USE OF BIOMETRIC (Fingerprint) SYSTEMS ON CAMPUS

Various concerns have been raised about the introduction of the biometric (fingerprint) access control system on campus such as the privacy and confidentiality of stored data (such as fingerprints).

Firstly, the university does have a policy on the expectation of privacy by both staff and students. This policy is available on the web at:

http://www.ru.ac.za/static/policies/monitor.php

There are further references to privacy expectations in the Rhodes acceptable use policy:

http://www.ru.ac.za/static/policies/rhodes-aup.html

specifically section 5.

Secondly however, the University's biometric system does ***not*** store fingerprints. There are no images of fingerprints stored on any Rhodes systems. What is stored is a hashed numerical encoding of a fingerprint - used as a unique token similar to the dallas chip i-button or barcode on your student card. The process used to compute this hash is both lossy and irreversible, meaning the original fingerprint can never be retrieved. When your fingerprint is scanned by a reader, the hash is re-computed and then compared against the stored hashes for the purpose of deciding whether or not to opening a door or doors, or for delivering a meal. The analogy is the storage of a password. In a well designed system, there is no way of recovering the plain text of a password from the hash encoded version.

Any further queries or concerns with regard to the biometric access system should be referred to the Director of the Residential Operations Division (i.l'ange@ru.ac.za).

The contribution of the Director of the Information Technology Division is gratefully acknowledged.