

Clipper II was an Orwellian nightmare come true, a practical impossibility, or a huge joke at the taxpayers' expense—take your pick. It was designed in response to a fear of the U.S. government that unbreakable codes would make intercept-intelligence impractical. And really, they had a point, but their solution was so draconian that it was doomed to failure from the start.

The Clipper II chip—like the original Clipper chip before it—was a chip designed to handle strong encryption. If it was made mandatory (which the government wanted), everyone would have to use it. And the encryption was guaranteed secure. Absolutely unbreakable.

Except that the chip contained a set of keys just for the government, just in case. If they needed to, they could look up the key for a particular chip, get a wiretap permit, and decrypt any messages that were sent using the chip. They would thereby bring to justice (they said) all kinds of Mafiosos, drug dealers, money launderers, and other lowlifes.

2000