Policing the dark web: Intelligence v. evidence

Chrisje Brants, professor of criminal law Northumbria Univerity

Professor em. of criminal law, Willem Pompe Institute, Utrecht University

Northumbria University NEWCASTLE

PDTOR

Police Detectives on the Tor Network

Policing policy/philosophy shifts

- Shift forwards in time: from evidence gathering (objective: identification and prosecution of offenders after the fact) to intelligence gathering prior to offending (objective: identification of – potential – offenders/offences, prevention/disruption)
- New police methodologies (new criminal methods/new technology); rise in undercover policing (objective: disruption, capture)
- Undercover policing poses risks

- to human rights: privacy, fair trial (entrapment, inability to challenge evidence or methods by which it was gathered) and
- to critical trust in police and justice authorities, where no external scrutiny possible (NL: major scandal in 1990's)

- Depending on jurisdiction and manner of control and scrutiny of police activity

Control of police intelligence gathering?

1. (EU) laws and regulations/ECHR, judicial scrutiny (UK); code of practice
2. Law/ECHR and control by (higher) authority (prosecution service, magistrate), judicial supervision and scrutiny (NL)
3. Enforcement exacerbated by secrecy and anonymity of dark web

Problem:

Ad 1. Supervision only possible if case brought to court but prosecution no longer always objective of policing

Ad 2. - Presupposes sufficient (technical) knowledge on part of prosecutors and magistrates

- Same as 1.

Intelligence as evidence

- Irrespective of jurisdiction, police reluctant to share intelligence, let alone use as evidence, because
- Intelligence used as evidence in course of prosecution must be able to be subjected to testing in court
  - UK: through cross examination, NL through inclusion in dossier
- Could mean revealing police methods and could endanger future operations
- Could reveal identity of (vulnerable) sources or undercover officers
- In this respect, undercover policing of dark web no different from ‘real world policing’
- But raises questions as to whether ‘TOR (or cyber)-policing’ requires new methods of critical scrutiny

Consequences

- In UK, police may decide no prosecution, in order to protect intelligence, police methods, identities etc.; in which case, despite being subject to law/ECHR (as yet), no judicial scrutiny
- In NL, where prosecutor directs and is responsible for police investigations, Code of Criminal Procedure/ECHR regulates what police may and may not do: all police activity must be regulated by law, proportionate and necessary. (Some provisions on digital investigation – search and seizure etc. – new legislation on cyber investigation forthcoming)
- If intelligence gathering had been used to ‘steer’ subsequent investigations

  issue is not only challenging intelligence used as evidence, but also the way it was gathered

Examining/Challenging intelligence (gathering) in NL

- As yet, jurisprudence and legislation mostly concerns non-cyber-policing
- Intelligence may be used as evidence, but rights of defence must be duly respected (Dutch Supeme Court)
- Legislation allows scrutiny of evidence while safeguarding police interests, e.g. identity police informants
- Runners of informants – or even officers from security services, may testify in court in disguise and using numbers rather than names
- Question as to how far such rules and their (legal) implications can apply to TOR/cyber-policing