# Code of Practice on Disinformation – Report of Logically for the period June – December 2022

## Table of Contents

## Executive summary

Logically is a technology company that combines advanced artificial intelligence (AI) with a world-class open-source intelligence (OSINT) team and one of the world's largest dedicated fact-checking teams to help government bodies, businesses and social media platforms uncover and address harmful misinformation and disinformation at scale. We have developed a suite of products and services to reduce and ultimately eliminate the harm caused by the spread of misinformation and targeted disinformation campaigns.

Logically is an award-winning international team of data scientists, engineers, analysts, developers and investigators united by the company's mission to enhance civic discourse, protect democratic debate and process, and provide access to trustworthy information. Our dedicated fact-checking and investigations teams produce frequent fact-checks as well as detailed analyses and reports on specific disinformation actors and trends. Our published fact-checks can be found here, and a selection of our deep-dive investigations into specific conspiracy theory trends can be found here.

We signed up to the EU Code of Practice on Disinformation in furtherance of our mission and values and took part in the drafting process alongside other key signatories. We have opted into Commitments geared towards countering the tactics employed by disinformation actors, boosting the impact of fact-checking operations and enhancing media literacy. This report will demonstrate how we adhere to those Commitments, as summarised below.

**Commitment 14**: This Commitment called upon Signatories to outline the policies and countermeasures they have in place to combat manipulative tactics, techniques and procedures (TTPs) employed by actors of disinformation. While Logically does not conduct any policing actions against actors perpetuating disinformation campaigns, we do publish fact-checks and OSINT investigations that spotlight these TTPs, thereby providing case studies that can feed evidence-based policies. The investigations we have highlighted in this report exemplify our identification of non-transparent promotions by influencers, the use of inauthentic reactions to boost credibility, the creation of inauthentic pages or domains, and the use of deceptive practices to manipulate platforms' algorithms. We have also outlined our criteria for identifying 'Coordinated Inauthentic Behaviour', which has resulted in our assessment that the systemic and proactive nature of such content coordination distinguishes it from spam or other forms of inauthentic engagement.

**Commitment 16**: This Commitment asked Signatories to provide qualitative examples of cross-platform migration tactics employed by actors of disinformation to circumvent moderation policies, engage different audiences or coordinate action on platforms with less scrutiny. Logically's case study demonstrates the attempt to mutually reinforce an actor's presence on separate platforms and the reposting of content from mainstream platforms to those that are more fringe.

**Commitment 17**: While Logically did not engage in media literacy activities during the specific implementation period for the Code (June - December 2022), we have responded to this Commitment to carry these out by exemplifying past activities that we intend to build upon in our future scope of work, such as training workshops and materials.

**Commitment 29**: This Commitment sought for Signatories to detail their methodologies for tracking and analysing influence operations and disinformation campaigns, as well as detailing the effectiveness of resilience-fostering measures employed. In response, Logically cited the same investigations as in Commitment 14, but from the perspective of methodology. These investigations demonstrate how disinformation campaigns are sophisticated enough for actors to take stock of how different tactics track and strategize to maximise this information accordingly, which can result in real-world consequences. We intend to keep our research contributions updated in the Transparency Centre, including via annual reporting under the Code. We have also detailed the functioning of our disinformation detection tool, Logically Intelligence, and cited the reach of several of our most-viewed in-platform fact-checks conducted as part of our client work with platforms.

**Commitment 30**: This Commitment asked for information on actions taken to facilitate fact-checking organisations' cross-border collaboration. Logically has responded by citing our involvement in the development of the European Fact-Checking Standards Network (EFCSN), our active cooperation with other organisations on specific fact-checks and subject matters, and our internal structural planning to prioritise such collaborations going forward.

**Commitments 31, 34, 35 and 36**: These Commitments sought information on how Signatories are contributing to the development of a repository of fact-checking content, as well as the Transparency Centre. Logically intends to contribute to these when we are called upon to do so by the Taskforce.

**Commitment 33**: In response to this Commitment to uphold ethical and transparency rules, we have cited our status as a verified Signatory to the International Fact-Checking Network, and our involvement in the development of the EFCSN. We have outlined our strict ethics and transparency policies, as well as our list of prohibited clients and use cases, and the internal rules to which we adhere to protect our independence and non-partisanship.

**Commitment 37**: This Commitment asked about the Signatories' engagement with the Taskforce. Logically has engaged with the Taskforce to the extent that resources have been available internally. We have kept up to date via Plenary attendance, meetings with other smaller Signatories, and proactive outreach to the European Commission and the European Regulators Group for Audiovisual Media Services.

**Commitment 38**: This Commitment called for Signatories to outline the internal teams dedicated to ensuring compliance with the Code. Logically has indicated the titles of the team members responsible for overseeing compliance, as well as the means that were undertaken to assure this. This has included internal cross-functional consultations, reviews of internal documentation and policies, and the maintenance of an open dialogue with the European Commission.

As a start-up in a growth stage, Logically is enthusiastic about building on our existing initiatives and activities. As indicated throughout this report, 2023 has been earmarked for an expansion of our disinformation detection and reporting service, Logically Intelligence, as well as a furthering of our media literacy efforts and collaborations with other fact-checking organisations. As experts in our field, we can help public authorities and platforms to monitor and mitigate harmful misinformation and disinformation at scale, and empower the general public with information on such campaigns in operation to build societal resilience. We intend to demonstrate such developments as these pertain to our Commitments under the Code of Practice in our next scheduled report due in January 2024.

## Guidelines for filling out the report

Baseline reports are detailing how Signatories have implemented their Commitments under the Code and provide the Qualitative Reporting Elements (QREs) and Service Level Indicators (SLIs), as they stand one month after the implementation. The baseline report should also include a comparison between the measures in place under the previous Code to the measures taken to implement the new Code. The measures taken to implement the new Code should be outlined per commitment in the dedicated field of the reporting template.

