

Supplementary Material for the article “How does Fake News Spread?
Understanding Pathways of Disinformation Spread through APIs”
<https://doi.org/10.1002/poi3.268>

By

Lynnette H. X. Ng¹ and Araz Taeihagh^{2,3}

¹ Institute for Software Research, Carnegie Mellon University, Pittsburgh, Pennsylvania, USA

² Lee Kuan Yew School of Public Policy, National University of Singapore, Singapore

³ Centre for Trusted Internet and Community, National University of Singapore, Singapore

Corresponding Author: Araz Taeihagh, Lee Kuan Yew School of, Public Policy, National University of, Singapore, 469B Bukit Timah, Rd, Li Ka Shing Bldg, Level 2, #02-10, 259771, Singapore. Email: sparaz@nus.edu.sg and araz.taeihagh@new.oxon.org

Appendix A1: Literature Review Methodology

In this study, we conducted a multidisciplinary exploration of studies in the social sciences (e.g., digital journalism, information and communications, public policy) and computer science (software engineering, information systems). To identify how social media platform APIs can facilitate the spread of disinformation, we first systematically search possible terms associated with social media platforms, shown in Supplementary Table 1. These terms were searched in conjunction with the keywords listed in Supplementary Table 2 are associated with fake news, its spread, and societal implications. We examined scholarly research published from the year 2010 onwards, given that the rise of digital platforms occurred predominantly from the mid-2000s (e.g. Google in 1998, Facebook in 2004, YouTube in 2005, Twitter in 2006) and given that only after 2010 did the spread of fake news on social media platforms start receiving more international recognition, particularly after the 2016 US election and the UK’s referendum to leave the European Union (Bastos & Farkas, 2019; Jr et al., 2018; Li & Su, 2020). Peer-reviewed journal articles were collected from reputed academic databases, including Scopus and Web of Science, and we utilised the Google Scholar search engine when the academic databases produced limited results.

Appendix A2: Social Media APIs and API Access Requirements

An API is a “programming framework that implements a set of standard behaviours” (Puschmann & Ausserhofer, 2017). Generally, APIs facilitate the use of data for new functions and enable greater utility of the social media platform as an application. They are often documented with specifications of data functions and object classes that can be accessed through them. Social media APIs are usually RESTful services delivered over the

web. RESTful services conform to the representational state transfer (REST)¹ framework, which has a set of constraints, such as client–server-based communication, stateless requests and the use of uniform interfaces (Maleshkova et al., 2010). The use of uniform interfaces enables us to identify the usage of APIs in open-source code repositories. The API is commonly invoked by the hypertext transfer protocol secure (HTTPS)² requests, and the data retrieved is determined by the parameter values sent.

This article categorises APIs into two categories: (1) official APIs; and (2) unofficial APIs. Official APIs involve a developer having a platform-issued developer key or an authentication secret. Developers usually send an HTTPS REST request from their running code to the platform’s data server. To be accepted, this request has to contain the platform-defined authentication string, i.e., the uniform interface of the RESTful API structure. The format of the authentication string can be found on the platform’s developer’s page. The authentication strings are thus identified by platform-specific identifiers, such as “consumer_secret”, which the platform requires to be present in a data request.

Social media platforms control the use of official API keys to varying degrees (see Supplementary Table 3). With these keys, developers can access two sets of data: (1) data without restriction, which refers to data that users choose to share publicly, and (2) data restricted only to information about the developer’s account. Twitter requires a phone number for authentication before the developer API can be used. Facebook requires the user’s app to go through an app review process, in which the developer must specify the permissions required (no additional permissions are granted). The available APIs for message dissemination are: Groups API, Pages API and Messenger API. Instagram APIs are only available for verified businesses, and an app review process is required. The Reddit API simply requires a Reddit account; in fact, their page states “We’re happy to have API clients, crawlers, scrapers, and browser extensions, but they have to obey some rules”. YouTube requires phone authentication and restricts information to the developer’s video channel. Pinterest only requires user permissions for the API, which then allows access to data only about the particular user. Telegram requires a phone number to log in to the platform and only provides user and group messages information. Weibo requires phone number authentication and only returns data about a particular user profile, timeline, and friendships if the user has granted permission. The ease of gaining access to data potentially affects the number of developers that will harness the APIs.

