Preface to the First Edition

In the spring of 1993, the White House announced an unprecedented plan for both promoting and controlling the use of secret codes to keep communications private. The plan, formally called *key escrow* but popularly known as "Clipper" after its star component, the Clipper chip, was to adopt a new federal standard for encryption, a standard that would ensure that the government could always read encrypted messages if it chose.

The Clipper proposal was met by a storm of protest. It was criticized by some as an outrageous violation of civil liberties, by some because the standard could only be implemented in hardware, and by still others on a wide variety of grounds. Despite the opposition, Clipper seemed, in a sense, to have won. After a mandatory public comment period, which produced two letters in favor and 300 against, the standard was adopted. In a more fundamental sense, however, the Clipper program seemed to have lost. Aside from the 9000 telephone security devices that the FBI purchased in an attempt to seed the market, very little Clipper-based equipment has been built.

The Clipper debate proved to be the opening engagement in an ongoing battle about the right to use encryption. Having tried to use its buying power and standards-making authority to impose key escrow, the government turned to the only other non-legislative tool available: export control.

The United States has approximately 5% of the world's population. In light of this, it is not surprising that, although the country's share of the world economy is way out of proportion to its population, most major

US corporations sell more than half their products in other countries. This makes the larger part of their markets subject to export-control laws.

It is also true that a key competitive strategy in modern business is to eliminate unnecessary versions of products. Duplication can be particularly costly in high-technology products such as computer software. If US corporations are unable to export the same versions of their products that they sell at home, the effect is a significant increase in costs. The government's subsequent attempts to achieve key escrow have turned on this fact.

In January 1997, the administration began to permit the export of some unescrowed encryption products for 2 years to companies that submit detailed plans for developing escrowed products within that time.

Why is all this important? Why should anyone who is not in the cryptography business be concerned about regulation of the export of cryptographic equipment? The answer lies in the rush to put society online.

For most of human history, most communication between individuals was conducted face to face. For a few thousand years some has been conducted in writing, but this is in many respects a poor substitute. Letters took weeks, months, or even years to travel long distances. The fact that a letter might be opened en route and thus was less private than a whisper was just one of many limitations.

For a little more than 100 years, some human communication has been carried by electronic media, particularly the telephone. This has brought to remote communication an immediacy that approximates face-to-face contact. The quality of telecommunication continues to improve, and the portion of relationships in which telecommunication is the primary mode of communication continues to increase. We are moving the fabric of our society into electronic channels as quickly as we can.

When telecommunication was merely an adjunct to physical communication, it was possible to hedge about privacy. When two people meet frequently as well as talking regularly by telephone, they can reserve indiscreet remarks for their face-to-face meetings. But as telecommunication becomes more the rule than the exception, this becomes less feasible. In a future society (which may not be far off) in which most communication is telecommunication and many close relationships are between people

who never meet in person, it becomes impossible. If people are to enjoy the same effortless privacy in the future that they enjoyed in the past, the means to protect that privacy must be built into their communication systems.

Were the discussion to stop here, the conclusion would be self-evident: we should design all our communication systems to guarantee confidentiality. Personal privacy, however, is not everyone's paramount concern. There are powerful elements of society—police and military organizations—that make use of intercepted communications in what they consider the protection of public safety. These groups view the ready availability of strong cryptography as threatening their ability to perform their functions. Moreover, these once-distinct government activities are drawing closer together in response to the perceived threat of international terrorism. Not surprisingly, this emerging coalition sees individual access to cryptography more as a curse than a blessing.

We see no simple resolution of this conflict. The debate so far has been largely an argument among partisans, all anxious to bias the evidence in their own favor. This is also a field with an extraordinary number of secrets. Neither the police and the spies, who oppose widespread cryptography, nor the big corporations, which support it, are the most open and forthcoming of society's institutions.

In this book, we attempt to lift enough veils to permit the reader to develop an informed opinion on the subject. We examine the social function of privacy: how it underlies other aspects of a free and democratic society and what happens when it is lost. We explore how intelligence and law-enforcement organizations intercept communications, what use they make of them, and what problems cryptography might create. We also describe how cryptography works and how it can be used to protect the secrets of both individuals and organizations.

If we have succeeded, the reader will come away from our book with a new understanding of an issue that, despite the publicity it has received in the past few years, has seemed mysterious and confusing.