## Reporting period

The reporting period to be covered in the baseline reports is from 16 December 2022 to 16 January 2023 for all Signatories. (The implementation period of the Code from 16 June 2022 to 16 December 2022 is followed by a one-month reporting period from 16 December 2022 to 16 January 2023.) Signatories shall submit baseline reports outlining policy updates and actions taken to implement the Code during the implementation period. Data, e.g. on the number of actions taken under a specific policy, should be reported on from the end of the implementation period (16 December 2022) until the cut-off date of 16 January 2023. In case specific data is not available for the first reporting period (from 16 December 2022 to 16 January 2023), please provide the monthly average based on the previous quarter, clearly outlining the methodology used in the relevant field. The submission date for baseline reports is January 31, 2023.

## Adjusting the reporting template

Non-VLOPs can adapt the template to specific commitments and measures they subscribed to. This may include adapted wording for commitments, measures, QREs and SLIs. Non-VLOPs signatories will report only on commitments and measures they subscribed to and provide Member State-level data only if feasible.

## Reporting per Service

When filling in a report for several services, use colour codes to clearly distinguish between services. At the beginning of the report, clarify what colour is used for which service.

## Reporting in text form

Reporting in the form of written text is required for several parts of the report. Most of them are accompanied by a target character limit. Please stick to the target character limit as much as possible. We encourage you to use bullet points and short sentences. Links should only be used to provide examples or to illustrate the point. They should not be used to replace explanations or to provide data in the forms. All relevant explanations and data must be included in the table directly, in written form.

## Reporting SLIs and data

Reporting on Service Level Indicators requires quantitative information to be reported in the reporting template. We ask you to report data in the format provided by the reporting template, not on external links.

## Reporting on TTPs

If subscribed to Commitment 14, Integrity of Services, we ask you to report on each identified TTP individually. The number of identified TTPs may vary per service. Where more than one TTP are reported under the same action, clarify the reasoning in the methodology. Where input is not provided, keep the placeholder for the relevant TTP and explain reasons and planned remedial action. Additionally, as with all other SLIs, data can be provided per Member State for each individual TTP.

## Missing Data

In case that at the time of reporting there is no data available yet, the data is insufficient or the methodology is lacking, please outline in the dedicated field (i.e. in the field about further implementation measures planned) how this will be addressed over the upcoming six months, being as specific as possible. Please also indicate inconsistencies or gaps regarding methodology in the field dedicated to methodology.

## Attachments

We ask you not to enclose any additional attachments to the harmonised reporting template.

## Uploading data to the Transparency Centre

After the submission of the baseline reports and the launch of the Transparency Centre website, all data from the reporting template must be uploaded to the Transparency Centre within maximum 7 days, allowing easy data access and filtering. It is the responsibility of the Signatories to ensure that the uploading takes place and is executed on time. Signatories are also responsible to ensure that the Transparency Centre is operational and functional by the time of the reports' submission, that the data from the reports are uploaded and made accessible in the Transparency Centre within the above deadline, and that users are able to read, search, filer and download data as needed in a user-friendly way and form

# IV. Integrity of Services

## Commitment 14

In order to limit impermissible manipulative behaviours and practices across their services, Relevant Signatories commit to put in place or further bolster policies to address both misinformation and disinformation across their services, and to agree on a cross-service understanding of manipulative behaviours, actors and practices not permitted on their services. Such behaviours and practices, which should periodically be reviewed in light with the latest evidence on the conducts and TTPs employed by malicious actors, such as the AMITT Disinformation Tactics, Techniques and Procedures Framework, include:

The following TTPs pertain to the creation of assets for the purpose of a disinformation campaign, and to ways to make these assets seem credible:

- 1. Creation of inauthentic accounts or botnets (which may include automated, partially automated, or non-automated accounts)
- 2. Use of fake / inauthentic reactions (e.g. likes, up votes, comments)
- 3. Use of fake followers or subscribers
- 4. Creation of inauthentic pages, groups, chat groups, fora, or domains
- 5. Account hijacking or impersonation

The following TTPs pertain to the dissemination of content created in the context of a disinformation campaign, which may or may not include some forms of targeting or attempting to silence opposing views. Relevant TTPs include:

- 6. Deliberately targeting vulnerable recipients (e.g. via personalized advertising, location spoofing or obfuscation)
- 7. Deploy deceptive manipulated media (e.g. "deep fakes", "cheap fakes"...)
- 8. Use "hack and leak" operation (which may or may not include doctored content)
- 9. Inauthentic coordination of content creation or amplification, including attempts to deceive/manipulate platforms algorithms (e.g. keyword stuffing or inauthentic posting/reposting designed to mislead people about popularity of content, including by influencers)
- 10. Use of deceptive practices to deceive/manipulate platform algorithms, such as to create, amplify or hijack hashtags, data voids, filter bubbles, or echo chambers
- 11. Non-transparent compensated messages or promotions by influencers
- 12. Coordinated mass reporting of non-violative opposing content or accounts

| Measure 14.3 | |
|---|---|
| **QRE 14.3.1** | Logically publishes fact-checks and open-source intelligence (OSINT) investigations to counter disinformation actors' manipulative tactics, techniques and procedures (TTPs). As we do not conduct any policing actions in response, we do not have formal policies in place to address these TTPs as such. However, our fact-checking partnerships with major platforms and OSINT investigations can educate audiences on such TTPs, and equip stakeholders with the case studies needed to feed evidence-based policies. |

Examples of identified TTPs

**Inauthentic coordination of content creation and amplification**

- June 2022: we identified individual Telegram channels targeting Indian Muslims with separate conspiracies; with channel descriptions linking to others within a disinformation-spreading cluster for inauthentic amplification. A 'Primary Hate Group' was found to have forwarded the bulk of the content in a coordinated manner across the cluster, which was then susceptible to further amplification via the links to the other channels. This shows that disinformation actors can coordinate the use of different channels for different narratives; to determine which of them gain more traction.
- August 2022: we identified the use of cross-platform (Facebook, Telegram and YouTube) accounts to amplify the reach of a Pakistan-based terrorist network's propaganda in India. Amplification was encouraged by the appearance of authenticity and sophistication, i.e. professionally edited videos, human rights advocacy language, and the use of graphic images and news coverage of real-world related sectarian violence. These coordinated campaigns also coincided with such real-world incidents and included emotive appeals e.g. references to prophesied holy wars.

