

## The Men Who Knew Too Much? NSA Wiretapping Whistleblowers Found Dead in Italy and Greece

**Adamo Bove and Costas Tsalikidis: Both uncovered a secret bugging system and both met untimely ends.**

Was That Just A Coincidence? And Who Made Your Cell Phone?

Posted By [Joseph Cannon](#) On 22nd August 2006 @ 19:23 In [NSA](#), [Whistleblowers](#) | [Comments Disabled](#)

*Guest blogged by [Joseph Cannon](#) <sup>[1]</sup>*

Is someone murdering people who know too much about NSA wiretapping overseas?

Two whistleblowers --- one in Italy, one in Greece --- uncovered a secret bugging system installed in cell phones around the world. Both met with untimely ends. The resultant scandals have received little press in the United States, despite the profound implications for American critics of the Bush administration.

Last month, Italian telecommunications security expert **Adamo Bove** either leapt or was pushed from a freeway overpass; he left no note and had no history of depression. Last year (March, 2005), Greek telecommunications expert **Costas Tsalikidis** met with a similarly enigmatic end. Both had uncovered American attempts to eavesdrop on government officials, anti-war activists, and private businessmen.

The Bove case relates to the long-standing controversy over the CIA's kidnapping of cleric Abu Omar, who was flown to Egypt and tortured. The post-Berlusconi government of Italy is attempting to arrest and try all of the CIA personnel involved. Bove used mobile phone records to trace more than two dozen American agents.

Bove had also revealed that his employer, [Telecom Italia](#) <sup>[2]</sup>, had allowed illegal "spyware" --- undetectable wiretaps --- to infest Italy's largest communications system. His testimony helped to uncover the [unsettling relationship](#) <sup>[3]</sup> between SISMI chief Marco Mancini and Telecom Italia head Giuliano Tavaroli. (Mancini, recently arrested by Italian investigators, has also come under some suspicion for his possible role in the strange affair of [Major General Nicola Calipari](#) <sup>[4]</sup>, killed by American troops in Iraq.) In the 1990s, Bove had received wide praise for helping to secure convictions of [two bosses in the Camorra](#) <sup>[5]</sup>, Naples' answer to the Sicilian Mafia.

The case of Costas Tsalikidis --- an engineer for Vodaphone, Greece's top telecommunications firm --- offers a similar picture. Tsalikidis discovered an extraordinarily sophisticated piece of spyware within his company's network. The Prime Minister and other top officials were [targeted](#), <sup>[6]</sup> along with Greek military officers, anti-war activists, various business figures --- and a cell phone within the American embassy itself. [This page](#) <sup>[7]</sup> gives a full list of the targets, very few of whom could be considered as having even a remote connection to terrorism.

As investigative journalists Paolo Pontoniere and Jeffrey Klein report:

The Vodaphone eavesdropping was transmitted in real time via four antennae located near the U.S. embassy in Athens, according to an 11-month Greek government investigation. Some of these transmissions were sent to a phone in Laurel, Md., near America's National Security Agency.

According to Ta Nea, a Greek newspaper, Vodafone's CEO privately told the Greek government that the bugging culprits were "U.S. agents." Because Greece's prime minister feared domestic protests and a diplomatic war with the United States, he ordered the Vodafone CEO to withhold this conclusion from his own authorities investigating the case.

The CEO of Vodaphone in Greece, George Koronias, has --- like Giuliano Tavaroli, his Italian counterpart --- come under the suspicion of having a hidden [relationship with American and British intelligence](#) <sup>[8]</sup>. At least three Vodafone communications hubs ([one expert](#) <sup>[9]</sup> says the number could be as high as 22) were compromised by the eavesdropping technology. Koronias had reported only two of these bugs, and had failed to alert a watchdog agency of the discovery of further listening devices.

[Vodafone](#) <sup>[10]</sup> is a British company, comparable to Sprint in the United States. Testifying before a Greek parliamentary committee, Koronias insisted that no-one in the U.K. could have had any connection to the ultra-sophisticated spyware.

'Only Ericsson's staff could have set up such a device,' he said. Ericsson furiously countered that Vodafone not only knew about the illegal software but had activated it at the request of British

intelligence agents.

More on [Ericsson's official response](#) <sup>[11]</sup>:

Ericsson, the company that produces the software used by Vodafone, issued an announcement clarifying that two types of software were employed for tapping the phone conversations.

The first one employed legally had been developed by Ericsson and had been installed in Vodafone, yet it was not activated. The second software, which was of unknown origins, namely it had not been developed by Ericsson, had been illegally installed in Vodafone's system to activate the legal software and erase the traces of the phone-tapping.

This is, by any measure, a troubling admission --- especially since Ericsson manufactures many mobile phones used in the United States. Vodafone insists they were never informed of this "feature" in Ericsson phones, although Ericsson executive Bill Zikou has testified that the [company disclosed the truth](#) <sup>[12]</sup> via its sales force and instruction manuals.

