

# Information Security Of Government Data: Practices and Challenges

Srinivas Kodali  
@digitaldutta

**Information wants to be free**

...

**Not all information should be public**

# Governance and Information

- Information Technology Act of 2000
- National Data Sharing & Accessibility Policy 2012 (NDSAP)
- National Cyber Security Policy 2013
- Regulations under IT act & other laws like Aadhaar Act  
Banking Act
- Standards in Information/Cyber Security from Industry
- Future: Data Protection Bill

# National Data Sharing and Accessibility Policy (NDSAP)

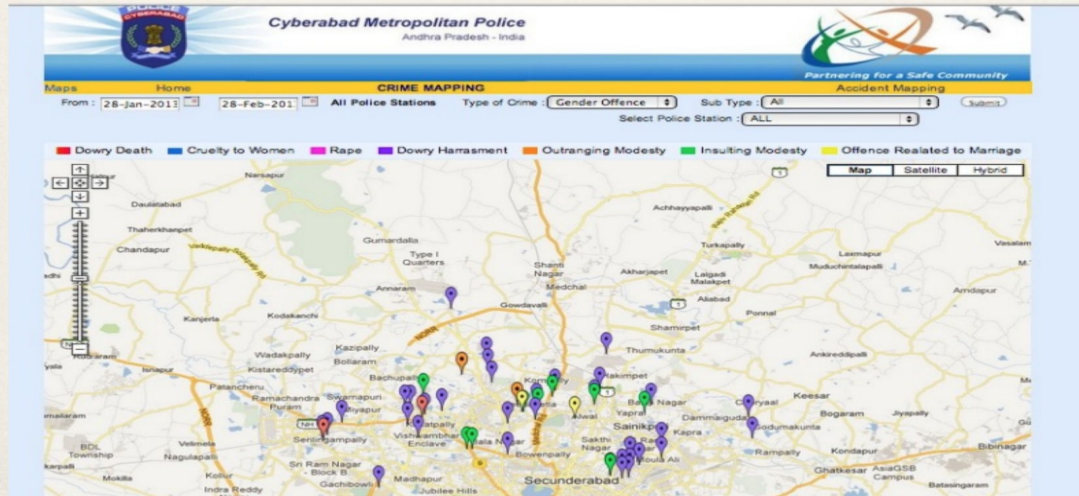
- Mandates data need to be classified into sensitive data, public data, restricted data
- Public data needs to be made available
- Data Controllers / Chief Data Officers responsible for implementing policy
- Not all government departments adopted it
- Classification of data have not been carried out at large

# National Cyber Security Policy 2013

- Ambitious Aims
- No real procedures and guidelines laid down
- Only two other state governments have a cyber security policy
- Telangana and Andhra Pradesh
- Low budget for Cyber Security to DeITY
- Decrease from 150 crores (2017-18) to 86 crores (current estimate)

# Information Practices - Police

## The Cyberabad metropolitan police's publicly accessible crime map



- Slide from Hyderabad Urban Lab presentation “Examining Data Practices: Cyberabad's Publicly Accessible Crime Map”

# Information Practices - Police

- Hyderabad Police Published names of victims of rape
- Sec 228A of IPC prohibits publications of information of victims
- Bangalore Police released 13,000 call data records for a hackathon
- Crime and Criminal Tracking System (CCTNS) have found with captcha bugs
- Lack of a Chief Information Officer

# Information Practices - Banking

- Practices inside Banking Industry has evolved over the years
- RBI Guidelines on Information Security make banks invest in security
- Security Incidents need to be reported to multiple entities
- Not all incidents are reported immediately
- Industry works on audits primarily



# Information Practices - UIDAI

- Aadhaar architecture is very complex
- Official policy may not exist/not available in public domain
- Information is leaky at every stage
- UIDAI does not has a Chief Information Officer
- No Official Bug Reporting Mechanism
- Security through Obscurity
- Every security incident is denied first

# Challenges in Reporting Incidents

- No clear roles of information officials defined
- Most officials do not understand risk, need capacity building
- CERT-In and NCIIPC two bodies which react to security incidents
- Often incident reports are not addressed
- Partial Fixes with no forensic audits

# Challenges in Information Security

- Lack of co ordination between cyber security agencies
- Most state government do not have the budget and capacity
- IT contractors do not want to take the risks of security incidents
- Policies and laws don't always help without enforcement
- Data Protection Law may address some of these