**Non-transparent promotions by influencers**

- June 2022: we uncovered a Ponzi Scheme of QAnon-affiliated influencers using conspiracies and poor investment advice to convince Telegram users to invest in fraudulent cryptocurrency tokens. Victims collectively lost millions; one took their own life. Genuine news articles and misleadingly presented official content of financial institutions were posted alongside curated lists of domains and tokens to appear authentic. These accounts then increased the tokens' price and traded them between each other at profit before sending them to a currency exchange via another account to be traded for Bitcoin or Ethereum and later appear on the curated lists. One perpetrator openly ran one of the channels and has been caught promoting tokens misleadingly associated with legitimate companies. In response to our request for comment, a former channel administrator said users are liable for their losses and should not interpret the information as financial advice.

**Creation of inauthentic pages or domains**

- One of the perpetrators of the same June 2022 Ponzi Scheme was found to have lied and misled her audience after receiving complaints about links to broken websites shared on her channel that claimed to be linked to legitimate financial institutions.

**Deceptive practices to deceive/manipulate platform algorithms**

- June 2022: we uncovered a Pakistan-based disinformation campaign on the death of a famous singer, Sidhu Moose Wala, stoking tensions in India. These accounts used hashtags to amplify their attribution of his death to India's foreign intelligence agency, Hindu extremism, or to pro-Khalistani sentiments. They also shared almost identical tweets on 9 different Twitter accounts, creating an echo chamber.

| | |
|---|---|
| | Internal processes to better identify TTPs<br>We are researching how to identify adversarial TTPs in our internal daily data collection. Our Data Science team has also carried out technical research on the identification of 'Coordinated Inauthentic Behaviour' (CIB) to understand its potential for harm and has published content to help users identify and report suspected CIB. Our research confirmed that many automatic detection systems have been developed to uncover deceptive behaviours, shifting the focus of detection from false information and single bad actors ("micro-level"), to coordinated strategies across multiple accounts ("macro-level"). Our investigations assess if a campaign is engaged in multiple strategies across multiple platforms and if the network is centrally coordinated with harmful and deceptive intent. A common tactic we have observed is a central instruction to post uniform or similar messages over a specific period. Suspicious patterns can be detected from astroturfing when all participants post the same message simultaneously. This systemic and proactive coordination distinguishes CIB from other TTPs e.g. spam. We are also currently developing an end-to-end automated CIB identification system as part of our disinformation detection and reporting service (Logically Intelligence - see Measure 29.2) to assist human experts. |

## IV. Integrity of Services

### Commitment 16

Relevant Signatories commit to operate channels of exchange between their relevant teams in order to proactively share information about cross-platform influence operations, foreign interference in information space and relevant incidents that emerge on their respective services, with the aim of preventing dissemination and resurgence on other services, in full compliance with privacy legislation and with due consideration for security and human rights risks.

| | |
|---|---|
| Measure 16.2 | |
| **QRE 16.2.1** | We regularly publish information on our website to reach fellow signatories and other stakeholders. Our scope of work for 2023 includes our intention to collaborate more with other organisations in a more streamlined way. The case study below qualitatively demonstrates cross-platform migration tactics we have observed being employed to engage diverse audiences i.e. the mutual reinforcement of cross-platform presence and the reposting of content from mainstream platforms to more fringe platforms where content moderation is applied to a lesser extent.<br>**Cross-platform amplification of Pakistan-based terrorist propaganda towards religious minorities in India**<br>- Tried to engage audiences across a network of 3 encrypted Telegram channels, 2 associated Facebook pages, and 3 YouTube channels<br>- We successfully identified the operation before it accrued a significant audience; cumulative cross-platform subscribers peaked at 200 - 400<br>- Identified by assessing the accounts' use of the same branding, content model and description |

| | |
|---|---|
| | **Process of cross-platform migration:**<br>- Initial Facebook pages were amplified on one of the Telegram channels, followed by the creation of YouTube channels to host and amplify terrorist recruitment videos alongside text citing associated hashtags and incidents of communal violence between Hindu extremists and Indian Muslims.<br>- The 3 Telegram channels disseminated evocative imagery and written calls for violence, while videos were accompanied by hashtags targeting Indian Muslim users. One of the Telegram channels provided links to the broader cross-platform network on Facebook, YouTube and Justpaste.it for further amplification e.g. to YouTube's more extensive user base in India. Content was also amplified in other Telegram channels affiliated with Islamabad-backed proxy terror groups in the region. When the main Telegram channel was removed, a replacement channel was found to have been created, albeit with a smaller audience.<br>- The network also used tlgur.com, a free content hosting service, and the video hosting website streamable.com to archive and amplify extremist content. |

## V. Empowering Users

### Commitment 17

In light of the European Commission's initiatives in the area of media literacy, including the new Digital Education Action Plan, Relevant Signatories commit to continue and strengthen their efforts in the area of media literacy and critical thinking, also with the aim to include vulnerable groups.

