Predictive Policing and Data Protection

Jesper Lund
IT-Political Association of Denmark

@je5perl
jesper@itpol.dk
www.itpol.dk

Freedom not Fear
7 October 2017

Outline of presentation

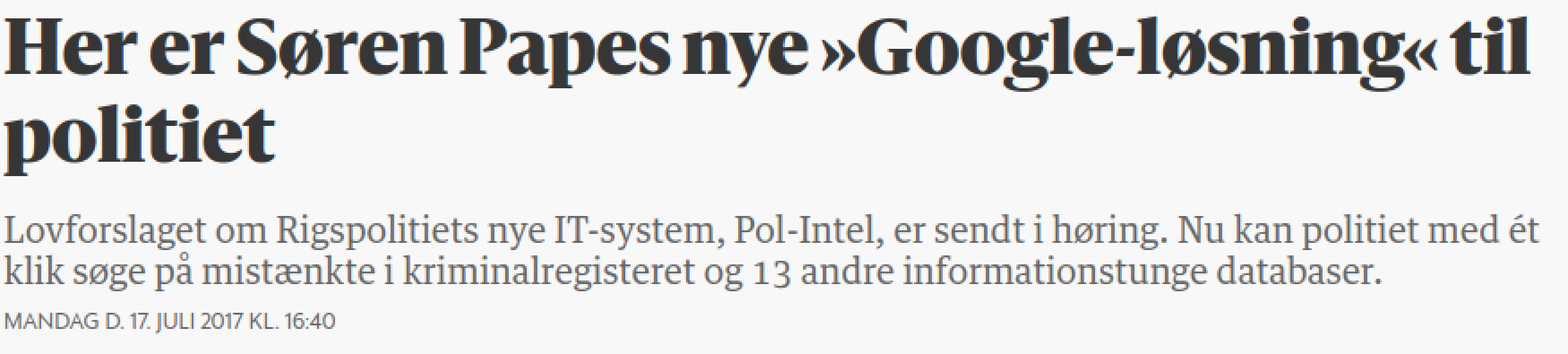
- Based on the Danish POL-INTEL system
  - EDRi-gram article from 22 February 2017
- Sources of information
  - Danish legal framework adopted in 2017
  - Official descriptions of POL-INTEL system and discussions with Danish National Police
- EU data protection law (2016/680)
- CJEU court cases (Tele2, EU-Canada PNR)

Predictive policing
Intelligence-led policing

- Big data analytics for police authorities
- Purpose is not necessarily to predict crime
  - Minority Report analogy can be misleading
  - Falling crime rates increases risk of false positives
- Data analysis to support police investigations
  - Backward-looking location tracking of suspects
  - Generate list of possible suspects from proximity to location or interaction with other persons
- Data collection on whom? Everyone?

POL-INTEL in Denmark

- Systems vendor is Palantir Technologies
- Based on Palantir Gotham
- Search and mapping tool across existing and new police databases
- Called "Google solution" in Danish media!



Her er Søren Papes nye »Google-løsning« til politiet

Lovforslaget om Rigspolitiets nye IT-system, Pol-Intel, er sendt i høring. Nu kan politiet med ét klik søge på mistænkte i kriminalregisteret og 13 andre informationstunge databaser.

