Ultra Sentient

Voice & Data Interception for Law Enforcement and Enterprise

Features

- Automated analyst assistance to identify conversations containing voice of person-of-interest
- Advanced biometric voice detection
- Store recorded conversations for up to 30 days
- Retrospectively analyze stored conversations based on new target information
- Integration with Cisco Call Manager to improve recording capabilities

Technology advances have resulted in the speed and variety of modern communications increasing significantly in recent years. These advances mean that it is easier and quicker for individuals to collaborate with each other resulting in significant efficiency gains for businesses.

As well as facilitating positive outcomes, more efficient communication can result in increased negative activities by terrorists, drug traffickers and other criminals who are able to coordinate their illegal activities more effectively. In addition, rogue employees are able to leak valuable intellectual property to competitors easier.

To counter these threats to security, Law Enforcement Agencies (LEAs) and enterprises need to monitor and analyze communications and take the necessary actions should signs of malicious activity be detected.

Law Enforcement Agencies use Ultra Sentient Voice & Data Interception to:

- Perform mass or target-centric collection of communications
- Monitor audio in near real-time to immediately assist with ongoing investigations
- Plot the locations of suspects using cell tower information
- Meet the increased recording needs of any investigations

Enterprises use Ultra Sentient Voice & Data Interception to:

- Monitor for specific keywords such as new product names and secret projects being discussed inappropriately
- Record evidence of inappropriate communications between employees and third parties

Ultra ELECTRONICS

Ultra Sentient for Law Enforcement Agencies

During intelligence gathering and counter terrorism activities, LEAs need the ability to monitor and record large volumes of voice and data communications to gather relevant information about large numbers of known and unknown persons-of-interest.

It is not possible for human operators alone to analyze the large volume of recorded communications to identify many different potential targets. Ultra Sentient has the industry's most advanced voice biometrics processing engine to identify the voices that are the closest match to the identified targets. Rather than relying on what is being said or how it is spoken, this technology relies on analyzing the effects of physical characteristics of the human anatomy (e.g. size and shape of the larynx, mouth and nose). As a result, it is very difficult for the target to disguise their voice by whispering, shouting, changing the pitch of their voice or talking from a noisy environment.

Once each conversation has been analyzed it is scored based on the probability of it containing a person-of-interest. This process means that analysts are only required to listen to a small subset of conversations in order to identify a target which makes them more productive.

As well as analyzing data as it is recorded for known targets, it is also possible for analysts to retrospectively analyze data if voice samples from new suspects become available.

Ultra Sentient for Enterprise Compliance Monitoring

In order to protect their businesses from competitive threat and legal issues, large enterprises need to ensure that proprietary and confidential information is not being leaked by employees.

Failure to protect against proprietary and confidential information being leaked could result in:

- Competitors coming up with alternative strategies to counteract future business plans
- Products being copied before rights can be secured
- Heavy fines from regulators due to market sensitive information (e.g. merger & acquisition details) being released at inappropriate times
- Loss of customer and stock market confidence due to the inability of the company to protect its assets

In order to prevent all of these from happening, companies should constantly monitor all forms of employee communications including telephone calls, email, instant messenger and social media. By doing so they can detect if corporate guidelines have been violated so that they can put remedial measures in place as quickly as possible.

The recording and analysis of communications can be limited to employees who:

- Are suspected of policy violations
- Have access to privileged company information such as product roadmaps, future acquisition targets or other business-sensitive information.

Ultra Electronics
SURVEILLANCE AND SECURITY SYSTEMS
316 Botley Road
Burridge
SO31 1BQ
United Kingdom
Tel: +44 (0)1489 557 373
Email: information@ultra-sss.com
www.ultra-sss.com
www.ultra-electronics.com