| | |
|---|---|
| Measure 17.2 | |
| **QRE 17.2.1** | We have not yet directly promoted media literacy campaigns to an EU user-base, although we do have operations in Ireland and Sweden, and we actively monitor for misinformation and disinformation across the EU. We did not engage in media literacy activities during the June - December 2022 implementation period, but we do intend to put learnings from past media literacy activities into practice in our future scope of work.<br>In our response to Commitment 14, we demonstrated our awareness-raising efforts on TTPs employed by malicious actors. By publishing such research on our website, we seek to empower any audience to better understand how disinformation campaigns can be disseminated. Where appropriate, we also work with national media in the US, UK and India to inform them of our findings, thereby contributing to public awareness-raising of the dangers of misinformation and disinformation online. |

|  |  |
|---|---|
|  | ‘Covishaala’ workshops<br>In the future, Logically intends to build on our Covishaala workshops held July - September 2021. We partnered with NewsMobile, an Indian news platform and fact-checker. In partnership with Facebook, the workshops sought to empower media literacy professionals with a sophisticated understanding of the contemporary media literacy landscape, and robust pedagogical strategies to translate this into clear, actionable advice for any Indian audience (including vulnerable populations). Covishaala focused on COVID-19 misinformation, as part of Facebook’s global campaign to help bring 50 million people a step closer to COVID-19 vaccines. This partnership built on NewsMobile’s and Logically’s statuses as signatories to the International Fact-Checking Network, and leveraged front-line expertise in fact-checking and surfacing disinformation affecting the public interest.<br>Designed according to modules and conducted by trainers who were local journalists and medical professionals, the four workshops targeted the impact of COVID-19 misinformation on vaccine hesitancy and mental health, particularly for women, children and persons with disabilities. The workshops also addressed:<br>- The state of COVID-19 misinformation in India;<br>- Communication, debunking and social media;<br>- The reliability of online evidence, and the psychology of bias patterns;<br>- Biases in reputable sources, the evolution of news sources, and OSINT guidance.<br>After each workshop, participants received certification from Facebook, as well as a media literacy toolkit offered in multiple languages to distribute to their peer groups. |
| **SLI 17.2.1 - actions enforcing policies above** | Methodology of data measurement:<br>Participants of the India-based Covishaala workshops were asked to provide feedback on the course content, delivery and resources, and to rate their confidence in delivering and designing media literacy courses and materials. Feedback on how informative participants found the workshops was gleaned from the 35 feedback forms collected. In September 2021, we collated this feedback into a report to feed recommended next steps. In 2023, Logically hopes to conduct similar workshops targeted at EU Member States, following the Covishaala template. |

| | Nr of media literacy/ awareness raising activities organised/ participated in | Reach of campaigns | Nr of participants | Nr of interactions with online assets | Nr of participants (etc) |
|---|---|---|---|---|---|
| **Data** | 1 activity outside of the implementation period - the Covishaala workshops | 13 participants said they would share knowledge gleaned from the sessions with more than 500 people each using social media and other means, while the remainder said they would share with at least 50 people | The four workshops had a total of 630 signups and a total of 160 attendees | All participants reported a feeling of empowerment as a result of knowledge gleaned from the workshops | The four workshops had a total of 630 signups and a total of 160 attendees |
| Measure 17.3 | | | | | |
| **QRE 17.3.1** | Logically primarily operates in the US, UK and India, therefore the most pertinent example provided does not derive from an EU Member State.<br>Training from OSINT Essentials<br>- 24 - 25 February 2022 (We acknowledge this falls outside of the June - December 2022 implementation period, however, we continuously apply learnings from this training in practice and will continue to do so. Therefore, we consider it relevant to outline this activity.)<br>- Provides resources and expertise for open-source investigations (OSINT) and media literacy<br>- Delivered by Eoghan Sweeney, an Irish Berlin-based OSINT specialist and trainer who runs OSINT Essentials, who has helped establish and develop online verification operations for global media<br>- Training included a focus on geolocation, fact-checking & debunks<br>- Instances of image misrepresentation for the fuelling of false narratives were exemplified, and the process of reverse image searches demonstrated<br>- Participants learned about methodologies to check the veracity of video footage and geolocation data, and to use timestamp analysis tools.<br>Training from Dart Centre for Journalism and Trauma, a project of Columbia University in the US<br>- 17 and 23 August 2022<br>- Project is dedicated to supporting informed, innovative and ethical news reporting on conflict and other traumatic events | | | | |

| | |
|---|---|
| | - Logically received specific training on online harassment and engagement with the traumatic content our fact-checkers and investigators routinely handle i.e. an investment into understanding coping mechanisms for fact-checking practitioners, to equip our teams with the skills and tools to deal with the mental toll of verification and trauma exposure.<br>Looking to the future, our Fact-Checking team will develop a new research structure where further training initiatives are expected. Among these is the intention to establish a media literacy function targeted towards the EU to build upon our previous work in this area. Logically has also appointed the former Executive Director of the International Fact-Checking Network, Mr Baybars Örsek as Vice President for the Fact-Checking business unit to lead media literacy efforts, which are anticipated for Q3/Q4 2023. |

## VI. Empowering the research community

### Commitment 29

Relevant Signatories commit to conduct research based on transparent methodology and ethical standards, as well as to share datasets, research findings and methodologies with relevant audiences.

| Measure 29.1 | |
|---|---|
| **QRE 29.1.1** | Ethical Standards<br>Logically is one of the organisations involved in the creation of OSINT Guidelines to help organisations engaged in public-facing OSINT work. The Guidelines aim to outline a common ethical framework comprising methodology, principles, and good practices to conduct OSINT investigations that organisations could adopt or adapt to best fit their requirements.<br>Data Governance<br>- We scan open-source data on social media, messaging services and other public sites. Some data (e.g. individual social media posts) is by definition personal data that has been knowingly shared by an individual and would be analysed if relevant to our specific scope of work for a client or public-interest investigation.<br>- Some of the data we access directly ourselves for research and training purposes; other data is provided by a variety of trusted third-party providers with strict contractual terms of use.<br>- We adopt a defence-in-depth strategy when it comes to network security i.e. we employ a layered approach from physical security, through to data security. Data to and from our public website (www.logically.ai) is encrypted in transit and at rest, by default.<br>- We use Role-Based Access Controls and adopt the principles of Least Privilege and Need To Know to manage access to data.<br>- Our full privacy policy is made public and is constantly reviewed, with updates noted in Section 13. Information about our transparency and ethics policies can be found elaborated in our response to Commitment 33 of this Code. |

Topics & Methodology

We publish information on our OSINT investigations to expose tactics used in disinformation campaigns. We have repurposed analyses of specific influence operations and disinformation campaigns from Commitment 14 below, to demonstrate the methodologies employed therein.

