Lecture 18:
Special Guests;
Tracking Architectures; Blame and Responsibility

CMSC 25900 / DATA 25900

Spring 2021

The University of Chicago

THE UNIVERSITY OF CHICAGO

Examining Two Alternative Approaches to Tracking/Targeting

Mozilla Pocket: Customization With Only Local Tracking

Mozilla Pocket: Customization With Only Local Tracking

Image taken from https://blog.mozilla.org/en/products/firefox/pocket-in-firefox/

Mozilla Pocket: Customization With Only Local Tracking

Your data stays private. Always.

In addition to dishing up captivating stories, we also show you relevant, highly-vetted content from select sponsors. Rest assured, your browsing data never leaves your personal copy of Firefox—we don't see it, and our sponsors don't either. Want more details? Here's the full scoop on how privacy works in Pocket.

Image taken from https://getpocket.com/en/firefox/new_tab_learn_more/
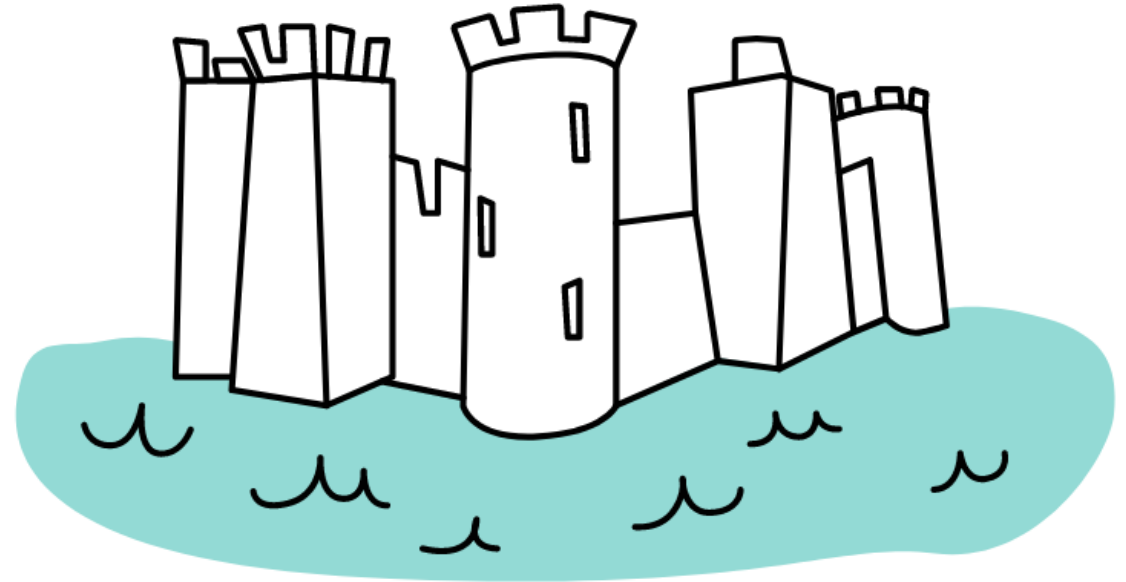
Mozilla Pocket: Customization With Only Local Tracking

Are these stories in the new tab personalized to me?

For the most part, no. Most recommendations on your new tab come from a general list of the best of stories on the web. But Pocket is actively exploring ways to deliver personalized recommendations in a way that vigorously protects users' privacy. Importantly, **neither Mozilla nor Pocket ever receives a copy of your browser history.** When personalization does occur, recommendations rely on a process of story sorting and filtering that happens locally in your personal copy of Firefox.

Is information collected when I interact with these new tab recommendations? What information is collected and what controls do I have?