Unofficial APIs include APIs meant for internal purposes that are used by third parties for unintended purposes. Common methods include using the web scraping method and downloading the HyperText Markup Language (HTML), then parsing the page to extract the

¹ For more information about Representational State Transfer (REST) framework see https://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm (accessed on 15th June 2021)

² Htps is used for secure communication over a computer network through encryption, and is widely used on the Internet. The authentication over the network requires a trusted third party to sign server-side digital certificates.

elements. An example is web scraping methods to log in to Instagram: this involves identifying the HTML tag of the LOGIN button on Instagram before sending an automated code to click the button. Another common method these repositories typically use is utilising the Selenium library (Muthukadan, 2018), a framework designed for web automation testing that can be used to perform interactions with third-party web pages. It scrapes the website through Chrome web browser automation and controls the keyboard and mouse movements to identify and interact with the elements.

Appendix A3: Details of Code Repositories and API Usage

For the repositories where authors reveal their locations, we performed an analysis of the origin location of the repositories. Supplementary Figure 1 highlights the distribution of code repositories across social media platforms. The United States, Canada, Europe, and Russia have the greatest number of repositories (Supplementary Figure 2). By analysing the words used in the code repository description, we formulated a word cloud representation (Supplementary Figure 3), which showcases the most common phrases used in the descriptions. The word cloud reflects that most code repositories are constructions of bots for social media platforms.

In comparison with 2018 (Assenmacher et al., 2020), the number of repositories had grown 1.7 times by 2020. However, there is no significant change in the distribution of platforms, the trend in the number of repositories over time and the trend in the origin of repositories. We note that the number of repositories that report a location has significantly decreased, which may be due to increased privacy concerns of the users. The most popular programming language used in the repositories is Python, followed by HTML and C# (Supplementary Figure 4). We infer that the process of obtaining and manipulating data via APIs is most easily done using Python. There is an even distribution of repositories that use official and unofficial Instagram APIs (Supplementary Figure 5). We thus infer that official APIs provided by social media platforms provide sufficient data and functionality for code developers to pull and push information from/to the platforms.

Appendix A4: Trend in social media platforms

In Supplementary Figure 6a, we present the trend of the number of code repositories for each platform across time. Telegram published their bot API in mid-2015, resulting in a sharp increase in the number of repositories. As the large number of Telegram repositories distorts the proportion of the graph below and in Supplementary Figure 6b, we provide a clearer view of the trends in other social media platforms (excluding Telegram).

Twitter implemented several new APIs in 2017 for their standard and premium tier users: its effect can be seen in the sharp increase in the number of repositories created. Standard and premium tier users are provided with free, basic API usage and pay-per-month billing. In contrast, enterprise users receive huge access to and high availability of data through annual contractual billings. In 2018, Twitter changed their Terms of Service, Privacy Policy and Twitter Development Agreement to include privacy, security, and data protection updates, which is reflected in the sharp decrease in the number of repositories. Though Facebook introduced its Messenger API in mid-2016, its number of repositories decreased. In 2018,

