06 NOV, 2022

Experts: Data manipulation ahead of polls may shift electoral mindset

The Sunday Post (Kuching), Malaysia

Experts: Data manipulation ahead of polls may shift electoral mindset

By Erda Khursyiah Basir

KUALA LUMPUR: Political surveys are crucial to any election process as they form the basis of the research on which the campaign revolves.

But be warned – some of these surveys also manipulate, helping to shape thoughts and shifting voter mindset, experts said.

Respondents are likely to receive calls from individuals introducing themselves from a certain political party to assess their preference to vote for a party or candidate running for election.

Among the questions asked: "Do you know which area you'll be voting? Who will you vote? Do you know that you are entitled to some allocation (money) if you vote for this party?" With the 15th general election (GE15) fever heating up, some questions come to mind: how do you distinguish between a genuine call from a political party conducting an opinion poll and from a syndicate or a scammer in disguise? Obviously, some questions are mind-boggling. How did they manage to obtain your data as voter including your telephone number? These are issues of concerns among electorates ahead of the GE15 to be held on Nov 19, when their personal data are indiscriminately accessed and manipulated by quarters with vested interests.

Voters, risky candidates

Deputy president of the Malaysian Cyber Consumer Association (MCCA) Azrul Zafri Azmi said data trading is usually rife with election season in the air, and those involved will obtain the data required including through surveys for political analysis purposes.

"The information could be very detailed such as full name, home address, phone number, identification card number and voting area. The information is believed to have been accessed from a telco and last year, news went viral that personal data of customers were (allegedly) leaked through the Inland Revenue Department (LHDN) and the National Registration Department (JPN).

"Investigation into such an allegation must be conducted immediately and in a transparent manner to prevent more leakages and indiscriminate trading of data. The authorities should probe individuals who are involved in the system maintenance and database servers," he told Bernama recently.

However LHDN, in a statement, has denied being involved in the alleged leak of personal data of four million Malaysians through a government platform under the purview of JPN.

"For your information, LHDN is only a user and not the owner of the myIDENTITY system," it said, according to a Bernama report on Sept 28, 2021.

Following the allegation, the agency said an internal investigation had found no such leak. Describing customers' data as an invaluable commodity in today's digital world, Azrul Zafri said the information is used for analysing an individual's behaviour for commercial and political purposes as well as by fraud syndicates.

"In the context of elections, be it electoral or candidates' data, both have risks. Voters' data can be sold to a political party to determine the effectiveness of its campaign, while candidates' data is also saleable to opponent parties to take advantage of personal weaknesses during the campaign," he explained.

Political, personal gains

The high demand for the data contributed to a surge in trading of information for manipulation for political, business, fraud and other nefarious activities.

While the trading process is usually related to the dark web, there are also quarters who undertake such operations in the open market such as online forums. For example, the Ministry of Communications and Multimedia (K-KOMM) on June 14 this year issued an order to Internet service providers (ISPs) to block the sale of data on an open-source intelligence website.

Its minister Tan Sri Annuar Musa said the order was issued around 6.30pm, the same day after the website and it activities were exposed on Twitter in the morning of June 12.

Azrul Zafri said data leakage poses risks for Internet users to various crime activities including Macau Scam, mule account syndicates and various fraudulent activities, which could result in financial losses as well as endanger their lives.

"Internet is an effective medium to a wealth of information such as education, business, etc. However, users must be given early education on the best platform to use without exposing to their own risks especially in matters related to personal data," he said, adding that cyber education is their last line of defence against scammers and from being manipulated by unscrupulous people.

IoT, IR4.0 era

Meanwhile Prof Dr Mohd Mizan Mohammad Aslam of the Department of International Relations, Security and Law, Faculty of Defence Studies and Management, National Defence University of Malaysia (UPNM) said manipulation of data is rampant in today's Internet of Things (IoT) era.

"The phenomenon is becoming prevalent during the Industrial Revolution 4.0 (IR4.0) or the 5G technology evolution, bringing about an information overload especially on the social media and the internet. As a result, users are unable to differentiate between true and false information.

"At the same time, we have become a community who will only read, listen and focus on what really matters and reject (information) that we're not interested in. This situation is what is known as echo chamber, and that is why many tend to be susceptible to false or fake information," he said.

