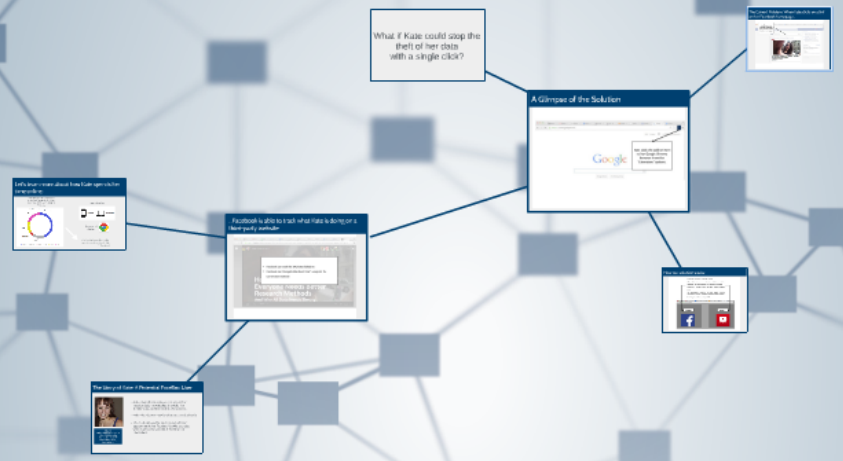
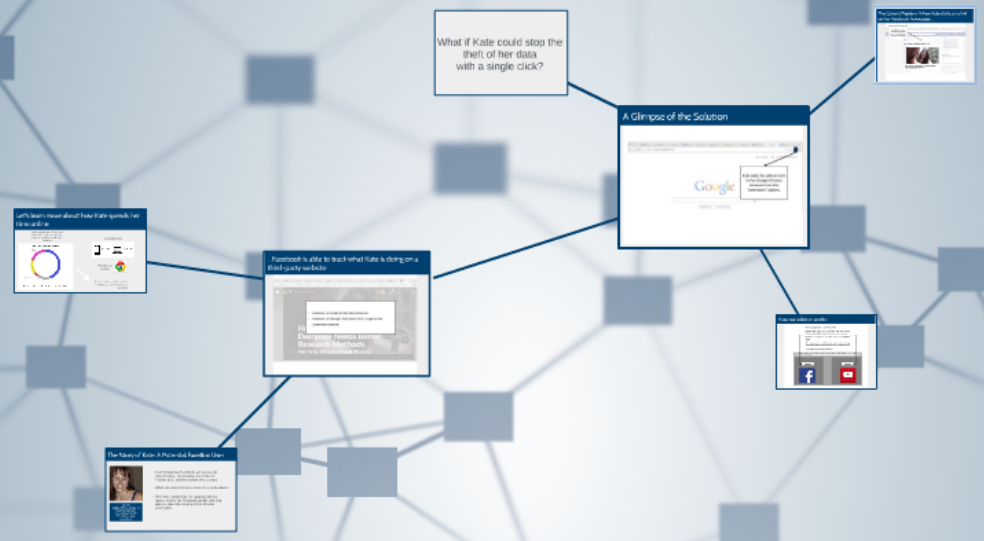


FaceBox

Track-free browsing



FaceBox

Track-free browsing

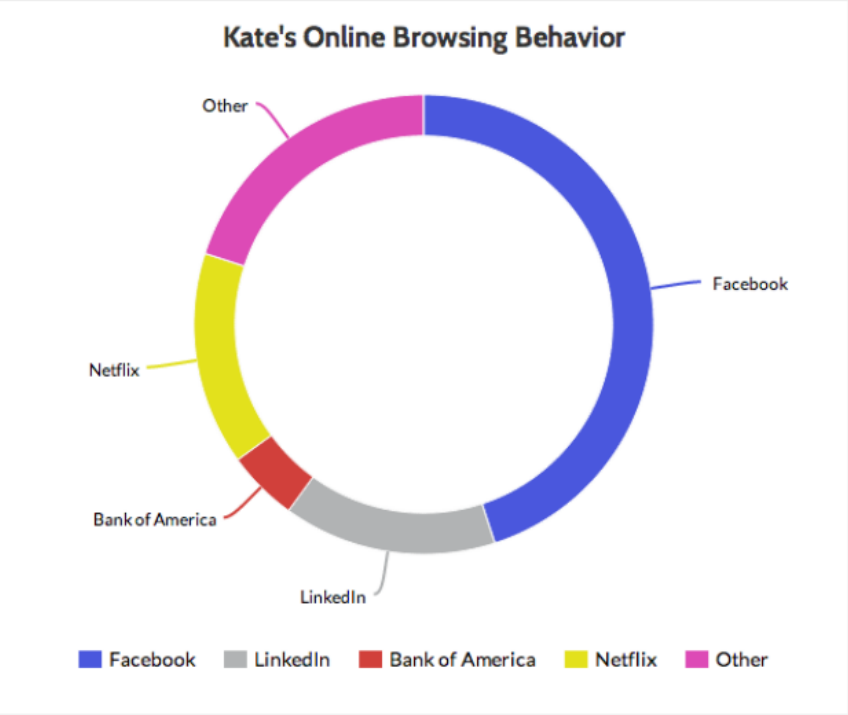
The Story of Kate: A Potential FaceBox User

