

# AIBO THE GROMIT CONSPIRACY: JAPAN AND THE WORLDWIDE INTELLIGENCE NETWORK

by Toshio Takagi

Menzies Library, Australian National University

## ABSTRACT

Aibo is the world's first artificial intelligent entertainment robot produced by Sony. As Aibo can be operated by remote control, a conspiracy theory has evolved about him. This theory says that a Japanese man controls all of the Aibo the Gromit robots, and he is using it to spy on its 5,000 owners world wide. It is easy to dismiss such a story as laughable. However, it has been revealed in the report presented to the European Union (EU) Parliament that the US operates a comprehensive global intelligence network known as ECHELON which monitors electronic communications not only in Europe but around the world. The report states that all e-mail, telephone and fax communications are routinely intercepted by the US National Security Agency (NSA). Japan's decision to enact Wire-Tapping Law and to develop her own spy satellite recently have met with strong condemnation as well as a certain scepticism. Are these stories inter-related in some way? How does Australia fit in this scenario? What should the general public know about these matters? This paper attempts to answer these questions.

---

## Introduction

Aibo the Gromit is the world's first artificial intelligent entertainment robot produced by Sony. The name, Aibo, literally means "a good companion" in Japanese. Aibo was unveiled on the Internet, selling 3000 in Japan (being sold out within 20 minutes) and 2000 in the US for US\$2500 each. Aibo is equipped with a 64 bit 100 MHz processor with 16 MB of memory. He sees through a 180,000 pixel digital camera in his nose and hears through stereo microphones in his ears. A multitude of motors allows him 18 degrees of movement and an 8 MB flashcard stores his experiences to allow his intelligent to develop. He should grow over time, in mind, from a cyber pup to an intelligent "Techno Terrier". Since he can be operated by remote control, an Aibo conspiracy theory has developed: that somewhere in Japan a man controls all the Aibo the Gromit robots and is spying on Aibo's 5000 owners around the world.

Whether or not you believe this story, according to some newspaper articles, there is a rumour that the National Security Council in the US is watching over Aibo matters closely and Aibo the Gromit robots have been banned from the Pentagon. The conspiracy theory is that a Japanese businessman is paying a fortune to spy on Aibo the Gromit robot owners around the world.

It is quite easy to dismiss this story as laughable, but, when one think of the United States of America intelligence network facility called ECHELON (which was recently revealed), it is understandable for the Pentagon to pay that much of their particular attention to the Aibo robot and the conspiracy theory about him.

## **1. New developments in Japan's defence initiatives**

Despite the fact that Japan is still the world's second largest economic power with defence spending of more than US\$40 billion a year, her assertiveness for playing an appropriate international role is somewhat limited over the years. However, in recent months, Japan has exhibited new initiatives, such as a new agreement to collaborate with US in developing advanced missile defences and to plan for building a Japanese spy satellite. Meanwhile, some serious discussions have begun on easing Japan's strict constitutional restrictions on the use of military force. The Japanese Parliament recently voted to restore official status to the country's old Rising Sun Flag and its former national anthem. According to some US Japan watchers, Japan's new assertiveness on defence is a healthy development.

According to Yoichi Funabashi (p. 38 Shukan Asahi 13/8/99) Japan is developing a more independent military capability, in case its alliance with the US may some day collapse. Japan is now strengthening its security ties with the US while preparing for a time when Japan may stand on its own. The conclusion drawn up by the report, "Japan's Evolving Strategic Calculus", produced by the National Intelligence Council (an umbrella organisation of the CIA), has the same view. The author stated that what caused Japan to adopt this course of action is firstly, the Clinton visit to China without first visiting Japan, and secondly, the major security shock caused by North Korea firing a new missile over Japanese airspace. Japan is at a crossroad in trying to adjust to post Cold War era defence needs in a time when Japan has achieved significant economic developments at astonishing speed.

## **2. Wire-tapping law**

According to the Japan Times of 25 June, 1999, over 8000 people protested against the Wiretap Bill (later it became law under very questionable circumstances, essentially in the way ballot was conducted). And this law was enacted by the Japanese Government as a result US pressure to do so. Privacy issues have taken centre stage as Japan adopted this law allowing police to eavesdrop on phone calls, intercept fax and computer transmissions, and read e-mail. According to a government authority it is intended to help law enforcement to prevent premeditated murders, drug trafficking, the entry of illegal immigrants and the spread of illegal guns in the community. The reality could be far more sinister and intrusive (as demonstrated in other countries), than anyone can imagine. Under the guide of restoring public order, such as in Aum Shinrikyo case in 1995, the law-enforcement authorities insist that their greater surveillance powers will prevent such happenings. In other words, civil liberty must be sacrificed so that Big Brotherhood can protect us. Some former executives of a manufacturer of hearing aids (<http://www.rion.co.jp/products-e/subindex.html>) said that the

Japanese Police have been bugging their phone because their company had been selling surveillance equipment to the police since 1957.

