HOW U.S BORDER CONTROL LEVELLED UP THEIR TECHNOLOGY TO IDENTIFY RISKS AND PROTECT THE NATION

SEARCH365

OVER WATCH

To protect the country from identified and potential threats, the United States Customs and Border Protection (CBP) hold the responsibility of safeguarding 328 ports of entry across all 50 states. On an average day (pre-pandemic), this can see staff processing close to one million visitors. To manage this, the agency uses sophisticated identity matching technology.

Identity matching, a popular technique with counter terrorism departments, is used to search multiple databases using key points of identity records to flag and keep track of suspected terrorists or anyone posing a risk. The technology is rapidly evolving and gaining popularity beyond its original purpose of government and national security.

The US Border's implementation of Over Watch's linguistic methodologies provides a good example of how and why Australian departments and organisations can benefit from identity matching.

In a bid to strengthen the Border Protection screening system, the United States Department of Homeland Security (DHS) Targeting and Analysis Systems Program Office (TASPO), were growing frustrated by the volume of both false positives and false negatives being generated when searching for suspicious personnel, by their incumbent identity matching technology.

While the technology claimed to be 'real-time', the reduced accuracy of the results meant that staff were wasting valuable time having to investigate flagged issues.

THE DEADLY RAMIFICATIONS OF THE BOSTON BOMBINGS

In 2011, Tamerlan Tsarnev – AKA the Boston Bomber – entered America when a linguistic variation of his name failed to register with the CBP, despite being on an official watchlist. When he entered the country in January, a new watchlist alert flagged his name as Tsarnayev, a linguistic variation, which did not match his passport name, Tsarnev. In this instance, identity matching accuracy was the difference between life and death.

Large volumes of false negatives and false positives are caused by a naïve approach of searching and generating all possible spelling and naming variations in a bid to increase matches. In effect this approach sees names as nothing more than a sequence of letters. The CBP's incumbent system did not allow adding or missing spaces, or new, unknown names. In addition, the technology's inability to intelligently consider cultural or linguistic norms hindered the accuracy of the identity matching results.

A naïve approach has other downsides, including the requirement to continuously collect and store name variations, and needing considerable computing power to continuously monitor names against an extensive, and growing, list.

EMBRACING A NEW APPROACH OFFERING ADVANCED ACCURATE RESULTS, FAST.

To improve the accuracy of identity matching, the CBP and TASPO wanted to integrate different approaches to name matching, to allow their results to benefit from multiple approaches instead of just one. As well as the security benefits being sought, the CBP also wanted to ensure they had a modern and scalable solution that could handle the huge volumes of data they needed to monitor.

To achieve this, the CBP looked at new technology which uses a knowledge-based approach. This approach uses Artificial Intelligence based taught automated linguistic methods and patterns. The technology uses both phonology (how words sound) and orthography (how words are written) and applies this to 18 different languages. Over Watch can search for linguistic name variations such as Charley or Charlie, where the phonology is the same, but the orthography varies.

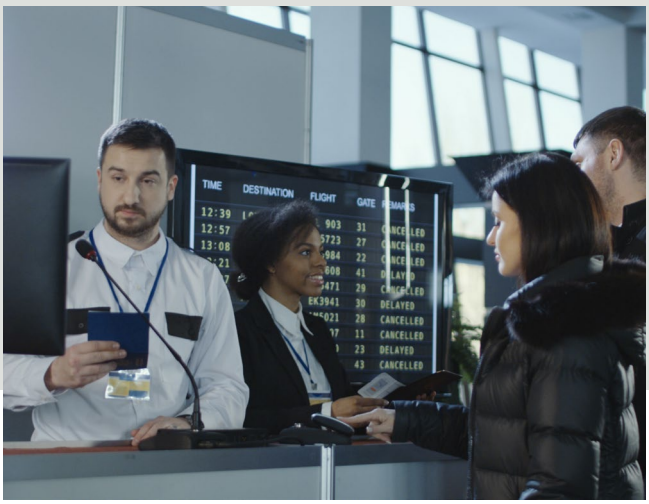
Cultural norms are a common source of false positives in identity matching technology that follows the naïve approach. Names that have spelling variations when translated can also be easily matched because the system maps the translated name back to the original, whether this is in English, Arabic script or other languages and dialects.

Having explored the options available, the CBP opted for Over Watch's linguistic methodologies, a dynamic and powerful system which are proven to be more effective than the naïve approach. The algorithms used can recognise cultural norms – for example, when surnames are entered in first or middle name entries and vice versa.

> **In the case of the Boston Bomber, a knowledge-based approach would have ensured that Tsarnev's entry to the country was flagged, regardless of the spelling variation.**

The faster and greater accuracy can also be attributed to Over Watch focussing on the original script, as opposed to translating it to English. This allows Over Watch to take advantage of all available contextual information and match names to lists without introducing errors caused by translation.

In short, embracing a knowledge-based approach increases security and improves the accuracy of alerts generated. Given security is the primary concern of the CBP, Over Watch's linguistic methodologies was a highly attractive option.



USING THE BEST TECHNOLOGY TO BEAT THE BAD GUYS

By deploying Over Watch's linguistic methodologies, the CBP were able to protect their borders with greater accuracy and efficiency. The switch from a naïve approach to a knowledge-based one led to a reduction in fewer false positives and fewer false negatives. It also resulted in much faster fact checking and the increase in accuracy meant the product was actually delivering real-time results.

The CBP and TASPO are now confident they are using the best technology available and protecting their borders, and their nation to the absolute best of their ability.

In addition to successfully identifying and reducing risks, staff have seen a reduction in time spent managing the system. Over Watch does not require user maintenance once implemented because the technology's intelligence is constantly evolving. The data is regularly updated to ensure the learned cultural and linguistic norms continue to expand and provide the most sophisticated identity matching service available and thus, the most effective shield of defence.

WHAT DOES THIS MEAN FOR AUSTRALIA?

The CBP operate on an enormous scale, with exceptionally high volumes of travellers entering and leaving the country daily. However, identity matching as a process is the same, regardless of scale.

Government departments, organisations and businesses can all benefit from implementing a knowledge-based approach to identity matching. The primary benefit is unmatched accuracy and superior security and safety. The scalability and intelligence of the system also has a positive impact as staff can significantly reduce the time spent in both maintaining the system and investigating issues flagged from inaccurate data.

Over Watch is available to be deployed rapidly, within hours, into a variety of operating environments including the public cloud, highly secure private infrastructure, and even a version on a battery powered portable device that can operate independent of a contested and congested network.