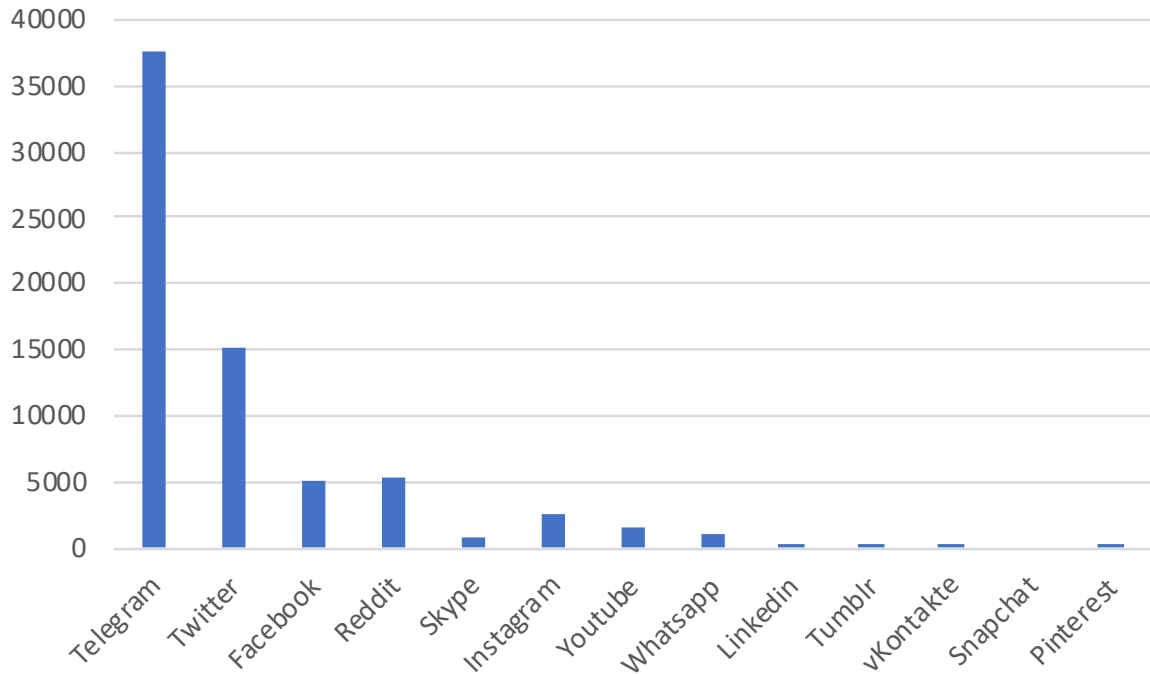
Facebook introduced a rigorous app review process for developers who want to use their API, and the number of repositories we collected decreased sharply after that period.

Data Analysis of API Usage of Code Repositories

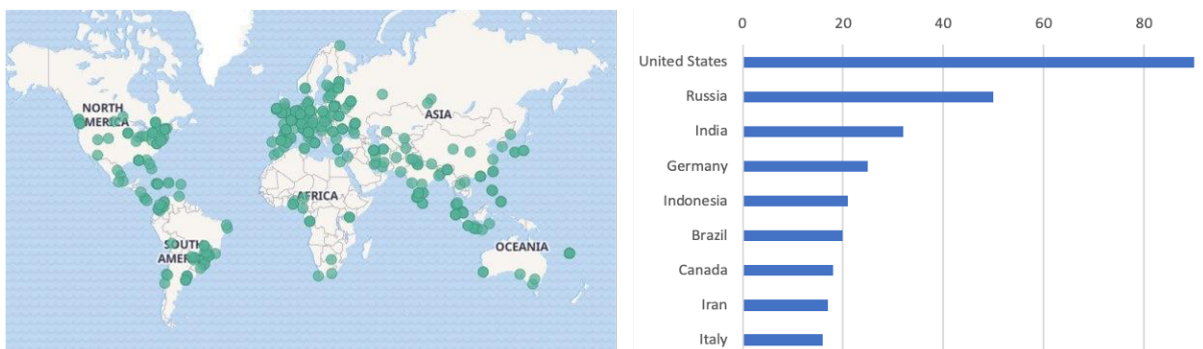
We note that not all queried repositories may have returned a result as repositories may use variable names not captured in our manual inspection. Also, we were unable to obtain information on all searched repositories due to GitHub/GitLab API restrictions. A total of 2,931 code repositories from GitHub returned positive results. Of this subset of code repositories, we observed that a significantly larger share of repositories use the Reddit and Twitter official APIs compared to unofficial methods.

