Logically.

Service Definitions

Description of Solutions

- Logically has built an ecosystem of products and services to meet modern challenges in combating misinformation, disinformation, propaganda campaigns and identifying problematic content in the digital domain space, our mature product offerings include:

- Automated Credibility assessment of webpages by producing and interpreting signals based on content, author, metadata, social network, and threat intelligence.

- Expert-based Semi-automated Veracity Assessment of claims and images from social media networks, news media content, messaging networks. Components include - content sourcing integrations, automated fact-checking system, image forensic analysis system, a stage-wise AI-assisted fact-checking and verification tool, and a CMS system for content and graphic production and distribution.

- Logically has a suite of consumer applications, including a mobile app and a browser extension. These tools give users an unparalleled ability to fact-check fake news, fake imagery, and get the latest perspectives from across the political spectrum with the Logically app. At the same time, our extension allows users to browse the web with confidence. See the credibility of the websites they visit, articles they read, fact check the information they find, and moderate the commentary in an often polarized and toxic social media landscape. We use AI to help normalize polarizing headlines and give our users a 'just the facts' reading of news and current affairs. Logically strive to help provide the fundamental skills of media and digital literacy, critical thinking, and helping to build psychological resilience.

  In certain applications our consumer ecosystem has become an integral part of a disinformation whistleblowing and intervention strategy that can have a meaningful impact on users, especially on closed networks such as WhatsApp whilst protecting user privacy.

We also provide managed services through prototype systems for:

- Classification of Domains as reliable or potentially harmful, including identifying domains with a high propensity to disinform. Our systems use historic content reliability, author expertise, domain ownership, domain metadata, and link graphs to generate our classifications.

- Identification of influence operations on Social networks, including detecting the pollination of claims, rumors, and narratives between platforms and predicting the likelihood of accounts or a group of accounts using automated, coordinated, or sock puppet attacks vectors.

We are currently working on adding the following capabilities to our ecosystem:

- Multimedia Deception detection, including memetic and GAN (Generative Adversarial Network) generated content.

- The ability for automated attribution of detected influence operations and disinformation campaigns to threat actors, including state and non-state.

Sample Use Cases

- Monitoring and Triaging Content and User Accounts
- Fact-Checking and verification of specific content and themes
- Disinformation threat intelligence feeds - content, actors and activity
- Threat Hunting Services on Domains and Social Networks
- Election Information Integrity Operations to identify disinformation and implement countermeasures through open networks, closed networks and public communications.
- Crisis Information Integrity Operations to identify disinformation and implement countermeasures through open networks, closed networks and public communications.
- Narrative-wise Content, Actor and Social Network Analysis
- Actor-wise Content, Actor and Social Network Analysis
- Location-wise Content, Actor and Social Network Analysis

Misinformation

We rely on information to make the meaningful decisions that affect our lives, but the nature of the internet means that false news reaches more people faster than ever before. Our services and tools are built to better today's fractured information ecosystem.

Fact Check - Logically employs the world's largest dedicated fact-checking team - working together with AI to provide rigorous, evidence-based fact checks.

Image Verification - Our Image verification API's are built to highlight manipulated imagery and extract text from images in order to stop the spread of harmful misinformation.

Credibility - Logically's ensemble machine learning models are constantly and iteratively evaluated to improve their efficacy. We benchmark the performance of our AI against our diverse, expert analysts, to eliminate the typical challenges associated with crowdsourcing data.

Article Credibility API - Our AI analyses and understands the content of an article, its metadata such as its authors and publishers, and its patterns of propagation on social media to determine its credibility.

Source Credibility API - We assess a source based on the content it produces, its metadata, and its direct and indirect associations with known agents of disinformation.

Disinformation

The anonymous nature of internet-based platforms allows malicious actors to spread computational propaganda. Their effects have shaken democracies, provoked public health epidemics and induced lethal violence. Our services are designed to detect, monitor and deploy countermeasures to mitigate risks posed by disinformation.

