

# Lecture 17: Responsibility

CMSC 25910

Spring 2024

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
- Used to prosecute George Hotz (*geohot*) for jailbreaking the PS3

# 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 <a href="#">Disclose.io</a> Safe Harbor project.						
Have a suggestion for an addition, removal, or change? Open a Pull Request to <a href="#">disclose</a> on Github. Special thanks to all <a href="#">contributors</a> .						
<div>Type here</div> <div>Filters</div>						
Program Name	New	Bug Bounty	Swag	Hall of Fame	Submission URL	Safeharbor
(ISC) <sup>2</sup>				✓		
.nz Registry				✓		
Ox Project		✓				
123 Contact Form				✓		
18F						
1Password Game		✓		✓		
21 Century Fox						

**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 <a href="#">proprietization</a> , <a href="#">license compatibility</a> )	Grants use rights, forbids <a href="#">proprietization</a>	Grants rights for noncommercial use only. May be combined with copyleft.	Traditional use of <a href="#">copyright</a> ; no rights need be granted	No information made public
Software	PD, CC0	<a href="#">MIT</a> , <a href="#">Apache</a> , <a href="#">MPL</a>	<a href="#">GPL</a> , <a href="#">AGPL</a>	<a href="#">JRL</a> , <a href="#">AFPL</a>	<a href="#">Proprietary software</a> , no public license	Private, internal software
Other creative works	PD, CC0	<a href="#">CC-BY</a>	<a href="#">CC-BY-SA</a>	<a href="#">CC-BY-NC</a>	<a href="#">Copyright</a> , no public license	Unpublished

Table from [https://en.wikipedia.org/wiki/Software\\_license](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

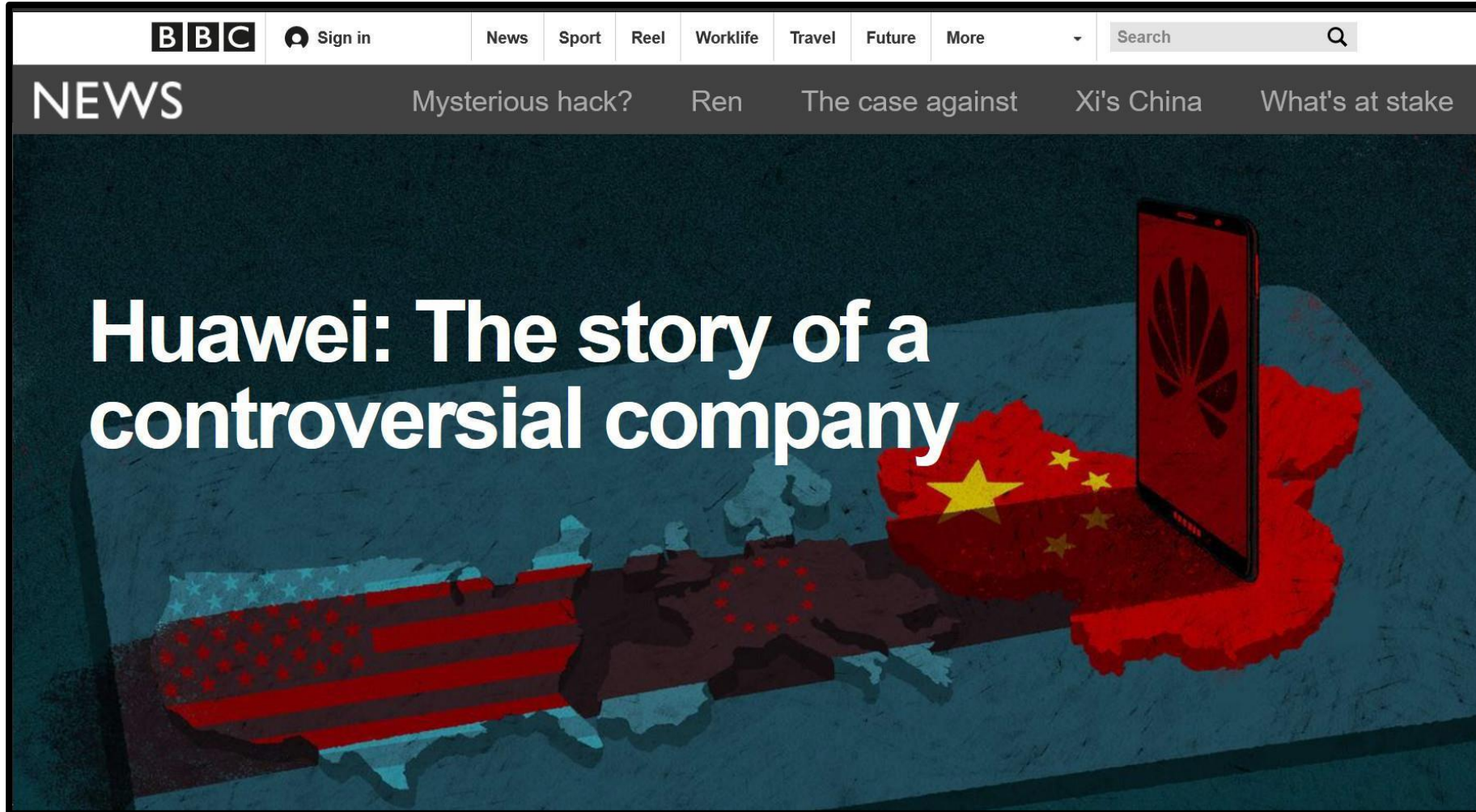
- The use of technical mechanisms to enforce rights
  - Can be characterized as an "arms race"
- Example from the 1990s: DVD Content Scrambling System (CSS)
  - DeCSS from Jon Lech Johansen and others