Supplementary Figures

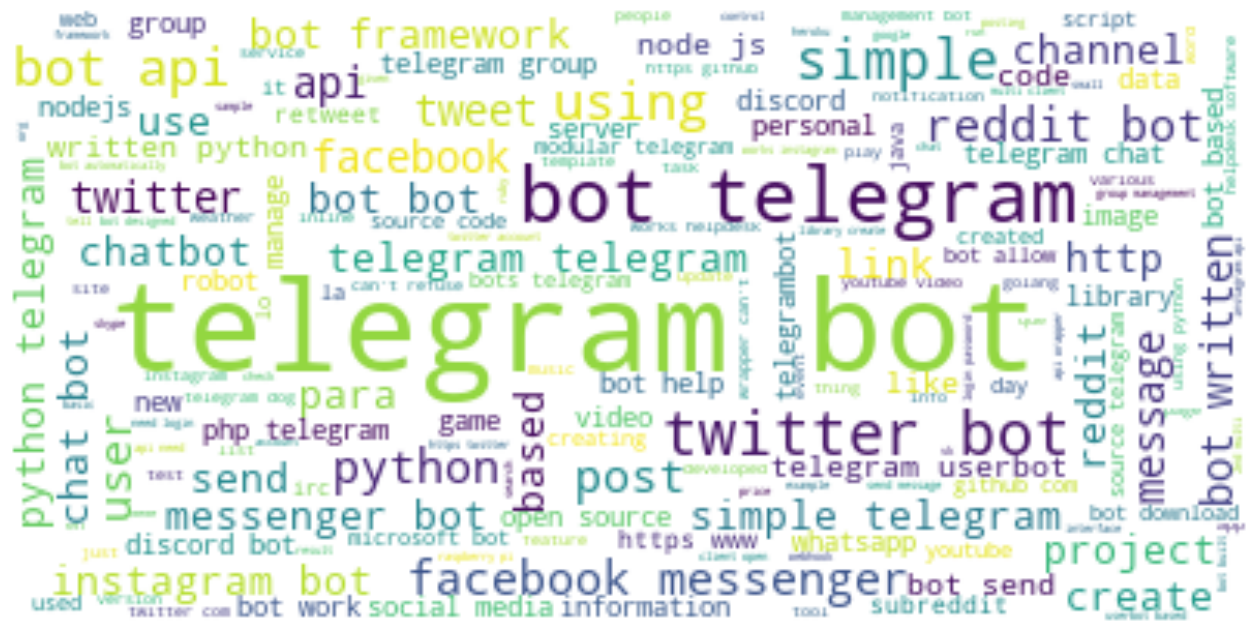
Supplementary Figure 1: Distribution of code repositories across social media platforms in May 2020



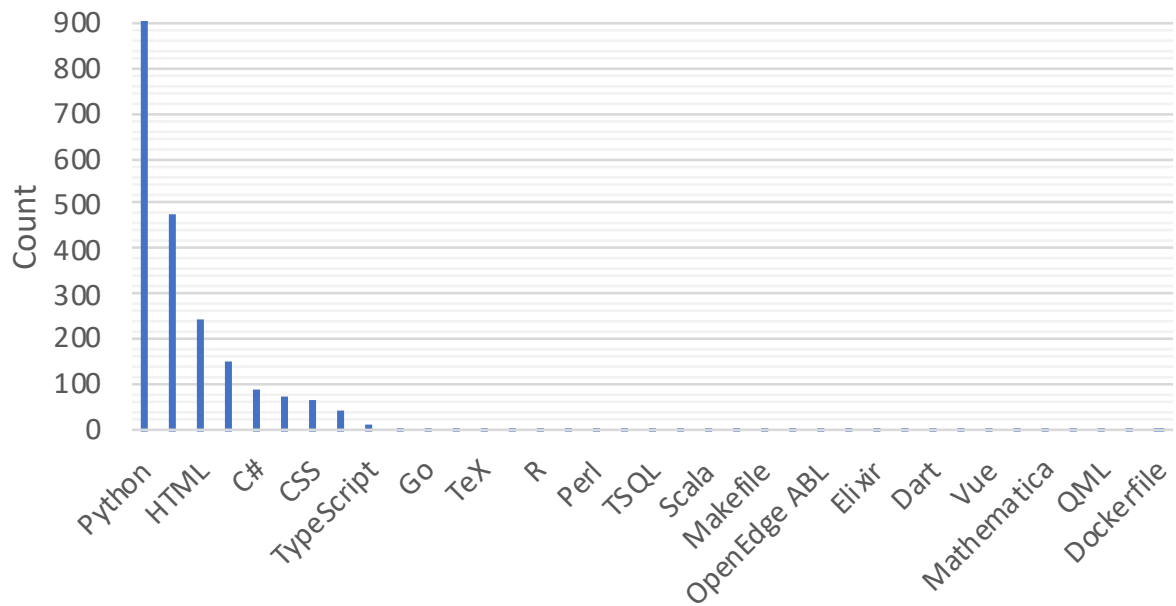
Supplementary Figure 2: Origin of data repositories collected in May 2020



