CALLSIGN: ADOPTING AI GOVERNANCE PRACTICES FOR IDENTITY AUTHENTICATION

Callsign is a London-based company that leverages deep learning techniques and combines biometrics, geo-location and behavioural analytics with multi-factor authentication to help clients authenticate user identities. Providing services to companies from all over the globe, Callsign helps clients from various sectors like finance, healthcare and e-commerce flag out potential risks in user authentication.

As a company that puts priority on solutions that are transparent, and at the same time, produce reliable and accurate results, Callsign understands the importance of building and maintaining trust with its clients to enable such solutions. With this in mind, they put in place processes to govern the development and deployment of their AI models, adapting and implementing practices as recommended in the Model AI Governance Framework.

ROBUST OVERSIGHT IN AI MODEL DEVELOPMENT

In overseeing the development of its AI models, Callsign included three parts in its implementation of **internal governance structures and measures**. The first part involved creating a multi-level assurance framework, where each department head formulates and oversees certain controls and policies under his or her purview. This framework is managed by the Chief Security Officer and Data Protection Officer.

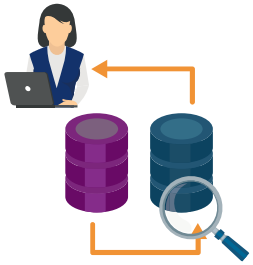
The second part comprised a three-stage process – concept, consult, and approve. The process coordinates the engineering, product, sales and research teams to ensure consistency in the data management and development of Callsign's AI models.

CONCEPT **CONSULT** **APPROVE**

An example of this process would be when the Product Owner conceptualisesa feature – either a perceived business or product value – and considers views from various teams such as the architects and security specialists. These views will then be used to enhance the security of the feature before it is presented to the Design Authority for approval. The Design Authority, comprising representatives from other teams as well as the leads of Callsign's Chief Technology Office, Chief Security Office and Chief Information Office, approves all the AI models that have been developed within the organisation. With the different teams' inputs and expertise, this second part helps build upon the robustness of Callsign's governance process for its AI models.

A data provenance process is essential in ensuring accountability for AI model development. For the third part, Callsign established a specialised Data Change Governance Committee to oversee the company's data provenance process. The Committee's responsibilities include:

Reviewing inclusion of data points to ensure the AI solutions meet its clients' business purpose;

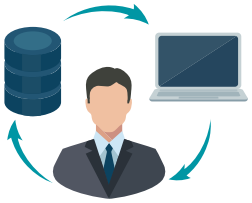


Assessing the types of data collected, including conducting reviews to check the validity and relevance of data; and

Ensuring that the end-to-end information lifecycle has considered controls addressing access, confidentiality, integrity, retention and movement of data.

HUMAN INTERVENTION ACCORDING TO CLIENTS' NEEDS

While Callsign adopts a **human-over-the-loop** approach in developing the AI model, the company works closely with its clients to **determine the level of human involvement appropriate for the specific application and context**. For instance, if Callsign's client is a bank using AI to authenticate user identities for fraud detection, various security considerations will come into play in Callsign and its client's assessment on the level of human involvement:



Client's risk appetite

A bank may have a larger risk appetite for corporate transactions as compared to transactions made by a retail customer. Flagging out potential risks and disrupting a corporate customer's transaction could result in serious consequences. Hence, in such cases the bank may opt for a lower degree of human intervention for corporate customer transactions;

User experience of its clients' customers

If Callsign's client received poor customer satisfaction scores, the client may consider improving their user experience journey and reduce levels of human intervention in the AI model deployment; and

Operational cost to the client

The cost of supporting customer feedback on the user authentication process may also urge the bank to lower the level of human involvement.

ACCOUNTABILITY THROUGH DATA GOVERNANCE PRACTICES

Callsign has in place good accountability practices to ensure the responsible use of data for its AI model development. These include measures to avoid over-collection of data and governance frameworks to ensure data protection.

