Claire Lobdell - LFI Week 5

As background, my school district voted to start a 1:1 Chromebook program for students in grades 3-12 starting in the 2018-2019 school year. The policies around this program have not yet been made public, so there are a number of outstanding questions. For example:

- Will families be able to opt out?
- Will all students will be able to take their laptop home, or will that only be for students in upper grades?
- Will the teachers and/or administrators have access to student accounts? If so, who, and under what circumstances? Will district staff be explicitly forbidden from turning on device webcams remotely?
- Does the student own the device or does the district?
- Are there third party apps that students will be required to install on their devices, if so, which ones, what are their data security policies, and do they comply with FERPA?

1. *What do you want to protect?*
Students' private data, including communications, demographic information, data about personal preferences and interests, location information, grades, webcam access, and search history, as well as that same information for family members who may use the device.

2. *Who do you want to protect it from?*
Data brokers, advertisers, Google, bullies, parents, teachers and administrators, and ICE (some students or family members may be undocumented).

3. *How likely is it you will need to protect it?*
100% likely from data brokers, advertisers and Google[1]. Somewhat likely from bullies, parents, teachers and administrators, and ICE. The individual risks vary based on the individual student.

4. *How bad are the consequences if you fail?*
Again, this depends on the individual student—if you compromise the privacy of an undocumented student, or an LGBTQ+ or sexually active student living with religiously conservative caregivers, you could endanger that child's physical safety. If you encourage/require the use of apps that harvest a large amount of personal data, you make students vulnerable to identity theft, as well as intrusive advertising[2].

5. *How much trouble am I willing to go through to prevent these consequences?*
The district should install Privacy Badger and Https Everywhere on all Chromebooks before they are distributed, and configure Chromebooks according to the EFF guides listed in the resources below.

In addition, the district must include curricula in every grade that will teach students about online safety and privacy. The district must also offer resources about these topics to parents in a variety of formats (in-person workshops, online guides, handouts, etc., in multiple languages).

---

[1] https://www.wired.com/2015/12/google-collected-data-on-schoolchildren-without-permission/

[2] The Electronic Frontier Foundation explains the data that Chromebooks and Google Apps For Education collect about students, as well as how that data is stored: https://www.eff.org/issues/student-privacy/faq#faq-What-data-does-Google-collect-about-students?

Finally, the district must address the policy questions above, in a way that includes input from all stakeholder groups (students, parents, teachers, administrators, district IT staff, privacy experts, and legal experts).

Resources:

EFF guide to Chromebook privacy settings for students: https://www.eff.org/deeplinks/2015/11/guide-chromebook-privacy-settings-students

EFF guide to Google Account privacy settings for students: https://www.eff.org/deeplinks/2015/11/guide-google-account-privacy-settings-students