MANDAG D. 17. JULI 2017 KL. 16:40

Danish legal framework

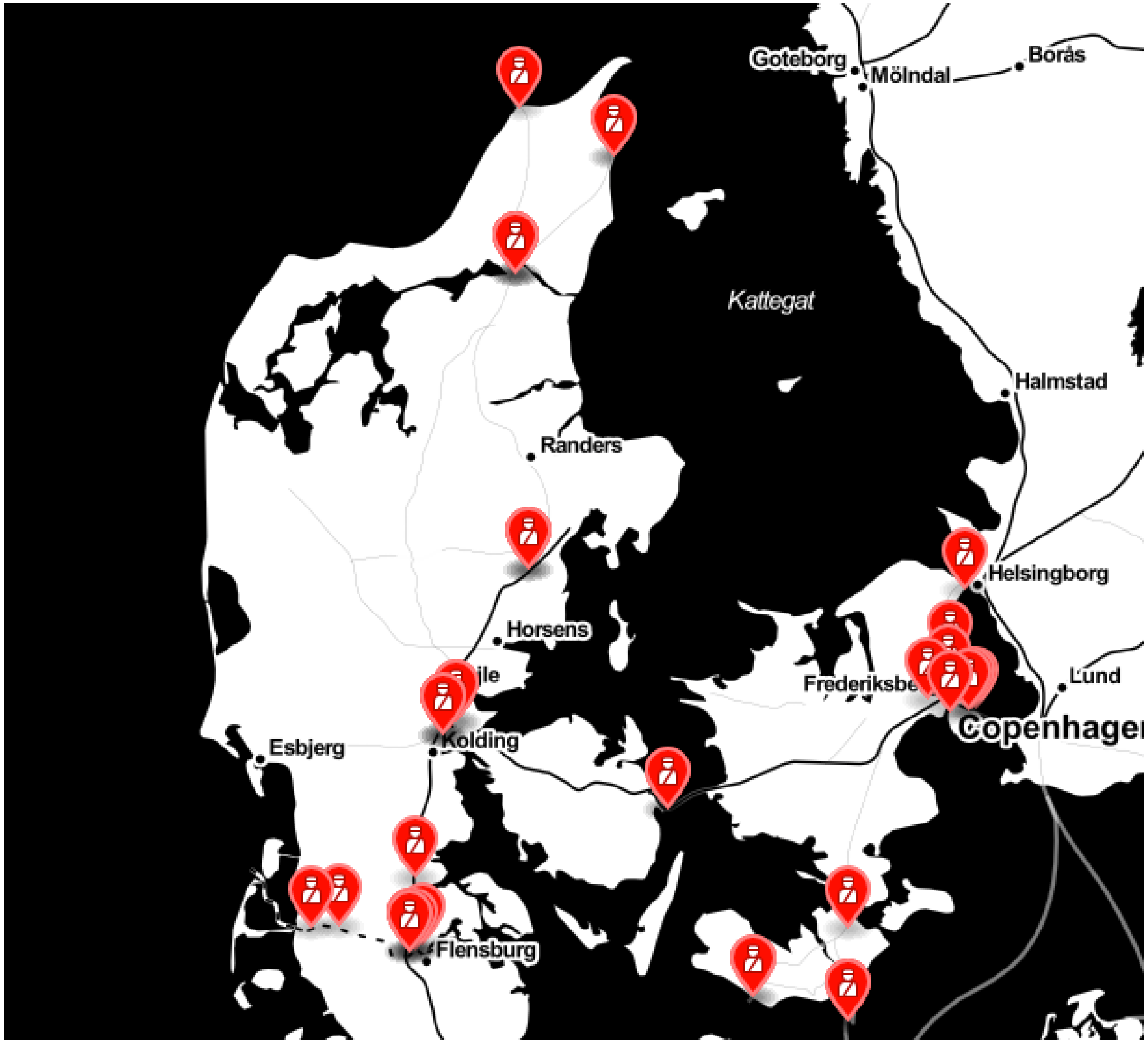
- Data input for POL-INTEL
  - All existing police databases
  - Other data sources that the police is allowed by law to use
- Claim: police is not granted any new powers
  - No new data is collected for POL-INTEL
  - Data processing within limits of data protection laws
  - POL-INTEL law “clarifies” that existing databases can be used and cross-linked for new data analysis
- Complete circumvention of purpose limitation

Existing police databases

- Crime database: convictions and investigations
- Special database for large investigations
- Wiretapping and communications metadata from other police investigations
- Automatic number plate recognition (ANPR)
- Information from SIS II and EIS (Europol)
- Database of all residents in Denmark
- Information collected from the internet and purchased from databrokers (“open source” intelligence)

