also the main sources that aided the considered largest data breaches, that was conducted by "Cambridge Analytica" on Facebook users in March 2018. "Cambridge Analytica" a political consulting firm, illegally obtained data from Facebook users without consent, creating psychographic profiles of more than 100 million registered US voters, enable to target voters with specialized advertisements in the 2016 presidential elections.

Cambridge Analytica harvested almost 5000 data points on every US voter, recording status updates, likes, user's most viewed content, user's most liked/ interested content category and private messages which can reveal descriptions over individual's personality. This enables the misuse of sensitive user information to influence voter's behavior through micro-targeting personalized political ads to any specific social groups.

Psychographics Behavioral Analysis

Psychographics was the behavioral analysis method that aided Cambridge Analytica to determine what cognitive factors drive the user's behaviors and interests. Knowing this, Analytica can adapt messages to an individual's personality traits, enabling for the message to be interpreted as similarly as possible by various character types e.g., a person can be on different levels of the spectrum: openness, introverted, argumentative etc. Analytica followed primarily the OCEAN (Big Five test) determining the various predictions of response from an audience. For example, a segment of voters can be identified as high in conscientiousness and neuroticism with another segment with higher extroversion and low openness would clearly show differentiation in response of same political ad, therefore Analytica delivered individually tailored ads on Facebook to the suitable users, designed to model the desired response, whether it is to vote in favor or against a candidate/ party, in this case the 2016 Donald Trump campaign. Facebook provide users content according to their algorithm, initially programmed to maximize audience interest engagement. Though this algorithm was also used to aid Analytica's data collection for personalized ads.



Additionally, American researcher "Aleksandr Kogan" gave access to 270,000 personality tests completed by Facebook users through an online app (See. Figure 1), providing the data to Cambridge Analytica without knowledge of Analytica's honest intent on the collected data's usage. This method could further be used not only by Analytica, but potentially by various malicious actors in the future if stringent action is not taken rigorously.

Moreover, A whistle-blower and former Facebook data engineer "Frances Haugen" reported several articles to well-known publishers "Washington Post" and "New York Times" regarding Facebook's company research on future expansion plans, which signified higher priority on profits than consumer safety. Emphasizing further the urgency of the issue, as this can pose damage to the principles of democracy. Commonly used platforms can be then utilized as a propaganda weapon for in the case of 2016 US elections, falsely manipulating user views and impressions to favor authoritarian regimes or in the Brexit elections, Aggregate IQ aided the "Vote Leave" campaign under non-EU party using a similar method of micro-targeting political advertisements. Ultimately, this is a violation of human rights as citizens' perspective on the situation is discretely deceived, where targeted users are unaware of the content given is not objective or accurate. This also eliminates citizen's true opinion and vote regarding any political disputes or situation, as the sources given to determine and construct their own view has already been manipulated.

Russian interference

Another cyberattack method is through "Spear-Phishing", which is a phishing method that targets specific individuals or groups within an organization. This was correspondingly used in 2016, where Russian involvement was found during the 2016 presidential elections, when the tracked IP address was in an unknown location within Russia. The Russian cyber espionage and military intelligence supposedly impersonated the institution's employees enable to send malicious emails and gain trust to several Florida Election staff. Another spear-phishing act was when emails that appeared like Google security notifications were sent to staff of Clinton's presidential campaign. The email content instructed the recipient to click a link to change their password for security reasons, giving the Russian agents entry to their accounts. This also allowed the Russian agents to install malware into the

Democratic Congressional Campaign Committee's (DCCC) computer networks, obtaining sensitive documents related to the election. The agents allegedly also released politically damaging information on the internet, including spreading propaganda on Twitter, Facebook, YouTube, and Instagram, along with launching a fake news website called "DCLeaks.com". The website posted the obtained confidential documents from the malware, downloaded by the targeted email recipients regarding any data associated with the campaign. A similar tactic was also used during the 2019 Ukraine elections on government officials by Russia's cyber interference.

In conclusion, AI techniques have become prevailing tools to gain access to sensitive data, not only in the political sector to election officials, political parties, and campaign staff but also potentially to nation's military information. Especially with the continuous advancements in technology, intelligence malware would

increasingly become more proficient in infiltrating organizations without being detected, which inevitably lead to damaging consequences, from exfiltrating credentials to commandeering the targeted institution's computing system. Additionally, social manipulation tactics are made possible from inadequate data protection against cyberattack techniques, these are also rising in African countries, such as South Africa, Kenya, Egypt, Nigeria and Ethiopia. Delegates are therefore encouraged to further read up on this issue, as it has become more critical to press global importance on strengthening cyber security to protect national economic, social, and political sectors from digital threats.

