

<https://voices.revealdigital.org/?a=d&d=BFBJFGD19740906.1.5&e=-----en-20--1--txt-txIN-----1>

Berkeley Barb, Volume 20, issue 8 (473), September 6-12, 1974

INTELLIGENCE REPORT

FEDERAL PHONE PHREAKS

by Winslow Peck (Winslow Peck is a former intelligence analyst for the National Security Agency.) (Winslow Peck is a pseudonym for Perry Fellwock: https://en.wikipedia.org/wiki/Perry_Fellwock)

Are you a freak talking on the telephone with friends in Amsterdam? Well, don't ask them to send you any of the Afghanistan hash that is semi-legal there. Are you a businessman in Los Angeles preparing to telex business information to your home office in Tokyo? Well, be careful that the information you send won't serve your competitors. Are you a radical calling friends in Latin America to investigate the direction of their movement? Well, don't use words like "Marx" or "revolution." And of course, if you're a diplomat we don't need to warn you about being careful with your overseas communications. Information leaked to Intelligence Report by reliable sources indicates that all of the aforementioned groups, and others, are being systematically monitored by the United States government when they communicate overseas.

This information elaborates allegations made by Ramparts magazine in August 1971, that the super secret National Security Agency routinely monitors the transoceanic communications of aliens and citizens living in the United States. Although this activity by NSA has been operational for years, the programs have apparently gained a new emphasis, and are now a major domestic operation of the NSA.

The National Security Agency was formed in 1952 to monitor foreign communications, break codes and ciphers, and to provide communications security for the US government. Since its creation, NSA has grown to become the largest and most secretive of all US intelligence agencies. Its budget exceeds even that of the CIA. NSA maintains a global network of monitoring stations on land, at sea, in the air, and, most recently, orbiting the earth. These stations systematically probe the military, diplomatic, and commercial communications of adversaries and allies alike. Virtually no means of telecommunicating escapes the ears of NSA.

The NSA coordinates a vast complex of US and Allied civilian and military agencies known as the "SIGINT and/or COMINT Community." SIGINT stands for Signals Intelligence, while COMINT-a division of SIGINT-stands for Communications Intelligence. The SIGINT Community is the most secret of all Western intelligence groupings, maintaining its own installations, transportation facilities, communications systems, cadre that are highly technically oriented, and its own security measures. These security measures include a system of security classifications ' far more complex and involuted than the simple 'confidential', 'secret', and 'top secret' used by other agencies of government.

In the United States, the SIGINT Community includes the NSA, with its headquarters at Ft. Meade, Md., and the semi-autonomous service cryptographic agencies -- the Army Security Agency (ASA), headquartered at Arlington Hall Station, Virginia; the Naval Security Group (NSG) headquartered at Arlington Hall Station, Virginia; the Naval Security Group (NSG) headquartered at 3801 Nebraska Ave., NW, Washington DC; and the Air Force Security Service (AFSS), headquartered at Kelly Air Force Base in Texas. Others involved with the SIGINT Community include: the Special Security Offices (SSC) attached to certain military commands, other government agencies, certain universities, corporations involved in defense contracting, and US controlled transnational corporations. A brief listing of NSA activities over the years gives an indication of the broad scope of this SIGINT Community.

The Community monitors and locates every airplane and ship in the world of military or economic importance to US foreign policy. The SIGINT Community's airborne monitoring platforms helped locate Che Guevarra for the CIA team that assassinated him. This technique was further refined for use in the Indochina War, where the SIGINT Community provided the location of NLF units for US and Vietnamese bombers. The Community monitors the conversations of Soviet Cosmonauts with their ground controllers, as well as the signals from foreign satellites. The Community has monitored communications during countless coup d'etats in Latin America and elsewhere.

Spy planes, ships -- like the Pueblo -- and even satellites are used to penetrate the territories of foreign countries. Even the United State's closest allies in Asia and Europe have been monitored by the NSA. And when the National Security Agency, with its vast numbers of scientists, computers, and advanced electronic gizmos, is unable to break the one-time usage diplomatic codes of foreign governments, it simply steals them from Embassies and military installations. In Indochina, ASA "Alpha Teams" were charged with stealing NLF codes. Investigations into the Watergate affair shed some light on NSA's domestic activities related to code-stealing.

The now famous 1970 Huston Plan for domestic surveillance was classified with super-secret NSA security classifications. Under the plan, NSA would have received its first known legal authorization for internal security work. While the scope of this activity was not revealed by the Senate Select Committee, other documents released inadvertently revealed that the NSA may have been involved in the break-in of the Chilean Embassy by Cuban operatives, prior to both the Watergate burglary and the coup d'etat in Chile. At this time we can only speculate that the diplomatic codes of Salvadore Allende's Popular Unity government may have been taken at that time.

The monitoring of transoceanic telecommunications began as a part of NSA's duties to collect "Commercial Intelligence." In recent years, Commercial Intelligence has come to equal Diplomatic and Military Intelligence in importance to NSA. The telex communications of virtually all Corporations doing business overseas, especially those that are foreign controlled, are monitored. Besides being disseminated to government agencies that determine trade policy, this Commercial Intelligence is distributed to US corporations competing with foreign companies.

This Commercial Intelligence has played an important role in assuring US corporate hegemony over trade and monetary transactions. Often this information has been used by unusually unethical corporations to destroy their foreign competitors. Occasionally, NSA provides information on one US controlled corporation to another US controlled corporation. While this is not the official practice of NSA, it is still commonplace. Graft and bribery are not unknown in the world of Commercial Intelligence. It has even been rumored that, on occasion, corrupt NSA officials have sold information on US corporations to foreign concerns. Many corporations have hired former NSA operatives to set up private SIGINT operations.

Almost all of the transnational oil corporations have their own SIGINT operations. In the late 1960's, the monitoring of transoceanic telex communications gave birth to monitoring telephone communications. Today, almost all overseas telephone communications are monitored, primarily by the ASA and the NSG. However, not all communications are recorded, analyzed or disseminated to consumers. Until recently, this depended upon who was calling whom, and to what country the call was placed to. Now computers are handling this monitoring, and are much more selective in their work, listening in on the actual conversations for certain key words which indicate that radical activities or drug trafficking may be the subject of the conversation.

Thus, if words like "marijuana", "hash", "cocain", or "dope" are mentioned in an overseas phone call, that particular conversation will be taped, and find its way to Federal Drug Enforcement authorities. Likewise, words like, "Marx", "Lenin", "Mao", "Castro", "revolution", "National Liberation", etc., also trigger the computers, and this information finds its way to the FBI, CIA, or appropriate agency. The computers begin working when the names of key individuals or the "jargon" of a variety of other activities is used. And it doesn't matter whether these words are used in context or are just said in an off hand manner.

The information received by Intelligence Report indicates that the "state of the art" of computer monitoring of telephone conversations is not perfect. Conversations are garbled for a variety of reasons, but NSA's technique is continually improving. Since the advent of the world monetary crisis, a greater emphasis has been placed on commercial intelligence. Likewise, the recent successes by revolutionary groups in Africa and Asia have resulted in a new emphasis being placed on calls to these areas.

So-called "terrorist" actions in various parts of the world have also served to have NSA place a greater emphasis on monitoring overseas phone conversations. By stretching the imagination, some legitimacy could be found in the actions of the National Security Agency, but the probabilities for abuse in the political and commercial arenas have a solid basis in reality, not to mention the possibilities of abuse through human mechanical error. So the next time you talk on the telephone overseas, be careful. Big Brother is listening to you.