# 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
    - 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

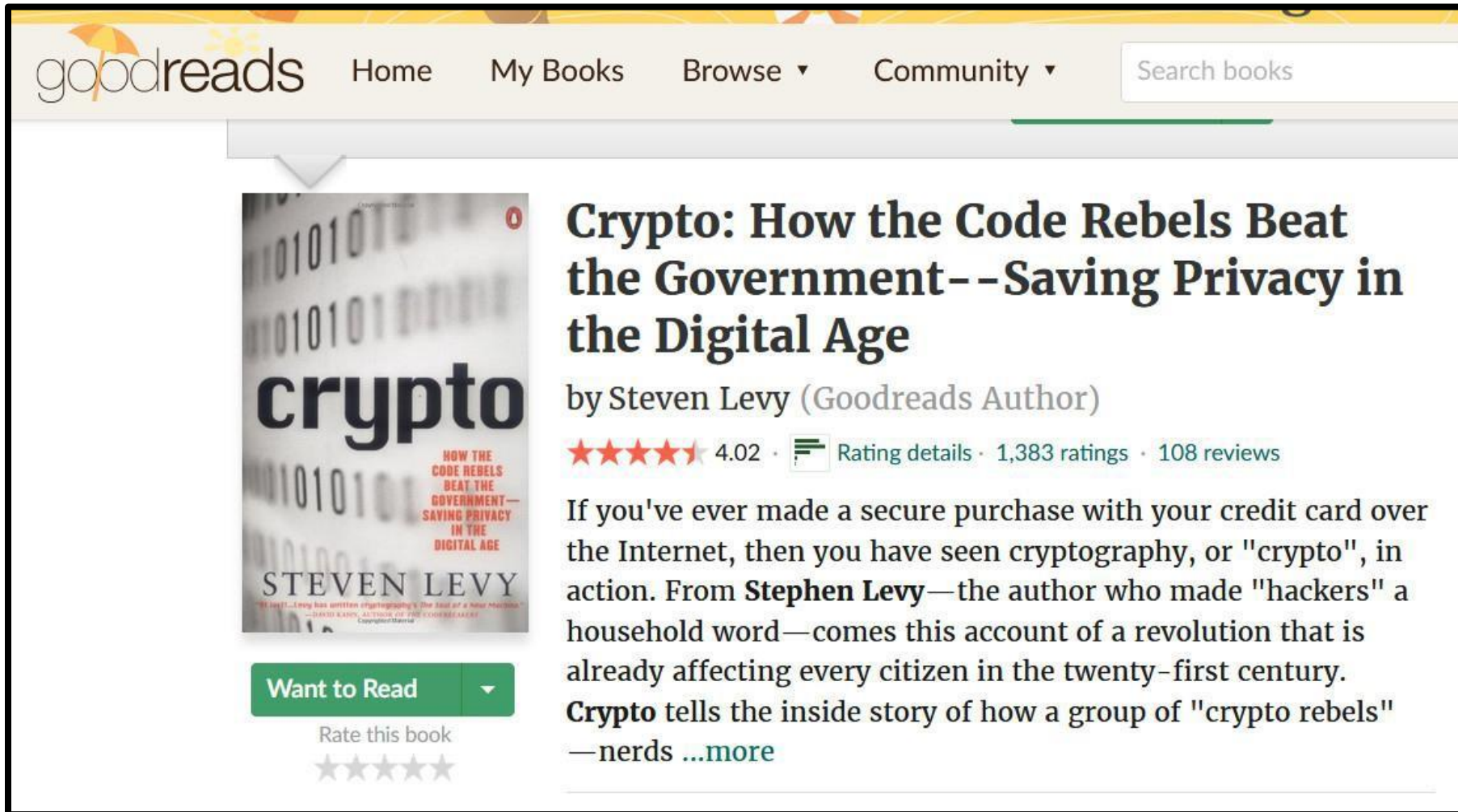


See <https://www.bbc.co.uk/news/resources/idt-sh/Huawei>

# 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 Goodreads logo and navigation links: Home, My Books, Browse, and Community. A search bar is on the right. Below the navigation bar, the book 'Crypto' by Steven Levy is featured. The book cover shows binary code and the title 'crypto' in large letters. To the right of the cover, the title 'Crypto: How the Code Rebels Beat