Obtaining mobile network big data for public purposes: LIRNE*asia*'s experience

Rohan Samarajiva & Sriganesh Lokanathan

Workshop on Big Data for Resilience, London, 5 June 2015

LIRNEasia

Pro-poor. Pro-market.

IDRC CRDI

Canada

This work was carried out with the aid of a grant from the International Development Research Centre, Canada and the Department for International Development UK..

UKaid

from the British people

LIRNE*asia*, disaster risk reduction & management (DRR/DRM) & big data

- LIRNE*asia* is a regional think tank, active since 2004 across South & South East Asia
  - In DRR/DRM space since 2005, e.g.,
    - Lokanathan, S. (2015, May). Emerging trends for DRM (including big data applications, at UN ESCAP workshop on ICT for promoting inclusive and disaster-resilient development, Ulaanbaatar.
    - Samarajiva, R. (2005) Mobilizing information and communications technologies for effective disaster warning: Lessons from the 2004 tsunami, *New Media and Society* (7(6); 731-47.
  - Has conducted research on mobile network big data (MNBD) since 2012, e.g.,
    - Samarajiva, R.; Lokanathan, S.; Madhawa, K.; Kriendler, G., & Maldeniya, D. (2015 May 30). Big data to improve urban planning, *Economic and Political Weekly*, Vol L (22): 42-48.
    - Lokanathan, S. & Gunaratne, R.L. (2015), Mobile Network Big Data for Development: Demystifying the Uses and Challenges, *Communication and Strategies*, Q1.

Mapping & critical assessment of evidence and novelty

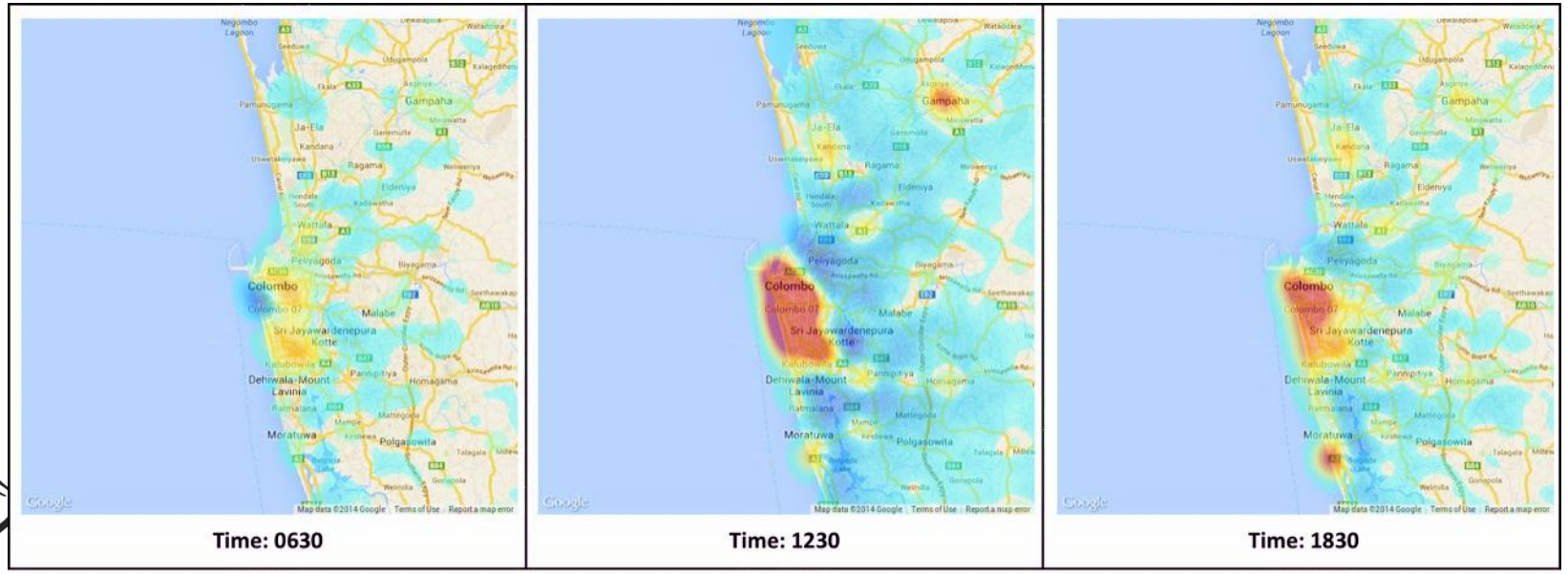
- LIRNEasia's focus was on urban and transportation planning in 2012-15
  - Moving into socio-economic monitoring & management of infectious diseases in 2015-17
- We have generated some insights of relevance to DRR (response) such as temporal changes in population density