Why does the Japanese government want to legalise wire tapping now? One government official's response to this question was that for Japan to become a "normal" country it needed to enact such legislation.

### **3. BRUSA/UKUSA/ECHELON**

#### **3.1 BRUSA**

##### **3.1.1 The BRUSA Agreement**

ECHELON has its origin back in summer of 1940 when France had collapsed under Hitler's war machine, and by August Germany had started bombing southern England. The Battle of Britain had begun and it was described by Churchill as "Wizard War". That was a war fought as much with science as with gunpowder. This was because Britain had managed to acquire a working model of Germany's highest-level cipher machine, the Enigma, making code-breaking a major element of military success. When Churchill learned that the US had successfully broken Japan's high-level diplomatic code he was not only impressed but also was convinced that Britain and US should cooperate in the fields of signal intelligence. It was on 17 May 1943 that Britain and US signed the BRUSA Agreement (James Bamford "The Puzzle Palace: A Report on America's Most Secret Agency" Penguin 1983). The cooperation, procedures, and security regulations set out in the BRUSA Agreement served as landmarks in the history of communications intelligence.

##### **3.2 UKUSA Agreement and beyond 1947**

The success of BRUSA quickly led to a series of conferences involving not only Britain and the US, but also Canada and Australia. In 1947, after 2 years of negotiations, the BRUSA Agreement included Canada, Australia and New Zealand making the five power UKUSA Agreement with the US as the first party to the treaty, and with Britain, Canada, Australia-New Zealand as second parties to the treaty.

Between the first and second parties there is a general agreement not to restrict data, but with countries of third party status (viz, NATO, Japan and Korea) who joined later, the sharing rights are far less generous.

The purpose of the UKUSA agreement was to create one vast global intelligence organisation sharing common goals and a common agenda, spying on the world and sharing the data. It is significant that since the agreement has been kept secret for such a long time it has made it possible to mount operations which may be outside the domestic law of any country including UKUSA member countries. Domestic laws were circumvented by a mutual pact between five nations. Under the terms of the UKUSA Agreement, Britain spies on US citizens whilst the US spies on British citizens, and the two countries trade data.

The member organisations of the UKUSA Agreement are: The US National Security Agency (NSA - <http://www.nsa.gov:8080>), The British Government Communications Head Quarters (GCHQ), Australia's Defence Signals Directorate (DSD), Canada's Communications Security Establishment (CSE), and New Zealand's Government Communications Security Bureau (GCSB).

### 3.3 ECHELON - 1999 and beyond

British journalist, Duncan Campbell, was the first person to publicly report the existence of ECHELON in a 1988 article in the *New Statesman* magazine.

The ECHELON system is a part of the UKUSA system and, unlike other spy systems developed during the Cold War, it was and is primarily designed for non-military facilities such as governments, bureaucracies, non-governmental organisations and businesses in virtually every country. According to Campbell there is a only a thin fine line of distinction between intelligence gathering and commercial espionage.

The ECHELON system indiscriminately intercepts vast amounts of communication signals and then siphons out matter considered valuable using artificial intelligence aids to find key words. It intercepts most of the world phone calls (using Intelsat satellites), e-mail, and telex messages. Most of the Internet traffic, whether satellite-based or not, runs through the US Internet backbones. This makes NSA's interception easier. Further, their activities include the use of specially built nuclear submarines to tap underwater cables around the world and not only those that pass through the US backbones.

Computers in stations around the globe, known as "Dictionaries", are interconnected with each other and to form an integrated system with the headquarters of the NSA as its centre. The intercepted messages pass into "Dictionaries" computers making them available over the UKUSA Internet network which is the equivalent of a "spy Internet" for UKUSA members.

According to CovertAction Quarterly magazine (<http://mediafilter.org/caq>) NSA pushed GCSB into contributing to a project targeting Japanese embassy communications and, from then, on all five UKUSA members were responsible for monitoring diplomatic cables of all Japanese posts within the range of each member country all over the globe.

#### 3.3.1 Silence Broken by New Zealand

In the late 1980s there were more than 50 people in New Zealand who were working or had worked in intelligence (and related fields) agreed to be interviewed. They had decided that these secrets had been too secret for too long and needed to be exposed. One of the most important discoveries from the interview revelations was the identification of ECHELON. Host countries never see most of the intelligence gathered by ECHELON. This means that whenever

the "Dictionary" encounters a message containing one of those agency's keyword, it automatically transmits the information directly to that agency.

