Chrome Privacy Settings
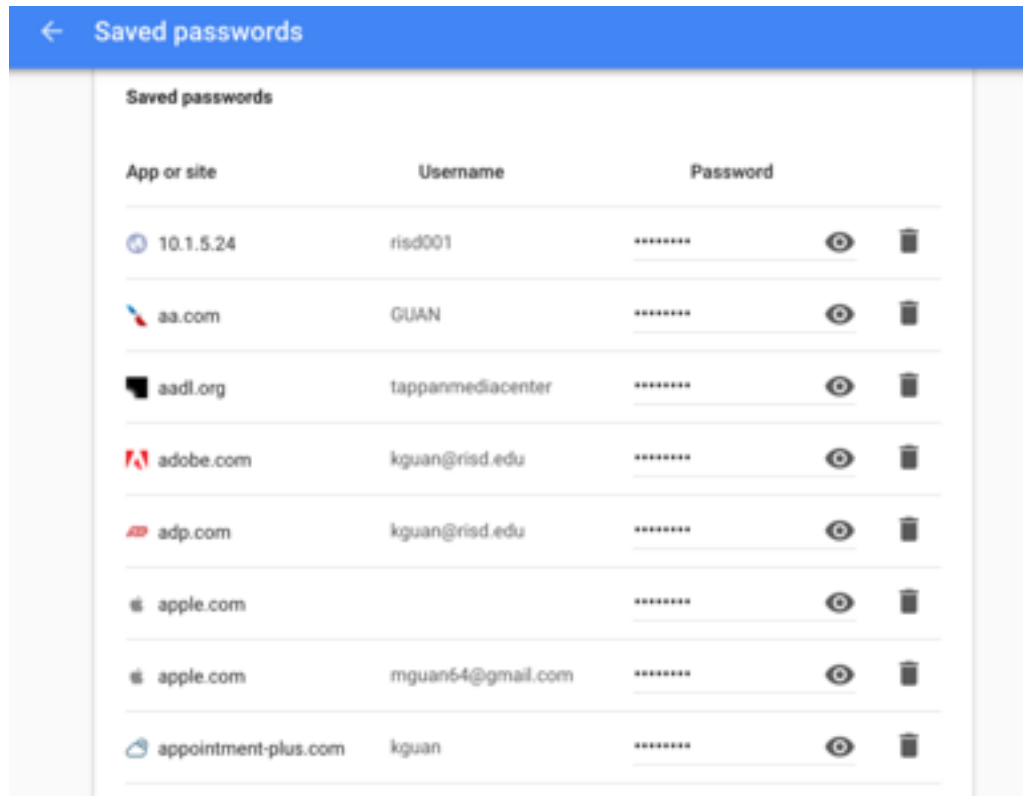
The data the Chrome browser collects:

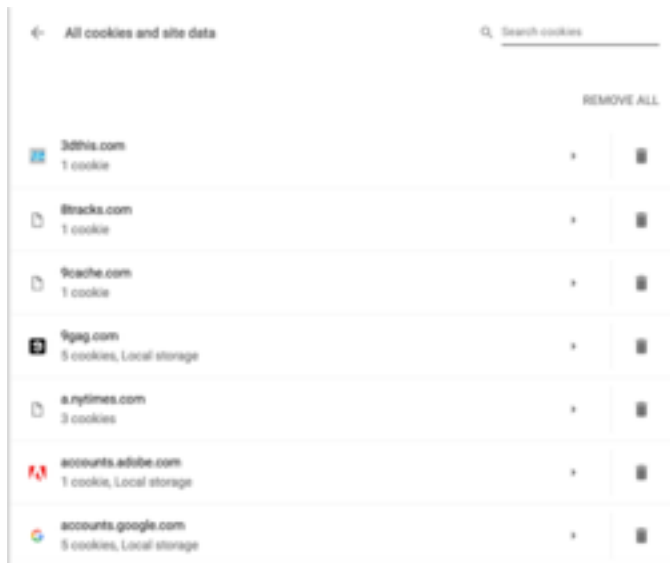Locally, passwords and payment information is collected for autofill fields.

Information sent to Google include searches, both complete and incomplete, as well as usage statistics and crash reports. The searches include voice searches. There is a separate page where you can see what audio files chrome has kept of yours, and you can delete them. There is also an option to take out this autocomlete.Usage means preferences, button clicks, and memory usage. It does not include web page URLs. This information is used to predict what you are searching for, and to suggest adjacent sites. It is also used for spellcheck.

Cookies:

These are tracking devices from other websites. The collect data from where you travel to on the web, and send this data to companies that use it to pinpoint advertise. They can be cleared from your history. You can view cookies in the privacy settings. There are also chrome extensions that block cookies, such as privacy badger. There is an option to send a "do not

track" message to websites. This does not mean you stop all tracking, it just means that you notified the website.

Content settings:

You can also regulate what websites have access to your location, microphone, and camera. The default or recommended setting is for a pop-up to ask you if the website can acess these things. Once you accept, websites can be added to a list of accepted websites. If a website is on this list, pop-ups will not show up to ask you again. The kind of camera and microphone recordings are usually done by phone, and not on a browser.