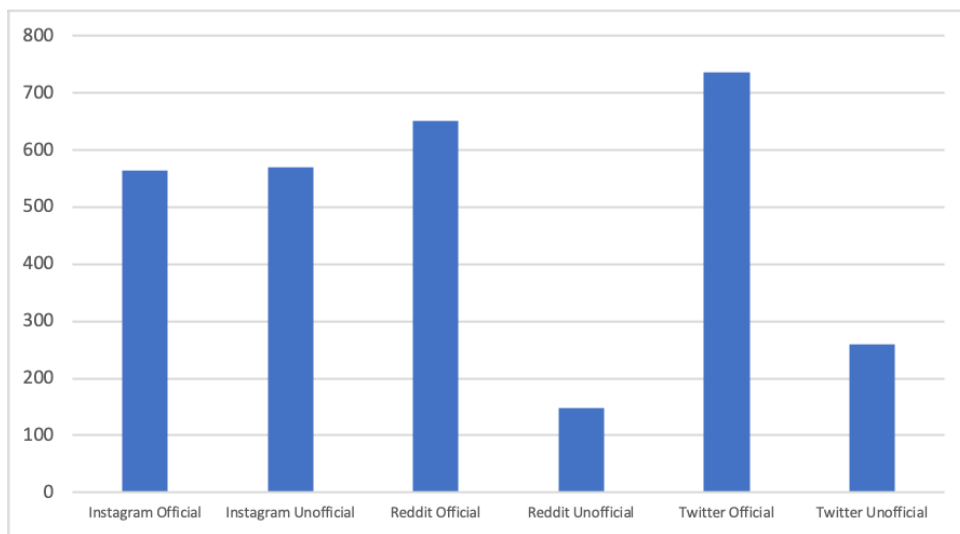
Supplementary Figure 3: Word cloud of descriptions from code repositories



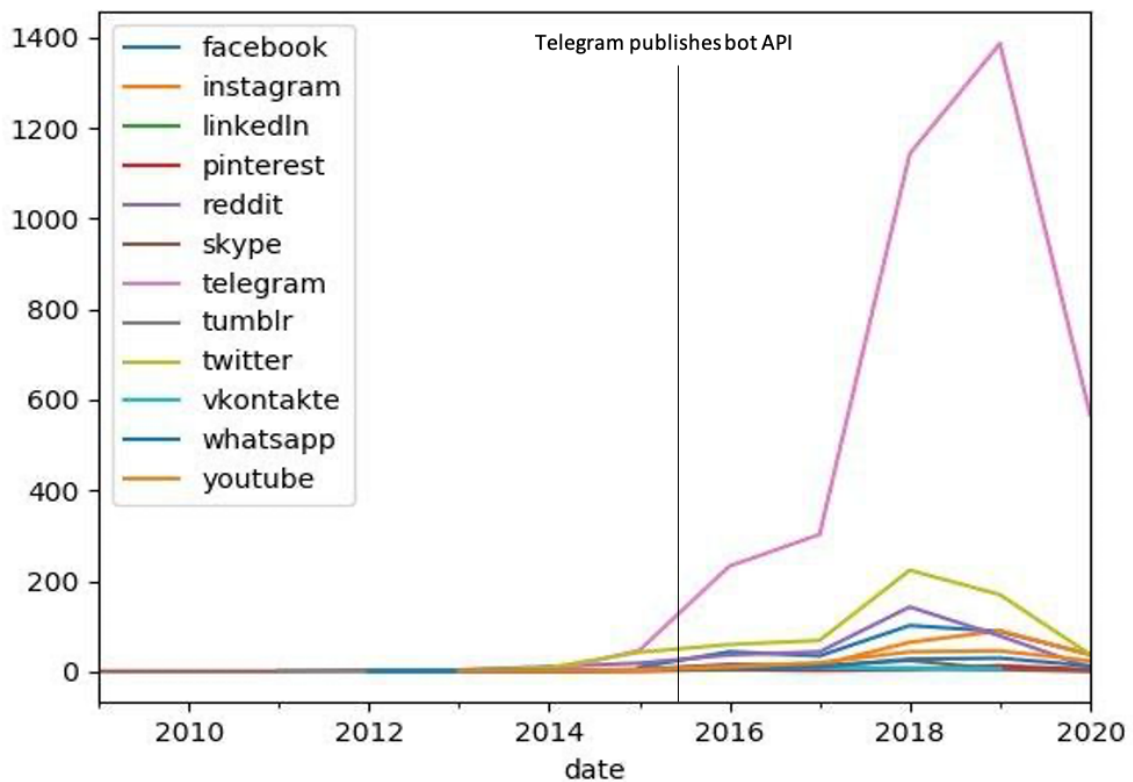
Supplementary Figure 4: Distribution of Programming Languages used in API Repositories