the Government--Saving Privacy in the Digital Age' is displayed, followed by the author 'by Steven Levy (Goodreads Author)'. The book has a 4.02 star rating from 1,383 ratings and 108 reviews. A green 'Want to Read' button is below the cover. A short description of the book is provided, followed by a '...more' link.

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

★★★★★



# 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](#) [SHARE](#)

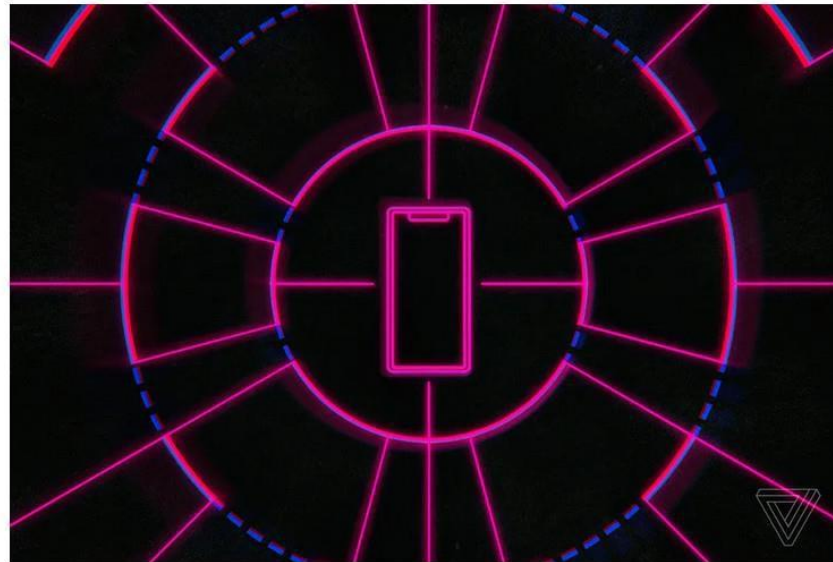


Illustration by Alex Castro / The Verge

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)

