"The Reform of the e-privacy Directive: How to get it right?”

Linnet Taylor

University of Amsterdam / Tilburg Institute for Law, Technology and Society (TILT)

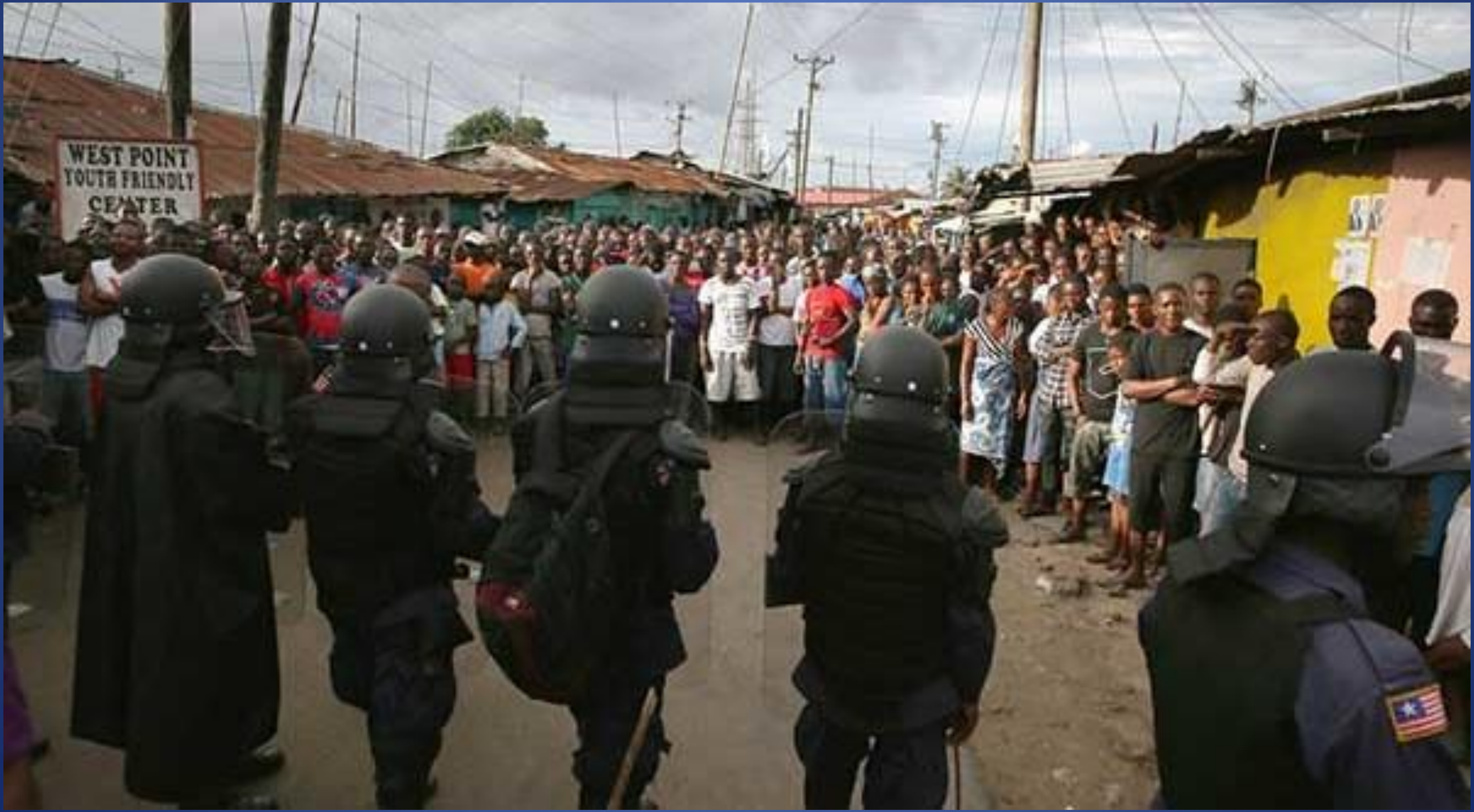
6 April 2016

Communications data as statistics

- (De-identified) mobile phone data are being used to
  - Count populations
  - Map and track human mobility across ethnic and conflict lines
  - Assess income and track business activities
  - Monitor behaviour
  - Track communication and exchange dynamics
  - Identify and monitor collective gatherings and events
- For good or bad?
  - Epidemiology
  - Political networks, activism, informal economic activity, undocumented migration

‘the global borderlands as an appropriate site for experimentation in the government of peoples ’ (Reid-Henry 2011)

What else can a quarantine map do?