Major Parties Involved

UK

Cambridge Analytica is a British political consulting firm and election management agency, founded in 2013 by "Nigel Oakes", "Alexander Oakes" and CEO "Alexander Nix". The founders have well-connected contacts with the UK Conservative Party, the British royal family, and the military.

Additionally, a Canadian technology company and political consultancy "Aggregate IQ" (AIQ) took part in aiding the official pro-Brexit group "VoteLeave" campaign led by Boris Johnson and Michael Gove. Campaign's finance records stated evidence of VoteLeave's £625,000 funding towards services from AIQ to support the anti-EU side in the referendum. Moreover, it was revealed that AIQ had in total been paid £3.5 million by four pro-Brexit campaigning groups: Vote leave, BeLeave, Veterans for Britain, and Northern Ireland's Democratic Unionist Party, designing a software aimed at collecting personal data to influence voters through personalized messaging on social media, including Facebook.

USA

Facebook has had a failure history to protect the personal data of over 50 million users. The largest Facebook data breach was the Cambridge Analytica 2018 scandal, with user's data utilized for conservative political projects, including Brexit and Donald Trump's presidential victory. Facebook was created in February 2004 (Cambridge, Massachusetts) under main founder and CEO "Mark Zuckerberg" with aim for users to stay connected to friends and family, share and express their interests and discover news concerning current issues. Facebook is the leading social media platform, making 59% of social media users' commonly used apps, and having 1.84 billion active users daily as of January 2021, therefore cumulating large personal information data.

Regarding Cambridge Analytica, they have provided analytical assistance in the 2016 presidential campaigns of Ted Cruz and Donald Trump. This was exposed by whistle-blower and former Analytica data consultant employee "Christopher Wylie" where personal data from over 87 million Facebook users have been improperly collected and millions of profiles were hijacked to influence voters' opinion on candidates' prior elections. Additionally, Analytica's CEO "Alexander Nix" was filmed by an undercover reporter from UK's Channel 4, caught claiming to Trump that Analytica could provide untraceable political ads on social media, using misinformation and bribery to win elections.

Russia

From March 2016, it was speculated that officers from Soviet military intelligence under Russian government, known as "Main Intelligence Directorate" (G.R.U) interfered with the Hillary Clinton campaign, Democratic National committee (DNC) and Democratic Congressional Campaign Committee (DCCC), releasing politically damaging information to the public, spreading propaganda on Facebook, YouTube, Instagram, and Twitter. Additionally, this party allegedly set up meetings with members from the Trump campaign, offering a business proposition to build a skyscraper in Moscow on behalf of the Trump Organization.

Furthermore, these agents hacked and utilized malicious emails to access Hillary Clinton's presidential campaign and DCCC's computer network. The reported hackers then installed malware via email phishing, allowing them to steal any related emails and documents to the 2016 elections. The indictment stated that the agents searched for terms under Hillary, Cruz, Trump and copied a folder of Benghazi Investigations. These agents were in position and were able to alter or delete voter registration and voting input data.

Google

American search engine company was founded on September 4th 1998 by "Brin Page" and "Larry Page", with headquarters in Mountain View, California (United States). More than 70% of global online search requests are undertaken by Google, therefore this platform has access and information of millions of user's search data, which can indicate AIOs enabling to decipher their psychographic profile. Google acted as one of Cambridge Analytica's main sources for profiling information.

Commission on Science and Technology for Development (UNCSTD)

United Nation's division on Technology, Logistics, and ICT Analysis, focusing on the development of implications in information and communication technologies. UNCSTD is a subsidiary body of the Economics and Social Council (ECOSOC), established by the General Assembly and conducts annual intergovernmental forums for discussion on current and appropriate issues affecting science, technology, and development.

Office of High Commissioner for Human Rights (OHCHR)
UN Human Rights division is part of United Nation's Secretariat, having around 1300 staff members, with headquarters in Geneva. OHCHR is to ensure universal human rights e.g., Right to free thinking, speech, including privacy rights, as well as ensure effective implementation of these rights through global co-ordination and cooperation through UNs system.