Age: 20
Studies Political Science at New York University
Lives in New York, NY
From Philadelphia, Pennsylvania

- Kate knows that Facebook can access her location data, the websites she visits, her friends' data, and the content she streams.
- What she doesn't know is what she can do about it.
- She feels annoyed by the targeted ads that appear next to her Facebook profile, and also worries about the security of her financial information.

Let's learn more about how Kate spends her time online:

Kate spends 80% of her time online on Facebook, Youtube, LinkedIn, Netflix, and Bank of America



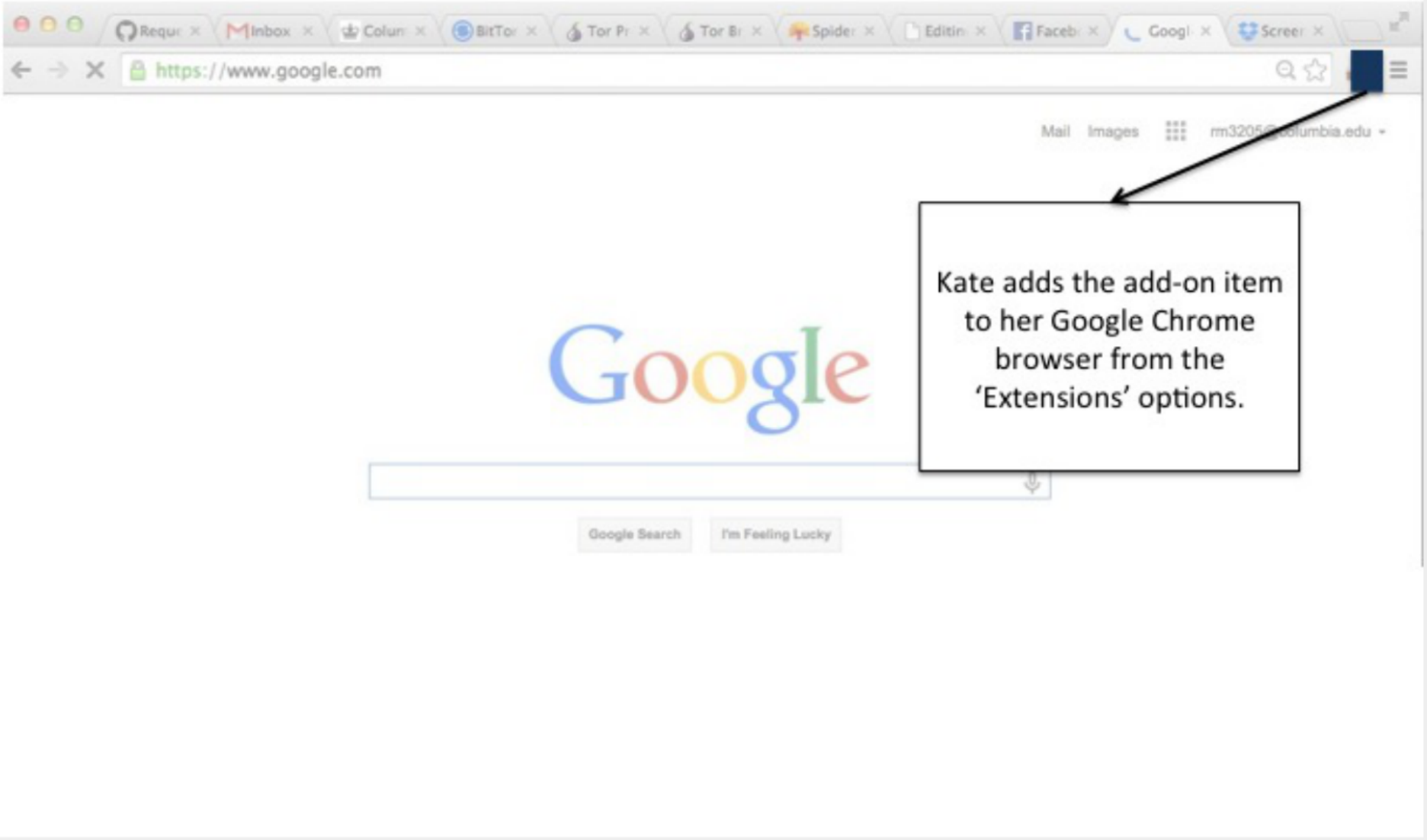
Kate's devices:

