Pitfalls and Possibilities with Intelligence-led Policing

Jesper Lund
@je5perl

IT-Political Association
(EDRi member)

CUPP seminar, ITU
14 December 2021
My work in this area

• POL-INTEL in Denmark (from 2016)
• EDRi position paper on amending Europol Regulation
  - Allow Europol to analyse large data sets (legally)
  - Research and innovation (AI)
• Data protection and law enforcement (mostly EU-level with EDRi)
POL-INTEL overview

• Interface with existing databases
• Cross-database search function (“Finder”)
• Data analysis tool (“Analyse”)
  - Links between objects (persons, events, etc)
  - Heatmaps (visualise objects in an area)
  - Investigators can find “needle in the haystack” by analysing vast amounts of data
Building social graph of persons

- Persons are tagged in documents
- Direct relationship if A and B are tagged in same document
- Interactions across multiple hops
- All kinds of linkages can be established
Existing databases

- **Police databases**
  - POLSAS (cases)
  - Criminal records (CKR)
  - PED (large investigations)
  - Facial images (NF)
  - SIS, Interpol
  - PNR/API
  - AML reports (banks)
  - Wiretaps and tele data
  - ANPR

- **Civilian databases**
  - Residence database (CPR/Index2)
  - Vehicle database
  - Weapons permits
  - Passport database
  - Drivers licenses
Big data for policing

• Why big data?
  – Police should collect data for criminal investigations
  – Data on suspects, victims and witnesses

• Big data systems will incentivise “NSA style” data collection
  – Retention of ANPR no-hits in Denmark
  – Random stops to generate field cards (US)

• “Needle in the haystack” often leads to growing the haystack..
Data analysis

• Finding the unknown connection
  – Objects links created with algorithms (opaque)
  – **All algorithms encode biases**

• Risk of finding spurious links
  – Algorithms will **amplify errors** in databases
  – Greater effect on individuals with more records in databases used by POL-INTEL
  – Risk of stigmatisation and discrimination

• Limitations of data-analytical evidence
  – Danish telecommunications data scandal
Hotspots and feedback loops

- Hotspot policing
  - More patrols in areas where crime is most concentrated (heatmap data analysis)

- Pitfalls
  - Reported crime is different from actual crime
  - More police patrols means more crime will be registered, which can lead to feedback loops

- Reinforce existing biases in policing
  - Marginalised communities are often overpoliced
  - This bias affects the data used for predictions
Political and societal context

- POL-INTEL law adopted in Spring 2017
  - Specific provisions in executive orders
  - Details in internal police regulations (non-public)
- Limited public debate about effects on policing and society more broadly
- Information flow tightly controlled by the police
- Media coverage of POL-INTEL reflects that
- No independent evaluation of efficacy
MP question on feedback loops

• Answer by MoJ (REU spm. 949, 2020-21)
  – The Danish National Police has understood the concept of "feedback loops" as a process in which a system's automated output is returned as input in the same system. POL-INTEL does not support such system technical feedback loops.
  – The Danish National Police is aware that data showing there is a lot of crime in a certain area will often lead to increased police attention. Through increased patrols, more crime will be detected.
  – This must be regarded as a premise for the police’s handling of crime.