June 2022 investigation of disinformation campaign on the death of Indian singer Sidhu Moose Wala

- Pakistan-based accounts found coordinating the spread of disinformation about his death to stoke tensions with India.
- We accessed open-source data to observe 389k Twitter mentions and 9629 Facebook posts with the hashtags #SidhuMooseWalaDeath, #RAWKilledSidhuMooseWala and #SidhuMooseWala.
- We conducted a network analysis using the open-source tool Gephi to produce a live snapshot of a conversation within a specific time frame; resulting in a dataset of more than 1900 accounts.
- This revealed coordinated Pakistan-based accounts using hashtags and sharing almost identical posts across different Twitter accounts to amplify claims that the death was attributable to India's foreign intelligence agency (RAW), Hindu extremism, or pro-Khalistani sentiment.

June 2022 investigation of a disinformation campaign targeting Indian Muslims with conspiracies on Telegram

- We used timestamp analysis data, Gephi network analysis and screenshots to confirm the coordinated posting of content from one channel across a disinformation-spreading cluster, with each channel's description linking to others within the cluster.
- We used the tool Telepathy to create an edge list of accounts, to then import into a Gephi dataset.
- We used archived data to compare messages forwarded by one channel and received by another. A 'Primary Hate Group' was found to have forwarded the bulk of content spread across the cluster (2,755 messages).
- We compared Telegram to WhatsApp and determined that Telegram is more attractive for disinformation campaigns, as channels can host up to 200,000 members and unlimited participants. It also has file storage that easily facilitates the retention and sharing of multimedia content. Telegram can also facilitate both public and private encrypted chats, and has significant reach in India, which accounted for 22% of all global downloads at the time of the investigation.
- From this investigation, we learned about the somewhat novel use of different channels for different narratives; thereby permitting the perpetrators to track which narratives gained more traction.

June 2022 investigation into Ponzi Scheme on Telegram (viewed by 16,131 users)

- QAnon-affiliated influencers combined conspiracy theories with poor investment advice to convince audiences via Telegram hub channels to invest in fraudulent cryptocurrency tokens. Victims collectively lost millions of dollars, with one subsequently taking their own life.
- We interviewed former channel administrators, analysed timestamp data, and archives of domain creations and recorded activity on the channels to determine that the creation and subsequent forwarding of minted tokens between accounts had all been created by the same original account.
- We investigated the websites of the legitimate companies purportedly attached to the tokens to confirm if any cryptocurrency assets or partnerships were listed; and requested comment.

| | |
|---|---|
| | August 2022 revelation of a cross-platform network of accounts amplifying Pakistan-based terrorist propaganda towards religious minorities in India<br>- We assessed the amplification patterns of Facebook videos posted since January 2022 to confirm a coordinated campaign to spread content in Facebook groups dedicated to socialism, Islam and minority rights. We analysed the audiences of these groups using the social media analysis tool, CrowdTangle, to ascertain the presence of domestic users who were critical of India's ruling party.<br>- While the content was subjected to platform moderation, the time-stamps and use of similar captions and descriptions of the videos suggested the presence of a copypasta campaign by a single entity.<br>- We contextualised these campaigns to identify shared timelines with real-world incidents of related violence, demonstrating the leveraging of the anonymity and audience of major social media platforms by malicious actors to exploit tensions to amplify the reach of disinformation campaigns.<br>- We used the list of individuals cited as terrorists by the Indian Ministry for Home Affairs and intelligence from Indian Governmental Agencies to track the identity of the perpetrator.<br>- This investigation exemplified the attempts by disinformation actors to capitalise on clashes between communal groups and off-line incidents of unrest to fuel these narratives.<br><br>September 2022 investigation into an India-based disinformation campaign on Twitter stoking tensions between UK Hindu and Muslim communities<br>- We determined that the tensions were driven by inflammatory claims on social media of hostage situations and flag-burning, some of which were amplified by known journalists and other influencers.<br>- We reached out to local police to confirm that no hostage reports had been filed; and to determine that people gathered inside a Hindu temple were being misrepresented as hostages to stoke tensions. We additionally sought police confirmation that reports of attacks on restaurants and cars were false, and that arrests were made from within both communities, to dispel claims of one-sided violence.<br>- We used a broad Boolean query for content from 17 - 21 September that used the hashtags #protectleicesterhindus, #stopleicesterislamicterrorism, #hindusunderattackinleicester, #hindusunderattackinuk, #hinduhateinuk or #muslim_kmbf.<br>- We identified that 81% of the 22,000 tweets with geolocation information analysed from 17 - 21 September were geotagged to India, with just 6% geotagged to the UK.<br>- We assessed the tweets' time-stamps to compare similarities in content, source and subsequent engagement.<br>- This investigation illustrated how hashtag dynamics on Twitter can influence domestic situations. |
| **QRE 29.1.2** | We look forward to updating the Transparency Centre with information on our research once the Centre becomes operational, including through the annual reporting under this Code. |
| **QRE 29.1.3** | We have circulated the aforementioned information on our methodology for investigations in more detail to the Taskforce via the Commission, and intend to keep the Taskforce informed of research activities we conduct that are of relevance, and the associated methodologies. Logically already publishes information on its investigations carried out on our website. |