Browser of choice:

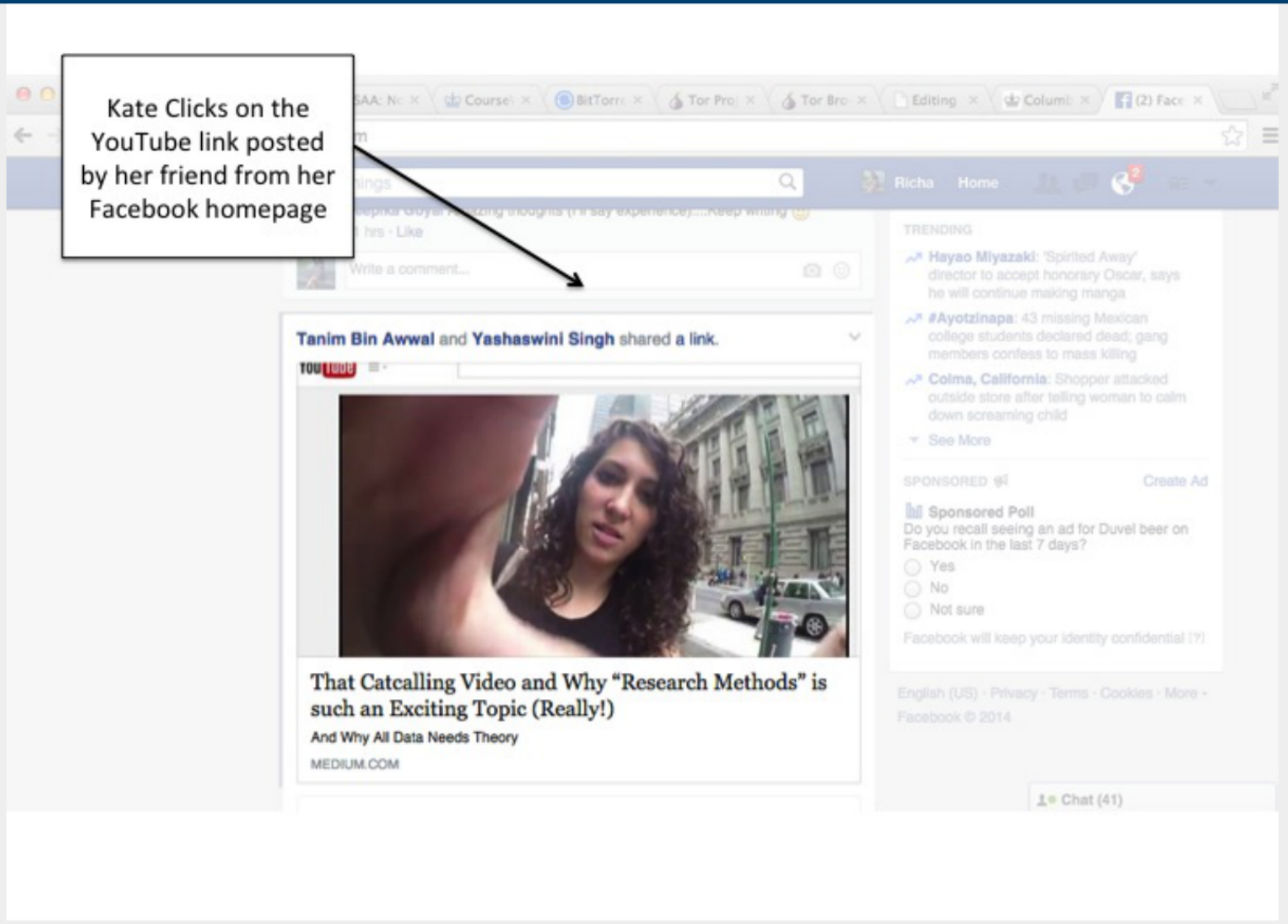
Kate's activities on these other websites are being tracked by Facebook

What if Kate could stop the theft of her data with a single click?