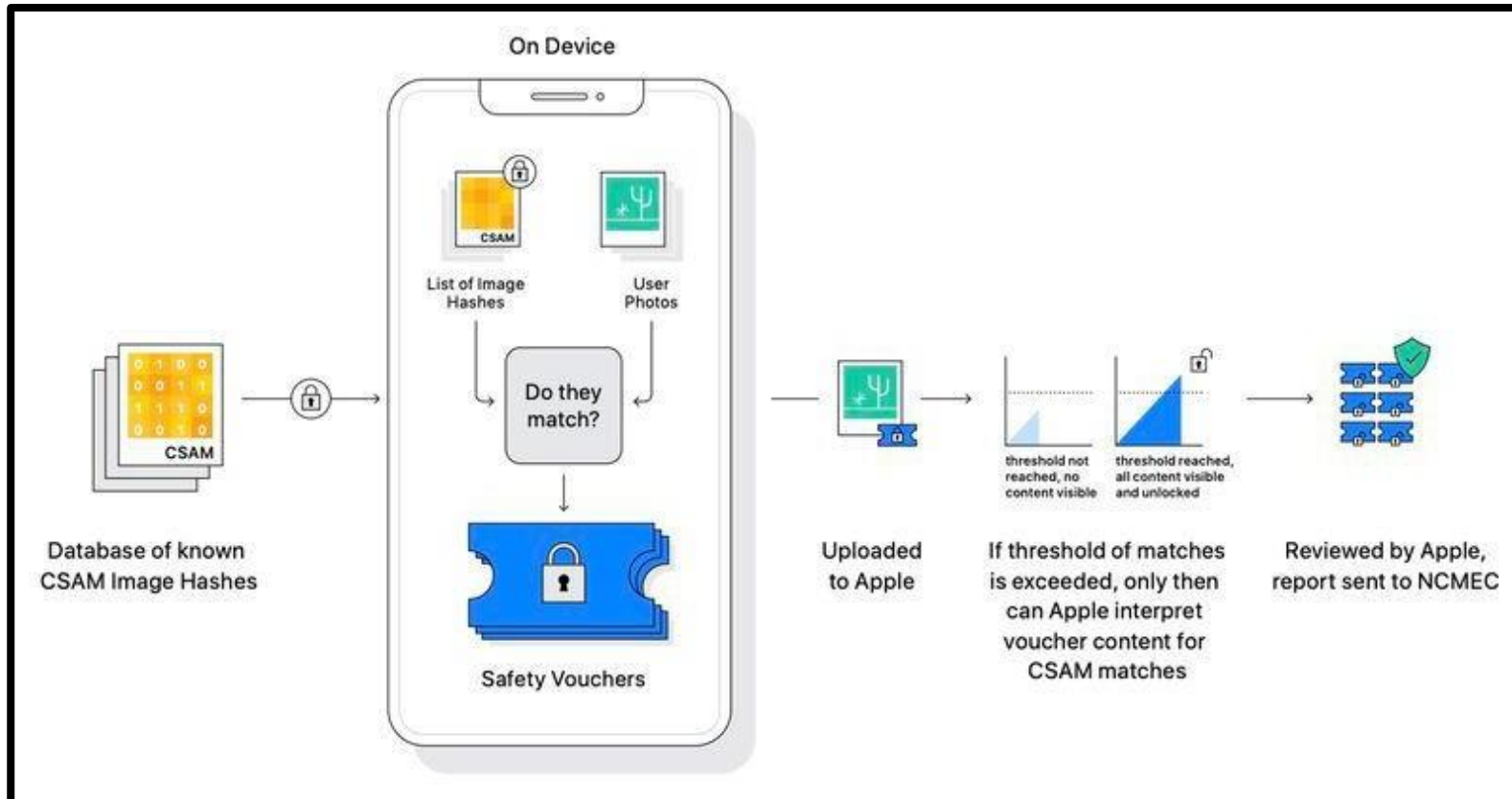


Image from <https://www.macrumors.com/2021/08/06/apple-to-consider-csam-detection-per-country/>

