

Lecture 18: Responsibility and Recap

CMSC 25910

Spring 2023

The University of Chicago



Legal Considerations in Computer Systems Research

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

Computer Fraud and Abuse Act (1986) --- May 2022 updates

- “The attorney for the government should **decline prosecution** if available evidence shows the defendant’s conduct consisted of, and the defendant intended, **good-faith security research** [...which...] means accessing a computer solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in a manner designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices, machines, or online services to which the accessed computer belongs, or those who use such devices, machines, or online services. Security research not conducted in good faith—for example, for the purpose of discovering security holes in devices, machines, or services in order to extort the owners of such devices, machines, or services—might be called “research,” but is not in good faith.”

Bug Bounties













PUBLIC BUG BOUNTY PROGRAM LIST						
The most comprehensive, up to date crowdsourced list of bug bounty and security vulnerability disclosure programs from across the web curated by the hacker community.						
This list is maintained as part of the Disclose.io Safe Harbor project.						
Have a suggestion for an addition, removal, or change? Open a Pull Request to disclose on Github. Special thanks to all contributors .						
<div>Type here</div> <div>Filters</div>						
Program Name	New	Bug Bounty	Swag	Hall of Fame	Submission URL	Safeharbor
(ISC) ²				✓		
.nz Registry				✓		
Ox Project		✓				
123 Contact Form				✓		
18F						
1Password Game		✓		✓		
21 Century Fox						

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

Funding and \$

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

Funding Models for Technology

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

The Difficulty of Managing Data Rights

Data Access Rights / Data Management / Data Freedom



Data Rights Management (DRM) Tech

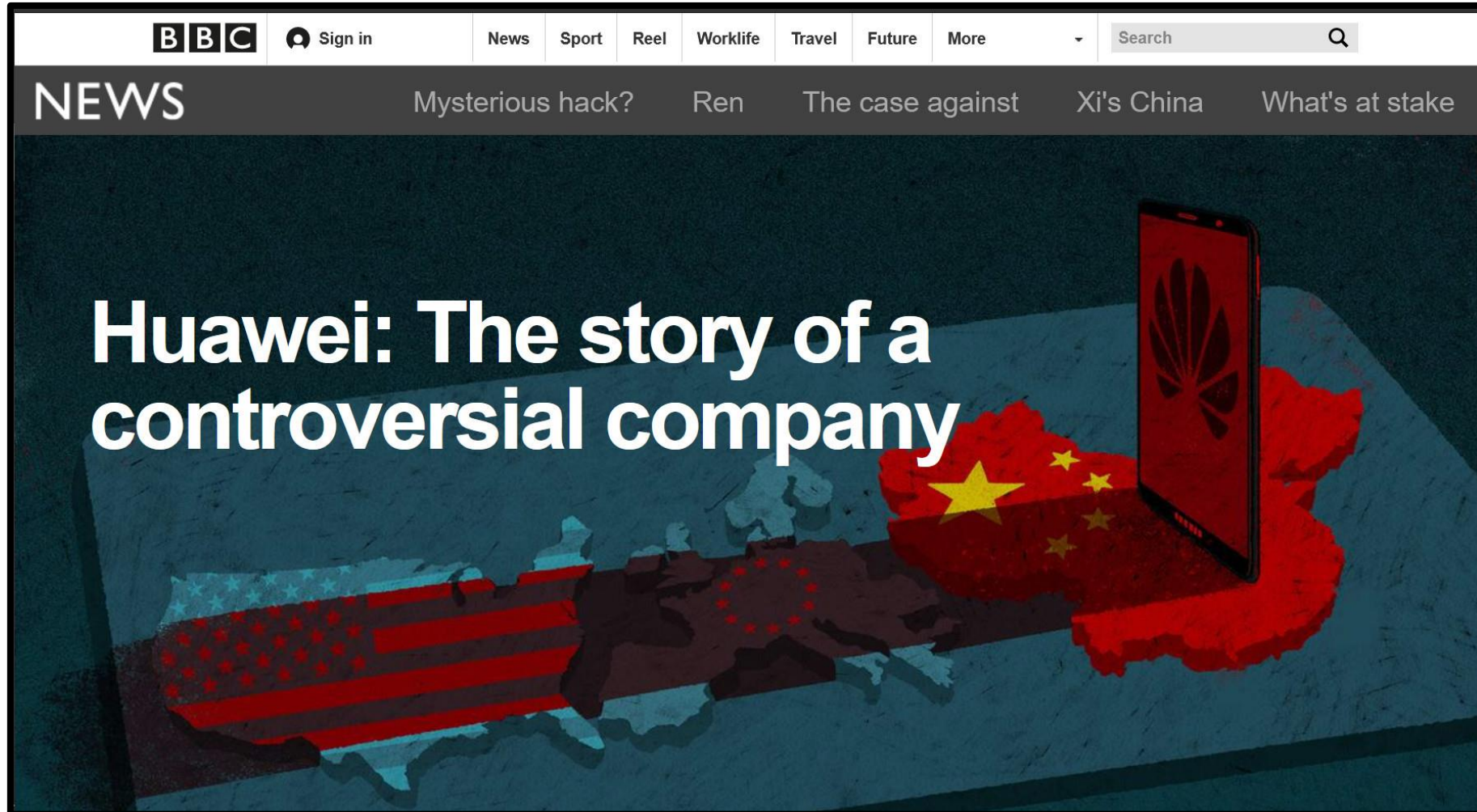
- The use of technical mechanisms to enforce rights
 - Pretty much an arms race
- Example from the 1990s: DVD Content Scrambling System (CSS)
 - DeCSS from Jon Lech Johansen and others

