Graves J. An Exploratory Study of Mobile Application Privacy Policies. *Technology Science*. 2015103002. October 30, 2015. http://techscience.org/a/2015103002/

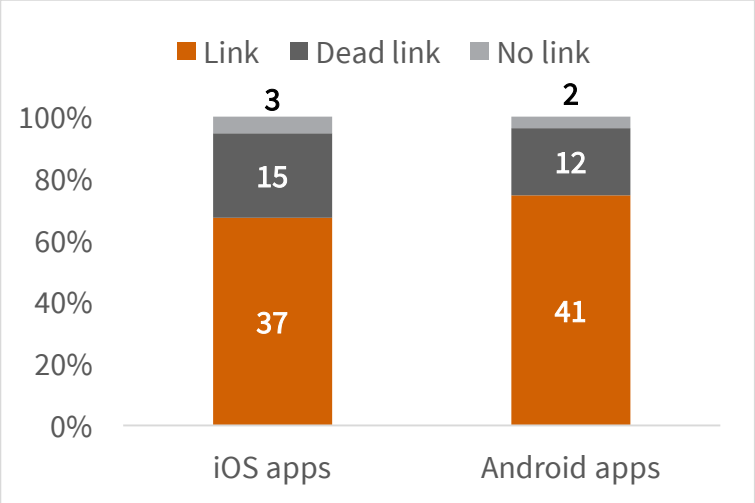
Technology Science

An Exploratory Study of Mobile Application Privacy Policies

James Graves

Highlights

- I examined privacy policies for 110 popular Android and iOS apps. App stores provided working links to privacy policies for 67% of iOS apps and 75% of Android apps
- 61% of privacy policies specifically stated that data would be encrypted. 31% had general language that could be read to imply that encryption would be used. Another 5% of privacy policies said nothing about security. One policy stated that it did not use encryption



Availability of links to privacy policies at online stores for the 110 apps examined

Abstract

I reviewed the privacy policies for the 110 apps included in a study of sensitive data sharing by mobile apps. [1] I focused on (1) the prevalence of privacy policies for mobile applications and (2) what, if anything, those policies said about the use of encryption for data in transit.

Results summary: For the 110 apps I reviewed, the app store pages provided working links to privacy policies for 67% of the iOS apps and 75% of the Android apps. Of the apps with accessible privacy policies, 62% contained general language saying that security measures would be used but did not specifically promise that encryption would be used, 31% included language implying that the apps encrypted some types of data in transit, 5% said nothing about security, and one policy (2%) affirmatively stated that encryption was *not* used (although, according to our testing, it actually did).

Introduction

The Federal Trade Commission began studying website privacy policies in 1998. In a report to Congress that year, it found that although 85% of the sites it surveyed collected personal information, only 14% provided any notice of those practices, and only 2% had comprehensive privacy policies. [2] Since then, the FTC has encouraged adoption of privacy policies through its notice-and-choice framework. Laws, including COPPA, HIPAA, Gramm-Leach-Bliley, and the California Online Privacy Protection Act, now require many websites to publish privacy policies. Today, the vast majority of large websites seem to have privacy policies. However, are privacy policies for mobile applications readily available?

Background

Privacy policies have received extensive research attention in the past 15 years. In 2000, the FTC followed up on its 1998 report with one of the earliest comprehensive surveys of privacy policies. [3] Two years after that, it looked at privacy policies of websites targeted at children. [4] More recently it has surveyed the privacy policies of mobile apps targeting children, releasing two reports in 2012 and conducting a follow-up survey in 2015. [5, 6, 7]

Privacy policies are also an active area of research in academia. Surveys have focused on privacy policies in areas including health data, [8][9] financial records, [10] children's privacy, [11] and online tracking. [12] An article published shortly after the FTC's 2000 report to Congress examined privacy policies of the Fortune E-50 for compliance with the Fair Information Principles. [13] A recent article in Technology Science tracked the evolution of Facebook's privacy policy over time [14]. All these studies focused on privacy policies for websites. I focused on two questions: (1) How prevalent were privacy policies for the apps tested in the mobile app survey, and (2) what do those privacy policies say about the use of encryption for data in transit?

Methodology

In August 2014, I used the Apple App Store (iOS) and Google Play (Android) stores to view the pages for the 110 applications (55 in each store) included in the mobile app survey. These are the same apps used in a simultaneous study that tracked flows of sensitive personal information. [1] In my study, I noted whether each app page included a link to the app

developer's privacy policy. If so, I used the link to visit the developer's website and download the policy. If an app page did not include a link to a privacy policy, I looked for a privacy policy at the developer's website.

I read each privacy policy to determine whether it said outright, or could be read to imply, that some data would be encrypted when transmitted. I categorized the language for each policy as either (1) making general statements about security, (2) specifically stating that some transmitted data is encrypted, (3) specifically stating that transmitted data is *not* encrypted, or (4) not addressing the issue.

