# Illegal Wiretapping

## Abstract

Beginning the 9/11 attack, the U.S. government’s need to protect its citizens against possible future acts of terrorism increased, while the need to detect possible terrorist connections became even more pronounced. Consequently, a presidential directive in 2002 allowed the National Security Agency to start using spying, wiretapping and surveillance measures to detect possible terrorist linked communications both within the U.S. and internationally. Following the directive, the National Security Agency embarked on the surveillance of both telephone communication and internet e-mail communications both communicated domestically within the U.S. and those communicated internationally between individuals within the U.S. and international recipients. The secretive communication monitoring of the U.S. government has been termed illegal, resulting in court battles that have effectively suspended such government surveillance programs and even issued more restrictive measures against the secret surveillance on the citizens. The need to avoid the secretive surveillance has led to the development of counter-surveillance measures, one of which is the IMSI Catcher Detector, a device that is helping to identify possible communication interceptions and notify the mobile phone users when they are being monitored or their communications intercepted.

## Illegal wiretapping

The issue of illegal wiretapping by the U.S. government over its citizens has become a major debate. He spying of the United Sates citizen by the government started immediately after the 9/11 attacks, when it became increasingly important for the government to apply counterterrorism measures that would help to thwart any future terrorist attacks before they actually happened. Thus, reports have emerged that President Bush allowed the National Security Agency of the United States to start spying on the citizens through wiretapping and listening to phone conversations, both without the knowledge of the citizens or the authorization of the courts (Albies, 2007). The government eavesdropping of the citizen’s phone conversation was meant to search for any possible evidence of terrorist activities. The monitoring the conversations was not only limited to the phone calls, but the United States government has extended its spying on other forms of electronic communication both within and outside f the United States. Thus, starting the year 2002, the United States has been spying on international phone calls and international e-mail communications between individuals within the United States communicating tom other individuals internationally, as well as the internal communications among the people inside the United States (Albies, 2007). The National Security Agency has sought the courts authorization t undertake domestic surveillance in different occasions, but the post 9/11 attack saw the issuance of a presidential order that allowed the agency to proceed with both the domestic and international communication surveillance without the first seeking the courts authorization.

The presidential directive authorizing the spying of the United States citizen by the National Security Agency has raised major concerns, considering the fact that the agency has historically played the role of international communications surveillance (Albies, 2007). Therefore, the spying of the National Security Agency over the American Citizens domestically has raised major legal issues, related to the violation of the fundamental rights to personal privacy for the citizens. The issue has ended up in the courts, with the courts finding that the government has been violating the constitutional rights of the American Citizens by illegally wiretapping and conducting other forms of illegal surveillance of the citizen’s communication, both without the knowledge of the courts or the citizens (Albies, 2007). The outcome of the court battles over the illegality of the government surveillance of the citizens’ communication both domestically and internationally has led to the suspension of such operations and the imposition of more restrictions on the government’s ability to do so (Albies, 2007).

 However, the government has held that such secret monitoring and surveillance of the citizen’s communication is relevant, to enable the government to access, disclose and even prevent against any possible security threats to the United States. Further, the defenders of the government secret surveillance have held that it is a necessary security practice, aimed at enabling the government to aid the government in disrupting possible terrorist attacks and in turn safeguard the United States citizens from the eminent threat of attacks posed by the terrorists (Albies, 2007). The government and the national security agencies have held that the surveillance was only limited to the communications that were suspected of having possible terrorist or other national security risks, but did not broadly cover the eavesdropping all of the United States communications (Albies, 2007). The government held that where it was necessary to spy on, undertake surveillance or use any other such measures on domestic communication in a broader and expanded manner, the government had always sought the authorization of the courts.

On the contrary, the civil rights groups have held that the present safeguards are adequate to enable the government to use intelligence services to access any possible information on planned terrorist activities, without necessarily eavesdropping on the citizen’s own communication. Additionally, the government faulted the media and the civil rights groups for publishing sensitive security information, which could jeopardize the security operations of the United States agencies, by alerting the would-be terrorists of their possible monitoring (Albies, 2007). The available information has indicated that the government has been eavesdropping on communication of the citizens in numbers of hundreds at a time, which means that several thousand people’s communication had been tapped into and listened by the government in the entire course during which the program was ongoing.

Nevertheless, while the governments spying on the citizen’s communication has been faulted for violating the citizen’s rights, it has also been associated with successful identification and prevention of planned terrorist activities in different parts of the United States. Additionally, reports have also indicated that several terrorist suspects have effectively been arrested and confessed to their linkage with the terrorist groups (Albies, 2007). Consequently, such terrorists have been arraigned in courts and charged accordingly.

In response to the threat of wiretapping and illegal surveillance by the government, several devices and sophisticated technologies have been developed for use as countermeasures protections against illegal wiretapping, spying and surveillance. One of such devices that is being applied as a spying and wiretapping countermeasure to help individuals now when they are being tracked, is the IMSI Catcher Detector (Steig, Aarnes, DoHai & Nguyen, 2016). This technological device has been developed in the form of a simple briefcase box, which detects any connected base stations or even mobile antennas that are connected to a mobile phone network to incept the mobile phone communication (Steig, Aarnes, DoHai & Nguyen, 2016).

The device has been devices such that it notifies the mobile phone user when the mobile phone connection either through phone calls or SMS text has been intercepted, when the ciphering to the mobile has been turned off or even when the mobile phone device is being tracked (Steig, Aarnes, DoHai & Nguyen, 2016). The IMSI Catcher Detector warns the mobile phone user when any form of interception to their communication has occurred in between the mobile phone subscriber and the mobile phone network provider. The device has been developed such that it is able to detect any remote IMSI catcher tower or base that is within the proximity of the mobile phone user, and notify the mobile phone user of the presence and the location of the remote communication interceptor (Steig, Aarnes, DoHai & Nguyen, 2016).

Additionally, he deice has also been developed such that it is able to detect the silent SMS-Sim based trackers, which are often used to detect the mobile phone location through a communication of silent messages between the IMSI Catcher and the mobile network service provider, without the knowledge of the mobile phone user (Steig, Aarnes, DoHai & Nguyen, 2016). In addition, the IMSI Catcher Detector device also provides a safe internet connection for the phone through either Wi-Fi or Wi-max, to ensure that the internet connection and communication of the mobile phone user is not detected or intercepted (Steig, Aarnes, DoHai & Nguyen, 2016).

## References

Albies, A. (2007). Ninth Circuit Rejects Bush's Attempt to Dismiss Challenge to Illegal Wiretapping. *Guild Notes*, *33*(4),1-9.

Steig, S., Aarnes, A., DoHai, T. & Nguyen, T. (2016). A Network Based IMSI Catcher Detection. *IEEE Journal.*