A. Jarvis,
Personal identification by the iris of the eye

Imagine being able to go to an ATM to withdraw money without the need for a card or a password. You simply look into an ATM camera, which detects the pattern of the specks on your iris and releases funds from your account. The convenience of this technology is not limited to your banking transactions. Proponents of the technology predict that iris recognition systems will soon become popular for use at work, home, and for retail and online purchases.

This technology not only offers convenience, but also promises greater safety and security. Top airport security officials have recently recognized iris identifiers as an important tool for increasing airport security and for improving upon current immigration practices. The United States is now experimenting with technology which European banking institutions and airports have been using experimentally for over a decade with much success.

Iris recognition is becoming increasingly attractive to American consumers. Historically, the U.S. market has been reluctant to accept any form of biometric technology due to the fear of identity thefts and out of concern for other privacy matters. Recent studies have shown, however, that iris identification systems are actually the least susceptible, of any biometric technologies, to violations of privacy and wrongful identification by authorities. One of the main reasons why these systems are so privacy-friendly is because the technology has been designed and marketed to effectuate less controversial security uses. The type of biometric, the iris or retina, lends itself perfectly to these uses.

Like other biometric devices, iris recognition systems act primarily as a screening tool to allow or deny access to a particular place, rather than as a law enforcement tool to track down suspected criminals, as are DNA and fingerprints. In recent years, the public's fear of privacy infringement by biometric technology was fueled by law enforcement's use of face scanning devices for the express purpose of finding suspected criminals on public thoroughfares and at the Super Bowl in Tampa, Florida. Iris identification systems, like many other less imposing biometric devices, are used to screen individuals who are trying to gain access to more highly secure places or accounts, not to scan the general public at random.

Even before September 11, airports were considered to be sites in need of iris scanning technology. In May 2001, Charlotte/Douglas International Airport in North Carolina implemented an iris-scanning program, which consists of software that takes a digital snapshot of employees' iris. The equipment is particularly valuable in limiting access to secure areas to bona fide employees of the airport or airlines. Employee identification is one of the most popular uses of iris biometric technology, particularly after September 11, in preventing airline terrorist activity.

British Airways and Virgin Atlantic Airways at Heathrow Airport in London are hoping to use the technology more for convenience and efficiency purposes – to expedite the passport control process. As a trial-run, 2,000 American and Canadian passengers, who previously had their iris' scanned at the airport, are allowed to proceed to a special line in the passport control area of the airline terminal to have their identity quickly and accurately verified by an iris reading camera. The first time the camera scanned a passenger's iris, the image was converted into a code and stored in a database. When the passenger goes through customs, he/she stands approximately 14 inches from a camera, waits a few seconds as the system attempts to match the image of the passenger's iris with those stored on the server, and is either granted or

denied passage through customs based on this assessment. A similar system has been used at the Netherlands' Amsterdam airport, but with the use of an ID card that stores a template of the passenger's iris. When the passenger looks into the scanner before traveling, if the live template matches the card's stored template, then the passenger can bypass long immigration lines.

Another important use of iris detection systems is in immigration security. The U.S. government and the INS are exploring various iris identification programs for use by border control facilities. Another system that will very likely become standard procedure for tracking immigrants is the use of a smart card, or ID card, like the ones used for airport security, where the immigrant's iris code, along with other biometric information, is stored on the card. This is a technology that also has incredible prospects in the terrorist-tracking industry. Many government officials, including U.S. Senator Dianne Feinstein (D-CA), feel that if this type of tracking system were in place before September 11, the terrorist acts could have potentially been prevented since false ID cards and disguises allowed them to pass through security checkpoints and under intelligence officials' noses.

While many industry observers predict widespread use of cameras, scanners, and smart-card readers, especially at airports, some also caution that this technology alone will not solve the war on terrorism. Too much reliance on such devices could be hazardous to national security since, like all computerized systems, any biometric system is vulnerable to skilled hackers. Still, the level of security that iris identification systems can provide is unparalleled. In fact, according to the most recent National Institute of Justice Research Report on Entry-Control Technologies, retina or iris pattern scanners are considered the most accurate of all biometric devices.