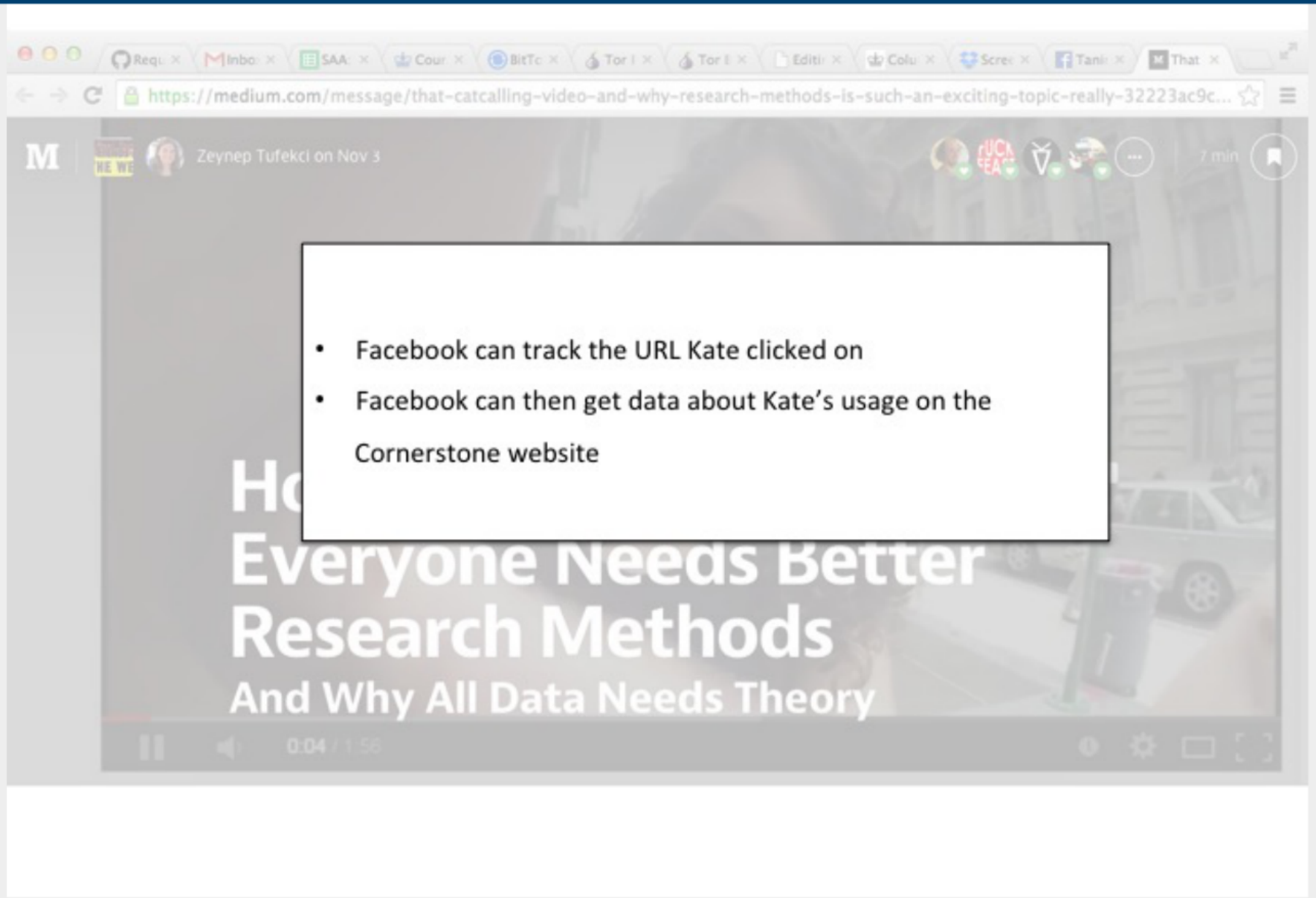
A Glimpse of the Solution



The Current Problem: When Kate clicks on a link on her Facebook homepage...