By default, when recommendations from Pocket are displayed on your new tab, we collect information about how many times they appear and how many times they are clicked. However, this information is not associated with any of the technical and interaction information about you or your copy of Firefox. You can learn more about the data we collect and you can opt out of data collection.
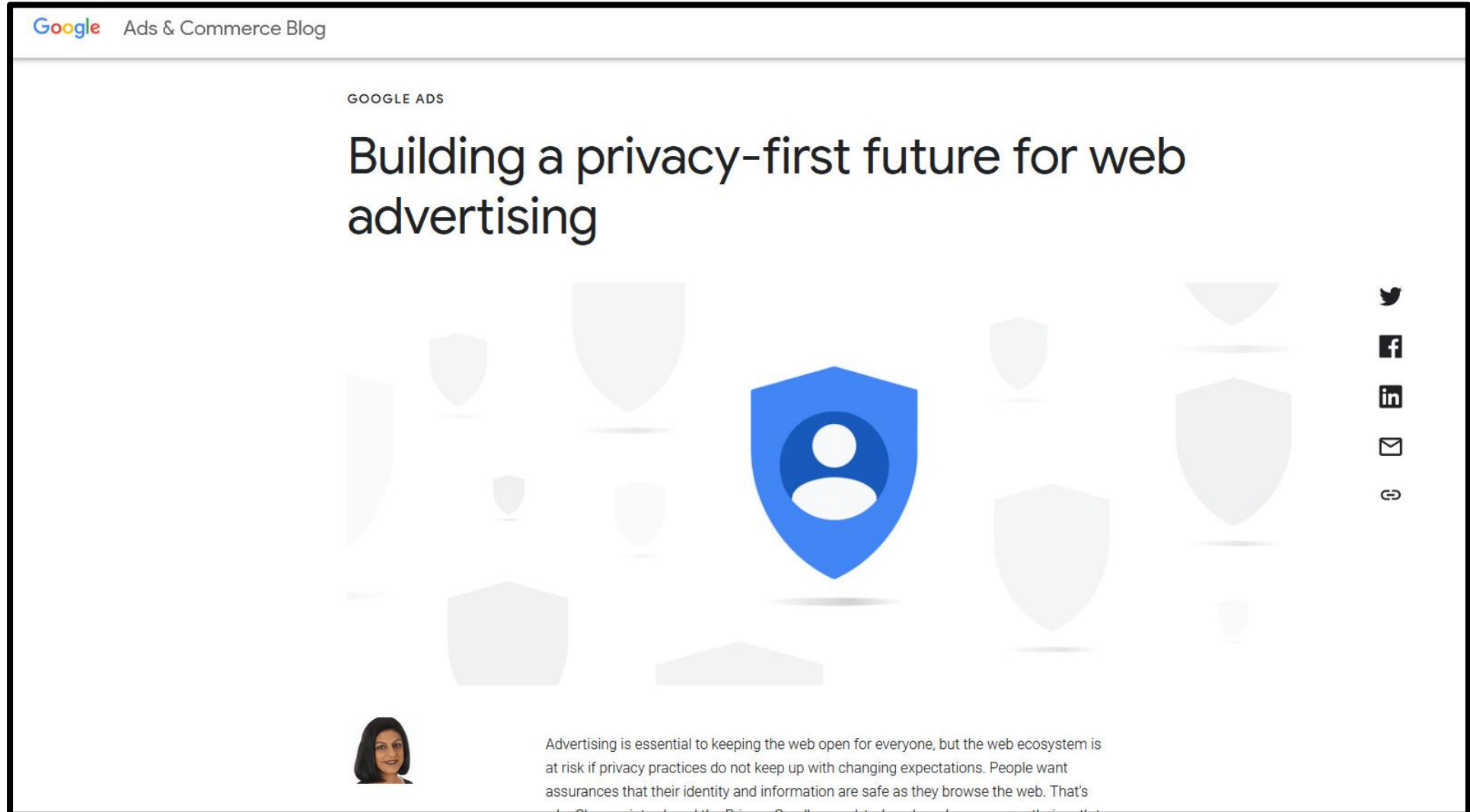
Google FLoC (Google's Perspective)

Image taken from https://blog.google/products/ads-commerce/2021-01-privacy-sandbox/

Google FLoC (EFF's Perspective)