Timeline of Key Events

August 2013	Yahoo data breach impacted 3 billion accounts, including credit card records, passwords, birth dates has been improperly accessed. Later in 2014, state-sponsored hackers stole unauthorized data from Yahoo.
September 12th, 2013	Political consulting firm and agency "Cambridge Analytica" was founded.
March 23rd, 2015	Presidential campaign for junior US senator "Ted Cruz" was announced.
June 16th, 2015	Presidential campaign for former American businessman "Donald Trump" as republican nominee was announced.
June 23rd, 2016	Pro-Brexit group "VoteLeave" campaign was established, in favor of non-EU referendum
March 4th, 2018	Whistleblower "Christopher Wylie" exposed Cambridge Analytica involvement with Facebook scandal. Facebook disclosed details concerning data breach to 50 million users.
March 27th, 2018	Facebook suspended Aggregate IQ (AIQ) from its platform after speculations that data firm has improperly accessed unauthorized data from Facebook users.
May 1st, 2018 July 1st, 2019	Cambridge Analytica is no longer operational and was shut down Facebook fined $5 billion USD by Federal Trade Commission (FTC) after settling Cambridge Analytica data breach scandal.
November 28th, 2019	AIQ tied their direct involvements with "VoteLeave" campaign and cooperation with Cambridge Analytica from financial transfers by these respective firms.
March 2020	Sina Weibo data breach is one of China's largest media platforms. Affecting 584 million accounts, the attacker was reported to have sold these user databases on the digital black market.

June 2021 LinkedIn data breach, 700 million users were affected, the malicious actor sold 500 million customer data bases to third parties, including phone numbers and geolocation addresses.

UN Involvement, Relevant Resolutions, Treaties and Events

The General Assembly has recognized how interception of digital communications and the collection of personal data may significantly impact human rights negatively. The Third General Assembly (GA3: Social, Humanitarian and Cultural) called on member states to establish or maintain existing oversight and supervision ensuring transparency on appropriate platforms that utilizes sensitive personal data collection, urging private firm's accountability on data surveillance.

- A resolution adopted by UN's General Assembly on the report of the second committee on 21 February 1997 (A/RES/51/191) "United Nations Declaration against Corruption and Bribery in International Commercial Transactions", requesting primarily the Economic and Social Council (ECOSOC) for action and its subsidiary bodies "Commission on Crime Prevention and Criminal Justice".

- A resolution adopted by UN's General Assembly during its 30th session, from 16 September to 17 December 1975 (A/RES/3514). Addressing the "Measures against corrupt practices of transnational and other corporations, their intermediaries and others involved", calling upon governments of members states to collect information on corrupt practices. Exchanging information bilaterally and multilaterally through UNCTC (UN Centre on Transnational Corporations).

Previous attempts to resolve the issue

Media Platforms
Before the 2020 elections, digital platforms including Facebook, Google, Reddit and Twitter introduced and expanded on their advertising policies. Some platforms banned new political ads from being provided when the election date is nearing or eliminated political ad campaigns completely. To promote easier tracking of deceptive information sources, platforms started transparency libraries, providing insight upon the political ads displayed on their service, such as the identity of the advertiser, source of advertiser or manager, whether the content was combined with other primary or secondary sources.

Nevertheless, civil rights groups and policymakers warned these attempts and changes were inadequate, as platforms are not consistently enforcing these transparency measures.

Federal Trade Commission (FTC)

The Federal Trade Commission ordered Amazon, ByteDance, Discord, Facebook, Reddit, Snap, Twitter, WhatsApp (owned by Facebook) and YouTube (owned by Google) to disclose information on the platform's method of collecting and storing user's data. Also requiring the companies to expose their algorithms used to analyze personal information for user's content engagement.

This act has to some extent successfully given regulators and the public further insight on how misinformation escalates on platforms, though this can be further strengthened through the federal privacy legislation mandating transparency requirements.

EU Data Protection Laws (GDPR)

Since May 25th, 2018, EU Data protection laws by General Data Protection

Regulation (GDPR) have been drafted and passed by European Union and European Parliament. It imposes data privacy standards and obligations onto organizations in Europe and whenever EU citizens' or resident's personal data collection is involved, regardless of if the provider is a non-EU member. The GDPR will levy high fines against those who violate their privacy security standards. Penalties can maximum reach €20 million or 4% of global revenue in addition to victim's right to obtain compensation from any damages caused by the data violation.

However, while the EU has established these laws, not all, as of September 2021, nonEU nations have federal privacy laws or strict enforcements regulating private companies. For example, most states in the US either have no obligation, inadequate stringent law implementation, or weak penalty of violations, thus companies have little government interference into using, sharing or selling any data collected in the firm's system without notifying the user.

