

Communiqué

HIGH TECH – SECURITY

The Future of Biometrics and Restricted Access in the Business World

The following is the fourth in a series of Klink & Co. Communiqués concerning corporate security.

This Communiqué discusses the issues facing corporations in the future.

The face of security is changing and changing rapidly. September 11, 2001 is the date that redefined how the world views security.

No longer will corporate security be confined to security guards, keys, codes, identification cards and badges.

Instead, the future of security will consist of rooftop cameras constructing digital “face-prints” as you approach a building; retinal or iris scans taken before you

enter the research lab; and finger or handprints analyzed to gain access to a facility.

The use of biometric technology is growing in the corporate world. Fears of sabotage and terrorism have prompted many corporations to rethink their opposition to these controversial techniques.

Many corporations with “open door” policies are struggling with the face of “new” security.

Biometrics is the science and technology of measuring and statistically analyzing biological data, including the analysis of certain unique biological traits or body “signatures.”

Examples of biometric technology include:

- Fingerprinting;
- Retinal and iris scanning;
- Palm print identification;
- Face recognition;
- Voice recognition; and
- Vein recognition.

Biometrics systems offer a distinct advantage over other electronic or mechanical systems, because, unlike a key or plastic scan card, they

cannot be lost, stolen or duplicated.

Still, biometrics is only now being adopted as a security system of choice. But, there are still concerns that plague biometric technology.

1. Privacy

Most Americans believe that higher security techniques mean less personal privacy. Thus, biometrics is seen as an attack on personal privacy and a method allowing the government to track them.

2. Cost

Biometrics technology is expensive. Businesses, government, and the general public have been unwilling to invest in high-tech security applications because of the costs.

Facial and palm recognition systems can cost over \$135,000.

3. Size

Biometric equipment is often large in size and cumbersome. Location of the machines is often difficult and unsightly.

4. Reliability

Many, still, question the reliability of biometric technologies. Camera angle, lighting, distance and temperature changes can affect some systems.

In addition, problems with facial recognition include

environmental problems such as smiling, changes in appearance over time, alterations of hairstyle, facial hair, and weight gain or loss can impact the effectiveness of the system.

Some technologies such as handprints, fingerprints can be lifted from objects used and transported to the equipment.

Biometrics may be in everyone's future. The Department of State is considering the use of biometrics to aid in their processing of 4 to 5 million passports.

This Klink & Co., Inc. Communiqué is prepared in summary form and is not to be construed as legal advice or opinion on any specific fact or circumstance.

For more information regarding Corporate Security, please call:

Jeffrey Klink, President & CEO at 1(800) 836-8916 or e-mail to jklink@klink-co.com

Bill Penrod, Vice President at 216-589-9750 or 412-201-9123 or e-mail to wpenrod@klink-co.com

David Nolan, Vice President at (212) 292-5116 or email to dnolan@klink-co.com