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

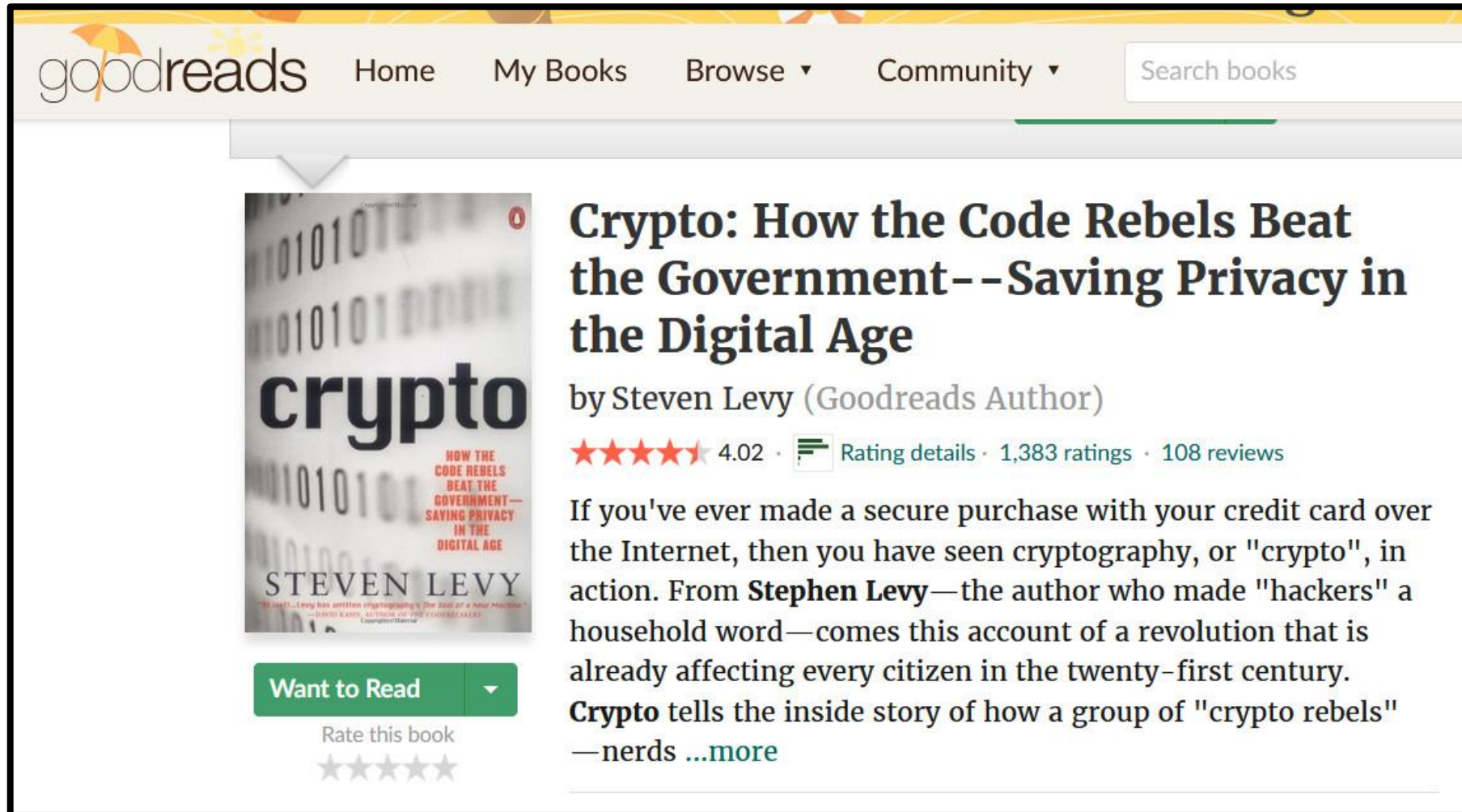


See <https://www.bbc.co.uk/news/resources/idt-sh/Huawei>

Crypto Export Rules

- Crypto was, until the 1990s, on the U.S. Munitions List
- Netscape SSL: “The ‘U.S. edition’ supported full size (typically 1024-bit or larger) RSA public keys in combination with full size symmetric keys (secret keys) (128-bit RC4 or 3DES in SSL 3.0 and TLS 1.0). The ‘International Edition’ had its effective key lengths reduced to 512 bits and 40 bits respectively (RSA_EXPORT with 40-bit RC2 or RC4 in SSL 3.0 and TLS 1.0).”
- See Bernstein v. United States court cases

The Crypto Wars (of the 1990s)



The screenshot shows the Goodreads website interface. At the top is the navigation bar with the Goodreads logo, links for Home, My Books, Browse, and Community, and a search bar. Below the navigation bar, a book card for 'Crypto' by Steven Levy is displayed. The book cover features binary code and the title 'crypto' in a large, bold font. To the right of the cover, the book title is repeated in a large, bold font, followed by the author's name 'by Steven Levy (Goodreads Author)'. Below the author's name is a star rating of 4.02, a link to 'Rating details', and the number of ratings and reviews (1,383 ratings, 108 reviews). A paragraph of text describes the