Google FLoC: Architecture

FLoC service	Browser	Advertiser *a site that pays to advertise its products* shoestore.example	Publisher *a site that gets paid to display ads* dailynews.example	Adtech *a company that provides services to deliver ads* adnetwork.example	Publisher *a site that gets paid to display ads* dailynews.example
Create FLoC model	Calculate browser cohort	Observe cohort activity	Observe visitor cohorts	Select ads relevant to cohort	Display relevant ads
The FLoC service creates a mathematical model with thousands of "cohorts". Each cohort corresponds to thousands of web browsers with similar recent browsing histories.	A user's browser, on their device, uses the FLoC model to calculate which cohort corresponds most closely to its own browsing history.	An advertiser observes the activity of cohorts on its site and shares this with its adtech platforms.*	A publisher observes the cohorts of visitors to its site and shares this with its adtech platforms.*	An adtech platform selects ads appropriate for the user's cohort.	The publisher displays ads that are relevant to the user based on their browser's cohort.

* The adtech platform may handle observing the cohort information on behalf of the advertiser or publisher.

Image taken from https://arstechnica.com/gadgets/2021/04/everybody-hates-floc-googles-tracking-plan-for-chrome-ads/
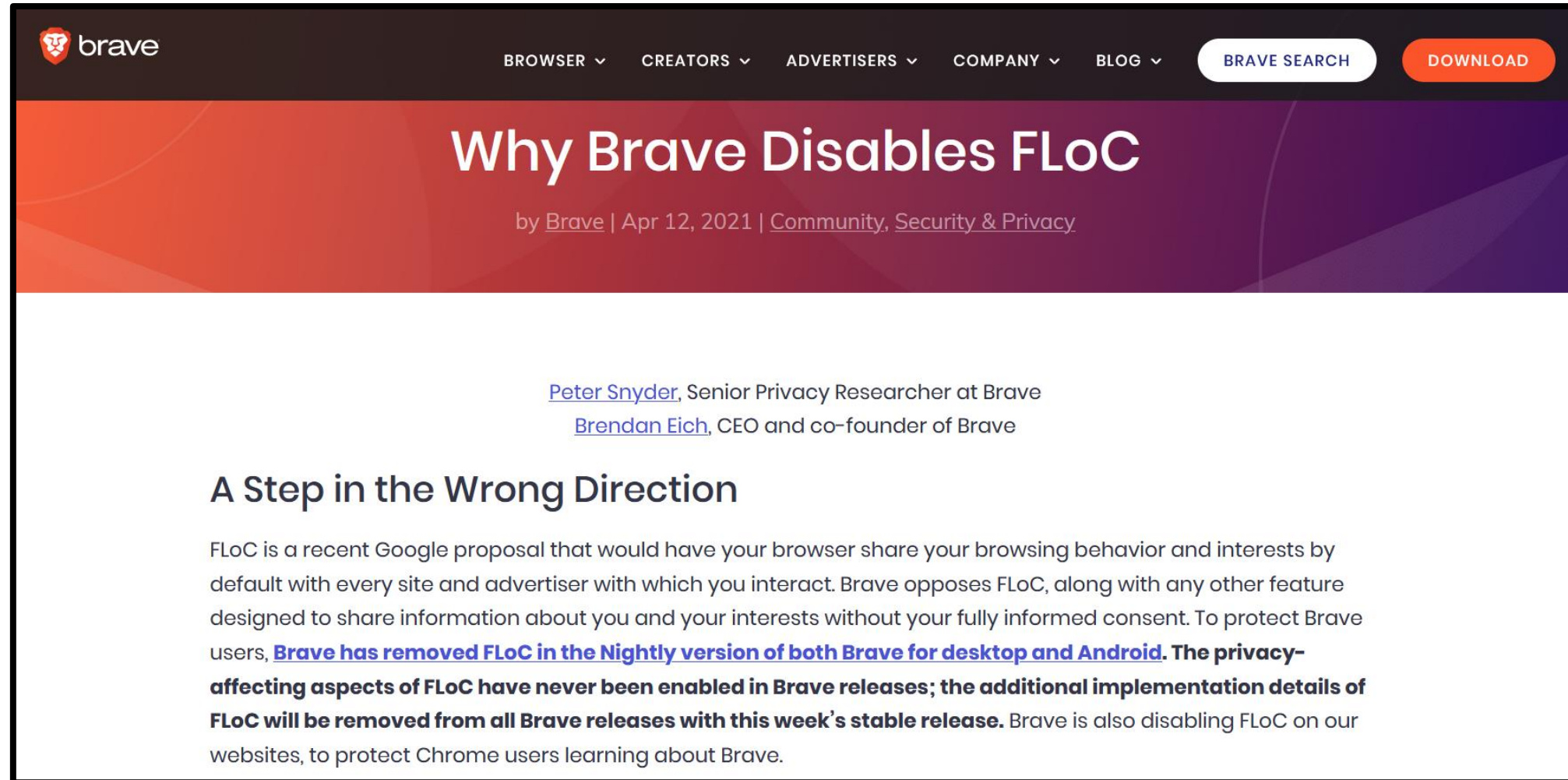
Google FLoC (Brave Browser's Perspective)