Possible Solutions

This issue requires political and regulatory solutions where higher data protection should be considered. Whilst enforcing the already existing EU GDPRs protection laws have already highly reduced privacy risks, applying GDPR laws into international regions would mitigate implications of data mining and profiling further. Additionally, it is also critical for organizations to recognize profiling as an alarming threat regarding data integrity before voting election processes. Furthermore, it is important to realize implementing data tracing methods more rigorously would prove effective, especially when data sets have been combined with multiple sources to determine the source of origin of the inaccurate information.

Transparency Libraries

Current media platform transparency libraries are restricted, for example

Facebook's library does not display how their content is provided and how user data are processed to stimulate algorithm's audience engagement. Displaying the number of shares, and likes political ads have encountered, and to what user category the ad has been targeted to can be useful, therefore it is easier to determine which audience group has been exposed to misinformation.

Mandating platforms to deliver notification clearly to users, noting when the platform has stored or utilized/processed the user's data could prove beneficial. Platforms could allow users to modify their opt-in or out of data collection at any time in cases of e.g., voluntary surveys. Additionally, these transparency requirements could be mandated by federal bodies.

Public Awareness

Spreading awareness and creating public recognition of social engineering techniques could prove effective in reducing cyberattacks success rates, through either knowledge on how to identify a social engineering attempt or who would be the appropriate confederacies to contact for support. For example, educating the public on methods to check whether the sender's address is suspicious and only is resembling a legitimate firm. These methods could include checking the following: if characters of the URL link are altered, if only general greetings are used and not personally addressing recipient on the email, if it is a different domain to the replicated firm's official URL link e.g., using ".net" instead of ".com", if it has poor spelling and grammar as official firms would have dedicated personnel to rigorously proofread their emails, or if it has attached documents where the sender would persuade the recipient to download with false urgency, a common delivery method for malware.

External Supervision

For technology platforms to allow an external party outside of their own firm to supervise their actions, enable to ensure platforms are prioritizing user privacy and personal data protection over profits. Thereby, placing a non-internal, meaning not any personnel employed under firm itself or shareholders which are affected by firm's total revenue, such as e.g., a UN or governmental group could monitor or limit where necessary their advertising content on the media platform. This ensures the firm's law enforcement on policies and potentially decrease violations of privacy policies to therefore lessen chances of misinformation.

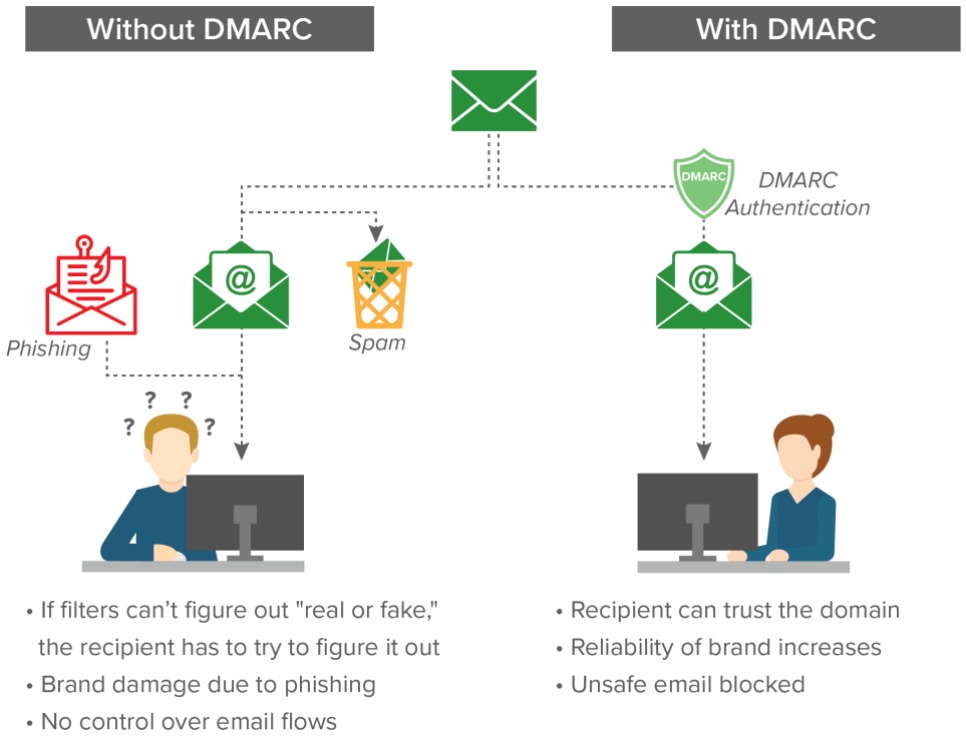
Red-Teaming

Conducting "red team" cybersecurity exercises to test media platforms' vulnerability to cyber-attacks, where the response can be assessed by testing the firm's present security system through simulation of real-world cyber incident acts. This should be conducted by national government unannounced, therefore enabling to simulate

