

WhiteSparks

+44 (0) 844 247 4538

whitesparks@whiterockglobal.com

www.whiterockglobal.com

THIS ISSUE :**Volume 3, Issue 44: 6 April 2011**US Confidential: **Obama's Counter Surveillance "Blue Tent"**Sex, Lies and Conspiracy: **Software AG and US Navy in the Commercial Espionage Scandal**Spying the Spy Plane Bid: **Indian CBI Investigating the Leak**Australians Eavesdropped: **iPhone App Leaves Police Powerless**

NEWS UPDATES

**US Confidential: Obama's Counter Surveillance "Blue Tent"**

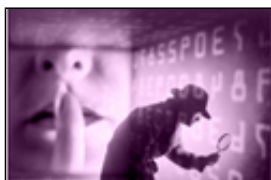
The White House released a photo that shows US President Barack Obama fielding calls from a special counter surveillance tent in Brazil to keep up with the events in Libya. The mobile secure area, known as a Sensitive Compartmented Information Facility (SCIF), was designed to allow world leaders to have top secret discussions on the move. Being one of the safest places in the world to have classified conversations, the tent withstands eavesdropping, phone tapping and computer hacking.

The technology is based on a Faraday Cage i.e. "ring of electronic waves", preventing radio frequency signals from getting in and out of the tent. The only signal that can get out is the encrypted communications through a secure and encrypted phone line, which sends conversations through a satellite. Only those authorised can go inside a SCIF, with entry usually requiring a combination of pin numbers, access badges and biometric data.

SCIFs can be permanent enclosures within a building, or mobile areas set up during official visits. Obama's tent was set up in his hotel so that he could hold a secure conference call with Secretary of State Hillary Clinton, National Security Advisor Tom Donilon and Secretary of Defence Robert Gates, among others. A photo released to the press on 22 March showed the President and advisers gathered around a videophone, inside what looked like a standard windowless blue tent.

Raili Maripuu, WhiteRock Managing Director: "Although the President's SCIF sets a great benchmark in terms of securing confidential discussions, it is not commercially viable. However, businesses can prevent information leaks by controlling and monitoring radio signals in designated discussion areas. Our 24/7 WhiteRoom service remotely monitors all radio signals (such as 3G, Bluetooth, GSM, WIFI etc) and alarms on all unauthorised and unknown signals. The purpose of the WhiteRoom is to have a sanitised "War Room" or "bug-free" environment to discuss high-level sensitive information."

[Read Full Story from Original Source...](#)

**Sex, Lies and Conspiracy: Software AG and US Navy in the Commercial Espionage Scandal**

The US middleware giant Software AG has conducted an elaborate corporate espionage conspiracy over several years, according to the allegations of a radio frequency ID (RFID) vendor GlobeRanger.



The company filed a lawsuit originally in its home state Texas, in December last year, however this was moved to federal court in March 2011. In response, Software AG, which dwarfs GlobeRanger in size, filed a motion to dismiss the case.

The complaint involves several companies and claims that Software AG manipulated personal relationships between themselves and GlobeRanger's former client, Navy AIT and its partners, Naniq and Mainsail, for the opportunity to provide an RFID solution to Navy AIT.

Although the main defendant, Software AG, insists that the accusations are without merit, GlobeRanger has painted a spy-movie-like scenario surrounding the tech secret theft that reportedly reaches into hundreds of millions of dollars.

Capitalising on an executive level love triangle, Software AG are said to have obtained sensitive material from GlobeRanger pertaining to the required RFID solution, according to the lawsuit. This in turn may have allowed Software AG to develop its own RFID technology in time to meet an otherwise unachievable deadline of several months. The timeline is stark in comparison to the decade of development claimed by GlobeRanger in the complaint, considering that the Software AG has allegedly no previous experience in the sector.

[Read Full Story from Original Source...](#)



Spying the Spy Plane Bid: Indian CBI Investigating the Leak

The Indian Central Bureau of Investigation (CBI) is investigating the role of a Research and Analysis Wing Officer, who allegedly passed on information about major spy planes' surveillance equipment bid.

