



Digital Preservation of Forensic Data

"Emerging Issues & Challenges"

Dr. M. S. Rao

**Director cum-Chief Forensic Scientist
DFS, MHA, GOI**



Forensic Digital Data Bank Management

- **Forensic Digital Data Bank Management** is a complex task/process. The data bank contains information on intimate & non-intimate objects.
- **Some forensic data banks need legal sanction**, (DNA Profile, voice) (without legal sanction, one can have data bank on intimate objects but the information from data bank can be used in legal matters only after getting legal sanction) (privacy, human rights & ethical issues are involved)

Characteristics features of Forensic Data Banks

- Some data banks are for **temporary period** (for identification)
- Some are to be preserved for **long period** (convicted persons)
- Retention of information in data banks are **subject to conviction period/death** of the individual
- Some data is for **volunteers** (for identification/insurance)
- Some forensic data banks on non-intimate objects need for **long preservation** (paint, glass, fiber, ink, toner, cartridge, bullet, etc.)



Forensic Digital Data Banks (Trusted Digital Repositories) on

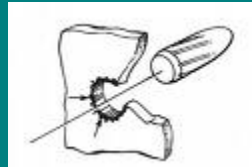
- Fingerprint/Palm print
(video archiving)



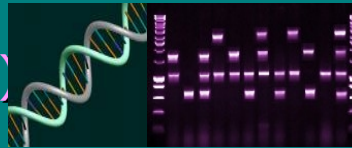
- e. Face
(video archiving)
- f. Voice
(audio archiving)



- g. Firearms signature
(video archiving)



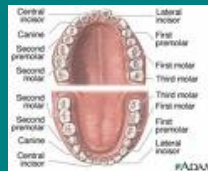
- b. DNA Profiling
(special law is to be enacted)



- h. Ink/Xerox toner



- c. Dental pattern
(video archiving)



- d. Ear pattern
(video archiving)



i. Glass



m. Gait

(video archiving)



j. Fiber



n. Counterfeit
Currency

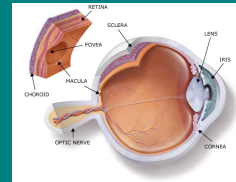


k. Shoe print



o. Iris/retina

(video archiving)



p. Travel
documents



l. IED's



Forensic Data Banks for three purposes

- **Forensic intelligence** ----for detection and prevention of crime -(face, voice, gait, fingerprint etc.)
- **For linking crime with criminal** ----or to prove innocence (DNA, fingerprint, biometrics, counterfeit currency, firearms signature etc.)
- **For identification** ---- (during disaster – biometrics like DNA, dental , fingerprint iris, ear, endangered animals/plants etc.)

(some data banks need to be preserved for long duration, some need not)

- For legal purpose – Data bank management needs
 - Authenticity of Data
 - Integrity and identity of the data
 - Chain of custody
- Preservation of digital data
 - Mirror image concept (disaster management)

- Data Input/data collection (a big problem)
- From Convicts/ suspects/ volunteers/ crime scene, PM centers
- Upgradation of tool and updating of data
- By Authorized persons only

Data for data banks from suspects/ convicts/ volunteers

- Fingerprint/palm print
- Ear
- Buccal swab/ blood/ hair
- Voice
- Signature
- Face
- Ear
- Dental pattern
- Gait

Data for data banks from dead bodies/unidentified dead bodies/

P.M. centers

- Blood
- Tissues
- Bone
- Hair/teeth
- Nails
- Fingerprint
- Palm print
- Face
- Ear pattern
- Dental pattern

Data for data banks from crime scene

- Above exhibits
- Glass
- Fiber
- Shoe/shoe print
- Paint
- Ink
- Paper
- Xerox toner
- IED
- Cartridge case
/bullet/firearm
- Counterfeit currency

After creation of Forensic data bank ----

- **Data retrieval** – (problem – compatibility with obsolete tools)
- By authorized person only
- **Data sharing** – with authorized persons only (privacy is maintained) (problem - compatibility) (sound mechanism)
- Data transmission – with minimum loss, no misuse, data encryption
- Data deletion (in some cases – fingerprint, DNA profiling) by authorised person only.

Data security

- Data manipulation/
Data
tampering/Data
sharing with
unauthorized
persons invites
legal
action/punishment



- Some kind of certification is required to establish whether archiving arrangements can provide adequate preservation guarantees.



- Bioethics standards are to be followed – for handling Biological samples



- Service against payment

- Audit Trails





- Poor collection process at crime scene.
- Poorly equipped P.M. centres (from where major chunk of data is collected)
- Poor collection of Information for archiving (creating and updating) the data
- **Updating forensic data** in r/o face, voice, signature, gait at regular intervals (Fingerprint are stubborn and remain unchanged before birth and even after death, whereas some biometrics undergo changes with passage of time like face, voice, signature, gait etc., but the changes are characteristics by themselves to fix the individual)

- Technological problem (2D/3D)
- Fund crunch/manpower constraint
- Data corruption/data security (by employees)
- Anti-forensic tools to defeat audit trails.

Case studies

- ❖ Linking serial shooting incidents through firearm signature data bank/Jessica Lal case
- ❖ Impersonation during exams
- ❖ Rural forensics
- ❖ Human identification in explosion cases
- ❖ Access control for high security zones(biometrics data)
- ❖ Endangered animal poaching /trafficking cases.

Thanks