American security expert John Brady Kiesling reveals further details about the bugging devices in Ericsson cell phones:

Built into the Ericsson (Sweden) software that runs the Vodafone (UK-owned) mobile telephony network switching system in Greece, and similar GSM service providers around the world, is a little-known "Legal Interception" software package designed to be used by law enforcement authorities. This software allows incoming and outgoing conversations from allegedly up to 5000-6000 mobile phone numbers to be recorded, on presentation of a valid judicial warrant. [A friend in telecoms claims governments require that telephone companies give law enforcement authorities the capability to monitor up to 5% of active calls as one precondition for an operating license]. However, to unlock and use the eavesdropping package, the company must pay Ericsson a hefty fee (allegedly four million euros). The Greek government allegedly refused to pay this fee, despite its desire for wiretapping capability during the 2004 Athens Summer Olympics. One reason was that a clear legal basis for such eavesdropping was not yet in place.

Apparently someone persuaded a Vodafone or Ericsson employee with access to the switching network to install a software parasite in at least four and possibly more of the 22 call management centers that Vodafone operates in Greece.

The family of Costas Tsalikidis, the whistleblower who was found hanged in his apartment, does not accept the verdict of suicide. Neither does his fiancée. The Greek press has hinted at [further skulduggery](#) <sup>[13]</sup>:

The prosecutor also visited the lawyer of Taslikidis' family, Themistoklis Sofos, who announced that his clients will be filing a lawsuit against unknown parties for embezzlement and falsification of documents pertaining to the deceased's emails. In addition, they will subpoena all those who participated in the much-publicised meeting just before the revelation of the wiretappings; a meeting Vodafone denies ever having taken place.

Perhaps most disturbing of all, Vodafone had eliminated the spyware from its system before Greek intelligence could conduct an examination. Greek spy chief Ioannis Korantis testified that this move amounted to [destruction of evidence](#) <sup>[14]</sup>.

Are Ericsson cell phones the only ones with the built-in spy technology? We can't be sure. But one thing *is* certain: When the fellow on TV asks "Can you hear me now?", the person he's addressing may not be the only one who can say yes.

---

Article printed from The BRAD BLOG: <http://www.bradblog.com>

URL to article: <http://www.bradblog.com/?p=3305>

URLs in this post:

[1] Joseph Cannon: <http://cannonfire.blogspot.com>

[2] Telecom Italia: <http://www.telecomitalia.com/>

[3] unsettling relationship:

[http://www.corriere.it/Primo\\_Piano/Cronache/2006/07\\_Luglio/23/biondani.html](http://www.corriere.it/Primo_Piano/Cronache/2006/07_Luglio/23/biondani.html)

[4] Major General Nicola Calipari:

<http://www.globalresearch.ca/index.php?context=viewArticle&code=BOH20050925&articleId=1003>

[5] two bosses in the Camorra:

<http://www.eurotrib.com/?op=displaystory;sid=2006/7/24/41816/5846>

[6] targeted,: [http://www.spy.org.uk/spyblog/2006/02/vodafone\\_greece\\_hacked\\_is\\_voda.html](http://www.spy.org.uk/spyblog/2006/02/vodafone_greece_hacked_is_voda.html)

[7] This page: <http://news.ert.gr/en/8/14825.asp>

[8] relationship with American and British intelligence:

<http://observer.guardian.co.uk/business/story/0,,1728795,00.html>

[9] one expert: [http://www.bradykiesling.com/vodafone\\_scandal.htm](http://www.bradykiesling.com/vodafone_scandal.htm)

[10] Vodafone:

[http://online.vodafone.co.uk/dispatch/Portal/appmanager/vodafone/wrp?\\_nfpb=true&#038;\\_pageLabel=Page\\_ProductDetails&pageID=BS\\_0701&Content\\_Id=VF004404#](http://online.vodafone.co.uk/dispatch/Portal/appmanager/vodafone/wrp?_nfpb=true&#038;_pageLabel=Page_ProductDetails&pageID=BS_0701&Content_Id=VF004404#)

[11] Ericsson's official response: <http://news.ert.gr/en/8/14957.asp>

[12] company disclosed the truth:

[http://www.schneier.com/blog/archives/2006/06/greek\\_wiretappi\\_1.html](http://www.schneier.com/blog/archives/2006/06/greek_wiretappi_1.html)

[13] further skullduggery: <http://news.ert.gr/en/8/14957.asp>

[14] destruction of evidence:

[http://www.schneier.com/blog/archives/2006/06/greek\\_wiretappi\\_1.html](http://www.schneier.com/blog/archives/2006/06/greek_wiretappi_1.html)

Click [here](#) to print.