The threat to identities posed by arbitrary surveillance

Dr Avelie Stuart and Prof. Mark Levine
The creep of surveillance

- Arbitrary surveillance is spreading, but this seems to make it less noticeable
- One particularly strong rhetorical defence of surveillance:

DANIEL J. SOLOVE

Nothing to Hide

The False Tradeoff Between Privacy and Security
What do people want to hide?

- Not just illegal activity
- Stigmatised identities
- Protect ourselves from unjust interference by illegitimate authorities
- Moreover, surveillance tech is flawed

David Barnard-Wills @DBarnardWills · Jan 27
"Don't worry about the panoptic sort, worry about the panoptic sort-of" data is often, often wrong. @MalJayaram
Privacy – too broad and too narrow

• While there are many things we legitimately want to hide, privacy is not just about hiding
  – Privacy as “selective control...” (Altman, 1974)
  – “....over who has access to the self or to one’s group”
• But this makes privacy very broad and nebulous
• Yet some researchers argue that ‘privacy’ is too narrow to capture the damage surveillance causes (Bennett & Parsons, 2013)
Research questions

- Under what conditions do people find blanket or arbitrary surveillance (un)acceptable?
- Are feelings of threat under surveillance due to:
  - personal privacy threat,
  - social identity threat,
  - and/or perceptions of unfairness, discrimination
- Moving privacy beyond a ‘individualised’ concern
Surveillance and social identity

• O’Donnell (2010a, 2010b)
  – Imposing surveillance undermines shared identity between leaders and followers in organizational settings
  – Identification with one’s city means CCTV surveillance is seen as more acceptable, if the purpose is to ensure safety

• Our research adopts a similar approach, and examines further whether people are concerned about the privacy of their group and/or their social identity reputation

• And in the second study considers fairness as well
Study 1

- Online survey with 83 undergraduate students at the University of Exeter
- Proposed different rationales for why the University is considering switching on the location-tracking feature of the iExeter app
- 2x2 design:
  - Reason for surveillance
    - Social identity threat: University is concerned about lad culture and poor attendance
    - Benefit trade-off: University is concerned about managing space on campus for student society use
  - Sports/non-sports society membership
Willingness to Oppose the App

Threat

Sports Society

Not Sports Society

Trade-Off

5.2

4.44

3.87

2.5
• Identity threat, e.g. “The use of the location tracking app is threatening to societies”
• Privacy threat, e.g. “The location tracking app is a breach of my privacy”
• Correlated $r = .5$
Discussion

• The threat and trade-off scenarios seem to have some relevance in shifting attitudes towards surveillance
  – The proposal is generally opposed, but there is decreased opposition by sports-societies for improved facilities
  – Identity threatening for sports societies when framed as cracking down on lad culture – “hit you where it hurts”

• Limitations:
  – Are these results are specific to this university?
  – Small sample
  – Link between privacy and identity threat is not entirely clear
    • Decided to try and distinguish between ‘collective privacy’ and identity threat
  – Third ‘pathway’ – perceptions of fairness
Study 2

- 291 students from across 85 universities in the UK (recruited via Prolific), ~51% female
- All members of at least one student society
- Experimental manipulations the same, except wording changed to “Universities around the UK are considering switching on location-tracking capabilities...”
Measures

• Privacy invasion (adapted from Alge, 2001), $\alpha = .86$
• Fairness: “I think the location monitoring used by my university would be fair” (Alder & Ambrose, 2005)
• Group threat/collective privacy (adapted from individual privacy measures), e.g. “Students in my society do not need to be monitored.”
  – Also items about reputation/recognition
    – “This location tracking would have a negative effect on the reputation of my student society”
    – “This location tracking would ensure the needs of my society were properly recognized”

Combined $\alpha = .6$
Results

• No significant difference across conditions
• Regression on behavioural intentions:
  \[ F(3,289)=145.37, \ p<.001. \quad R^2 = .61 \]

<table>
<thead>
<tr>
<th></th>
<th>Beta</th>
<th>( T )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collective privacy</td>
<td>.228</td>
<td>5.67</td>
</tr>
<tr>
<td>Individual privacy</td>
<td>.513</td>
<td>10.28</td>
</tr>
<tr>
<td>Fairness</td>
<td>-.202</td>
<td>4.07</td>
</tr>
</tbody>
</table>

**all significant at \( p < .001 \)

• Individual privacy correlates with collective privacy \( r = .36 \), and with fairness \( r = -.65 \)
Discussion

• The scenarios aren’t generalizable across the UK
• But collective privacy and individual privacy appear to be distinguishable
• Measures still need some refinement
• How does fairness relate to privacy?
General Discussion

• The self relevance of surveillance may also be a tool for increasing awareness,
  – If you can find scenarios that are relevant to the group

• When does concern turn into action?
  – Surveillance resistance is hard to connect to a political collective identity
The end (but not of privacy)

Please contact us if you have further questions or suggestions:

a.stuart@exeter.ac.uk, m.levine@exeter.ac.uk
@AvelieS @ProfMarkLevine

Acknowledgements: Thanks to Jade Butler for her contribution to study 1, and to the Social, Environmental and Organisational Research Group at Exeter for their helpful feedback