

12. Instead--as NSA's foreign intelligence targets presumably know well--NSA must focus its interception activities on those particular communications lines, channels, links or systems which yield the highest proportion of useful foreign intelligence information.

What foreign government officials do not know, however, is which of the vast number of radio communications NSA attempt to intercept, which are intercepted, and, of those that are intercepted, which yield to NSA processing methods and techniques. It is the protection of this critical information that is at the heart of the instant case.

13. The continued efficacy of NSA's vital intelligence activities requires that the lines, channels, links and systems actually monitored remain unidentified. If a foreign government obtains sufficient reason to suspect that NSA is able to

intercept and process that government's radio communications, that government would be expected to take immediate steps to defeat that capability. This can be accomplished in a number of ways. A foreign government might shift to communications links that U.S. cannot intercept. It may also choose to use alternate methods of communications. The foreign governments may possess the technical capability to either upgrade or initiate cryptography to secure its communications. Finally, a communication channel believed to be targeted by NSA can be used by a foreign government to pass misleading information.

14. If a foreign power is successful in defeating an interception operation, all of the intelligence from that source is lost unless and until NSA can establish a new and equivalent intercept. The risk involved is great. The