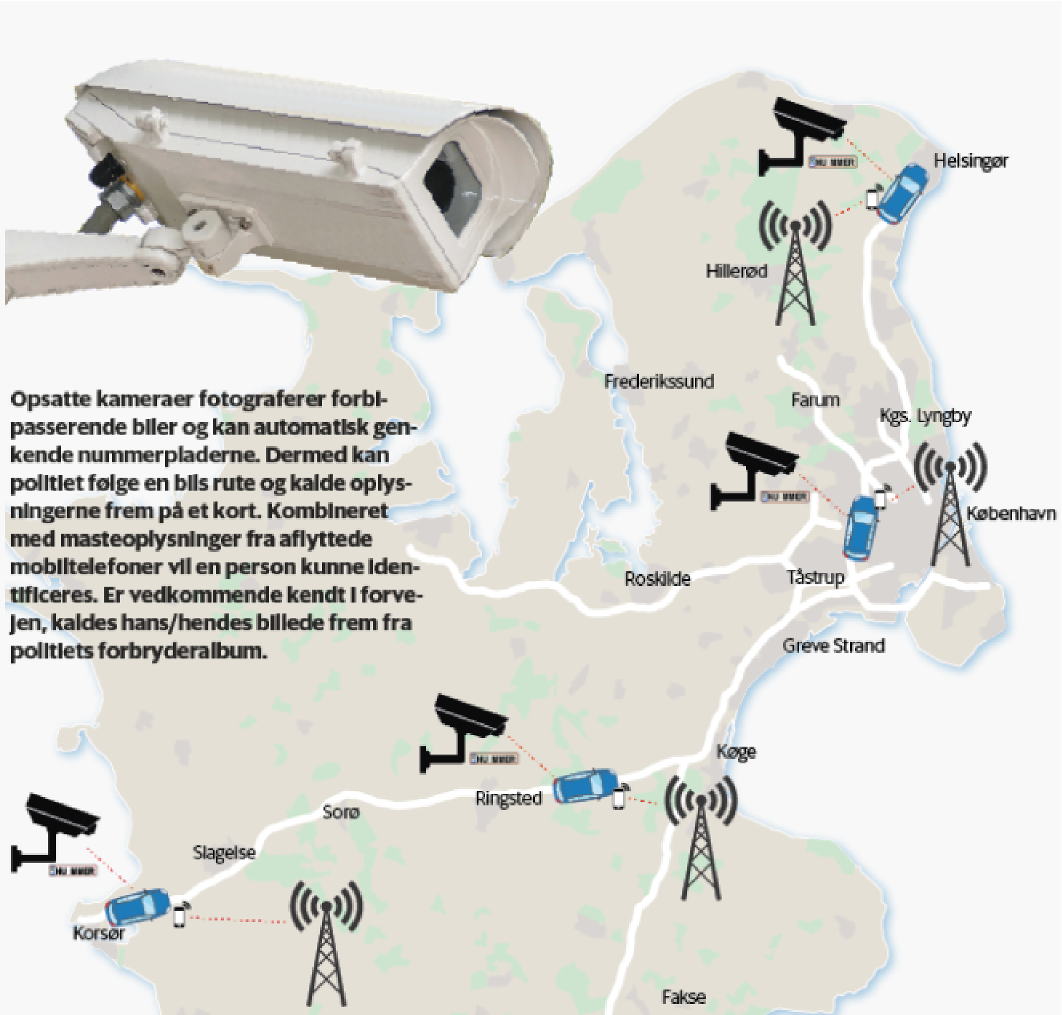
ANPR in Denmark

- 24 locations with stationary ANPR
- Borders area and large traffic intersections
- ANPR no-hits can be retained for 30 days
- **830K no-hits per day**