Data misuse scenarios

1. Migrants crossing undocumented into the EU can be tracked, analysed, and subjected to preemptive decisionmaking based on origin/activities/networks before an asylum claim can be made

2. EU firms’ analytics on foreign users have unforseen effects on their countries’ sovereignty/security, causing diplomatic/trade/security problems for EU

3. EU firms’ analytics market ‘solutions’ internationally that facilitate abuses of privacy, other fundamental rights

Conclusion 1:

Take into account that fundamental rights cross borders, because EU-based firms are part of a global data market

‘The obligation to erase traffic data or to make such data anonymous…’

- De-identification is ineffective:

  ‘there are no perfect ways to de-identify data and there probably never will be.’ (Kendall et al. 2014)

- Location can re-identify:

  ‘Four spatio-temporal points are enough to uniquely identify 95% of individuals ‘ [in an anonymised CDR dataset] (de Montjoye et al. 2013)

- Aggregation does not always help:

  ‘the uniqueness of mobility traces decays approximately as the 1/10 power of their resolution’ (de Montjoye et al. 2013)

Safe data, unsafe consequences

‘There is intelligence-grade situational awareness in the case of sensors: what can be used to document a human rights abuse can also be used to target an artillery strike.’

-- Nathaniel Raymond, HHI, 25.2.2015

‘Even if you are looking at purely anonymized data on the use of mobile phones, carriers could predict your age to within in some cases plus or minus one year with over 70 percent accuracy. They can predict your gender with between 70 and 80 percent accuracy. One carrier in Indonesia told us they can tell what you’re religion is by how you use your phone. You can see the population moving around.’

-- Robert Kirkpatrick UN Global Pulse, 2012

Conclusion 2:

Anonymisation ≠ deletion because Identification is evolving: activities, movements, behaviour, location are all identifying factors

Group privacy: PII vs. DII

- Big data can proxy for categories where data is restricted (e.g. political affiliation, ethnicity, religion, movement patterns)

- Calling patterns or an active leader make groups trackable across space as networks (Sharad and Danezis 2013)

- There is overlap between platforms – mobile operators, search companies, app-developer partners, all operate together and are partners in identificaction and tracking

- Potential group harms from big data:
  - Ethnic/religious/economic/political persecution
  - Restriction of free movement
  - 'Aiding surveillance' (Privacy International 2014)
  - Identifying activist networks (McKinnon 2012)
  - Manipulation & influence (elections, moods, behaviour)

Conclusion 3:

Consider collective visibility due to big data because identifiability and harm are no longer individual-level issues

References

- de Montjoye Y. A., Hidalgo, C. A., Verleysen, M., & Blondel, V. D. (2013). Unique in the crowd: The privacy bounds of human mobility. *Scientific reports, 3*
- Kendall, Jake; Kerry, Cameron F.; and Montjoye, Alexandre de. "Enabling Humanitarian use of Mobile Phone Data," Issues in Technology Innovation (online) November 2014: http://www.brookings.edu/~/media/research/files/papers/2014/11/12-enablinghumanitarian- mobile-phone-data/brookingstechmobilephonedataweb.pdf.
- MacKinnon, R. (2012). Consent of the networked: The worldwide struggle for Internet freedom
- Hosein, G., & Nyst, C. (2013). Aiding Surveillance: An Exploration of How Development and Humanitarian Aid Initiatives are Enabling Surveillance in Developing Countries. *Available at SSRN 2326229*
- Reid-Henry, S. (2011). Spaces of security and development An alternative mapping of the security–development nexus. *Security Dialogue*, 42(1), 97-104
- Sharad, K., & Danezis, G. 2013 De-anonymizing D4D Datasets. The 13th Privacy Enhancing Technologies Symposium. July 10–12, 2013, Bloomington, Indiana, USA