How do youth protect their digital privacy across contexts?

UC Irvine

Allison Starks, M.A.T, Stephanie M. Reich, Ph.D., Nicholas Santer, M.S., & Adriana M. Manago, Ph.D.

BACKGROUND

- Digital spaces, an important part of youth culture[1], involve privacy negotiation across contexts (e.g. person-to-person, person-to-corporation).
- In the US, COPPA offers children (<13 yrs) privacy protection online from corporations, but this is regularly violated.[2, 3] Such business practices, coupled with youth's active sharing with peers[4] requires that adolescents actively managing their privacy online.
- Currently, not much is known about what young adolescents understand and do online in relation to information sharing and privacy protection.[5]

RESEARCH QUESTIONS

RQ1 What kinds of privacy practices do youth use with other people (person-to-person) and corporations (person-to-corporation) online?

RQ2 What are youth's beliefs and preferences for digital privacy?

RQ3 To what extent do student characteristics (e.g. gender, age, race), beliefs, and preferences predict privacy behaviors online?

METHOD

Online survey completed at middle schools in June 2019

Participants

- 6th-8th graders aged 11-14 years (M=12.58, SD= 0.94), 54% male
- 52% White, 12.3% Multi-Ethnic, 8.9% Latino/a, 8.5% Black, 8% Asian
- 414 students completed section 1 of the survey (behaviors and beliefs) and 293 students completed the additional section 2 (preferences)

Privacy Beliefs and Preferences

5-pt Likert scale: 1) Strongly Disagree to 5) Strongly Agree

Subscales	# Item	Mean (SD)	Sample Item
Corporate Surveillance Beliefs	3	3.08 (1.05)	Companies use information about what you do online to try and sell you things
Future Orienting Thinking Beliefs	2	3.53 (1.0)	Having a positive reputation online is important for getting a job in the future
Potential Predators Beliefs	2	3.82 (1.0)	You can never be really sure who you are talking to online
Corporate Surveillance Preferences	4	2.91 (0.91)	I like it when I can log in with Google or Facebook
Peer Relationship Preferences	2	3.00 (0.98)	I like it when a friend tags me in a positive post
Peer Relationships with Risk Preferences	4	2.71 (0.93)	I like it when social media tags my location
Corporate Surveillance Preferences	4	2.91 (0.91)	I like it when I can log in with Google or Facebook

Privacy-Protecting Behaviors

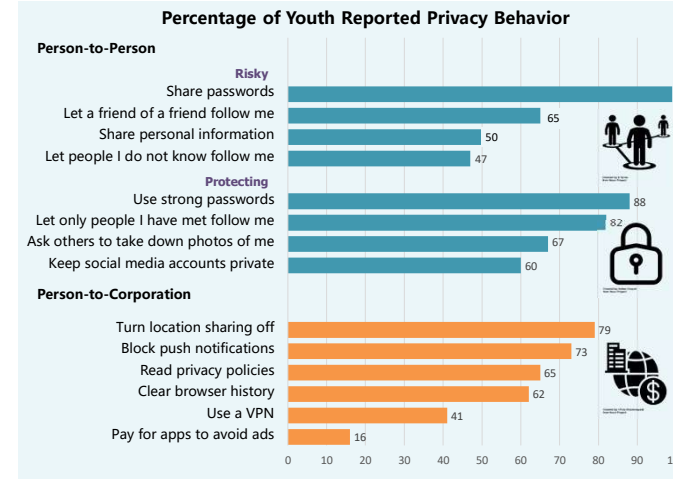4-pt Likert scale: (1) Never, (2) Sometimes, (3) Most of the time (4) Always

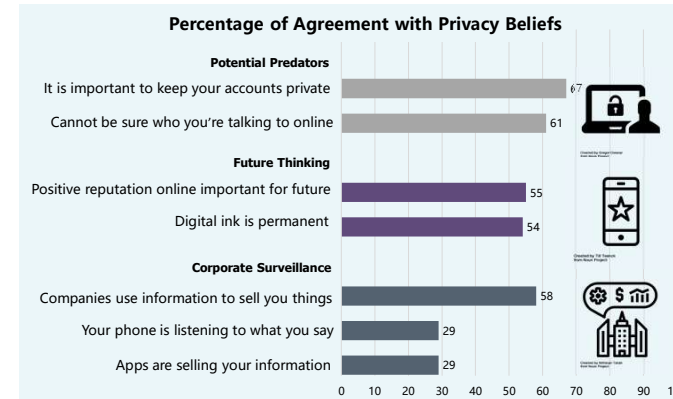| Type of Privacy	Items	Mean (SD)	Sample Item
Person-to-Person	8	2.98 (0.5)	Use strong passwords; Keep social media accounts private
Person-to-Corporation	6	1.99 (0.55)	Read privacy policies for apps/websites; Turn location sharing off

Analysis

Frequency and t-tests for RQ1 & RQ2, OLS regression with student characteristics, privacy beliefs, and preferences as predictors of privacy behaviors

RESULTS

RQ1: Youth engaged in more person-to-person (M=2.98, SD=0.5) than person-to-corporation discrete privacy-protecting behaviors (M=1.99, SD=0,55), t(422)=32.18, p<0.0001.