Legal Considerations in Computer Systems

Software Licensing

	Free and open (software must have source code provided)			Non-free		
	Public domain	**Permissive license**	**Copyleft (protective license)**	**Noncommercial license**	**Proprietary license**	**Trade secret**
Description	Grants all rights	Grants use rights, including right to relicense (allows proprietization, license compatibility)	Grants use rights, forbids proprietization	Grants rights for noncommercial use only. May be combined with copyleft.	Traditional use of copyright; no rights need be granted	No information made public
Software	PD, CC0	MIT, Apache, MPL	GPL, AGPL	JRL, AFPL	Proprietary software, no public license	Private, internal software
Other creative works	PD, CC0	CC-BY	CC-BY-SA	CC-BY-NC	Copyright, no public license	Unpublished

Table taken from https://en.wikipedia.org/wiki/Software_license

Computer Fraud and Abuse Act (1986)

- Prohibits unauthorized access to a computer system
- "Creates new Federal criminal offenses of: (1) property theft by computer occurring as part of a scheme to defraud; (2) altering, damaging, or destroying information in, or preventing the authorized use of, a Federal interest computer; and (3) trafficking in computer access passwords."
- First felony conviction: Morris Worm of 1988
- Used to prosecute Aaron Swartz for downloading JSTOR articles en masse
- Used to prosecute George Hotz (*geohot*) for jailbreaking the PS3 → settlement

