Privacy and Confidentiality Challenges in Health Survey Research

Discussion

Douglas Williams – Westat

March 6, 2020
Three Challenges Related to Assurances In the Digital/Social Media Era
Challenges Related to Assurances

❯ Respondent beliefs
  • Widespread belief that government shares FSS data (Gerber, 2003)
  • Belief in confidentiality of data in FSS by ~50% (Childs et al, 2018)
  • Belief that government tracking (privacy) unavoidable ~60% (Pew, 2019)

  *The gov’t already knows a lot about me*

❯ Contrasting protections (Social Media, Technology, Apps)
  • Informed Consent vs Terms of Service & Privacy Policies
    – IC driven by protecting respondent / ethics in research
    – TOS/PP driven by protecting company / legal requirements
  • About 20% read privacy policies (Pew, 2019)
Challenges Related to Assurances (2)

› Respondent ignorance
  • Knowing when data is being collected
  • Knowing what data is being collected
  • Knowing who has data, or when shared
Effect on Perception of Assurances

- Respondent privacy concerns shaped by perception and experiences
- Commercial interactions more common/influential than government
- Lack of control over information is common experience, expectation

Do expectations of privacy persist?

- Use of information consequence of product or service.
- Blurring of “protected health” data and “user health” data
Growing Privacy Landscape

- EU General Data Protection Regulation (GDPR)
  Aims to give persons *some* control over data
- California Data Privacy Protection Act (CDPP)
  Persons required to identify misuse/breach
  Possibly lead to incentivizing personal disclosure

Will respondents want something similar for FSS data?
Confidentiality – Differential Privacy

Differential Privacy:

- A mathematical mechanism for ensuring **confidentiality** of collected data.
  - Permits public use of information / secure use by more data users
  - More data available to researchers?
  - Could this encourage broader collection of information – overconfidence of *privacy*?
  - Doesn’t eliminate the need for data security – still collecting private information.

- 55% view hacking as biggest threat to medical privacy (CHCF, 1999)
Differential Privacy:

• Challenging in assurances
  – If my data will not change findings, then why do you need it?
  – Your vital to accurate data, then we’ll make it less accurate.

• Creates opposing interest: researchers want $e = 1$; participants want $e = 0.1$.
  – 31% not willing at all to risk privacy (Eggleston, HSRM)
Thank You

Douglas Williams
douglaswilliams@Westat.com