### 3.3.2 Silence Broken by European Union

On the 12th August 1999 the Japan Times ran an article from the Los Angeles Times written by Simon Davies entitled "NSA has you in its sights and in its ears". The article said that NSA had established a surveillance capacity over the entire European communications network. Super computers known as ECHELON were capable of scanning vast areas of communications throughout Europe.

Two reports have been made to the EU Parliament so far, about ECHELON. The reports stated that all e-mail, telephone and fax communications within Europe were routinely intercepted by the NSA transferring all target information from the European mainland via the strategic hub in London, then passing to the crucial hub at Menwith Hill (England) and from there by satellite to Fort Meade in Maryland, Virginia USA.

The first of these reports to the EU parliament, *An Appraisal of Technologies of Political Control*, (<http://cryptome.org/stoa-atpc.htm>) was written on behalf of a research unit of the EU Department for Scientific and Technological Option Assessment (STOA) by Steve Wright, an analyst with the Omega Foundation, based in Manchester. It was sent to the Civil Liberties and Interior Committee, European parliament on 6 January 1998 and it asserts that the NSA was conducting its commercial espionage activities. It claimed that the NSA has been routinely intercepting sensitive traffic relating to bids, takeovers, mergers, investments and tender offers, all being of economic benefit to the US Parliamentarians in Germany, Norway, Denmark, Holland and Sweden subsequently raised questions about this matter.

The second report, *Interception Capabilities 2000*, ([http://www.iptvreports.mcmail.com/interception\\_capabilities\\_2000.htm](http://www.iptvreports.mcmail.com/interception_capabilities_2000.htm)) was commissioned in May 1999 and was sent to the EU Parliament's Science and Technology Options Assessment Panel (STOP). It describes the technical specifications of the ECHELON intercepting system. The report revealed details of a secret plan to create a seamless web of telecommunications surveillance across all national boundaries. It is known as the International Law Enforcement Telecommunications Seminar.

A certain number of US people also expressed their concerns over their national privacy rights. The House of Representatives, Permanent Select Committee on Intelligence, has ordered the NSA to hand over documents relating to ECHELON. The NSA has for the first time in the history refused claiming attorney-client privilege. This has made a US parliamentarian, Bob Barr, a member of House of Representatives, voice his concern about potential breach of constitutional privacy rights. He introduced an amendment to the fiscal 2000 Intelligence Authorisation Act requiring the directors of the CIA, the NSA and the Attorney General to submit

a report outlining the legal standards employed within ECHELON, in order to safeguard the privacy rights of US citizens.

### 3.3.3 Silence Broken by Australia

In Australia, the Director of the DSD (Defence Signals Directorate), Martin Brady, officially admitted in his letter to Channel Nine's TV program the existence of the UKUSA Agreement. This was to make Australia the first country of the five to break rank. The program also reported about an article entitled "Careful, they might hear you" by Duncan Campbell.

An ultra-modern intelligence base at Kojarena near Geraldton in Western Australia was built in the early 1990s. There are four satellite tracking dishes designed to intercept Indian and Pacific Ocean communication satellites. Most of intercepted messages are sent automatically from its Dictionary computer to NSA without ever being seen or read in Australia. There are British and US personnel employed in key personal posts like at Pine Gap. The data collection specifications are to look for North Korean economic, diplomatic, military messages and data: Japanese Trade Ministry plans, and Pakistani nuclear weapons developments.

The Australian government's decision to be open about the UKUSA pact was motivated partly by the need to respond to the growing international concerns about their operations and also to assure Australian citizens that their privacy was under control and the activities of the UKUSA people was tightly supervised and strictly limited.

## 4. Conclusion

Until the end of the Cold War Washington complained of insufficient Japanese defence spending which had been held around one percent of Japan's GNP. Despite the fact that Japan contributed a large sum of money to finance the Gulf War, Washington's response was, too little, too late. Despite the fact that Japan's defence budget has declined slightly in the last two years, the provocative headlines such as "Japan Returns to Nationalism" in Time Magazine (16 August 1999) and "The Land of the Rising Gun" in Newsweek, March 29 (1999) appeared to have been attempting to negatively insinuate that Japan was returning to its historical past of the 1930s.

Because of the way Japan's relationship with US is set up it is almost impossible for Japan to be seen to do anything correctly. According to Professor Morris-Suzuki's statement in the Australian Senate Hearing, there has been an increasingly anti-American tone in the media and from the leading media analysts as well as Japanese intellectuals.