Percentage of Youth Reported Privacy Behavior

Person-to-Person
- Risky
  - Share passwords — 99
  - Let a friend of a friend follow me — 65
  - Share personal information — 50
  - Let people I do not know follow me — 47
- Protecting
  - Use strong passwords — 88
  - Let only people I have met follow me — 82
  - Ask others to take down photos of me — 67
  - Keep social media accounts private — 60

Person-to-Corporation
- Turn location sharing off — 79
- Block push notifications — 73
- Read privacy policies — 65
- Clear browser history — 62
- Use a VPN — 41
- Pay for apps to avoid ads — 16

RQ2: Youth agreed more with messages about privacy protection from potential predators or around future-oriented thinking, than from corporate surveillance. 'Companies' and 'apps' collecting person information were viewed differently.

Percentage of Agreement with Privacy Beliefs

Potential Predators
- It is important to keep your accounts private — 67
- Cannot be sure who you're talking to online — 61

Future Thinking
- Positive reputation online important for future — 55
- Digital ink is permanent — 54

Corporate Surveillance
- Companies use information to sell you things — 58
- Your phone is listening to what you say — 29
- Apps are selling your information — 29

RQ3: Age and race were associated with more person-to-corporation privacy protection, while gender was associated with person-to-person privacy behavior.

- Privacy-protecting behavior from corporations was more frequent (β=0.10, p<0.01) among older tweens.
- White youth (β= -0.13, p<0.05) reported fewer privacy-protecting behaviors against corporations and criminals such as turning location sharing off or keeping accounts private, compared with their non-white peers.

RESULTS (cont'd)

- Girls reported more person-to-person privacy-protecting behaviors (β=0.13, p<0.01). However, gender became nonsignificant when controlling for preferences around peer relationships and corporate surveillance.
- Beliefs about corporations and future thinking were unrelated to person-to-person and person-to-corporation privacy behaviors.
- Stronger beliefs about protection from potential predators predicted more privacy-protecting behaviors, both with people (β= 0.17, p<0.001) and corporations (β= 0.13, p<0.001).

DISCUSSION

- Youth use more privacy-protecting behaviors with people than with corporations; perhaps due to the emphasis schools place on person-to-person privacy protection in digital literacy or citizenship curricula[6].
- Older middle-schoolers reported more privacy protection from corporations online, although a large amount of variance in privacy behavior was unexplained.
- These findings call into question the extent youth, 13 yrs and younger, can reasonably be expected to protect their interests online in the absence of governmental or corporate regulation, building on recent work at the intersection of privacy, law, and child development.[7]
- Findings suggest that youth could benefit from the opportunity to learn about corporate surveillance practices, how their data are used, and how to protect their privacy across corporate and institutional contexts.

Limitations

- Due to time constraints, the full sample (n=414) did not complete section 2, reducing the number (n=293) of completed surveys. There were no significant differences in age, gender, race, ethnicity, or social media activities for students with and without preferences data.
- Causal relationships between privacy beliefs, preferences, and behaviors cannot be determined.

CONCLUSION

Marketing, profiling, and datafication of youth's digital behavior can have far-reaching consequences to employment, education, civic engagement, and healthcare.[8 ,9,10] Thus, youth need information and tools to manage their digital privacy and participate freely in online spaces, especially in the absence of governmental and corporate regulation. These findings highlight some of the gaps in tweens' digital literacy and areas of digital privacy that need support.

ACKNOWLEDGEMENTS & REFERENCES

[1] Holloway, D., & Green, L. (2016). The Internet of toys. Communication Research and Practice, 2(4), 506–519. https://doi.org/10.1080/22041451.2016.1266124 [2] Mascheroni, G., & Holloway, D. (2019). The quantified child: Discourses and practices of dataveillance in different life stages. In O. Erstad R. Flewitt, B. Kümmerling-Meibauer, I. P. Pereira, (Eds) The Routledge Handbook of Digital Literacies in Early Childhood. London: Routledge (pp. 354-365). Routledge, https://doi.org/10.4324/9780203730638 [3] Kuster, A. & Schakowsky, J. (2020, May 28). Kuster and Schakowsky Letter to FTC on TikTok [letter] Retrieved from 4] Boyd, D. (2015) It's Complicated: The Social Lives of Networked Teens. Yale University Press. [5] Stoilova, M., Nandagiri, https://kuster.house.gov/sites/kuster.house.gov/files/Kuster%20Schakowsky%20letter%20to%20FTC%20on%20TikTok.pdf [R., & Livingstone, S. (2019). Children's understanding of personal data and privacy online–a systematic evidence mapping. Information Communication and Society, 1–19. [6] Hollandsworth, R., Donovan, J. & Welch, M. Digital Citizenship: You Can't Go Home Again. TechTrends 61, 524–530 (2017). https://doi.org/10.1007/s11528-017-0190-4 [7] Costello, C. R., McNiel, D. E., & Binder, R. L. (2016). Adolescents and social media: Privacy, brain development, and the law. Journal of the American Academy of Psychiatry and the Law, 44(3), 313–321. [8] Crawford, K., & Schultz, J. (2014). Big data and due process: Toward framework to redress predictive privacy harms. Boston College Law Review, 55(1), 93-128. [9] Doffman, Z. (2020, June 26) Black Lives Matter: U.S. Protesters Tracked By Secretive Phone Location Technology. Forbes. Retrieved from https://www.forbes.com/sites/zakdoffman/2020/06/26/secretive-phone-tracking-company-publishes-location-data-on-black-lives-matter-protesters/#3430f4384a1e [10] Fussell, S. (2020, June 2). Protests Renew Scrutiny of Tech's Ties to Law Enforcement. Wired. Retrieved from https://www.wired.com/story/protests-renew-scrutiny-tech-ties-law-enforcement/