- *Network and computer login security*—Other security measures, such as ID cards and passwords, can be copied or stolen, which is not likely with biometric security measures. Fingerprint readers, for example, are already available at moderate prices.
- *Web page security*—Biometric measures could add another layer of security to Web pages to guard against attacks and eliminate or reduce defacing (a kind of electronic graffiti). For example, a stock-trading Web site might require customers to log on with a fingerprint reader.
- *Voting*—Biometrics could be used to make sure people do not vote more than once, for example, and could be useful for authentication purposes in voting via the Internet.
- *Employee time clocks*—Biometrics could uniquely identify each employee and verify clock-in and clock-out times. This technology could also prevent one coworker from checking in for another.
- *Member identification in sports clubs*—Fingerprint scanners are used in some sport clubs to allow members admittance. This technology improves convenience and security.
- *Airport security and fast check-in*—Israeli airports have been using biometrics for this purpose for years. Ben Gurion International Airport in Tel Aviv has a frequent flyer's fast check-in system based on smart cards that store information on users' hand geometry. With this system, travelers can pass through check-in points in less than 20 seconds.[32]
- *Passports and highly secured government ID cards*—A biometrically authenticated passport or ID card can never be copied and used by an unauthorized person. Citizens of such countries as Germany, Canada, and the United States can apply for an ePass, a passport containing a chip that stores a digital photograph and fingerprints. Other biometric identifiers, such as iris scans, could be added. It is also being used to enter the U.S. at immigration kiosks.
- *Sporting events*—Germany used biometric technology at the 2004 Summer Olympic Games in Athens, Greece, to protect its athletes. NEC, Inc. created an ID card containing an athlete's fingerprints, which was used for secure access.
- *Cell phones and smart cards*—Biometrics can be used to prevent unauthorized access to cell phones and smart cards and prevent others from using them if they are lost or stolen. An example is Apple's iPhone, which uses a fingerprint sensor and face id scan.

The "Face Recognition Technology in Action" box highlights several potential real-life applications of face recognition technology.

Face Recognition Technology in Action

FINANCE | TECHNOLOGY IN SOCIETY | SOCIAL AND ETHICAL ISSUES


karelnoppe /shutterstock.com

Companies such as Apple, Google, Facebook, and Tesco are increasingly using face recognition technology for security and other purposes. Google uses it for image search of billions of photos that exist online to recognize its users. It is also used in Google Glass. Facebook uses it in order to identify its users and also for potential target marketing. Apple uses it to identify users of its devices.

According to Facebook, its facial recognition technology, DeepFace, demonstrated 97.25 percent accuracy as compared to 97.53 percent for a human recognizing a face among others—nearly identical results.[33]

The potential commercial market for this technology is huge. A woman standing by a digital ad display might suddenly see cosmetic items displayed, with directions to the nearest store that sells these items or a URL address. The system has recognized the potential customer as a female in her 20s and displayed potential sales items accordingly. The technology enables the system to tailor its messages to a particular person.

Kraft Foods Inc. and Adidas are planning to use face recognition technology to promote their products. A group of bar owners in Chicago are using face recognition technology to keep tabs on the male/female ratio and age mixes of their crowds.[34]

Face recognition technology as a biometric measure is fundamentally different than other biometric measures such as fingerprint or retina identification because an individual does not need to opt in to be recognized by the system. Any camera in a public place can take a picture of a person and recognize him or her with a high degree of accuracy. For that reason, security and privacy concerns are more challenging, and careful consideration must be given to this technology's potential use.[35]

Questions and Discussions

1. What are examples of three companies that are using face recognition technology for security and other purposes?
2. For which purpose a group of bar owners in Chicago are using face recognition? Do you see any ethical issues related to this type of use? Discuss.

5-4b Nonbiometric Security Measures

The three main nonbiometric security measures are callback modems, firewalls, and intrusion detection systems.

Callback Modems

A **callback modem** verifies whether a user's access is valid by logging the user off (after he or she attempts to connect to the network) and then calling the user back at a predetermined number. This method is useful in organizations with many employees who work off-site and who need to connect to the network from remote locations.

Firewalls

A **firewall** is a combination of hardware and software that acts as a filter or barrier between a private network and external computers or networks, including the Internet. A network administrator defines rules for access, and all other data transmissions are blocked. An effective firewall should protect data going from the network as well as data coming into the network. Exhibit 5.3 shows a basic firewall configuration.

A firewall can examine data passing into or out of a private network and decide whether to allow the transmission based on users' IDs, the transmission's origin and destination, and the transmission's contents. Information being transmitted is stored in what's called a *packet*, and after examining a packet, a firewall can take one of the following actions:

- Reject the incoming packet
- Send a warning to the network administrator

A **callback modem** verifies whether a user's access is valid by logging the user off (after he or she attempts to connect to the network) and then calling the user back at a predetermined number.

A **firewall** is a combination of hardware and software that acts as a filter or barrier between a private network and external computers or networks, including the Internet. A network administrator defines rules for access, and all other data transmissions are blocked.

Exhibit 5.3
Basic firewall configuration