I also downloaded terms of service and license agreements for each app when available. In the case of iTunes, this was no easy task. Although privacy policies in iTunes are provided via links to developer websites, license agreements are presented within iTunes itself, which does not allow license agreements to be selected, copied, saved, or printed. I did not refer to the terms of service or license agreement documents when interpreting the language of the privacy policies.

Results

Prevalence of Privacy Policies on App Store Pages

Of the 55 apps reviewed in each store, the pages for 37 iOS apps (67%) and 41 Android apps (75%) included working links to privacy policies (Figure 1). The pages for another 3 iOS apps and 2 Android apps had links that did not lead to privacy policies ("dead links").

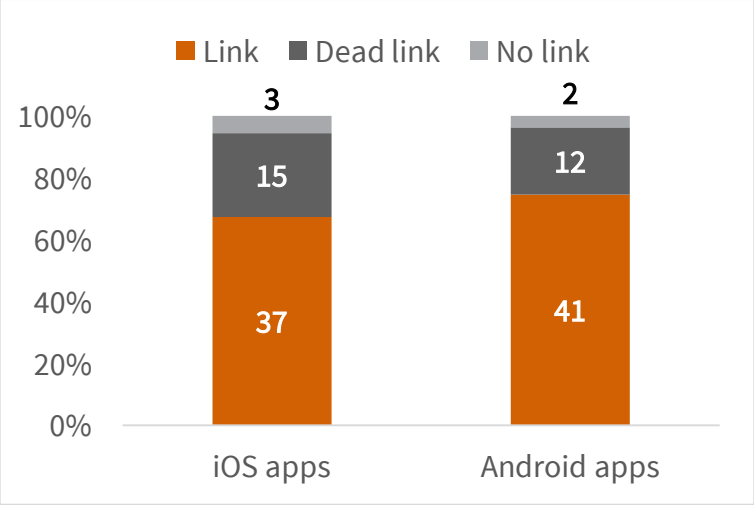


Figure 1. Availability of privacy policies in the Apple (iOS) and Android app stores for the 110 apps tested.

There was overlap in privacy policies between apps. For each app that we reviewed, the developer or publisher had a single privacy policy that applied to all its apps. Some developers had multiple apps in our list (for example, Halfbrick with Fruit Ninja and Fish Out of Water), and some apps in our list appeared in both the Apple and Google stores. There were also a few privacy policies that could easily be found on the developers' web pages but that were not linked on the app store pages. In total, I reviewed 55 privacy policies.

Privacy Policy Language

Of the 55 policies, 34 (62%) contained general language about the use of security measures that could be read to imply—but did not specifically state—that the app would encrypt some transmitted data. For example, Adobe's privacy policy said that they "provide reasonable administrative, technical, and physical security controls to protect your personal information." The policies that spoke in general terms often used phrases like "appropriate" measures or safeguards (Adobe, King.com), "reasonable care" (GoodRx), "reasonable security" (MyFitnessPal), "industry standard measures," (GoodRx), "commercially reasonable efforts" (Kik), or "generally accepted industry standards" (Yelp).

Another 17 policies (31%) included language stating that the apps encrypted some types of data in transit. Some policies named specific technologies. For example, the policy for Drugs.com included the statement, "We use SSL (Secure Socket Layer) technology to protect your sensitive information (if any) on our site." Others referred to encryption more generally. ContextLogic's privacy policy for Wish, for example, said, "We have implemented encryption or other appropriate security controls to protect Personal Information when stored or transmitted by ContextLogic."

One policy (2%) specifically said that the app did *not* use encryption. The Points2Shop privacy policy read, in part, "Points2Shop LLC does not employ the use of secure transmission methods to send personal data." In our tests, however, the Points2Shop app actually *did* encrypt almost everything it sent, raising the question of whether the policy language was a typo or perhaps a holdover from when a previous version of the app did not use encryption. Or perhaps Points2Shop did not believe that the encryption method it used (SSL) was secure.

Finally, 3 policies (5%) did not say anything about security.

Discussion

Nearly all (51/55) of the policies included some statement either explicitly or implicitly indicating that data in transit would be encrypted.

As mentioned above, the privacy policies applied to companies, not specific applications. Most of the policies appeared to have been written with websites in mind and their

applicability to mobile apps was not always clear. Some policies, however, explicitly included mobile apps either as "online services" or in their definitions of websites.

Most of the policies also contained disclaimer language that could be interpreted as hedging statements made elsewhere about security. For example:

- The privacy policy for King.com, the makers of Bubble Witch Saga and Candy Crush Saga, included the statement that "since the internet is not a completely secure environment we cannot guarantee that information you transmit via our Games will not be accessed, disclosed, altered or destroyed by breach of any of our safeguards."