Open Source Intelligence - Our investigators use a suite of advanced Open Source Intelligence tools to map malicious information flows through social media and across the Internet - tracing and attributing viral and memetic disinformation campaigns to malicious actors or groups.

OSINT - Our skilled investigators use a suite of advanced Open Source Intelligence tools to monitor and map malicious information flows through and between social media platforms and across the wider Internet.

Attribution - We trace and attribute viral and memetic disinformation campaigns to malicious actors - both nation-state and for-profit.

Social Network Analysis - We use a variety of Social Media Intelligence tools to detect and monitor automated (bot) accounts, cyborg accounts, and other coordinated user disinformation strategies.

Information Operations - We monitor known threat actors 24x7 to identify information operations by nation-state and politically motivated actors. Our analysts and investigators also support our Information Integrity War Rooms we set up alongside our public sector partners during elections and crisis events.

Synthetic Content

It's never been easier to dupe the public with manipulated content. From Instagram filters that dramatically change the look of a landscape, text written by AI and Deepfakes that allow you to be anyone; synthetic content's pervasive spread affects us all. We build technology that helps you demystify synthetic content.

Deepfake Detection - Logically build machine learning models capable of identifying the increasing use of Deepfake technologies.

Synthetic Text Detection - Our AI can determine whether a piece of text has been written by a human or using Natural Language Generation AI.

Natural Language Generation for Good - We use Natural Language Generation to contextualise verified information and remove the barriers to navigating today's convoluted information ecosystem.

Information Overload

Processing too much information can be counterproductive and it's a common occurrence while on the internet. Our tools are built to help businesses and individuals separate the wheat from the chaff.

AI-generated summaries of news Stories - We provide users with a concise summary based on the facts of each story, without spin, slant, or bias, by reading and analysing all articles related to that story.

Comprehensive Narrative Timelines - We contextualise each story and recent development with historic context so that our users can understand how a situation has evolved from its very beginning.

Intelligence Reporting - Our team of dedicated fact-checkers and OSINT specialists bring clarity to today's labyrinthine digital ecosystems.

Filter Bubbles & Echo Chambers

Exposure to diverse perspectives is vital for fostering critical thinking and developing informed decisions, but today algorithm-based platforms choose the content that you see based on what you like. Persistent exposure to belief-confirming content can result in a narrow-minded view of the world or a problem. That's why we build tools to improve civic discourse and facilitate critical thinking.

Contrasting Views - Our AI picks out the most divergent viewpoints from publishers across the political spectrum.

Political Bias - Our machine learning algorithms are capable of determining political bias within text.

Credibility Rating - Our advanced AI uses a combination of domain, metadata and content analysis to provide an accurate credibility rating.

Analyse trends, mitigate risks and seize opportunities.

Our AI is built on a set of modular processes which can be customised to analyse boundless amounts of data.

Underlying Data - Platform Agnostic with Limitless Possibilities. Whether broad and extensive or meticulously targeted, we continually collect data from every corner of the internet. We actively monitor over a million domains and major social media platforms in real-time, and can add news sources including niche platforms within hours.

Knowledge Extraction

Automatically Extract and Link Entities, Topics and Concepts.

We use advanced Natural Language Processing (NLP) and Knowledge Engineering techniques to identify, resolve and disambiguate entities, topics and concepts to truly begin to understand content.

Contextualising Information - The sheer volume of information online can make it difficult for any individual or organisation to sort through the noise and identify the most salient signals, trends and insight . Our advanced contextualisation algorithms group structured and

unstructured information to show you undiscovered patterns so you can make informed decisions based on sound reasoning and evidence.

Narrative Context - Appreciate nuance and empathise with alternate views. We compare and contrast aggregated information and identify agreement and disagreement between content, their authors and their audiences.

Temporal Context - Navigate dynamic subjects and understand their history to see the whole picture. We update our analysis in near real-time and link related events together to provide a chronology of developments that have resulted in emergent situations and threats.

The Précis - Multi Document Summarisation - Insight made easy.We identify the most salient points from across multiple documents to produce controllable summaries that get you up to speed in seconds. The Précis can be guided by specific goals such as informational value, objectivity, diversity and actionability.

