Is Police Surveillance of Online Social Media Out of Control? A UK Legal Perspective

Barcelona, 2014

Professor Lilian Edwards – University of Strathclyde
Lachlan Urquhart – University of Nottingham

mixed reality lab

horizon
CENTRE FOR DOCTORAL TRAINING

CENTRE FOR INTERNET LAW AND POLICY

Structure

- Context and Shifts in Policing
  - Intelligence Led Policing,
  - London Riots and Contemporary Practices
- Legal Issues
  - Privacy in Public? ECHR and UK
  - Regulation of Investigatory Powers Act 2000 (RIPA) and SOCMINT
  - Issues
- Final questions

SOCMINT AND OSINT

- Intelligence Led Policing?
- NB NOT talking about backdoor
- extralegal access #PRISM

- OSINT?
  - Publically available, open sources
- SOCMINT? (Bartlett and Miller 2013)
  - Network and sentiment analysis e.g. EMOTIVE
  - Crowdsourcing
  - Event Detection and situational awareness
  - Predictive analytics eg IBM Memphis P.D.
- Policy challenges (Omand 2012):–
  - Public trust
  - Legitimacy and necessity?
  - (Demos 2013) also stress need for necessity, proportionality, transparency

flickr™

DEMOS

Contemporary Practices

- UK Summer Riots 2011
  - Flickr Stream
    - 770 arrests & 167 charges
  - Facewatch
  - "Shop a Looter" (Pieri 2014)
  - Twitter and BBM
- Risks?
  - Sampling Bias & "Reading the Riots" (Omand 2012)
  - Human Error eg Boston Bombings

Contemporary Practices (2)

- Met Police "5 Days in August" (2012)
  - Police unequipped to deal with SOCMINT

- HMIC "Rules of Engagement" (2011)
  - Police want stronger capabilities
  - Real time analytics

Legal Perspectives (1): Privacy in Public?

- Do **public** social media posts raise any expectations of **privacy**?
  - "*What Planet is this individual on? Her Tweets are Public domain*."
  - Gillespie (2009) (UK) – no. Cf Bartow (2011) (US) – "*Facebook is a giant surveillance tool, no warrant required, which the government can use.. with almost no practical constraints from existing laws*"
- **Data protection law** –exemptions (UK) for detection & prevention of crime; no need for consent, no subject access rights
- **ECHR art 8**? More promising. *Von Hannover* ECtHR (2004) – influential in UK privacy law after HRA98 – eg JK Rowling, Paul Weller cases – but cf *Wood v Metropolitan Police* (2008)
- Result – clearly *some* expectation of *privacy in public*; interference must be *necessary, proportionate and according to law*; but how much? & how balanced against other values eg security?
- Note also arts 7&8, EU Charter – *DRts Ireland* decision 2014 opposing blanket surveillance even in name of security (para 56-58)

Legal Perspectives (2): RIPA control

- Eric King, PI: "*SOCMINT simply did not exist when RIPA 2000 was conceived and it is hard to simply slot into the existing categories and typologies established by RIPA*"
- No *official* ACPO guidance or Code of Practice – Demos (Bartlett and Miller) 2013 report.
- Envisaged "digital" scheme in RIPA : Pt 1 Ch 1 covers real time interception of emails, warrant from Sec of State needed ; Ch 2, access to records of "communications" (=meta) data, granted automatically in most cases.
- "Analog world" scheme in Pt 2 RIPA
  - *Directed covert surveillance* – eg secretly following suspect
  - *Covert human intelligence source* (CHIS) eg befriending someone under false ID to acquire info
  - Both require authorisation of senior officer but **not** warrant of S of S
- How if at all does SOCMINT fit in?

Legal Perspectives (3): SOCMINT

- Demos 2013 assert SOCMINT collection needs **no** authorisation of any kind UNLESS:
  - Protected data , and fake profile used to obtain access -> CHIS or Directed Surveillance may apply
  - Where a "*detailed profile*" is made of "*named individual*", even from open sources -> Directed Surveillance? (O'Floinn & Ormerod, 2011)
    - Cf *Rotaru v Romania ECtHR (2000)* – "*public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities*"
    - *Cf* Stasi surveillance in former GDR – *Wood v Metropolitan (para 27-28)*
  - "Back door" collection of protected data might fall within RIPA Pt1 Ch 1, "*interception*" – but fits very badly indeed
- What about public profiles? Argued that *no expectation of privacy* so long as user knew from T&C that public data might be collected (?) – so OK, as long as API used not screen scraping where API available.

Issues

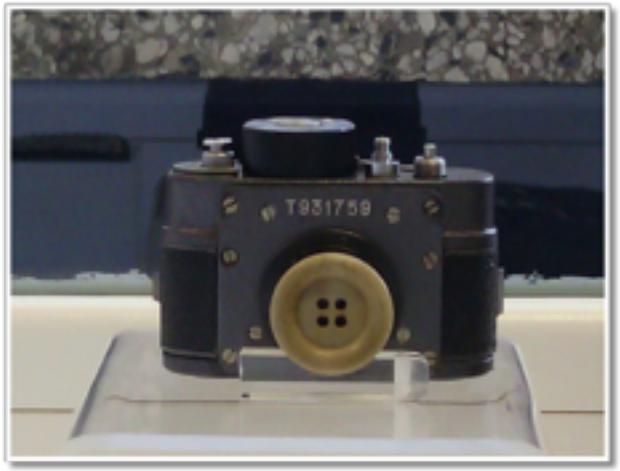
Q1. Can it be assumed everything done in public is "public"?

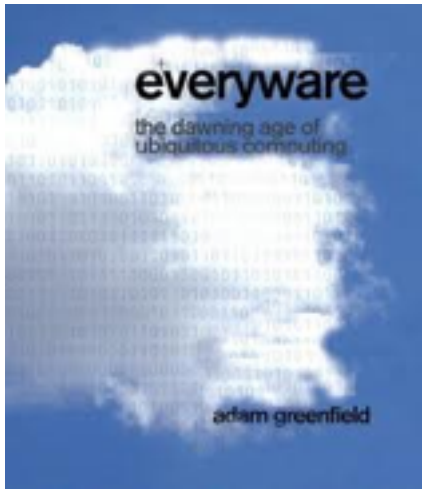
- No :
  - material about A is exposed by B;
  - users often cannot protect meta or network data;
  - asserting consent to T and C removes any expectation of privacy does not fit social reality where
    - online standard term contracts are rarely read or understood,
    - market for competition on privacy has not evolved in network effects industries
    - exclusion is fatal for social life & expression for many groups
  - boyd (2014) young adults/kids choose social media as "networked publics" without giving up expectations of privacy
  - Cannot anticipate "invisible audiences, collapsed contexts and persistent content" (how true of *all* users?)

Q2. Is SOCMINT valuable as evidence when ripped from context (eg Twitter "rape" usage) and subject to disinhibition effect and "social steganography"?

Final questions

- Are we writing a blank cheque for mass panoptic surveillance by treating SOCMINT as largely "public" & unregulated – the "new Stasi"?
- Does the *Rotaru* distinction between structured data in files held by police, and unstructured data "in the wild" hold up in the age of Google and data-mining?
- What rules *should* guarantee our expectations of privacy re "public" OSINT and SOCMINT, and how?
- If we can't get this right now re SOCMINT – what happens when police start using *ubicomp* data next?





Contact

Thanks for Listening

Questions?

Contact Details:

- lilian.edwards@strath.ac.uk - @lilianedwards
- lachlan.urquhart@nottingham.ac.uk - @mooseabyte