Bug Bounties

Table taken from https://www.bugcrowd.com/bug-bounty-list/

The Difficulty of Managing Data Rights

Data Access Rights / Data Management / Data Freedom
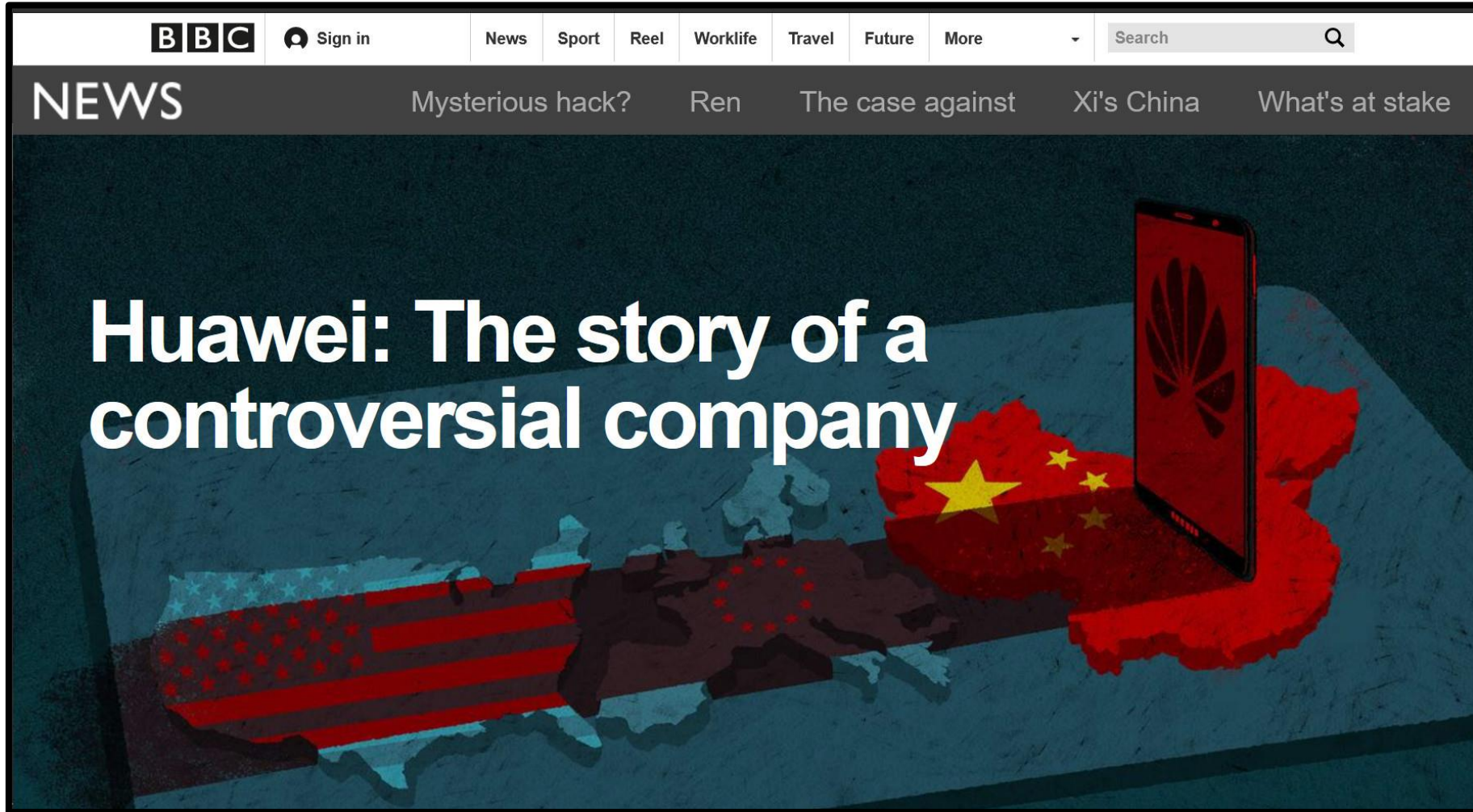
Data Rights Management (DRM) Tech

- The use of technical mechanisms to enforce rights
  - Pretty much an arms race
- Example from the 1990s: DVD Content Scrambling System (CSS)
  - DeCSS from Jon Lech Johansen and others