Structure & Analyse

Types of Data.

We support the analysis of long-form content such as news articles as well as short-form content such as social posts. These are processed through fine-tuned models to identify:

- Claims
- Opinions
- Quotes
- Events
- Lenses of Analysis.

Our primary lenses of analysis for phrases, sentences and longer form content include:

- Sentiment
- Bias
- Toxicity
- Patient Zero

Example:

“More than ****11,400 investors are likely to lose more than £230m in savings due to the collapse of London Capital & Finance after it was announced that only 159 affected mini-bond customers would receive compensation.”

Publisher: The Guardian

Domain:
https://www.theguardian.com/uk-news/2020/jan/09/investors-face-230m-loss-in-london-capital-finance-collapse

Date Published: Thu 9 Jan 2020 16.19 GMT

Last Modified: Thu 9 Jan 2020 16.44 GMT

Author: Kalyeena Makortoff

Title: Investors face £230m loss in London Capital & Finance collapse

Content:

More than (Modifier) 11,400 (number) investors (units) are likely to lose more than £230m (number | currency | gbp) in savings due to the collapse of London Capital & Finance (entity) after it was announced that only 159 (number) affected mini-bond customers (units) would receive compensation.

“I appreciate that the initial decisions and outlook we are announcing today are likely to be disappointing to many LC&F customers. (NEGATIVE SENTIMENT) We are, however, working as quickly as we can to establish a suitable process for determining customers’ claims, and expect to be in a position to start this process in the next few weeks.”

Disinformation Investigations

Logically’s cutting edge technology and expert investigations team work together to perform in-depth social network analysis of users, their communities, the content they produce and their engagement patterns to identify signals for automated and coordinated campaigns.

Our state-of-the-art forensics and attribution techniques are able to identify the involvement of nation-state actors such as Russia, China and Iran, as well as know for-profit actors by correlating indicators of compromise (IOCs) and attack signatures. This allows us to identify signals for sock-puppeting, and brigading attack vectors and also provide us with an early detection mechanism for narratives proliferating from fringe networks and sources with a high propensity to disinform.

Automated Credibility Assessment

Our three-pronged approach to verification:

Network - Using propagation analysis to model the virality of content, the authenticity of engagement and the incentives of actors who promote it..

Metadata - We examine associates data; In the case of article assessment, we model authors, ad networks, domain ownership and track records to evaluate content.

Content - We identify semantic and psycho-linguistic indicators of misinformation within text to accurately assess it's credibility and produce interpretable inferences.

Source Credibility

We assess a source based on the content it produces, its metadata, and its direct and indirect associations with known agents of disinformation. Our automated source assessment systems will soon be paired with dedicated expert analysts to validate and verify our automates assessments. Our ensemble models are trained using an extensive database of over 30k known sources of disinformation.

Article Credibility

In-line with our three-pronged approach our article credibility is an extension of our source credibility models which then pick out what particular kinds of reliable or unreliable information, and make a prediction on a web page's credibility; labelled as Highly Credible, Medium Credibility and Low Credibility.

Brand Safety

Although geo-politically motivated misinformation and disinformation have been in prominent focus over the last few years, for-profit misinformation and disinformation has been equally prominent and impactful in poisoning our information feeds. Advertisers risk associating their brand with problematic content unless they deploy mechanism to mitigate the risks of advertising on websites and webpages with a propensity to misinform.

Veracity

Automated Fact-checking

Claim Extraction & Matching

Logically employs advanced AI to identify claims within a text and rank them based on plausibility and their fact check worthiness. Once a claim has been extracted or submitted we match them against trusted sources and fact-checks using state-of-the-art, natural language understanding technologies that highlight the inherent syntactic and semantic details.

EI-Lead Fact-Checking

Our powerful workflow maximise fact-checking efficiency by cross-referencing data related to the claim before it's manually verified — bringing the most questionable and pressing claims to fact-checkers and allowing them to thrive by co-working with bots dedicated to tasks such as retrieving evidence and creating visual assets.