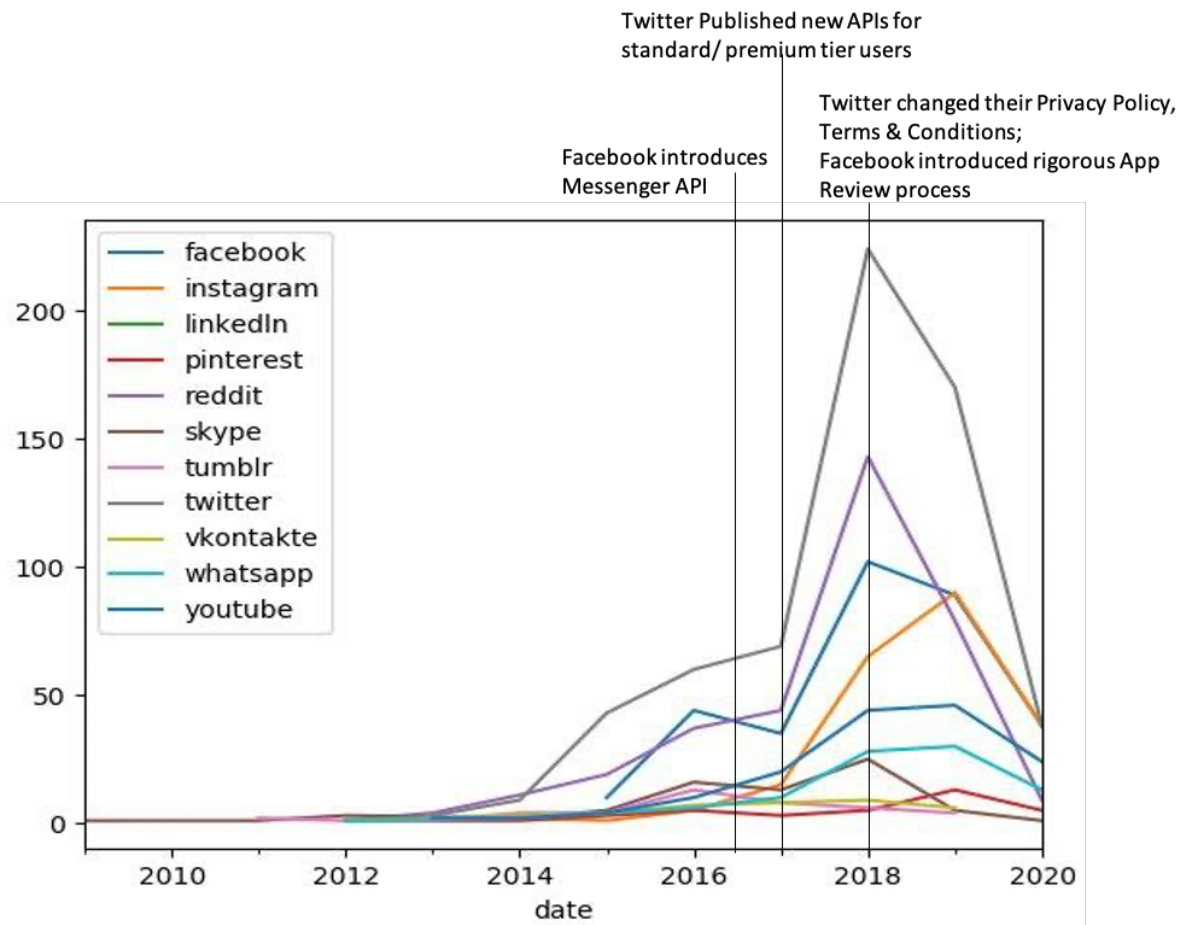
Supplementary Figure 5: Distribution of code repositories using official and unofficial APIs



