W3C Workshop on Permissions

Serge Egelman (egelman@cs.berkeley.edu)
University of California, Berkeley / ICSI / AppCensus

The mass collection of personal information about online consumers has necessitated platforms to develop "permissions" systems, as a way for consumers to regulate how third party apps and services access their sensitive information. For nearly two decades, I have been conducting basic research to understand consumer privacy preferences and expectations, as well as how existing systems and interfaces are meeting consumers' needs (or not). Specifically, I have extensively examined how consumers make decisions about their privacy on mobile devices and how mobile apps may be violating various privacy laws, regulations, and policies. Based on this experience and current research interests (including having participated in a precursor W3C workshop on permissions in 2018), I would like to participate in this workshop.

This stream of research specific to permissions started with examining consumer understanding of Android app permissions [4].[1] In order to further study consumer understanding of these types of privacy disclosures, My laboratory instrumented the Android operating system, APIs, and kernel, to study the circumstances under which permission-protected sensitive user data are accessed by mobile apps [26]. We also collected additional contextual data, such as what other activities occur on the device when an app accesses sensitive user data, and then trained a classifier to predict "appropriate" permission requests (applying Nissenbaum's "Theory of Privacy as Contextual Integrity" [12]). The feature set—the contextual information captured by the instrumentation—allowed us to modify the permissions enforcement mechanism to dynamically regulate access to sensitive data, which resulted in greater accuracy than prior approaches to managing mobile privacy via permissions [27]. Subsequent studies showed that users found the new permissions interface easier to use and users made fewer privacy errors when using them [22, 28].[2]

This instrumentation was later combined with Lumen (né Haystack), a mobile network traffic monitor also developed by other researchers at ICSI [15]. Combined

[1] This paper received the 2012 SOUPS Best Paper Award and the 2017 SOUPS Impact Award.
[2] This paper received the ACM SIGCHI Honorable Mention Award.

with a UI fuzzer [7], we built an end-to-end system for automatically examining the sensitive user information accessed and shared by mobile apps [17]. As a proof of concept, and to demonstrate the limits of current mobile permissions systems, we used this infrastructure to automatically examine mobile app compliance with the US Children's Online Privacy Protection Act (COPPA) [18][3] We automatically downloaded almost 6,000 child-directed apps, automatically ran those apps in our testbed, and concluded that more than half of them were potentially violating COPPA. This research has had demonstrated impact on industry and policy:

- **Platform Policy Changes:** The Google Play Store began requiring child-directed Android apps to only use pre-approved ad SDKs [20]; the Apple App Store banned third-party advertising and analytics in child-directed iOS apps [1].
- **Enforcement Actions:** The New Mexico Attorney General filed suit against one particularly egregious app developer [24], citing this research in the complaint.
- **Regulatory Updates:** The Federal Trade Commission (FTC) sought public comment on COPPA rulemaking [23], including specifically seeking feedback from me based on this research.
- **Legislative Action:** Lawmakers in both the Senate and House introduced bills to address several of the issues identified by the research [14, 13], seeking my feedback on both bills, and later asking me to testify at a US Senate hearing in May of 2021 [3].

Our subsequent research used these tools to automatically identify covert and side channels that allowed mobile apps to circumvent the Android permissions system [16].[4] We received multiple CVEs and bug bounties for identifying apps and SDKs that were actively exploiting these vulnerabilities (i.e., accessing sensitive user data outside of the permissions system), and Google announced multiple privacy changes to Android [8]. This research was subsequently commercialized as the startup, AppCensus, Inc., which is continuing to have impact on the online privacy ecosystem [9, 21, 5, 6, 11, 19, 10, 2, 25]. An additional impact of this research was that it led to ongoing relationships with various regulators, who now regularly consult members of my lab for data and guidance on privacy-related issues.

In sum, I believe that my experience performing research in this area will be beneficial to the goals of the workshop.

[3]This paper received the 2020 Caspar Bowden PET Award.

[4]This paper received the USENIX Security Distinguished Paper Award, as well as privacy research awards from two international data protection authorities (DPAs): AEPD (Spain) and CNIL (France).

References

[1] Apple, Inc. Updates to the app store review guidelines. https://developer.apple.com/news/?id=06032019j, June 3 2019.

[2] J. Cox. Location Data Firm Got GPS Data From Apps Even When People Opted Out. https://www.vice.com/en/article/5dgmqz/huq-location-data-opt-out-no-consent, October 25 2021. Accessed: November 15, 2021.

[3] S. Egelman. U.S. Senate testimony for hearing on "protecting kids online: Internet privacy and manipulative marketing". https://www.commerce.senate.gov/services/files/0DC78E9D-88B2-4D54-8F4A-AE7B4C7D0EF6, May 18 2021.

[4] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner. Android permissions: user attention, comprehension, and behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, New York, NY, USA, 2012. ACM.

[5] T. Germain. How to use apple's privacy labels for apps. https://www.consumerreports.org/privacy/how-to-use-apples-privacy-labels-for-apps-a1059836329/, December 18 2020. Accessed: November 15, 2021.

[6] T. Germain. Mental health apps aren't all as private as you may think. https://www.consumerreports.org/health-privacy/mental-health-apps-and-user-privacy-a7415198244/, March 2 2021. Accessed: November 15, 2021.

[7] Google. UI/Application Exerciser Monkey. https://developer.android.com/studio/test/monkey.html, 2017. Accessed: October 12, 2017.

[8] Google. Privacy changes in Android 10. https://www.commerce.senate.gov/services/files/0DC78E9D-88B2-4D54-8F4A-AE7B4C7D0EF6, 2019.