To avoid over-collecting data, and at the same time, still deliver its services effectively, Callsign conducted extensive research and developed new, intelligent ways of gathering valuable results from a minimal amount of data. In addition, Callsign tokenised all personally identifiable information.

For username data, they are hashed by both Callsign and its clients for protection against rainbow attacks.[1] The hashing also allows Callsign to identify individuals while maintaining their anonymity.

For device data, Callsign adopts persistent device tagging methods to allow for device identification whilst maintaining the obfuscation of the user in its AI models.

For behavioural data, Callsign is mindful not to collect specific keys or pin codes that were entered on mobile phones or websites.

For location data modelling, Callsign adopts a data protection by design approach by masking the longitude and latitude data collected.

Developing data governance frameworks has also helped Callsign in its accountability approach to AI model development. Using the frameworks and international standards like the ISO guidelines as references, Callsign applied internal data classification principles to classify data sensitivity and created risk-based outlooks to avoid the misuse of data in situations such as data breaches.

As part of its efforts to support point-in-time explanations for its data collection and analysis, Callsign also developed data inventories [2], data dictionaries[3], data change processes, control mechanisms, forums and collaterals. Having a **clear understanding of the lineage of data** and being able to provide point-in-time explanations to various stakeholders has enabled Callsign to improve operational efficiency and offer better services to its clients.

[1] Rainbow attack is a type of attack that attempts to uncover the password from the hash
[2] Data inventory is a dataset containing metadata on contents of data, its sources, and other pieces of useful information.
[3] Data dictionary is a dataset describing the relationship between the data, where and how the data is used.

To ensure the performance of their AI models, Callsign collects and carefully creates **distinct datasets to train, test and validate its AI models**. The company conducts intensive testing on the performance of its AI models with the use of proof of concepts, prototypes and through peer reviews from its network of research communities. On top of that, Callsign puts its AI models through behavioural biometric models and tools, such as the ISO/IEC 19795 Biometric performance testing and reporting, to build the model's accuracy. These public tests not only verify the model prototypes, but also provide much needed assurance to Callsign's clients.

Once the performance of the AI models has been tested and baselined, Callsign integrates the performance evaluation into Continuous Integration[4] and Continuous Delivery[5] practices. Through this, Callsign is able to enhance **the reliability of its AI models and ensure that they serve the intended purpose** of providing well-tested services to its clients.

Explainability of AI model outcomes can help tremendously in building understanding and trust with its clients. Cognisant of this, Callsign **documents the development process of its AI models** and extracts insights of its key contributing factors. Such **documentation facilitates explainability**, and with this, Callsign is able to explain outcomes such as model and database description, evaluation parameters and error rate metrics. When technical explanations of the AI model may not be as comprehensible, Callsign provides a non-technical explanation to its clients. This boosts the clients' understanding of the AI solution and encourage buy-in from their internal stakeholders.

AN OPEN AND TRANSPARENT APPROACH

When it comes to communicating to its clients and their users, Callsign adopts an open and transparent approach, notifying them on the types of data collected, the reasons for collection and the use of such data.

The company's Data Processing Notice is an exemplary example of this openness. In this Notice, Callsign not only details their device, location and behavioural data collection and use, but also explains how clients may use Callsign's product to manage authentication, authorisation and transaction risks. These policies can be configured or used to make automated decisions by its clients. Callsign further **provides an email address in its Notice** for clients to provide feedback on its data processing policies.

CONCLUSION

As businesses look towards AI to solve challenges, Callsign's early adoption of governance best practices provides the necessary client confidence in using its services. These practices have also enabled Callsign to engage a diverse range of internal stakeholders that help shape an open discussion and contributed to an accountable development of its AI models.

[4] CI is a development practice that requires developers to integrate code changes to a shared repository several times a day; each code change triggers an automated build-and-test sequence.
[5] CD is an extension of CI; teams ensure changes in the code are releasable, and the integration process is fully automated.