Logically are also developing Multimedia Forensics tools to identify manipulated media including deep fakes.

Questionnaire

How does your system help to solve the problems of propaganda, disinformation, and/or radicalization to violence?

Our systems help to improve situational awareness and orient our customers. We help to find the root causes of the problem and contextualize the narratives around disinformation and propaganda campaigns. Logically's systems and services identify problematic activity and give decision and policymakers expedited decision trees to ensure appropriate countermeasures can be taken in a time-sensitive environment.

How was your system conceived and what was your original goal?

We conceived our ecosystem to improve social discourse by providing our users access to unbiased news and helping to tackle the spread of misinformation.

We quickly discovered that our expertise in machine learning and artificial intelligence analysis meant we could understand how both social media and traditional media sources can act as conduits for broader state and non-state sponsored campaigns. Allowing us to tailor our tools to maximize the impact Logically can have on giving policy, and decision-makers access to information far quicker and more efficiently than is possible with analysts.

Tell us what problems will occur during implementation & how to resolve

While we do not anticipate any technical problems arising in the implementation phase, We take special care to ensure we meet any operational security and data protection requirements for bespoke or sensitive data sources. Logically want to ensure that we provide the level of confidence in our systems that meets our customer's expectations. For sensitive use cases, Logically offers customers with cloud-hosted and on-premises deployment solutions.

As the volume of data processing for large initiatives can be more than 100 million posts and articles, self-hosted customers will need to scale their infrastructure to deploy Logically. They must ensure their Logically account manager is notified of any expected large workloads and surge usage so that our capacity planning team can work alongside our Google Infrastructure partners. Furthermore, Logically and its customers may have differing definitions of various threat types and actors based on their policies. We offer the flexibility to customize our platform to suit your specific requirements and sensitivities - however, these must be disclosed during on-boarding.

How does your system integrate with other systems?

Logically's systems are designed with extreme flexibility in mind. Our core system architecture is platform-agnostic. It provides the ability to ingest external, sensitive, or proprietary data sources in a plug-and-play configuration and output raw and processed data via encrypted endpoints integrated into existing systems.

How quickly can we put your system to use?

We want our customers to be up and running as quickly as possible. Time is a precious commodity in the fight against disinformation and propaganda campaigns, and even more so when it comes to the problem of radicalization and violence in our societies. Any new customer will have a dedicated and transparent team at their disposal to ensure our systems can be integrated into their workflow as quickly as possible while simultaneously maintaining a high level of operational security. Our rapid response team can initiate use cases within 24-48 hours with 7-10 days being typical for less time-sensitive situations.

How many people are required to implement, use, and maintain your system?

Logically offers three types of implementations:

1) **Fully Managed service**
Fully Managed services can operate with a single point of contact for niche operations, and up to 50 people for managed war-rooms.

2) Cloud-hosted platform
Operational from 1 person client-side and 3 people provided by Logically.

3) On-premises solution
Operates with 5-10 people client-side and 5 from Logically; this estimate is based on deployment complexity.

Can your system be fully automated?

The majority of our systems already work with an extremely high level of automation; this ensures that decision-makers only need to get involved when problematic content is detected.

How would we transfer your system's results to decision makers? And what is the nature of the output?

Here at Logically, we pride ourselves on our ability to produce full Product and service ecosystems built in a modular way. Our customers have the flexibility to choose when it comes to their preferred output of results. We can offer everything from raw data endpoints that can integrate into existing systems. To fully serviced dashboards and platforms developed in-house or custom reports for operational situations where digital coverage may be limited.

What are your current technical limitations and where do you see future limitations arising?

Logically's systems are not limited by scale. We use cutting edge infrastructure to ensure our services are available on any scale. The primary consideration when it comes to limitations is access to raw data. Some Logically capabilities are language agnostic, however more complex natural language models such as stance comparison are at present limited to english.

How accurate are your system's results?