She also states that in Japan until about two years ago, there had been a lot of talk about internationalisation or "kokusaika": the intention is to open up markets, create a multicultural society and create closer links with other countries. But, according to Professor Morris-Suzuki, the new buzzword is "globalisation",

something that Japan sees as out of her control and something very threatening to traditional social structures.

Against this background it is not very easy to predict which way Japan is heading. In particular, her future is less clear since Japan has found out what the EU has found out about the world intelligence network, namely UKUSA (ECHELON) which is expressly intercepting world communications for its own economic advantage.

At official levels in Japan, either in public or private, nothing has ever been said much about UKUSA (ECHELON). However it is almost certainly the case that Japan has known of the existence of ECHELON and has already begun developing strategies to meet these new world developments.

It is understandable that the US should be ambivalent about Japan, on the one hand asking Japan to be more assertive on her own developments of military capabilities in co-operation with US, and on the other criticising Japan's military build-up, according to some US Japan watchers. Japan's relationships with China and Russia will remain a key to the way Japan develops her role in the world of the twenty-first century.

This paper began by asking certain questions and trying to find answers for them. In the process, somewhat more questions have been created than answers. I would be interested in hearing your responses to the questions I have presented here and of course your answers to them.

## Bibliography

*An Appraisal of Technologies of Political Control* written by Steve Wright and reported by the EU department for Scientific and Technological Option Assessment (STOA) to the Civil Liberties and Interior Committee, European parliament on 6 January 1998.

Bamford, James *The Puzzle Palace* Boston: Houghton Mifflin, 1982.

*Examination of developments in contemporary Japan and the implications for Australia* Monday, 24 May 1999 Canberra Senate, Foreign Affairs, Defence and Trade References Committee, Official Committee Hansard  
<http://www.aph.gov.au/hansard/senate/commtee/comsen.htm>

Hager, Nicky *Secret Power : New Zealand's Role in the International Spy Network*, Nelson, NZ: Craig Potton, 1996. ISBN 0-908802-35-8 [http://www.fas.org/irp/eprint/sp/sp\\_c2.htm](http://www.fas.org/irp/eprint/sp/sp_c2.htm)

*Interception Capabilities 2000*, report to the European Union Parliament commissioned 1999.  
<http://www.iptvreports.mcmail.com/ic2kreport.htm>

Richelson, Jeffrey T. and Ball, Desmond *The Ties that Bind* London: Unwin Hyman, 1990.

Richelson, Jeffrey T. *The U.S. Intelligence Community* 4th ed., West View, 1999.

Sunday, Nine Network Australia program *The World's Biggest Spy Secret*

reporter, Ross Coulthart ([http://sunday.ninemsn.com.au/inv\\_sleuth2.htm](http://sunday.ninemsn.com.au/inv_sleuth2.htm))

#### Web sites

Campaign for the Accountability of American Bases (CAAB)  
<http://www.gn.apc.org/cndyorks/caab/index.htm>

Campaign for Nuclear Disarmament  
<http://www.gn.apc.org/cndyorks/mhs/index.htm>

Codename: ECHELON <http://www.qainfo.se/~lb/echelon.htm>

Covert Action Quarterly "Exposing the global surveillance system"  
<http://caq.com/CAQ/CAQ59GlobalSnoop.html>

Electronic Privacy Information Center  
<http://www.privacy.org>

Echelonwatch (ACLU - The American Civil Liberties Union)  
<http://www.aclu.org/echelonwatch/index.html>

European Parliament - an appraisal of the technologies for political control  
[http://www.icdc.com/~paulwof/iu\\_stoa\\_2.htm](http://www.icdc.com/~paulwof/iu_stoa_2.htm)  
<http://cryptome.org/stoa-atpc.htm>

Interception Capabilities 2000  
[http://www.iptvreports.mcmail.com/interception\\_capabilities\\_2000.htm](http://www.iptvreports.mcmail.com/interception_capabilities_2000.htm)

London Sunday Times Spy Station F83: Cracking the Menwith Codes 31/5/98  
<http://www.icdc.com/~paulwolf/lontimes.htm>

Paul Wolf's ECHELON links  
<http://www.icdc.com/~paulwolf/echelon.htm>

Privacy International <http://www.privacyinternational.org>

QA Information Security AB  
<http://www.qainfo.se/~lb/echelon.htm>

Statewatch Magazine EU and FBI Launch Global Surveillance System 2/97  
[http://www.privacy.org/pi/issues/tapping/statewatch\\_tap\\_297.html](http://www.privacy.org/pi/issues/tapping/statewatch_tap_297.html)

The UKUSA Community  
<http://watserv1.uwaterloo.ca/~brobinso/cseukusa.html>

For more references on the topic see: <http://www.qainfo.se/~lb/echelon.htm>