DMCA Safe Harbor

- Digital Millennium Copyright Act (DMCA) of 1998
  - Criminalizes circumvention of DRM
  - Criminalizes circumvention of access control (regardless of intent or subsequent actions)
  - Raises penalties for copyright infringement on the internet
- Creates safe harbor for online service providers, including ISPs
  - Copyright holders submit DMCA takedown notices
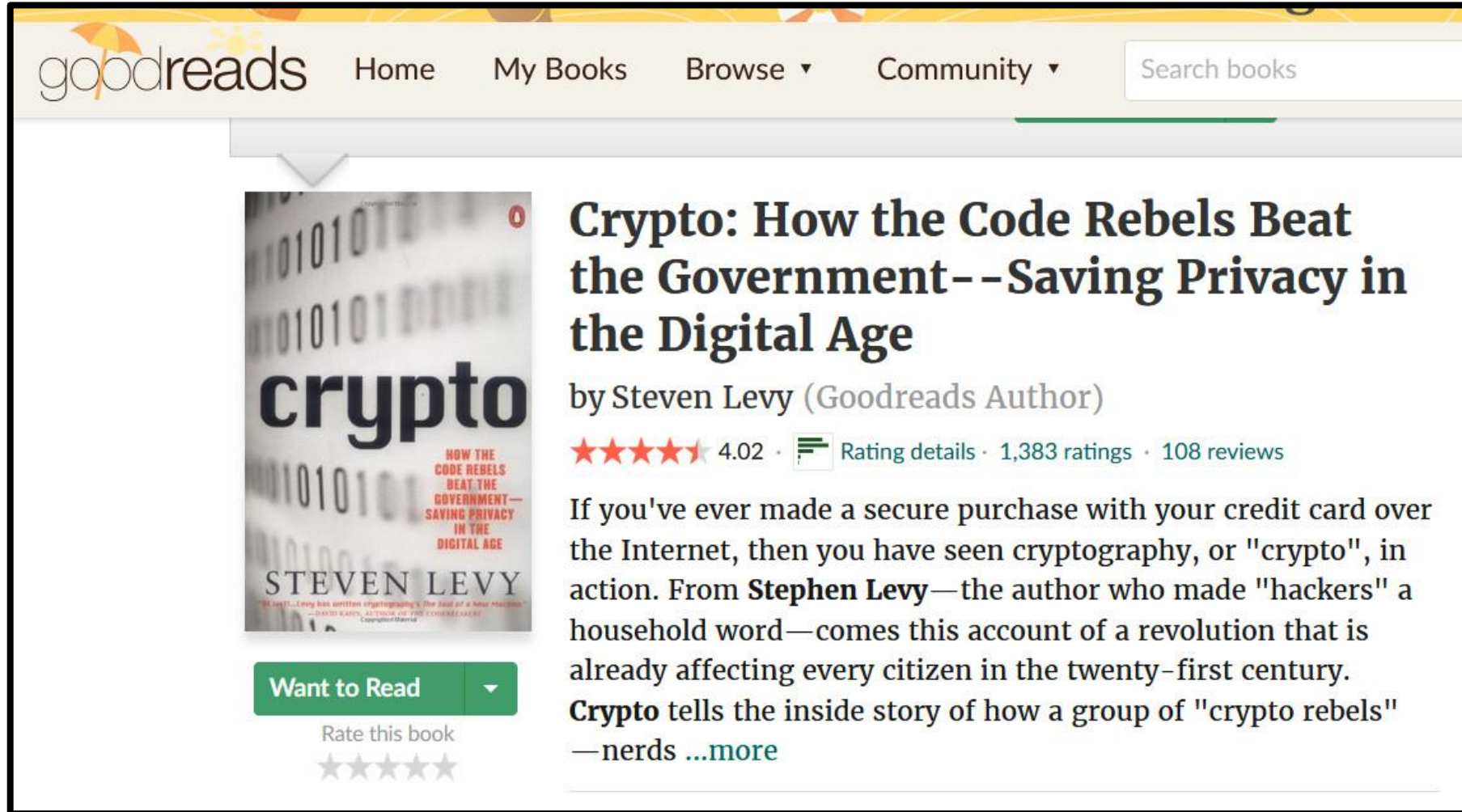 - Takedown notices are now often automated or semi-automated

The Politicization of Technology

Huawei and 5G Politics

See https://www.bbc.co.uk/news/resources/idt-sh/Huawei

The Crypto Wars (of the 1990s)

The Crypto Wars (of the 2010s)

San Bernardino iPhone: US ends Apple case after accessing data without assistance

With the court filing, Silicon Valley and Washington are poised to return to a cold war over the balance between privacy and law enforcement in the age of apps

▲ Justice Department lawyers wrote in a court filing Monday evening that they no longer needed Apple's help in getting around the security countermeasures on Syed Farook's device. Photograph: Mark Lennihan/AP

The US government dropped its court fight against Apple after the FBI successfully pulled data from the iPhone of San Bernardino gunman Syed

See https://www.theguardian.com/technology/2016/mar/28/apple-fbi-case-dropped-san-bernardino-iphone

22

The Crypto Wars (of the 2010s)