as close as possible to a real offensive attack for both digital infrastructure and firm's staff members, allowing to identify the weak points in system's security by testing the organization under stress and time pressure.

Anti-Virus Tools

Most contracts for enterprises already state a provision to protect their customer's sensitive data, requiring regular inspection procedures regarding the storage of users' data and how they are processed, though in practice this is rarely done by the media platform itself. Thus, a more realistic measure is for the service provider, UN party or national government to equip the user with a security assessment tool to gather data on procedures of platform's data processing methods, storage, recording of user's data, like DMARC (Domain-Based Message Authentication, Reporting and Conformance) mechanism (See. Figure 2) which handles mails that fails an authorization test. Enabling users to alarm and notify the appropriate authorities early on whenever their sensitive information is utilized, violating the platform's privacy policies before the damage is done by any malicious actors. Additionally, governmental institutions could be urged to consistently use email authentication methods before replying or downloading any attachments from a sender, example protocols include SPFs (Sender Policy Framework), and DKIMs (Domain Keys Identified Mail), to validate if sender's address is who it claims to be and can determine whether sender is truly authorized to enter the institution's domain for minimum damage if phishing attacks occur.



In conclusion, considering the security and peace implications regarding safety of civilians and the representative image of political candidates or institutions that this issue poses, it has made measures to be enforced become a multilateral obligation.

The UN along with their member states should therefore promote engagement from electoral management and corporate bodies to recognize measures or enforcement of existing laws should be developed and more rigidly implemented collectively across sectors to manage these violated privacy risks, enabling for maximum anticipation from stakeholder's response team for any future emerging digital threats.

Appendix/Appendices & Further Readings

- GDPR, The EU's new Data Protection Laws. https://gdpr.eu/what-is-gdpr/

- GovTech Singapore, Red-Team Cyberattack https://www.tech.gov.sg/media/technews/behind-the-scenes-look-at-govtech's-red-teamcyberattack

Bibliography

"What Is GDPR, the EU's New Data Protection Law?" *GDPR.eu*, 13 Feb. 2019, https://gdpr.eu/what-is-gdpr/.

Abrams, Abigail. "Here's What We Know so Far about Russia's 2016 Meddling." *Time*, Time, 18 Apr. 2019, https://time.com/5565991/russia-influence-2016-election/.

Amber, Eric. "Select Committee on Intelligence United States

Senate." *RUSSIANACTIVEMEASURESCAMPAIGNSANDINTERFERENCE INTHE2016U.S.ELECTION*, VOLUME 1:RUSSIANEFFORTSAGAINSTELECTION INFRASTRUCTURE, 1 Jan. 2017, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

Bannan, Christine. "Perspective | More Cybersecurity Won't Secure Our Elections, but Privacy Protections Might." *The Washington Post*, WP Company, 28 Dec. 2020, https://www.washingtonpost.com/outlook/2020/12/29/electionsecurity-privacy-social-media/.

Benenson, Peter. "'The Great Hack': Cambridge Analytica Is Just the Tip of the Iceberg." *Amnesty International*, 11 Oct. 2021, https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/.

Bienkiewicz, David. "What Are DKIM, SPF, and DMARC? Why Are They so Important to Your Organization?" *Compass IT Compliance*, 5 June 2020, https://www.compassitc.com/blog/what-are-dkim-spf-and-dmarc.

Carey, Alexis. "How Facebook's Huge Gamble Could Backfire." *News*, News.com.au - Australia's Leading News Site, 29 Oct. 2021, https://www.news.com.au/technology/online/social/facebooks-rebrand-to-meta-could-be-doomed-tofail/news-story/de5e6fadf91672519065e2b556d020a9.

Culley, Brad. "Spear Phishing: The Greatest Threat to Democracy." *PhishProtection.com*, 30 July 2019, https://www.phishprotection.com/blog/spear-phishing-the-greatest-threat-to-democracy/.