[9] S. LaMotte. Marketers are gathering data on your kids from the apps they use, study finds. https://www.cnn.com/2020/09/08/health/privacy-violations-kids-apps-wellness-trnd/index.html, September 15 2020. Accessed: November 15, 2021.

[10] D. Leprince-Ringuet. Contact-tracing apps: Android phones were leaking sensitive data, find researchers. https://www.zdnet.com/article/contact-tracing-apps-android-phones-were-leaking-sensitive-data-find-researchers/, April 29 2021. Accessed: November 15, 2021.

[11] A. Ng. Google promised its contact tracing app was completely private—but it wasn't. https://themarkup.org/privacy/2021/04/27/google-promised-its-contact-tracing-app-was-completely-private-but-it-wasnt, April 27 2021. Accessed: November 15, 2021.

[12] H. Nissenbaum. Privacy as contextual integrity. *Washington Law Review*, 79:119, February 2004.

[13] Office of U.S. Representative Kathy Castor. Rep. castor reintroduces landmark kids privcy act to strengthen coppa, keep children safe online. https://castor.house.gov/news/documentsingle.aspx?DocumentID=403677, July 29 2021.

[14] Office of U.S. Senator Ed Markey. Senators markey and cassidy propose bipartisan bill to update children's online privacy rules. https://www.markey.senate.gov/news/press-releases/senators-markey-and-cassidy-propose-bipartisan-bill-to-update-childrens-online-privacy-rules, June 24 2021.

[15] A. Razaghpanah, N. Vallina-Rodriguez, S. Sundaresan, C. Kreibich, P. Gill, M. Allman, and V. Paxson. Haystack: In situ mobile traffic analysis in user space. *CoRR*, abs/1510.01419, 2015.

[16] J. Reardon, A. Feal, P. Wijesekera, A. E. B. On, N. Vallina-Rodriguez, and S. Egelman. 50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System. In *Proceedings of the 24th USENIX Security Symposium*, USENIX Security '19, Berkeley, CA, USA, 2019. USENIX Association.

[17] I. Reyes, P. Wijesekera, A. Razaghpanah, J. Reardon, N. Vallina-Rodriguez, S. Egelman, and C. Kreibich. "is our children's apps learning?" automatically detecting coppa violations. In *The Workshop on Technology and Consumer Protection*, ConPro '17, 2017. http://www.ieee-security.org/TC/SPW2017/ConPro/papers/reyes-conpro17.pdf.

[18] I. Reyes, P. Wijesekera, J. Reardon, A. E. B. On, A. Razaghpanah, N. Vallina-Rodriguez, and S. Egelman. "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. *Proceedings on Privacy Enhancing Technologies*, (2018.3):63–83, 2018.

[19] T. Riley. The cybersecurity 202: Lawmakers want to create a reserve corps of cybersecurity experts to respond to the next solarwinds. https://www.washingtonpost.com/politics/2021/04/28/cybersecurity-

202-lawmakers-want-create-reserve-corps-cybersecurity-experts-respond-next-solarwinds/, April 28 2021. Accessed: November 15, 2021.

[20] K. Sachdeva. Building a safer google play for kids. https://android-developers.googleblog.com/2019/05/building-safer-google-play-for-kids.html, May 29 2019.

[21] T. Sonnemaker. As zoom classes take over during the pandemic, edtech companies provide a lifeline, but only for schools and parents willing to surrender their students' privacy. https://www.businessinsider.com/virtual-learning-privacy-tech-teachers-parents-schools-student-data-2020-10, October 13 2020. Accessed: November 15, 2021.

[22] L. Tsai, P. Wijesekera, J. Reardon, I. Reyes, S. Egelman, D. Wagner, N. Good, and J.-W. Chen. Turtle guard: Helping android users apply contextual privacy preferences. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 145–162. USENIX Association, 2017.

[23] U.S. Federal Trade Comission (FTC). FTC seeks comments on Children's Online Privacy Protection Act rule. https://www.ftc.gov/news-events/press-releases/2019/07/ftc-seeks-comments-childrens-online-privacy-protection-act-rule, July 25 2019.

[24] J. Valentino-DeVries, N. Singer, A. Krolik, and M. H. Keller. How game apps that captivate kids have been collecting their data. https://www.nytimes.com/interactive/2018/09/12/technology/kids-apps-data-privacy-google-twitter.html, September 12 2018.

[25] J. Wakefield. Location data collection firm admits privacy breach. https://www.bbc.com/news/technology-59063766, October 29 2021. Accessed: November 15, 2021.

[26] P. Wijesekera, A. Baokar, A. Hosseini, S. Egelman, D. Wagner, and K. Beznosov. Android permissions remystified: A field study on contextual integrity. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 499–514, Washington, D.C., Aug. 2015. USENIX Association.

[27] P. Wijesekera, A. Baokar, L. Tsai, J. Reardon, S. Egelman, D. Wagner, and K. Beznosov. The feasability of dynamically granted permissions:
aligning mobile privacy with user preferences. In *Proceedings of the 2017 IEEE Symposium on Security and Privacy*, Oakland '17. IEEE Computer Society, 2017.

[28] P. Wijesekera, J. Reardon, I. Reyes, L. Tsai, J.-W. Chen, N. Good, D. Wagner, K. Beznosov, and S. Egelman. Contextualizing privacy decisions for better prediction (and protection). In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, pages 1–13, New York, NY, USA, 2018. Association for Computing Machinery.