Leveraging ANPR with mobile phone wiretaps from other cases

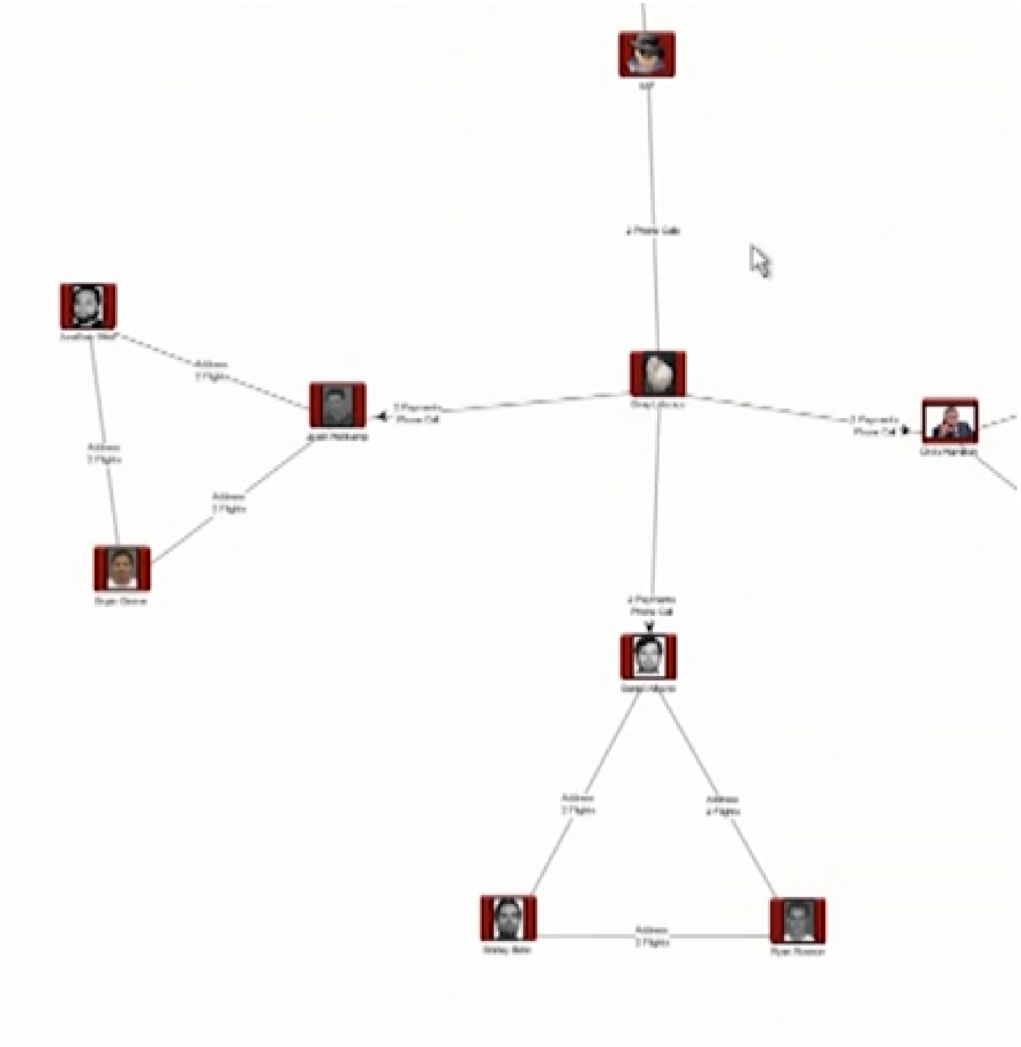
- ANPR used to track car (historically)
- Location data for mobile wiretaps is used to determine passengers in car
- Access to other info about person(s) from database, e.g. their picture



Opsatte kameraer fotograferer forbipasserende biler og kan automatisk genkende nummerpladerne. Dermed kan politiet følge en bils rute og kalde oplysningerne frem på et kort. Kombineret med masteoplysninger fra aflyttede mobiltelefoner vil en person kunne identificeres. Er vedkommende kendt i forvejen, kaldes hans/hendes billede frem fra politiets forbryderalbum.

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



Data protection concerns

- Profiling and big data
- Personal data processed for new purposes
  - Communications metadata from a specific investigation could be further processed on a general basis in order to associate persons with locations or establish connections between persons
- Incentive for blanket collection of data ("big data")
  - Example: ANPR no-hits become more useful when combined with data analytics that can find unknown suspects (who was in area X yesterday?)
- Retention of data in POL-INTEL system
  - Data that has been processed for an analysis in POL-INTEL can be retained for up to 10 years!
- Use for other police tasks, e.g. border control

Directive (EU) 2016/680

- Data protection for law enforcement
  - Prevention and investigation of criminal offences
  - Processing based on law, where necessary for competent authority (Article 8(1))
  - Data processing for border control falls under GDPR
- Weaker protection than GDPR
  - Only general information must be provided to the data subject (Article 13)
- Right of access by data subject (Article 14)
  - Limitations of that right (Article 15)
  - Denmark has transposed the Directive and managed to keep previous blanket exemptions from the right of access

CJEU case law

- Tele2 (C-203/15 and C-609/15)
  - Access to retained communications data must be limited to what is strictly necessary (para 118)
  - Hardly the case if the data is made searchable in POL-INTEL system for other investigations
- EU-Canada PNR agreement (Opinion 1/15)
  - About PNR (passenger name records)
  - Some principles may apply to predictive policing, like POL-INTEL
- Interesting (open) questions
  - Blanket retention of non-communications data, like ANPR no-hits
  - Limitations on profiling
  - Substantive and procedural conditions when retained data is used for a new purpose

Opinion 1/15 (PNR)

- Retention of data (para 191)
  - Legislation must satisfy objective criteria that establish a connection between the personal data to be retained and the objective pursued.
- Use of legitimately retained data (para 192)
  - EU legislation cannot be limited to requiring that access to such data should be for one of the objectives pursued by that legislation, but must also lay down the **substantive and procedural conditions** governing that use.
- Further use of data [in Opinion 1/15 about PNR]
  - Retention and use of PNR data for all passengers is allowed in order to facility entry checks to Canada (para 197)
  - Subsequent use of retained PNR data while in Canada requires new information justifying that use (paras 200-201)
  - No general retention after passengers have left Canada (para 205)