No, Secure and Transparent AI is not an Oxymoron

In the current environment of mistrust and regulatory pressure, security is increasingly moving to the forefront of the discussion. Silicon Valley has seen its share of scandals in recent years (Facebook/Cambridge Analytica, Uber, and many more) showing that the opportunism surrounding tech can cause problems if not properly managed. The writing is on the wall - organizations everywhere are adopting a more cautious approach when choosing partners in innovation.

The regulatory landscape is shifting as well. You've undoubtedly heard of GDPR (General Data Protection Regulation) - the EU directive aiming to protect the privacy of its citizens' personal data.

Key requirements of GDPR include:

- Requiring the consent of subjects for data processing
- Anonymizing collected data to protect privacy
- Providing data breach notifications
- Safely handling the transfer of data across borders
- Requiring certain companies to appoint a data protection officer to oversee GDPR compliance.

Article 22 is particularly challenging: *"The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".* In plain English - every user has the right to control how his or her personal data will be used.

These shifts are especially meaningful for Artificial Intelligence. "Automated processing" is at the heart of AI, and without a clear "map" of how an enterprise AI makes its decisions (e.g. a complete log of all decision points), corporations will not be able to provide proper traceability concerning user data. Especially, algorithms like Deep Learning, which essentially rely on a black box, are in deep trouble.

In a climate of change, it's easy to be reactive. Large companies with huge organizational momentum to overcome still face the same threat of competition. Everyone is still looking for an edge - but the layers of complexity and conflicting objectives can seem overwhelming. But it's not all doom and gloom!

For companies looking to reduce cost on repetitive, error-prone workflow and utilize valuable insights lost in the sea of “big data”, AI can seem like the holy grail. But how should such an organization vet potential partners? Data security is at an all-time high in priority; must they sacrifice time to deploy or accuracy? What security features should enterprise be looking for in AI providers? And what’s actually available?

Current spate of regulations and privacy concerns are particularly meaningful, as well as challenging for AI companies. Coseer has made data security and transparency its core design feature.

Coseer addresses this issue by weaving strong data security measures throughout its suite of products and solutions. Data security is enmeshed in the musculature of Coseer - so there is no need to sacrifice on time or accuracy.

1. We deploy a bespoke solution to each problem, ensuring that no data ever leaks.

Coseer's solutions deploy on private cloud or on-premise servers. While this is not trendy in Silicon Valley, we understand that data privacy is very important to our customers. There is another advantage - this architecture lets us configure for each customer's unique needs, and achieve 95-98% accuracy.

2. We log evidence of every decision made by our engine, ensuring that customers have a complete map of the process.

Coseer does not use “black boxes”. Our algorithm, Calibrated Quantum Mesh , logs all the evidence that was used to come to any decision. This evidence can be brought out on demand for regulators, auditors, or simply for your internal team in their quest to better understand unique insights in the data.

3. We’ve decided to forego “transfer learning” (also called inductive transfer), so you can be sure your data doesn’t end up anywhere it shouldn’t.

We’ve made the decision not to use transfer learning across organizations. We respect that your data and your insights are yours and yours alone. We successfully reuse whatever the machine learns from one application to make sure that another application for the same organization is successful. However, even if your solution is hosted on our cloud, not a single byte of your data is used for training someone else's solutions. This does come at a cost - transfer learning acts like a catalyst in training an AI engine on small datasets by repurposing “lessons learned” from one dataset to another, our engine learns “one at a time.” By neglecting to use this technology, what you may lose in time you will get back get in security and peace of mind - and in a clear-cut log of every decision Coseer has made, giving you a powerful reference which is 100% auditable and available for regular review. As we’ve mentioned, there

are no black boxes at Coseer.

4. We use of all the latest encryption and security standards for you data.

Whether the information is stored in your cloud, or on our cloud, the same philosophy extends to access to IT infrastructure or the application. Everything is encrypted, password protected, two-factor authenticated, or, simply put, secure.

5. Our team is trained to the highest security standards, and passionate about keeping your data safe.

One final component of security is our people. Every employee that comes anywhere near your data has been thoroughly background checked in US and internationally. We take great pride in our team - they've been selected for their talent and alignment with our core values, which include putting you, the customer, first. They then sign multiple confidentiality and compliance agreements, and their success at Coseer, and a big part of their compensation, is connected to continued adherence to these agreements.

Depending on your requirements, the timeframe may be tight - but with a **turnaround time of only 4-12 weeks on average, 95-98% accuracy, and industry-leading data security standards**, we're confident that you'll be satisfied, especially if you place a high value on your (and your customers') own competitive advantage - your data.

There is truly no need to spend resources on tedious, boring tasks. AI done the right way can be safe, secure, transparent, and transformative in all the ways you want it to be.

A big part of being a Responsible AI vendor is to treat our client's data responsibly, and to respect their own needs for both compliance and review. We have been committed to this responsibility from the Day 1, with no breach in our history. When your work with us, you get the bleeding edge of AI without compromising on transparency or on security of your data.

Want us to prove it to you? **Setup a demo here** and we'd be happy to answer all your toughest questions.

What is Tactical Cognitive Computing?

At Coseer we believe humans should focus on creativity and judgment, while technology takes care of everything else. Tactical Cognitive Computing is our solution to automate all the tedious, repetitive and mundane workflows that are language driven, and hence still need a human.

- Tactical Cognitive Computing uses AI, NLP, Cognitive Calibration and other advanced sciences to process natural language, other unstructured data or even structured information to get meaningful insights and automate business decisions.

- Tactical Cognitive Computing models and trains for each specific workflow resulting in very high accuracy. It is designed modularly, is highly transparent and trains very fast.
- Tactical Cognitive Computing solutions run on regular hardware either on premise or in cloud giving customers high level of flexibility, data security and accessible costs.

Tactical Cognitive Computing technology is designed for ubiquitous application, low cost trials and high accuracy.To learn more please visit our blogs or contact us to setup a call.