book's content, mentioning cryptography and the author's background. The text ends with a '...more' link. Below the book cover is a green 'Want to Read' button and a 'Rate this book' section with five stars.

goodreads Home My Books Browse Community Search books

Crypto: How the Code Rebels Beat the Government--Saving Privacy in the Digital Age
by Steven Levy (Goodreads Author)

★★★★★ 4.02 · [Rating details](#) · 1,383 ratings · 108 reviews

If you've ever made a secure purchase with your credit card over the Internet, then you have seen cryptography, or "crypto", in action. From **Stephen Levy**—the author who made "hackers" a household word—comes this account of a revolution that is already affecting every citizen in the twenty-first century. **Crypto** tells the inside story of how a group of "crypto rebels"—nerds [...more](#)

Want to Read ▼
Rate this book
★★★★★

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

The Crypto Exceptional Access 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>

The Crypto Exceptional Access 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](#) [t](#) [s](#) SHARE

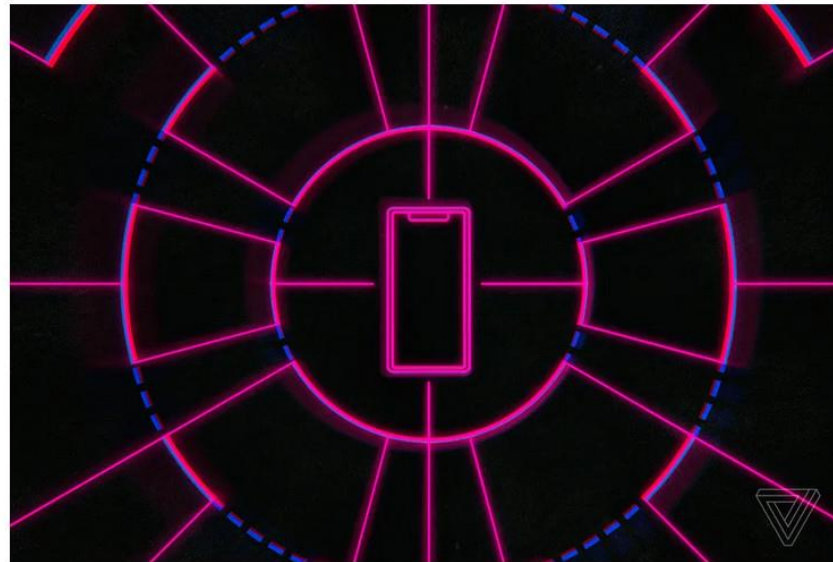


Illustration by Alex Castro / The Verge

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>

The CSAM Wars (of the 2020s)

- Apple planned to detect Child Sex Abuse Material (CSAM)