| Measure 29.2 | |
|---|---|
| **QRE 29.2.1** | Logically Intelligence (LI) is our flagship threat detection and platform analysis tool, combining advanced AI and human expertise to facilitate users' mapping and analysis of multilingual, multimodal and cross-platform data at speed and scale. LI ingests millions of data sources online, including public channels on closed networks such as Telegram. It then applies advanced Natural Language Processing and knowledge-engineering techniques to identify and disambiguate entities, topics and concepts. Users, such as government agencies and platforms, benefit from threat monitoring and mapping, as well as 24/7 early-warning services.<br>An example of resilience-fostering measures on LI is its use of labels and warnings. LI's ingestion of data includes annotation i.e. multiple AI models are trained to classify various pieces of content ingested according to the correct label, which is then displayed to the user on the platform. The pipeline works as follows: a match is determined based on matching keywords or topics; followed by the models' scanning and classification of the content with potentially multiple labels. An example of warnings would be those that fall under the dedicated LI 'Threats' page, and then specific labels would identify the exact type of threat from there. For example, a user would see all threats relating to their areas of concern on the 'Threats' page, but individual posts and articles would be classified e.g. Threat Intent/Toxicity Detection. So the Threat Intent Model would label the content according to the specific threat presented e.g. threat to life, attack on the author, content from a source of low credibility etc. For information on our Data Governance policy, please see our response to Measure 29.1.<br>It is difficult to obtain information on the outcomes, and therefore efficacy, of labels and warnings as resilience-fostering measures on LI, given that Logically has no oversight of what actions users take following their perusal of the LI platform and the information gleaned therefrom. However, we receive continuous feedback from our users on an ongoing basis from which we have ascertained the product's usefulness in assisting them in the fight against the harms associated with disinformation. Internally, our OSINT team makes use of LI in concert with other tools to conduct public interest investigations. |
| **SLI 29.2.1** | Methodology of data measurement:<br>In lieu of data on the outcomes of labels and warnings on LI, we would like to exemplify our fact-checking operations as an example of ex-post notifications as resilience-fostering measures for which we can quantify reach. While we are contractually prohibited from sharing the exact number of users reached by our in-platform fact-checks conducted as part of our client work, we have outlined below the website views of our top five fact-checks i.e. how many people clicked on them to read. We believe that this significant traffic demonstrates the societal need for such fact-checks. |
| | Reach of stakeholders or citizens informed about the project:<br>● Iran issues mass execution of over 15,000 protesters detained amid anti-Hijab protests - 98,673 views<br>● New Facebook/Meta rules will make all private posts on the platform and deleted messages public - 92,976 views<br>● The Metropolitan Police has opened an investigation into COVID-19 vaccines - 53,036 views<br>● Four AI robots have killed 29 scientists in Japan - 48,568 views<br>● Dr. Robert Malone invented mRNA vaccines - 46,319 views |

## VII. Empowering the fact-checking community

### Commitment 30

Relevant Signatories commit to establish a framework for transparent, structured, open, financially sustainable, and non-discriminatory cooperation between them and the EU fact-checking community regarding resources and support made available to fact-checkers.

| | |
|---|---|
| Measure 30.2 | |
| **QRE 30.2.3** | Upon the upcoming launch of the procedure to adhere to the European Fact-Checking Standards Network's (EFCSN), an EU-backed effort to create a Code of Professional Integrity for fact-checkers across the continent, Logically aims to demonstrate our adherence to this Commitment. |
| Measure 30.3 | |
| **QRE 30.3.1** | Logically's participation in the development of the EFCSN:<br>- Part of the Wide Group since the project's inception in February 2022;<br>- In March 2022, we were elected to a 15-member Working Committee guiding the discussions and drafting the articles that became part of the Code;<br>- Participated in the Working Committee meeting in Oslo from 20 - 21 June 2022 to finalise the first draft of the Code;<br>- Participated in the Wide Group meeting in Madrid from 28 - 29 September 2022 to finalise the statute on its implementation and governance. (On the sidelines of this, Logically attended Meta's latest Fact-Checking Partner Summit to learn how fact-checkers overcome challenges e.g. increasing digital literacy, finding sources, providing extra context to claims, and using different platforms to diversify the audiences for their work.)<br>- Logically will apply to the EFCSN in its second round of applications in May 2023.<br><br>Logically's cooperation with other fact-checkers:<br>- In August 2022, Georgia's Reforms Associates (GRASS) fact-checkers contacted us about the spread of a fake educational pamphlet, allegedly distributed among UK schools, encouraging children to befriend unknown adults, disregarding safety concerns.<br>- Images of the pamphlet were used to spread the false narrative that paedophilia is accepted in the UK; a claim repeated in several languages globally, before being picked up in the UK itself. Polish fact-checkers, fakenews.pl, traced the original images of the pamphlet to Russian propagandists and found that no physical copy existed. The claim had been amplified by the anti-LGBTQ account LibsOfTikTok, which has been known to conflate sexual abuse with the LGBTQ community.<br>- As the first UK fact-checkers to debunk the claim, Logically demonstrated how the "groomer" conspiracy was being peddled by pro-Kremlin sites, and how such claims spread region-to-region.<br><br>Logically collaborated with cross-border fact-checkers via the UkraineFacts initiative, a global database of daily fact-checks for disinformation deriving from Russia's invasion of Ukraine. Fact-checks are published in English, with fact-checkers from over 80% of EU Member States contributing, as well as those across the globe. |

| | |
|---|---|
| | In December 2022, Logically announced the hiring of its new Vice President of Fact-Checking, Mr Baybars Örsek, whose focus will include promoting knowledge-sharing and collaboration across the fact-checking community. Finally, Logically has plans to engage in other fact-checking collaborations in the future, specifically those that specialise in climate- and health-related misinformation and disinformation in 2023. |

## VII. Empowering the fact-checking community

### Commitment 31

Relevant Signatories commit to integrate, showcase, or otherwise consistently use fact-checkers' work in their platforms' services, processes, and contents; with full coverage of all Member States and languages.

| | |
|---|---|
| Measure 31.3 | |
| **QRE 31.3.1** | We look forward to contributing to the repository as and when we are called upon to do so by the Taskforce. |
| Measure 31.4 | |
| **QRE 31.4.1** | We look forward to contributing to the repository as and when we are called upon to do so by the Taskforce. |

## VII. Empowering the fact-checking community

### Commitment 33

Relevant Signatories (i.e. fact-checking organisations) commit to operate on the basis of strict ethical and transparency rules, and to protect their independence.

| | |
|---|---|
| Measure 33.1 | |
| **QRE 33.1.1** | IFCN & EFCSN<br>- Verified Signatory of IFCN since 2020; successfully applied for renewal in 2021 and 2022<br>- Involved in the EFCSN's development (see QRE 30.3.1)<br><br>Ethics<br>- Internal ethics process includes an Ethics Charter, compliance with which is overseen by our Ethics Subcommittee;<br>- Client Ethics Policy (e.g. requiring staff members to disclose potential conflicts of interest);<br>- Due diligence mechanism: Senior employees review prospective clients and the intended scope of work to identify risks of prohibited users or use cases (see below). Largely derives from the International Chamber of Commerce's guidance on due diligence for SMEs;<br>- Ethics process derives from commitments to Logically's shareholders and Board, and the IFCN; |

- All our commercial contracts include a limited and targeted scope for the use of our products and services; any violation thereof will result in termination of services.