Supplementary Figure 6a: Trend in surveyed platforms in May 2020



Supplementary Figure 6b: Trend in surveyed platforms excluding Telegram in May 2020



Supplementary Tables

Supplementary Table 1: Keywords used to identify articles relating to social media platforms

Topic	Keywords
Platform	platform(s), social media, social media/digital/internet platform(s), Twitter, Facebook, Instagram, Reddit, Google, LinkedIn, YouTube, WhatsApp, Telegram
API and other technologies	application programming interface, algorithm(s), algorithmic, automate, automated, automating, automation, bot(s), bot network(s), bot net(s), advertising technology, (digital) infrastructure, (digital) tools, (digital) marketing, (digital) techniques, data mining/extraction, machine learning, ecosystem

Supplementary Table 2: Keywords used to identify articles relating to the spread of fake news and its societal implications

Topic	Keywords
Disinformation	fake news, propaganda, misinform/misinformation, disinformation, misuse/abuse/manipulation/distortion/fabrication/falsification of information/content/fact(s)/message(s), information misuse/abuse/manipulation/distortion/deception/fabrication/falsification, misused/abused/manipulated/distorted/fabricated/false/incorrect /misleading/deceptive information/content/fact(s)/message(s), scam(s)
Spread	spread, disseminate, dissemination, promote, promotion, amplify, amplification, magnify, magnification, reach, circulate, circulation, distribute, distribution, propagate, propagation, broadcast, broadcasting, diffuse, diffusion, communicate, communication
Societal implications	society, social, politics, political, hate, discord, polarise, polarisation, privacy, security, transparency, implication(s)/consequence(s)/effect(s)/impact(s)/ risk(s)/concern(s), accountability, election(s), trust

Supplementary Table 3: Landscape of Official APIs

✓: no restrictions on API access. ✓: Restricted only to information about the developer's account

Platform	Requires phone number authentication	Requires app review	Requires user permission	API access		
				User information	Group information	Search
Twitter	✓			✓	✓	✓
Facebook	✓	✓	✓	✓	✓	✓
Instagram	✓	✓	✓	✓	✓	✓
Reddit					✓	✓
YouTube	✓			✓	✓	✓
Pinterest			✓	✓	✓	
Telegram	✓			✓	✓	
Weibo	✓			✓		

Supplementary Table 4: Search terms and content identifiers used for the data collection on API implementation

Platform	Search terms	Type	Content identifier
Twitter	“twitter bot”, “twitter scraper”, “twitter crawler”, “twitter posting”	Official	“consumer_secret”
Twitter	“twitter bot”, “twitter scraper”, “twitter crawler”, “twitter posting”	Unofficial	“lxml”, “selenium”, “data-item-id”
Facebook	“automated facebook”, “facebook bot”, “fb”, “auto post”, “facebook group”, “group api”, “messenger api”, “facebook scraper”, “facebook crawler”, “fb scraper”, “fb crawler”	Official	“graph.facebook.com”, “access_token”
Facebook	“automated facebook”, “facebook bot”, “fb”, “auto post”, “facebook group”, “group api”, “messenger api”, “facebook scraper”, “facebook crawler”, “fb scraper”, “fb crawler”	Unofficial	“selenium”, “username”, “password”
Instagram	“automated instagram”, “instagram bot”, “auto like instagram”, “instagram account creator”, “instagram scraper”	Official	“access_token”, “client_secret”
Instagram	“automated instagram”, “instagram bot”, “auto like instagram”, “instagram account creator”, “instagram scraper”	Unofficial	“password”, “selenium”
Reddit	“reddit bot”, “reddit scraper”, “reddit crawler”, “reddit posting”, “reddit responses”	Official	“client_id”, “client_secret”, “reddit_username”, “praw”
Reddit	“reddit bot”, “reddit scraper”, “reddit crawler”, “reddit posting”, “reddit responses”	Unofficial	“selenium”

