Browsers, social media, and advertising:
Talking points

1. Large internet companies are primarily advertising companies (use stats from April's lecture: Google gets 84% of their revenue from advertising and receives 40% of all US online ad revenue. Facebook receives another 20% of US online ad revenue).

2. Cookies, "likes" and social engineering are used to target this advertising, sometimes in hugely nefarious ways (cite ProPublica exposés about Facebook ad targeting by race, hate group affiliation, etc.[1][2][3]).

3. Cookies also enable online retailers to use "personalized pricing" or "dynamic pricing"—in other words, they charge different people different prices for the same product.[4]

4. Instead of using Google, you can use a search engine like DuckDuckGo, which does not track your web browsing, along with Privacy Badger as a browser extension to block ad tracking.

5. Google and Facebook's revenue comes largely from hyper-focused advertising based off the user data we give them for free. They have demonstrated through the Cambridge Analytica revelations[5] (Facebook) and Google's policy of allowing app developers to read users' private email messages[6], that the desires of their paying customers are more compelling than the privacy of the free users of their services.

---

[1] https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin

[2] https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race

[3] https://www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters

[4] https://www.theguardian.com/commentisfree/2016/dec/06/cookie-monsters-why-your-browsing-history-could-mean-rip-off-prices

[5] https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[6] https://www.wsj.com/articles/techs-dirty-secret-the-app-developers-sifting-through-your-gmail-1530544442