aligned, the numeric keypad is right-aligned), and ergonomists have studied how this affects wrist postures that are associated with musculoskeletal disorders, such as carpal tunnel syndrome. Particularly in the 1990s there was an explosion in the range of alternative keyboard designs that are available. Many designs split and angle the alphabetic keys for the left and right hands to reduce ulnar deviation, according to an early design developed by Klockenberg in 1926. However, research studies generally have not found significant postural improvements with these designs. Other keyboards completely split the two halves of the alphabetic keys; some dish the keys rather than step the keys to better fit the curvature of the fingers as they flex; and some orient the keyboard halves vertically to eliminate wrist pronation. These completely split keyboards generally produce beneficial postural improvements. The problem with all split keyboards is that non-touch typists cannot easily use them, so the rectangular keyboard remains the most common design.

FURTHER READING

Baber, Christopher. *Beyond the Desktop: Designing and Using Interaction Devices.* San Diego, Calif.: Academic Press, 1996.

Dvorak, August, Nellie L. Merrick, William L. Dealey, and Gertrude C. Ford. *Typewriting Behavior: Psychology Applied to Teaching and Learning Typewriting.* Boulder, Colo.: Freelance Communications, 1936.

Kroemer, K., and H. Eberhard. "Human Engineering the Keyboard." *Human Factors,* Vol. 14, No. 1, 1972, pp. 51–63.

Liebowitz, S. J., and Stephen E. Margolis. "The Fable of the Keys." *Journal of Law and Economics,* Vol. 33, 1990, pp. 1–27.

Noyes, Jan. "The QWERTY Keyboard: A Review." *International Journal of Man-Machine Studies,* Vol. 18, No. 31, 1983, pp. 265–328.

—Alan Hedge

Key Escrow Encryption

For law enforcement agencies, a disadvantage of the wide availability of computers is that encoded communication cannot be monitored as easily as telephone lines. In the United States, government agencies have sought to prevent the use of cryptographic schemes that cannot be broken while promoting more law-enforcement-friendly types of **encryption**, such as key escrow.

The most prominent example of key escrow encryption is the **Clipper chip**, announced in 1993. The Clipper proposal detailed hardware that would allow the government to decode private messages. Such schemes, which allow a third party to decode encrypted communication between a sender and a receiver, rely on the existence of a master key for the encoding chip. This is called *key recovery* or *key escrow*, since in the case of the Clipper chip, a master key is kept "in escrow" (entrusted to) and can be released to law enforcement agencies when needed.

Systems with an *escrow agent* require that a session's data be sent along with the keys used for the session, encrypted with the master key. The owner of the master key can recover the session keys, and through them, also the plain text. It is possible to distribute parts of the master keys—two parts, in the case of the Clipper chip—between different agents so that they have to collude in order to decrypt the private messages. Nevertheless, the public outcry after the initial presentation of the Clipper chip led to national debate about security and privacy in the electronic age.

A report released to the European Parliament in 1999 made clear that some European countries were concerned about the decryption **back doors** installed in U.S. **hardware**. The report stated that the National Security Agency had installed "sniffer" **software** to collect traffic at major Internet traffic points. The report also speculated that some information about economic rivals had been stolen from the Internet and had been given to U.S. companies. Even if such reports are inaccurate, they show that it is very difficult to define who should be the trusted party in a global economic system.

FURTHER READING

Denning, Dorothy E., and Dennis K. Branstad. "A Taxonomy for Key Escrow Encryption Systems." *Communications of the ACM,* Vol. 39, No. 3, 1996, pp. 34–40.

Gurak, Laura J. *Persuasion and Privacy in Cyberspace: The Online Protests over Lotus MarketPlace and the Clipper Chip.* New Haven, Conn.: Yale University Press, 1997.

—Raúl Rojas