Draegen, Shannon. "What Is DMARC and Why Is It Important for Email?" *Dmarcian*, 14 Jan. 2021, https://dmarcian.com/why-dmarc/.

Fessler, Pam, and Michel Martin. "Russians Believed to Have Used Spear-Phishing in Election Hacking." *NPR*, NPR, 18 June 2017, https://www.npr.org/2017/06/18/533438850/russians-believed-to-have-used-spear-phishing-in-electionhacking.

Henderson, Juliana Gruenwald. "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on

Facebook." *Federal Trade Commission*, 28 Apr. 2020, https://www.ftc.gov/news-events/press-releases/2019/07/ftcimposes-5-billion-penalty-sweeping-new-privacy-restrictions.

Hern, Alex. "Cambridge Analytica: How Did It Turn Clicks into Votes?" *The Guardian*, Guardian News and Media, 6 May 2018, https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopherwylie.

Husain, Mishal. "Twelve Russians Charged with US 2016 Election Hack." *BBC News*, BBC, 13 July 2018, https://www.bbc.com/news/world-us-canada-44825345.

Kelly, Makena. "AOC Calls Facebook a 'Cancer to Democracy' after Meta Rebrand." *The Verge*, The Verge, 29 Oct. 2021, https://www.theverge.com/2021/10/29/22753046/facebook-meta-aoc-instagram-rebrand-france-haugen-blumenthal.

Khern, Chee. "Behind-the-Scenes Look at GovTech's Red Team Cyberattack." *Government Technology Agency*, 4 June 2018, https://www.tech.gov.sg/media/technews/behind-the-scenes-look-at-govtech%E2%80%99s-red-teamcyberattack.

Krebs, Cristopher C. "Avoiding Social Engineering and Phishing Attacks." *Security Tip (ST04-014)*, CISA, 25 Aug. 2020, https://www.cisa.gov/uscert/ncas/tips/ST04-014.

Lewis, Paul. "Leaked: Cambridge Analytica's Blueprint for Trump Victory." *The Guardian*, Guardian News and Media, 23 Mar. 2018, https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory.

Maina, David. "Facebook Data Privacy Scandal: Here's What You Need to Know: Easyllama." *Sexual Harassment Compliance Training*, EasyLlama, 14 June 2021, https://www.easyllama.com/blog/facebook-data-privacy-scandal.

Martin, David. "What Role Did Cambridge Analytica Play in the Brexit Vote?: DW: 27.03.2018." *DW.COM*, 27 Mar. 2018, https://www.dw.com/en/what-role-did-cambridge-analytica-play-in-the-brexit-vote/a-43151460.

O'Neill, Patrick Howell. "The Russian Hackers Who Hit the 2016 Election Have Been Very Busy Since." *MIT Technology Review*, MIT Technology Review, 2 Apr. 2020, https://www.technologyreview.com/2019/10/17/335/kremlinhackers-are-back-in-the-spotlight-after-2016-election-breach/.

O'Neill, Patrick Howell. "The Russian Hackers Who Interfered in 2016 Were Spotted Targeting the 2020 US Election." *MIT Technology Review*, MIT Technology Review, 14 Sept. 2020, https://www.technologyreview.com/2020/09/10/1008297/the-russian-hackers-who-interfered-in-2016-were-spottedtargeting-the-2020-us-election/.

Taylor, David. "Top 10 Data Protection Problems." *BCS*, 16 Aug. 2021, https://www.bcs.org/articles-opinion-andresearch/top-10-data-protection-problems/.

Vazquez, Maegan. "Trump Isn't the Only Republican Who Gave Cambridge Analytica Big Bucks." *CNN*, Cable News Network, 21 Mar. 2018, https://edition.cnn.com/2018/03/20/politics/cambridge-analytica-republican-ties/index.html.

Voisard, Amanda. "General Assembly Backs Right to Privacy in Digital Age | | UN News." *United Nations*, United Nations, 13 Dec. 2017, https://news.un.org/en/story/2013/12/458232-general-assembly-backs-right-privacy-digital-age.

Wade, Michael. "Psychographics: The Behavioural Analysis That Helped Cambridge Analytica Know Voters' Minds." *The Conversation*, 4 Oct. 2021, https://theconversation.com/psychographics-the-behavioural-analysis-that-helped-cambridgeanalytica-know-voters-minds-93675.