Prohibited clients include:

- Political parties/movements;
- Terrorist organisations;
- Religious organisations;
- Unaccredited public bodies;
- Government clients in countries with unacceptably low levels of democracy (per the Global State of Democracies Indices, with the exception of Singapore).

Prohibited use cases include:

- “Offensive” or “attack” intentions i.e., use of Logically’s products, data or analyses to target rivals;
- Hacking, spying or the intention to deliver automated or high-velocity responses;
- Political advertising;
- Surveillance of individuals/groups that harasses, infringes, or threatens to infringe upon their privacy, security, or human rights;
- Use of personal data collected without consent, or any unauthorised data;
- The use of only part of our product, data or insights to misrepresent the client’s position;
- Any violation of applicable law.

Transparency

- Details on our funding are published on our website;
- We emphasise the importance of record-keeping in all of our processes, reviews and feedback to ensure transparency and accountability, using the collaborative workspace, Confluence.

Independence & Non-partisanship

- Committed Signatory to the IFCN Code of Principles i.e. non-partisanship and fairness in our fact-checking work, transparency of sources, and transparency of funding and organisation;
- Staff are obliged not to conduct any activity which might unduly damage Logically's reputation, including for non-partisanship e.g. prohibited from publicly expressing on social media any interest in, affiliation to or association with any political party, political candidate, or politically aligned movement;
- Logically has no commercial, institutional or financial relationships with any politician or political party.

Our Fact-Checking team uses data and analytics to identify and prioritise claims, based on their reach, traction, influence or relevance to current affairs. Claims will only be fact-checked if they (as outlined on our website):

- Are made in a public forum;
- Can be broadly assessed as reasonable/truthful or not;
- Can be checked using publicly available evidence and standard reasoning;
- Can be interpreted as an assertion of factual information;
- Are in the public interest, and not from any one side of a debate - in respect of our apolitical stance;
- Meet the appropriate standards of interest and fairness; and
- If it is not irresponsible to do so i.e., due to a lack of expertise or sufficient context, dissemination by trolls, or the claim is a harmful conspiracy without journalistic impetus for rebuttal.

| | |
|---|---|
| | Editorial control<br>- Exercised by our Global Head of Fact-Checking who is responsible for editorial policy and standards in the Fact-Checking team (i.e. any potentially contentious editorial decisions, complaints or necessary corrections);<br>- Our Regulatory Policy Manager assists in ensuring that the Fact-Checking team's workflow and standards remain in sync with the best practices and policies of the global fact-checking community;<br>- Each fact-check includes a call to action, encouraging users to contact our editorial team with comments, questions, complaints, and more claims to fact-check;<br>- Our policy on editorial independence applies to all fact-checking staff. |

<table>
<tr><th colspan="2">VIII. Transparency Centre</th></tr>
<tr><td colspan="2">Commitment 34<br>To ensure transparency and accountability around the implementation of this Code, Relevant Signatories commit to set up and maintain a publicly available common Transparency Centre website.</td></tr>
<tr><td>Measure 34.1</td><td></td></tr>
<tr><td>Measure 34.2</td><td></td></tr>
<tr><td>Measure 34.3</td><td></td></tr>
<tr><td>Measure 34.4</td><td></td></tr>
<tr><td>Measure 34.5</td><td></td></tr>
</table>

<table>
<tr><th colspan="2">VIII. Transparency Centre</th></tr>
<tr><td colspan="2">Commitment 35<br>Signatories commit to ensure that the Transparency Centre contains all the relevant information related to the implementation of the Code’s Commitments and Measures and that this information is presented in an easy-to-understand manner, per service, and is easily searchable.</td></tr>
<tr><td>Measure 35.1</td><td></td></tr>
<tr><td>Measure 35.2</td><td></td></tr>
<tr><td>Measure 35.3</td><td></td></tr>
<tr><td>Measure 35.4</td><td></td></tr>
<tr><td>Measure 35.5</td><td></td></tr>
<tr><td>Measure 35.6</td><td></td></tr>
</table>

## VIII. Transparency Centre

### Commitment 36

Signatories commit to updating the relevant information contained in the Transparency Centre in a timely and complete manner.

| | |
|---|---|
| Measure 36.1 | |
| Measure 36.2 | |
| Measure 36.3 | |
| **QRE 36.1.1 (for the Commitments 34-36)** | We look forward to contributing to the Transparency Centre as and when we are called upon to do so by the Taskforce. In follow-up baseline reports, we intend to outline any changes we have made via the Transparency Centre e.g. by uploading our reports. |
| **QRE 36.1.2 (for the Commitments 34-36)** | We look forward to contributing to the Transparency Centre as and when we are called upon to do so by the Taskforce. In follow-up baseline reports, we intend to outline any changes we have made via the Transparency Centre e.g. by uploading our reports. |
| **SLI 36.1.1 - (for Measures 34 and 36) meaningful quantitative information on the usage of the Transparency Centre, such as the average monthly visits of the webpage** | Methodology of data measurement: |
| | Our company would like to provide following data: |
| **Data** | We look forward to contributing to the Transparency Centre as and when we are called upon to do so by the Taskforce. |

## IX. Permanent Task-Force

### Commitment 37

Signatories commit to participate in the permanent Task-force. The Task-force includes the Signatories of the Code and representatives from EDMO and ERGA. It is chaired by the European Commission, and includes representatives of the European External Action Service (EEAS). The Task-force can also invite relevant experts as observers to support its work. Decisions of the Task-force are made by consensus.