Supplementary Table 5: Summary of actions in The Pathways of Disinformation Spread Framework

Action type	Description	Facilitation of disinformation	References
Stage 1: Network Creation			
<u>1a. Procedural account generation</u> Create user account: define account purpose, define account traits	Use web browser automation to procedurally create account	Mass account generation, while avoiding detection through posing as real account	Jr et al., 2018
<u>1b. Follow/ friend own-created accounts</u>	Follow other accounts Like/ share posts from own/ other accounts	Create a network of pseudo-/ user-accounts Create a false impression of popularity User-accounts like/ follow pseudo-accounts	(Woolley, 2016)
Stage 2: Profiling			
<u>2a. Tracking user engagement</u>			
Cookies to track engagement with ads/ clicks/ shares/ likes/ retweets	Insert cookies in webpage to track user preferences	Collect personally identifiable information	Ghosh et al., 2018
Web beacon to track users' actions	Track user preferences by demographic groups with Facebook Audience Network API		Facebook, 2020a
Location tracking	Integrate services like YouTube, Google Maps and Google Search into applications to leverage on the precise location mapping and rich consumer profiles that may be obtained through paid advertising services		Russell, 2019
<u>2b. Attribute-based selection of audiences</u>			
By topics/ interests through...	Finding users that have certain keywords in posts or like specific posts	Profile/ identify potential audiences for own narrative	Guilbeault, 2018
By demographic features through...	Identifying audiences through societal segments like gender/ age		Speicher et al., 2018
By customer audiences through...	Using Facebook Pixel on webpage to collect data of visitors to the page for users that developers may have access to		Facebook, 2020b
By country/ language through...	Identifying potential targets through searching by country/		

	locale, or keywords in target language		
2c. Network-based selection of audiences			
Identify influential users	Find users that have a large network structure	Identify users that can broadcast a message	Ghosh et al., 2018
By friend/ follow network	Identify users who friend/ follow a predefined list of users of interest and select active users through network structure	Identify potential influencers	Speicher et al., 2018
Stage 3: Content Generation			
3a. Text generation			
	Generate specific synthetic propaganda reflecting an ideology by fine-tuning language models	Generate messages for dissemination	OpenAI, 2019; Solaiman et al., 2019
3b. Media generation			
	Generate synthetic instances of audio/visual data that is very similar to real data	Generate profile images for procedural account generation, generate image posts for dissemination on the network	4chan, 2020
Stage 4: Information Dissemination			
4a. Coordinate posts of multiple accounts			
Posting timing	Post at the same time Post at staggered intervals	Mass dissemination of messages across wide network Reiterate messages over a prolonged period	Ghosh et al., 2018; Shao et al., 2018; Ferrara, 2017 Neudert, 2017
Post legitimate content	Relay breaking news, post about a mundane user's daily life	Establish reputation	Bastos & Mercea, 2018; US Senate, 2020
Post disinformation	Construct messages relating to desired narrative and post in social network	Disseminate disinformation using multiple accounts to amplify desired topics	D. Linvill & Warren, 2020
4b. Interact with posts from own network			
Respond to posts by own network of users	Use own botnet to like own posts, as platforms' recommendation algorithms tend to prioritise content with more responses	Increase engagement of own network's posts, leading to information amplification	Bastos & Mercea, 2018
4c. Engage with users			
Direct messages to targeted users	Send messages to users via @mentions or direct replies	Get pseudo-accounts to be noticed and trusted by human user-accounts	Chamberlain, 2010; D. Linvill & Warren, 2020
Direct messages through attribute-based targets	Gain attention from attribute-based targets through mentioning/ tagging influential users, or replying to posts by influential	Increase prominence of pseudo-accounts Plant/alter views of large group of users	Lokot & Diakopoulos, 2016

	users	Use influential users to spread own message, hiding trace	
4d. Interact with users' posts			
Like/ share posts	Promote posts of network of users	Develop character	Lokot & Diakopoulos, 2016; Zannettou et al., 2019
Respond to posts at certain locales Comment on selected posts	Gain attention from attribute-based targets through responding with replies, comments, likes or shares		