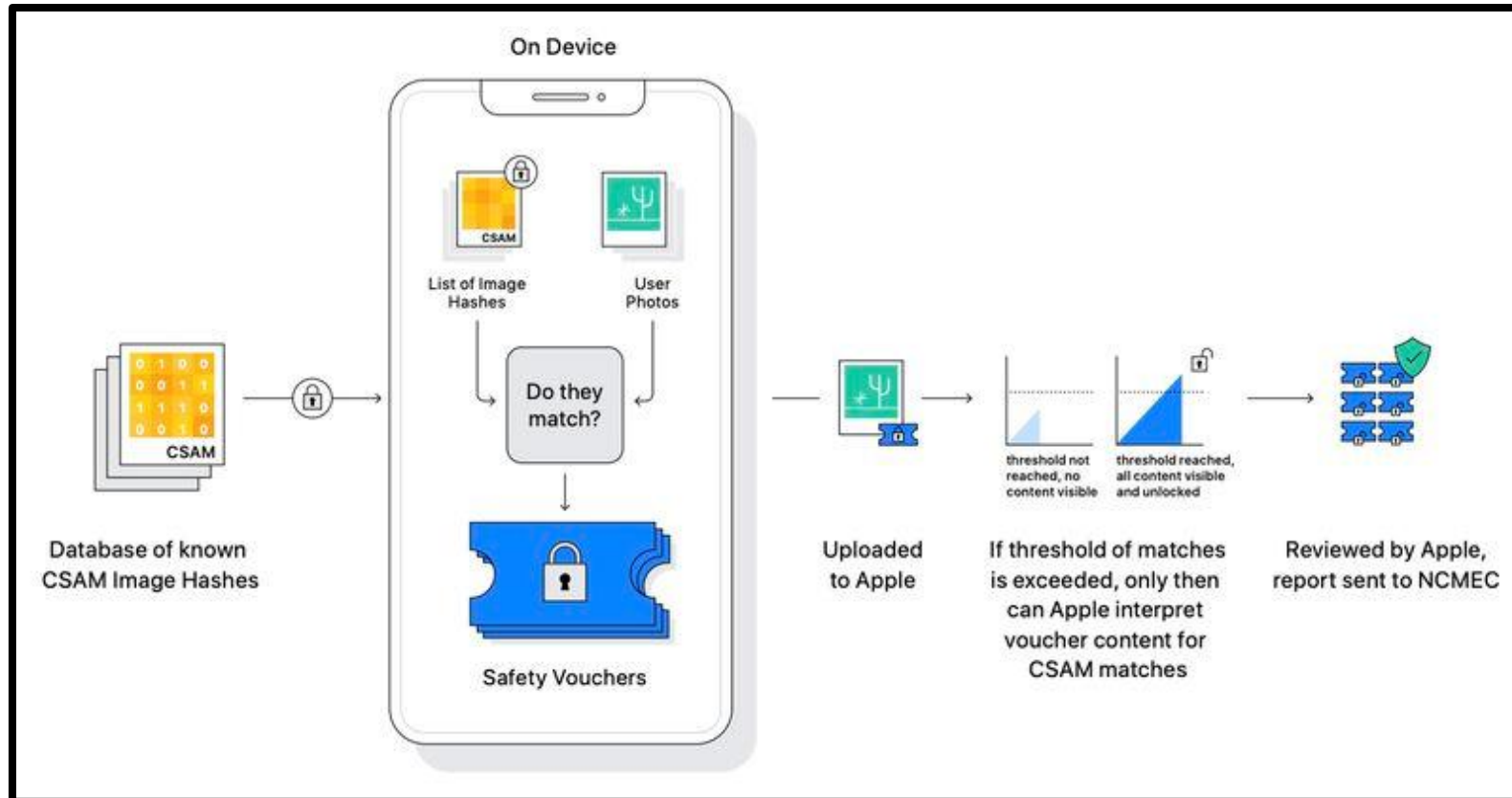


Image from <https://www.macrumors.com/2021/08/06/apple-to-consider-csam-detection-per-country/>

The CSAM Wars (of the 2020s)



<https://www.eff.org/deeplinks/2021/08/apples-plan-scan-photos-messages-turns-young-people-privacy-pawns>

The CSAM Wars (of the 2020s)