Our systems are trained and refined towards any specific use case. While we have high confidence in our results out of the box, our intelligent systems become more accurate, the more they study and learn the complex narratives and data applied to any given use case. User feedback from individual customers, as well as updates to our data lakes are incorporated in nightly updates to our machine learning models. All automated capabilities on the Logically platform are regularly tested and benchmarked to ensure an F1 score of 0.85 for standard capabilities, 0.95 for more mature capabilities and 0.8 for any capabilities in beta. We also maintain high data coverage on our platform with customers provided with 4 tiers of coverage (1%, 10%, 30%, 100%) based on their use case.

How can we measure the performance of your system?

Depending on the services customers require, we can provide KPIs based on outcomes, information detail, events, and threats identified: from counts of unique fact-checks, credibility assessments, and threats. We can also use Latency as a measurable: time from a user request or threat origination to response or threat flagging as well as Accuracy in the form of correct classifications.

What kind of support do you offer?

Logically employs a wide array of domain experts that strive to provide both intellectual and technical support to our customers proactively. With Logically's Managed services full support is offered to ensure customer success while our Cloud-hosted solutions come with on-boarding and maintenance support and implementation and analysis workshops

Is training/on-boarding included? How long does the process take?

Training and on-boarding package is available to any new customer; this process typically takes 1-5 days, depending on the scope of the project.

Can we customize your system according to our needs? How fast?

When creating a new account or setting up a new project, we can offer a plug and play customization service for our customer's requirements, as well as through platform settings. Custom capabilities such as novel data sources and threat types can be added in 1-4 weeks depending on the complexity of the integrations.

How often is your system updated?

Data on our system is updated every minute, with all our inference updated within 15 mins. Our systems and underlying automation are actively updated daily. As the nature and direction of the threat are continually evolving, so too are our systems. Our dedicated team of domain experts regularly evaluate, verify, improve, and update our methods, ensuring we continuously meet our customers' needs and to ensure we are meeting the needs of the communities they serve.

Who are some of your current customers?

Logically current customers include the Government of Maharashtra and The Government of India. We have collaborated at an agency level in the United Kingdom with the Counter-Terrorism Internet Referral Unit (CTIRU) of The Metropolitan Police, The Mayor of Londons office, and the Home Office. Logically was proud to welcome UK Home Secretary Priti Patel and officials to our offices presenting our work detecting inauthentic coordinated behavior on social media during UK Elections.

In Sweden Logically provided verification and fact-checking training for students, journalists & technologists, Monitoring misinformation and trending claims in multiple languages, and establishing an election day task force to prevent attacks on first-time voters.

Logically also has vendor and partner relationships with major social media platforms to help moderate, factcheck and takedown problematic content and provide threat intelligence feeds.

Why should we choose you over competitors? Who are your top competitors?

Logically provides the only full-stack solution to the misinformation and disinformation space and cuts across media intelligence, credibility assessment, veracity assessment, and social network investigations. Our broader focus across these 4 capabilities, helps improve each capability area due to the inherent dependencies between each of these concepts. Our inferences are backed by nightly updating automation as well all expert analyst teams, such as our fact-checking team - the largest of its kind in the world. This positions us, uniquely, to focus on delivering outcomes and not just activity.

Logically's platform and underlying capabilities have been built by cutting edge researchers from MIT, Cambridge, Oxford, Princeton, IIT, Deepmind, IBM, and Microsoft.

What are the differences between your system and similar technologies?

Our systems operate in both fully automated and semi-automated modes and can be customized based on policy, meaning Logically can tailor our services to both geographic and cultural nuances.

We pride ourselves on building Full-stack misinformation and disinformation solutions with Explainable AI, empowering both analysts and decision-makers with the tools they need to achieve their strategic goals.

How is your system sold i.e., as a service / product / other?

Logically has multiple offerings, these include fully serviced consultancy and analysis as well as 'as a service' platforms and packaged products.

Do you offer a free trial use of the system?

Due to the high on-boarding costs associated with data processing Logically does not currently offer free trials of our systems, we can provide paid pilot schemes to ensure our systems meet customer requirements.