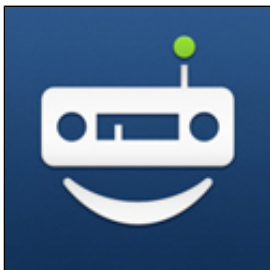
The deal, in which the US company Raytheon and Israel's Elta Systems were competing to facilitate two Bombardier aircrafts is now under review by the Prime Minister, Manmohan Singh, after discrepancies in the bidding process were flagged. Israel's Elta System was the lowest bidder with \$300 million and should have been the winner. However, Raytheon, intensely backed by the US Government, applied pressure on the Indian Government complaining that the Israeli system was not tested. The raid that followed resulted with seizing several documents. The investigation revealed that the officer, who held a prominent position in the agency, had provided important leads regarding the contract to the US company.

[Read Full Story from Original Source...](#)

DID YOU KNOW?

Senator Herb Kohl sponsors the US Economic Espionage Penalty Enhancement Act, which increases the maximum sentence for stealing trade secrets from 15 to 20 years.

Source: [Senator Herb Kohl's website](#)



Australians Eavesdropped: iPhone App Leaves Police Powerless

The Queensland Police Department has found shocking evidence that iPhone users can use an application to tap into police radio frequencies.

The officers often name victims of domestic violence, sexual assaults and other crimes when using those frequencies. The Tuneln Radio app for iPhones features a pre-programmed menu from which users can listen to and record police radio frequencies in several large regional centres in Australia. Needless to say that the police now have strong privacy concerns for victims of crime, as well as operational safety and potential impacts on ongoing investigations.

The app was initially created to pick up thousands of commercial stations and only receives analogue frequencies. This means that the application doesn't pick up networks that are digital or encrypted, a solution the Queensland Police Department would be wise to consider implementing.



[Read Full Story from Original Source...](#)

NEWS UPDATES:

Renault Meeting Secret Recording Released

Read more: **WhiteSparks, Issues 38, 39 and 43**

Renault's espionage turned fraud scandal recently took a new turn as the French media aired secret recordings of the carmaker's executives begging its former security manager to help them out "of this mess".

The 14 February recording reveals Renault's General Counsel, Christian Husson, talking to Dominique Gevrey, the ex-security manager who is now accused of fraud in the case. In the recording Husson asks Gevrey to reveal his Brussels source, who had provided the crucial base information for espionage allegations against other managers. In the recording, the former security manager replies that the information "won't stand up in court". It is claimed that it was Gevrey, who is currently under arrest, who made the tape public in an attempt to defend himself.

The revelation is a further embarrassment to Renault's head, Carlos Ghosn, who is already facing widespread criticism over the industrial espionage fiasco. The carmaker's chief executive made a public apology in March and promised to give up a bonus of €1.6 million after admitting that the accusations of espionage were unfounded. However, the recording reveals that, while still claiming in the media that Renault had been the victim of a spy network, month earlier he already privately admitted that the company had been "stitched up".

[Read Full Story from Original Source...](#)

NOTW Former Journalists Arrested for Phone Hacking

Read more: **WhiteSparks, Issue 38**

News of the World former chief reporter Neville Thurlbeck (50) and former news editor Ian Edmondson (42) were arrested on suspicion of unlawfully intercepting mobile phone voicemail messages of British celebrities. The men remain in custody for questioning.

The reopened phone hacking inquiry about the illegal information gathering methods used by tabloid newspaper has made headlines in the UK media over recent months. It started in 2010 when the actress Sienna Miller obtained a court ruling ordering mobile phone provider Vodafone, to disclose data relating to other users. Miller is seeking damages for articles about her published during 2005 and 2006, which she claims made use of private information found by hacking into her voicemails.

Since then a number of other alleged victims of phone hacking have come forward, including film actor Jude Law, footballer Paul Gascoigne, former MP George Galloway, comedian Steve Coogan and sports commentator Andy Gray.

[Read Full Story from Original Source...](#)



INVESTOR IN PEOPLE

© Cope Whiterock Limited 2011 - Critical Information Defence® - SEC® - ISO9001 Registered Firm - Certification Number GB2000647

WhiteRock - A Bond of Trust