Apple quietly pulls references to its CSAM detection tech after privacy fears

Carly Page @carlypage_ / 8:24 AM CST • December 15, 2021

 Comment



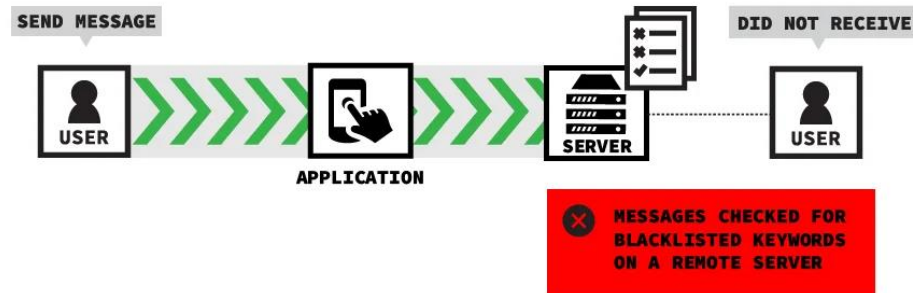
See <https://techcrunch.com/2021/12/15/apple-removes-csam-detection-website>

Censorship on WeChat

YY USES CLIENT-SIDE CENSORSHIP



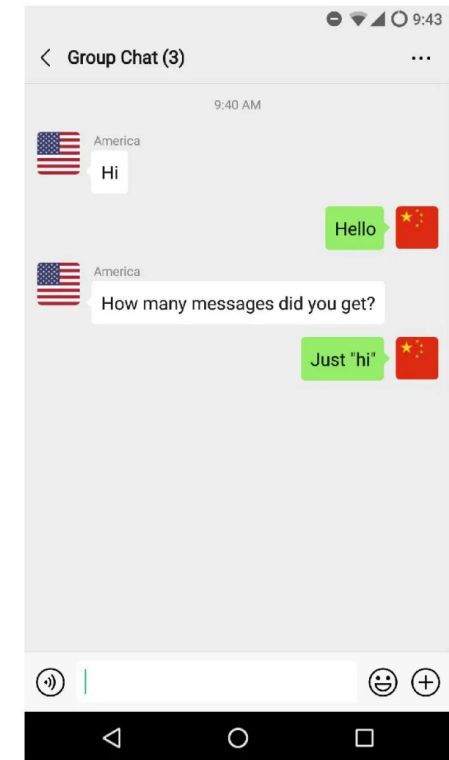
WECHAT USES SERVER-SIDE CENSORSHIP



United States account



China account



Responsibility

Who is responsible for...

- ...a bug in code?
 - ...a security flaw caused by a bug in code?
 - ...the Heartbleed vulnerability?

Who is responsible for...

- ...an ML model?
 - ...an ML model that makes an automated decision?
 - ...an ML model that causes someone to be jailed incorrectly?

Who is responsible for...

- ...a self-driving car?
 - ...a self-driving car that crashes?
 - ...a self-driving car that crashes after being cut off by a human?

Who is responsible for...

- ...a robot?
 - ...a robot that is offensive?
 - ...a robot that bullies someone and causes them harm?

Who is responsible for...

- ...automation software?
 - ...automation software that saves a company money?
 - ...automation software that puts someone out of work?

Consideration of Ethics



Joe Redmon @pjreddie · Feb 20, 2020



“We shouldn’t have to think about the societal impact of our work because it’s hard and other people can do it for us” is a really bad argument. [twitter.com/RogerGrosse/st...](https://twitter.com/RogerGrosse/status/1224444444444444444)

Roger Grosse @RogerGrosse

Replying to @kevin_zakka @hardmaru

To be clear, I don't think this is a positive step. Societal impacts of AI is a tough field, and there are researchers and organizations that study it professionally. Most authors do not have expertise in the area and won't do good enough scholarship to say something meaningful.



Joe Redmon

@pjreddie

I stopped doing CV research because I saw the impact my work was having. I loved the work but the military applications and privacy concerns eventually became impossible to ignore. [twitter.com/RogerGrosse/st...](https://twitter.com/RogerGrosse/status/1224444444444444444)

What will you do?

- Real-world scenarios rarely have a perfect decision. Instead, you'll make and participate in myriad decisions that, together, will have consequences, good and bad.

Recap

Topics Covered in the Last Nine Weeks

- The influence of UI / dark patterns
- Anonymity
- Privacy law / regulation / philosophy
- Data lifecycles / data rights (erasure, access, portability)
- Ethical experiments
- Data quality, data errors, and statistical pitfalls
- Generalization in ML
- Fairness and bias in ML and NLP
- Documenting, auditing, and explaining models
- Differential privacy
- Privacy engineering techniques
- Data formats, accessibility, and internationalization
- Wasting human's time; wasting energy to prove work
- Tracking and inference, surveillance
- Responsibility and values