Population density changes in Colombo region: weekday/ weekend

Pictures depict the change in population density at a particular time relative to midnight

Weekday

Sunday



How we obtained MNBD

- Negotiated access to pseudonymized Call Detail Records (CDRs) from multiple mobile network operators (MNOs) subject to non-disclosure agreements (NDAs)
  - Based on trust developed through long-standing engagement with MNOs
- CEO level agreement helped in complex negotiations at operational level that led to data being released for batch-processing at our location
  - All researchers bound by NDAs
  - Work conducted only at our location, subject to layered-access terms
    - MIT researchers travel to Colombo to work on the data
- Dissemination of results subject to prior clearance by MNOs

Example: Establishing a data sharing agreement with an unnamed operator in Sri Lanka

- Initial meeting between LIRNEasia's Founding Chair and CEO of MNO
  - Concept note on potential collaboration sent prior to meeting
  - Obtained in-principle agreement
  - Letter containing agreement provided
- Specifics, including NDA, negotiated with 2nd and 3rd tier management
  - 7 in-person meetings
    - Marketing, Business Intelligence, Network Engineering, Regulatory & Legal
    - ~7.5 hours in total
  - 4 conference calls
    - ~1 hour in total with operator; ~1 hour in total with LIRNEasia lawyers
  - 16 email exchanges
    - 11 with operator; 5 with LIRNEasia lawyers
  - 6 rounds of revisions of basic agreement
  - 11 people involved in total
    - 7 from operator; 3 from LIRNEasia; 1 from LIRNEasia's lawyers
- Agreements signed

LIRNEasia
Pro-poor. Pro-market.

Our strategy to facilitate access for public-interest research

- Demonstrate what can be done with MNBD to escape from hype/fear scenario spinning
- Reduce transaction costs of releasing data
  - Primarily through consultative development of self-regulatory guidelines and language that could be used in NDAs
  - Based on identification of actual harms, through survey of judicial decisions & actual engagement with the research
  - In longer term, work toward YODA [Yale University Open Data Access] type solution that would reduce demands on computing resources as well as legal departments
- Obtain data approaching n=all from multiple countries

Harms relevant to MNBD

- Privacy (9 out 16)
  - Surveillance
  - Aggregation
  - Identification, individual and group
  - Insecurity
  - Secondary use
  - Exclusion
  - Breach of confidentiality
  - Disclosure
  - Increased accessibility
- Anti-competitive effects
- Marginalization

Remedy	Identified potential harm	Include in agreements transferring identifiable MNBD	Include in agreements transferring anonymized MNBD
Mobile Network Operators (MNOs) will not engage in active surveillance of their customers, except as required by applicable law. MNOs will desist from collecting more data than are needed for the efficient operation of the networks and the supply of good service to customers. To the extent feasible, data collection practices will be transparent.	***Active surveillance***	No. Applying only to MNOs, this need not be included in agreements. However, active surveillance is a root cause of problems that could be manifested in other forms at the subsequent information processing and dissemination phases.	No. Applying only to MNOs, this need not be included in agreements. However, active surveillance is a root cause of problems that could be manifested in other forms at the subsequent information processing and dissemination phases.

Remedy	Identified potential harm	Include in agreements transferring identifiable MNBD	Include in agreements transferring anonymized MNBD
Best efforts will be made to prevent de-anonymization. Working groups may be formed with data users to monitor the state of knowledge in techniques of anonymization and de-anonymization.	***De-anonymization***	No	Yes

Remedy	Identified potential harm	Include in agreements transferring identifiable MNBD	Include in agreements transferring anonymized MNBD
Individually identifiable data will not be released to third parties, unless the purposes are specified in the agreement and have been approved by an ethics review committee, if one is available. If an ethics review committee is not available, an equivalent third-party review should be sought.	***Individual identification***	Yes	No

Remedy	Identified potential harm	Include in agreements transferring identifiable MNBD	Include in agreements transferring anonymized MNBD
Any agreement transferring identifiable data to a third party will also transfer responsibility to maintain safeguards to ensure security of individually identifiable data.	***Insecurity***	Yes	No

Remedy	Identified potential harm	Include in agreements transferring identifiable MNBD	Include in agreements transferring anonymized MNBD
The agreement governing the transfer will include provisions to minimize risks posed by increased accessibility when data are released to third parties.	***Increased accessibility***	Yes	Yes

Remedy	Identified potential harm	Include in agreements transferring identifiable MNBD	Include in agreements transferring anonymized MNBD
The principle of non-discrimination shall govern the release of MNBD to third parties who do not compete with the MNO. Those in the same class will be treated equally, subject to reasonable accommodation for resource constraints.	***Anti-competitive effects***	Yes	Yes