| | |
|---|---|
| Measure 37.1 | |
| Measure 37.2 | |
| Measure 37.3 | |

| | |
|---|---|
| Measure 37.4 | |
| Measure 37.5 | |
| Measure 37.6 | |
| **QRE 37.6.1** | As an SME, our engagement was limited to the extent that resources were available.<br>- 13 June: Attended a gathering of fact-checkers to discuss any issues with the Commitments in the Code;<br>- 12 September: Met with European Commission officials from Unit I.4. "Media Convergence and Social Media" at the Directorate-General for Communications Networks, Content and Technology to enhance our understanding of obligations under the Code. We maintained email correspondence with the Commission for steering purposes;<br>- 16 September: Met with the European Regulators Group for Audiovisual Media Services (ERGA), which receives the research outlined in Commitment 29. Logically informed ERGA of past media literacy activities, and ERGA informed of its work in coordinating the Monitoring and Reporting Subgroup;<br>- 20 September: Attended the 3rd Plenary Session of the Taskforce, where the Commission outlined priorities for the reporting period, and Subgroup Coordinators presented updates and confirmed the adoption of their Terms of Reference;<br>- 29 September: Met with Avaaz, who invited us to attend the recurring monthly meeting of smaller Signatories to boost our awareness of ongoing developments;<br>- 17 October: Participated in the 2nd monthly coordination meeting of smaller Signatories, who informed each other of recent developments to coordinate responses to shared challenges;<br>- 7 November: Participated in a call with members of the Integrity of Services Subgroup alongside other smaller Signatories and the Commission, in order to follow-up on the list of Taskforce-amended malicious Tactics, Techniques and Procedures (TTPs) as drafted in this Subgroup and as pertain to Commitment 14. Signatories, including Logically, posed questions to Google (who presented the amended list of TTPs on behalf of the Subgroup) and Commission representatives to ensure full understanding of the list for accurate reporting;<br>- 28 November: Participated in the 3rd monthly coordination meeting of smaller Signatories to hear updates on Subgroups' progress e.g. as regards the Transparency Centre, the fact-checking repository and the templates for the Baseline Reports. Signatories also discussed the process for new Signatories;<br>- 6 December: Attended the 4th Plenary Session of the Taskforce in Brussels, where the Commission and Signatories took stock of existing efforts made to implement the Code and preparations ahead of the first reporting round in January 2023. Subgroup Coordinators presented the state of play of their deliverables. Signatories also participated in a Spotlight Session to exchange views on lessons to be learned from disinformation disseminated on the war in Ukraine. Finally, the Commission summarised the upcoming deliverables and their respective timelines for Signatories to prioritise accordingly;<br>- 19 December: Participated in the 4th monthly coordination meeting of smaller Signatories, where the development of the Transparency Centre and the upcoming submission of Baseline Reports were discussed. |

## X. Monitoring of Code

### Commitment 38

The Signatories commit to dedicate adequate financial and human resources and put in place appropriate internal processes to ensure the implementation of their commitments under the Code.

| | |
|---|---|
| Measure 38.1 | |
| **QRE 38.1.1** | Logically primarily operates in the US, UK and India, therefore our coverage can include, but does not specifically target, EU Member States.<br>The team members authoring this report and overseeing Logically's overall compliance with the Code are the Global Public Policy Officer and the Regulatory Policy Manager; both of whom report to the Head of Government Affairs.<br>Our internal processes to ensure compliance with the Code included:<br>- Verification of documentation on the company's communal Google Drive and Confluence workspace (particularly the folders relating to our applications and status as a verified signatory to the International Fact-Checking Network) to ascertain existing compliance;<br>- Organising meetings with the European Commission and the European Regulators Group for Audiovisual Media Services to confirm our understanding of how to ensure our compliance, construct our report, and share the research findings sought in Commitment 29;<br>- Meeting with our Global Head of Fact-Checking and other Fact-Checking team members to ascertain the state of play and future timeline for media literacy activities in order to fulfil Commitment 17 (particularly with a view to expanding our repertoire of such activities for the 2024 annual report), as well as to glean information on our cross-border cooperation with the broader fact-checking community in order to fulfil Commitment 30;<br>- Meetings with our OSINT investigations and Fact-Checking teams to obtain the research methodologies and outcomes required to fulfil Commitments 14, 16 and 29;<br>- Meetings and documentation exchanges with our Data Science and Fact-Checking teams to obtain evidence on our use of labels, warnings and fact-checks, and the efficacy and reach thereof, to fulfil Commitment 29;<br>- Reviewing the content of our ethics and transparency policies, and our IFCN verification to ensure compatibility with the requirements of Commitment 33. Our compliance with the IFCN Code of Principles is facilitated by the promotion of our ethics and transparency policies at the heart of all our teams' work, particularly to new starters and in the due diligence process of engaging with new clients i.e. facilitating checks and balances to limit the possibility for conflict with our policies. Such promotion is done by organising dedicated ethics and transparency training and presentations, and ensuring that the relevant documentation is easily accessible on our Confluence workspace. |

**X. Monitoring of Code**

## Commitment 39

Signatories commit to provide to the European Commission, within 1 month after the end of the implementation period (6 months after this Code’s signature) the baseline reports as set out in the Preamble.

**X. Monitoring of Code**

## Commitment 40

Signatories commit to provide regular reporting on Service Level Indicators (SLIs) and Qualitative Reporting Elements (QREs). The reports and data provided should allow for a thorough assessment of the extent of the implementation of the Code’s Commitments and Measures by each Signatory, service and at Member State level.

| | |
|---|---|
| Measure 40.1 | |
| Measure 40.2 | |
| Measure 40.3 | |
| Measure 40.4 | |
| Measure 40.5 | |
| Measure 40.6 | |

**X. Monitoring of Code**

## Commitment 43

Relevant Signatories commit to provide, in special situations like elections or crisis, upon request of the European Commission, proportionate and appropriate information and data, including ad-hoc specific reports and specific chapters within the regular monitoring, in accordance with the rapid response system established by the Taskforce.