Here's how the FBI managed to get into the San Bernardino shooter's iPhone

An Australian firm helped hack into the device, starting with a Lightning port exploit

By Mitchell Clark | Apr 14, 2021, 3:58pm EDT

f 🐦 ↗ SHARE
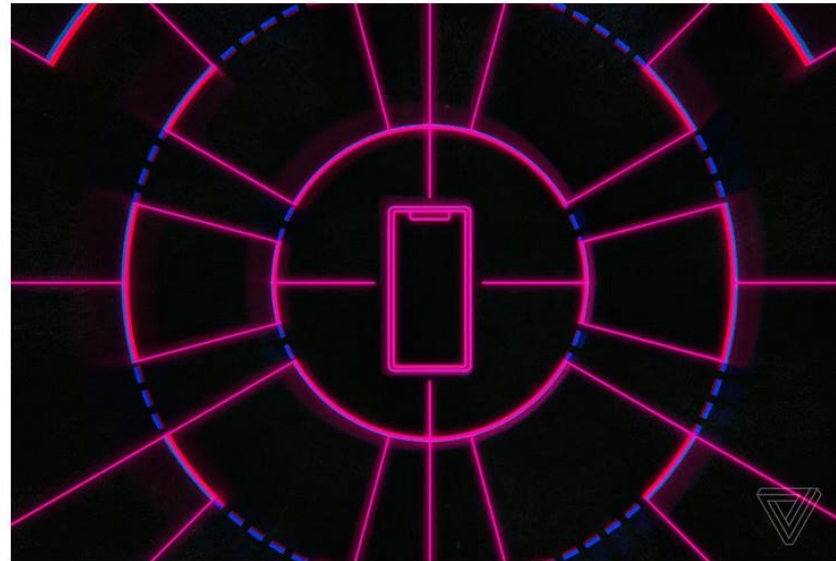
Illustration by Alex Castro / The Verge

The FBI partnered with an Australian security firm called Azimuth Security to gain access to an iPhone linked to the 2015 San Bernardino shooting, a new report from *The Washington Post* reveals. Before now, the methods the FBI used to get into the iPhone were kept secret.

See https://www.theverge.com/2021/4/14/22383957/fbi-san-bernadino-iphone-hack-shooting-investigation

Funding Models for Technology

- Who is funding technology?
- What are their goals?
- Who will benefit?
- How will the workforce be affected?

Course Wrap-up:
Engineering for Ethics, Privacy, and Fairness in Computer Systems

Course Description

This course takes a **technical approach to understanding ethical issues** in the design and implementation of **computer systems**. Tensions often arise between a computer system's utility and its privacy-invasiveness, between its robustness and its flexibility, and between its ability to leverage existing data and existing data's tendency to encode biases. The course will demonstrate how computer systems can violate individuals' privacy and agency, impact sub-populations in disparate ways, and harm both society and the environment. It will also introduce algorithmic approaches to fairness, privacy, transparency, and explainability in machine learning systems. Through hands-on programming assignments and projects, students will design and implement computer systems that reflect both ethics and privacy by design. They will also wrestle with fundamental questions about who bears responsibility for a system's shortcomings, how to balance different stakeholders' goals, and what societal values computer systems should embed.

Topics Covered

- User Interfaces (1 lecture)
- Data (3 lectures)
- World (2 lectures)
- Machine Learning (4 lectures)
- Privacy (4 lectures)
- Lifecycles (1 lecture)
- Tracking & Surveillance (2 lectures)
- Politicized Ecosystems (1 lecture)
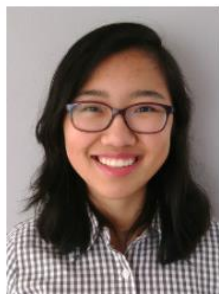
THANK YOU!

Instructors

Blase Ur
blase@uchicago.edu
CMSC 259 instructor

Raul Castro Fernandez
raulcf@uchicago.edu
DATA 259 instructor

Course Staff

Valerie Zhao
Primary TA

Ahmad Bamba
Course Staff

Annika Hildebrandt
Course Staff