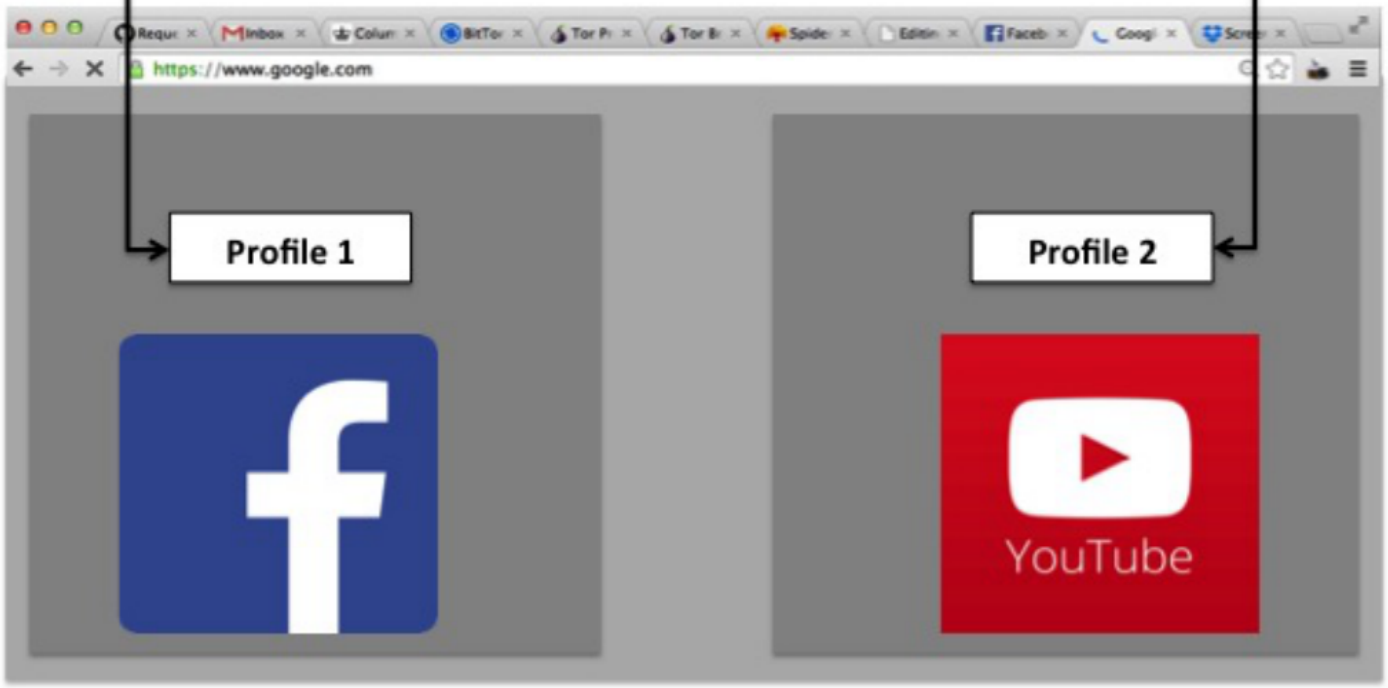


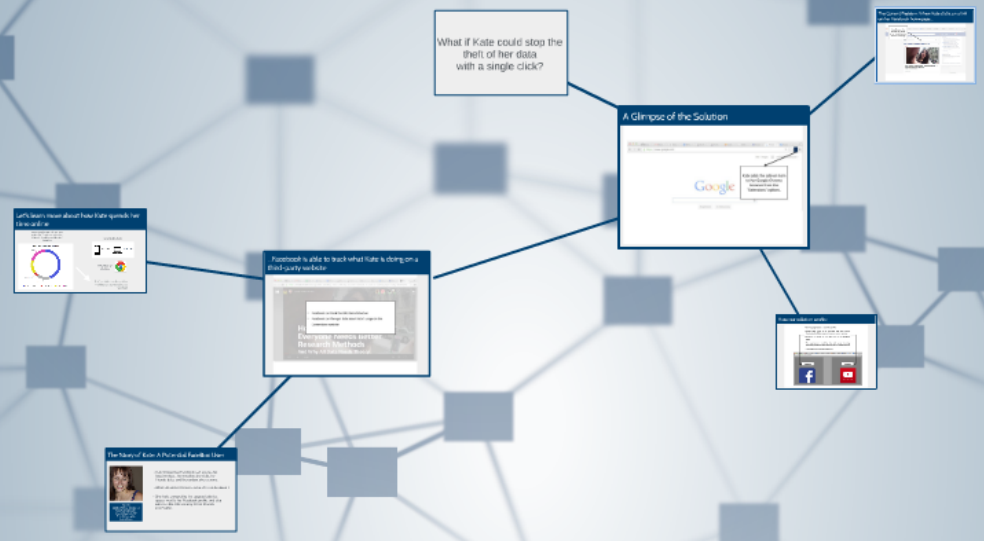
...Facebook is able to track what Kate is doing on a third-party website



How our solution works:

- Each page generates a separate 'profile'
- When Kate clicks on a YouTube link from within Facebook, YouTube is opened in a new secure window
- Facebook is unable to track the data on the YouTube page
- The application modifies the URL used, thereby preventing Facebook from tracking the URL Kate clicks on
- Tracking information is stripped off





FaceBox

Track-free browsing