According to him, several quarters especially those directly involved in the elections will use various tactics to win seats by swaying public opinion as

06 NOV, 2022

Experts: Data manipulation ahead of polls may shift electoral mindset

The Sunday Post (Kuching), Malaysia

opposed to making a decision towards a political party or group. He said trends of data manipulation were seen in elections in the US, Russia and more recently in the Philippines, which saw electoral decisions largely influenced by data or information harvested from various platforms

Modus operandi

Data manipulators usually buy information available from various platforms including Meta, which has control over personal data and information through Facebook, Instagram and other social media. There are also groups who take the easy and quick route by stealing data from various platforms. This way, they do not have to seek approval from any parties and that they are not legally bound by any restrictions.

Mohd Mizan said among the widely used methods include profiling, which refers to collecting and gathering related data from various sources and they are kept for certain purposes.

"As examples, the period an individual uses the Internet, social friends and topics of interest, websites they surf or programmes they watch. Profiling will be made based on the type of information obtained and from the data, they will know the pattern or mindset of an individual, community as well as the nation.

"Data manipulation can happen to anyone including the majority or what is known as bottom million or large community. It can happen to the top few groups. Both groups risk being used by certain groups to achieve their goals," he added.

Data is secretly traded either on certain websites or among hackers who have their own community, are inter-connected and engage in exchange of information required.

"Their groups (hackers) are strong, devious and well guarded and it would be difficult for a (data) security (personnel) to stop their activities unless they work together or become part of their operation. Hackers reap profits from data that are sold and are usually in great demand especially from today's borderless world.

"However, those who buy data are not doing it blindly, but with a certain purpose and the data is manipulated as much as possible and finally generating profits for them, such as when winning elections," he said, adding that high value data is based on the difficulty of obtaining the information.

ESIM theory

Data manipulation is used as a vehicle to change public perception, mindset and understanding through modification. The modification technique is used to provide better information about a candidate in an election.

"Public perception of a candidate is based on data made available to them. Hence, the individual with favourable data and information will automatically be the voters' choice. In the past, character assassination was used by slandering an individual with the intention of destroying public confidence in the person through smear campaigns in the print media, to the extent of 'physically abusing' the individual.

"However today, the social media is widely used to launch manipulative campaigns on various issues, causing the public to reject and despise an individual; hence having an impact on the election results," he said, adding that data manipulation is likely to poison the minds of the people.

He said the data manipulation phenomena is linked to the theory of Elaborated Social Identity Model (ESIM) on crowd behaviour, noting that its objective is to access data and influence the psychology as well as the social behaviour of the community

He also said the approach has proven to be effectively used in several studies including the elections and for better understanding of issues related to war.

Threats, legal empowerment On a wider perspective, data manipulation risks threats from the social aspects, political stability, economy and national security, when secret and sensitive data is used as a 'weapon' for certain groups to weaken the people and the nation.

"As an example, information from a phone conversation between the Prime Minister with an individual including from abroad with issues centred on policies, international relations, intelligence information, overseas operations, etc, if exposed, would automatically be unsafe for the nation and place it as the subject of intrusion.

"On the election issue, when a data is manipulated, political decisions made would definitely be different from their previous considerations. Leaders who are chosen are no longer based on merit, but due to their success in championing certain issues effectively; hence, winning the hearts and minds of the people," he said, adding that the matter is feared to have negative long-term implications including issues on ethnic conflict and religion.

All quarters need to strengthen their data defence system at least reducing the risks of attacks, he said, noting that data manipulation and attacks would worsen and that the people may not be able to distinguish between genuine and fake information after the 5G technology has been widely disseminated.

"The scope of technology's expanse is so great. As long as there is demand and buying and selling of data, manipulation and leakage of information will take place. We can't avoid from using technology but we can educate the public to be more responsible.

"Laws and existing acts need to be empowered and fully utilised in every issue related to manipulation or leakage of customers' data," he added.

In this respect, he said, the Personal Data Protection Act 2010 as an example can be read together with the Communications and Multimedia Act 1998, the Official Secrets Act 1972, Defamation Act 1957 and others, to give individuals the right to exercise control over how their data is used and prevent data leakage and misuse. — Bernama

AUTHOR: Erda Khursyiah Basir SECTION: HOME PAGE: 11 PRINTED SIZE: 643.00cm² REGION: KL
MARKET: Malaysia PHOTO: Full Color ASR: MYR 8,768.00 ITEM ID: MY0050208161

06 NOV, 2022

Experts: Data manipulation ahead of polls may shift electoral mindset

The Sunday Post (Kuching), Malaysia

SUMMARIES

Opposed to making a decision towards a political party or group. He said trends of data manipulation were seen in elections in the US, Russia and more recently in the Philippines, which saw electoral decisions largely influenced by data or information harvested from various platforms Modus operandi Data manipulators usually buy information available from various platforms including Meta, which has control over personal data and information through Facebook, Instagram and other social media.