Developing a Windows Privacy Walkthrough Experience: Executive Summary

Carnegie Mellon University
Privacy Engineering Capstone Project, Fall 2017
Team Members: Dhanuja Shaji and Javed Ramjohn

Privacy can be leveraged as a competitive advantage in the market, and it is only increasing in its importance as the public is continually inundated with stories about data breaches and privacy violations.

Windows is the most popular operating system on the market, so its privacy experience impacts many. Developing a usable and comprehensive privacy experience lends further evidence to Microsoft's commitment to user privacy and adds another advantage to using Windows.

This project provides data to help inform Microsoft on how to deliver a state-of-the-art privacy experience for Windows 10 desktop that empowers the user.

Microsoft, our client, had a clear roadmap for the direction our project would take. The three components that they asked for in the project proposal are delivered. The first component, a study on consumer preferences, habits, expectations, and experiences with operating system privacy, helps get a sense of what's important to consumers with regard to operating system privacy and how they would like to manage their operating system privacy. The next component is a competitive analysis of privacy experiences on major online platforms and operating systems. Seeing how Windows 10 compares with popular platforms enables a benchmark of where Windows 10 stands, what current best practices appear to be, and what gaps need to be addressed that the major players haven't already tackled. Finally, drafts for a prototype walkthrough tutorial on Windows 10 privacy settings are presented for Microsoft to do further iteration, usability testing, and eventual implementation.

With these well-defined components, it was our job to define a feasible scope and come up with implementation plans that were appropriate and well-suited for our client's needs. Through continual iteration and discussion of our plan and interim deliverables with our client, we crafted a project plan and goal that was met with approval and mutual understanding.

A research survey (N=364) hosted on Qualtrics would be conducted on Amazon Mechanical Turk that would ask questions about a participant's operating system privacy, their privacy expectations, what they thought their operating system collects, and how participants would like to manage their operating system privacy.

We found that while only 27% believe that their operating system does not respect their privacy. Furthermore, Participants were strongly opposed to third-party sharing, with 50% being against OS vendors sharing anonymized information with third parties and 75% against sharing personal information with third parties.

While we expected participants to want most control over activities that involve a lot of data collection, such as personalized ads, diagnostics, and digital assistants, these three were ranked among the least important to have control over in lieu of application access to information like camera, microphone, contacts, messages, and call history.

Interestingly, while participants wanted control over application permissions, they mostly allowed access when given concrete scenarios, such as video conferencing or productivity applications keeping them updated based on the information collected.

Participants strongly disliked the collection and use of browsing information, usernames, anonymized typing input, and disliked giving access to emails and messages.

Finally, 80% of participants want an occasional privacy review, 67% want notifications to review their privacy settings, and 68% want to be directed to a walkthrough from those notifications. Only 27% of participants felt they received too many notifications, suggesting that privacy walkthroughs and privacy notifications would not burden users.

The competitive analysis focuses on 8 of the 10 top web services on Alexa's ranking for the United States. Specifically, we selected Google, Amazon, Twitter, Facebook, Reddit, LinkedIn, ESPN, and Netflix. In addition, for a more direct comparison, we analyzed the major operating systems: macOS Sierra, Android 8.0 Oreo, Chrome OS, and iOS. Objective criteria for analyzing privacy experiences were crafted in consultation with our client and were used to compare these various services and platforms. In addition, we provide in-depth analysis of each along with similarities, differences, gaps in the market, and our own expert commentary and recommendations based on the analysis.

Unfortunately, the results from the competitive analysis show that most major services don't offer a proactive privacy walkthrough experience. Even among platforms that offer privacy nudges and walkthrough experiences, those that have many services and products can have privacy settings scattered throughout with no centralized way to manage them all, even from privacy dashboards. The good news is that Microsoft has positioned itself to already being a leader by having granular privacy settings and a centralized privacy dashboard.

For the walkthrough drafts, we took the format of tutorials on the Microsoft Tips App and created similarly styled tutorials for modifying the privacy settings listed on the privacy menu within Windows 10's settings. Informal user testing was done to get feedback on clarity and usefulness.

Overall, participants found the walkthroughs helpful and would be interested in seeing similar walkthroughs in Windows 10. However, there are issues such as wordiness and length that need to be fine-tuned for some walkthroughs. Participants also wanted more pros and cons and information based on their own usage habits that would enable them to make a decision that best matches those usage habits.

We recommend focusing on more transparency and control around privacy settings, especially since our findings show users will still allow access once there's a clear use for giving such access. Educating Windows users about "no content-based targeting" and allowing for greater transparency into local account data collection can help resolve inaccuracies in users' mental models. We also recommend implementing a notification-based privacy walkthrough experience.

Our work also gives rise to new questions surrounding further user testing of a walkthrough experience in Windows 10, studies on control and transparency, improving the explanation of services like Cortana and location, and studies on device synchronized privacy preferences in an IoT context.