- Halfbrick, developer of Fish Out of Water and Fruit Ninja, includes the following statement in its privacy policy: "There are inherent risks in transmitting information over the Internet and it is possible that we could be hacked. You should feel comfortable with this level of risk before you provide information to us, or use our Services. If you are not comfortable with this risk, please do not use our Services."

- Statements like Adobe's are common: "Despite our efforts, no security controls are 100% effective and Adobe cannot ensure or warrant the security of your personal information."

In a policy that explicitly promises that encryption is used, these disclaimers may merely stress the fact that no technical measure is guaranteed to completely protect data. But when this language appears in the same policy as a general statement that the company takes "reasonable" controls (as is the case with the King.com, Halfbrick, and Adobe examples listed above), it is hard to know what level of security, if any, the company is promising in its policy.

Although most apps had links to privacy policies, privacy policies do not appear to be as prevalent (as of mid-2014) in the mobile space as they are for websites overall. That may change as laws and regulations catch up with mobile applications.

References

1. Zang J, Dummit K, Graves J, Lisker P and Sweeney L. Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps. Technology Science. October 30, 2015. http://techscience.org/a/2015103001/

2. Federal Trade Commission 1998. Privacy Online: A Report to Congress. https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf

3. Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress: 2000. https://www.ftc.gov/sites/default/files/documents/reports/privacy-

online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf. Web: 2015-10-19.

4. Federal Trade Commission 2002. Protecting Children's Privacy Under COPPA: A Survey on Compliance. https://www.ftc.gov/sites/default/files/documents/rules/children%E2%80%99s-online-privacy-protection-rule-coppa/coppasurvey.pdf

5. Federal Trade Commission 2012. Mobile Apps for Kids: Current Privacy Disclosures are Disappointing. https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing/120216mobile_apps_kids.pdf

6. Federal Trade Commission 2012. Mobile Apps for Kids: Disclosures Still Not Making the Grade. https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-disclosures-still-not-making-grade/121210mobilekidsappreport.pdf

7. Kids' Apps Disclosures Revisited: https://www.ftc.gov/news-events/blogs/business-blog/2015/09/kids-apps-disclosures-revisited. Web: 2015-10-20.

8. Antón A, Earp J, Vail M, Jain N, Gheen C, Frink J et al. HIPAA's effect on Web site privacy policies. Security & Privacy, IEEE. 5, 1. 2007, 45–52. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4085593

9. Carrión Señor I, Fernández-Alemán J and Toval A. Are Personal Health Records Safe? A Review of Free Web-Accessible Personal Health Record Privacy Policies. Journal of Medical Internet Research. 14, 4. August. 2012. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3510685/

10. Cranor L, Idouchi K, Leon P, Sleeper M and Ur B. Are they actually any different? Comparing thousands of financial institutions' privacy practices. The Twelfth Workshop on the Economics of Information Se-Curity (WEIS 2013). 2013. http://www.econinfosec.org/archive/weis2013/papers/CranorWEIS2013.pdf

11. Privacy Policies on Children's Websites: Do They Play by the Rules? 2001. http://www.annenbergpublicpolicycenter.org/Downloads/Information_And_Society/20010328_Children_Privacy_on_Web/20010328_Childrens_Privacy_on_Web_report.pdf. Web: 2015-10-19.

12. Hoke C, Cranor L, Leon P and Au A. 2015. Are They Worth Reading? An In-Depth Analysis of Online Trackers' Privacy Policies. I/S: a journal of law and policy for the information society. 2015. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418590

13. Ryker R, Lafleur E, McManis B and Cox K. Online privacy policies: An assessment of the fortune E-50. Journal of Computer Information Systems. 42, 4, 15–20. 2005. http://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1175&context=jiim

14. Shore J, Steinman J. Did You Really Agree to That? The Evolution of Facebook's Privacy Policy. Technology Science. 2015081102. August 11, 2015. http://techscience.org/a/2015081102

Authors

Jim Graves is a PhD student in Engineering and Public Policy at Carnegie Mellon University, where his research focuses on the law and economics of data privacy. Before returning to school, he worked as a data security and networking professional for over 15 years. Jim earned his JD from William Mitchell College of Law, where he was Editor-in-Chief of the Law Review, and holds an M.S. in Information Networking and a B.S. in Mathematics and Computer Science, both from Carnegie Mellon University.

This work was conducted at the Federal Trade Commission during the summer of 2014 as part of the Summer Research Fellows Program. All statements, analyses and conclusions are the authors' and do not necessarily reflect any position held by the Federal Trade Commission or any Commissioner.

Referring Editor: Latanya Sweeney

Citation

Graves J. An Exploratory Study of Mobile Application Privacy Policies. *Technology Science*. 2015103002. October 30, 2015. http://techscience.org/a/2015103002/

Data

Under review for data sharing classification.