# 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

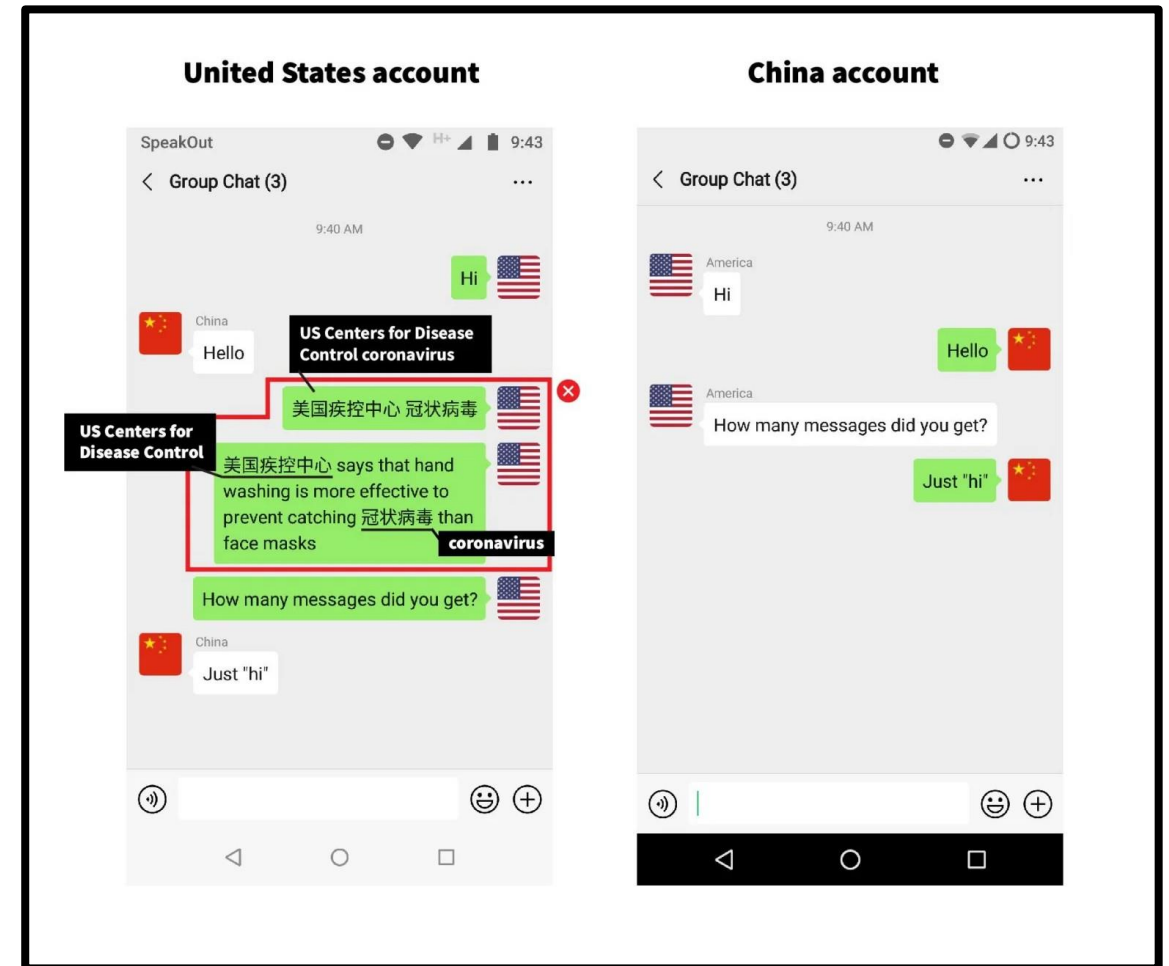
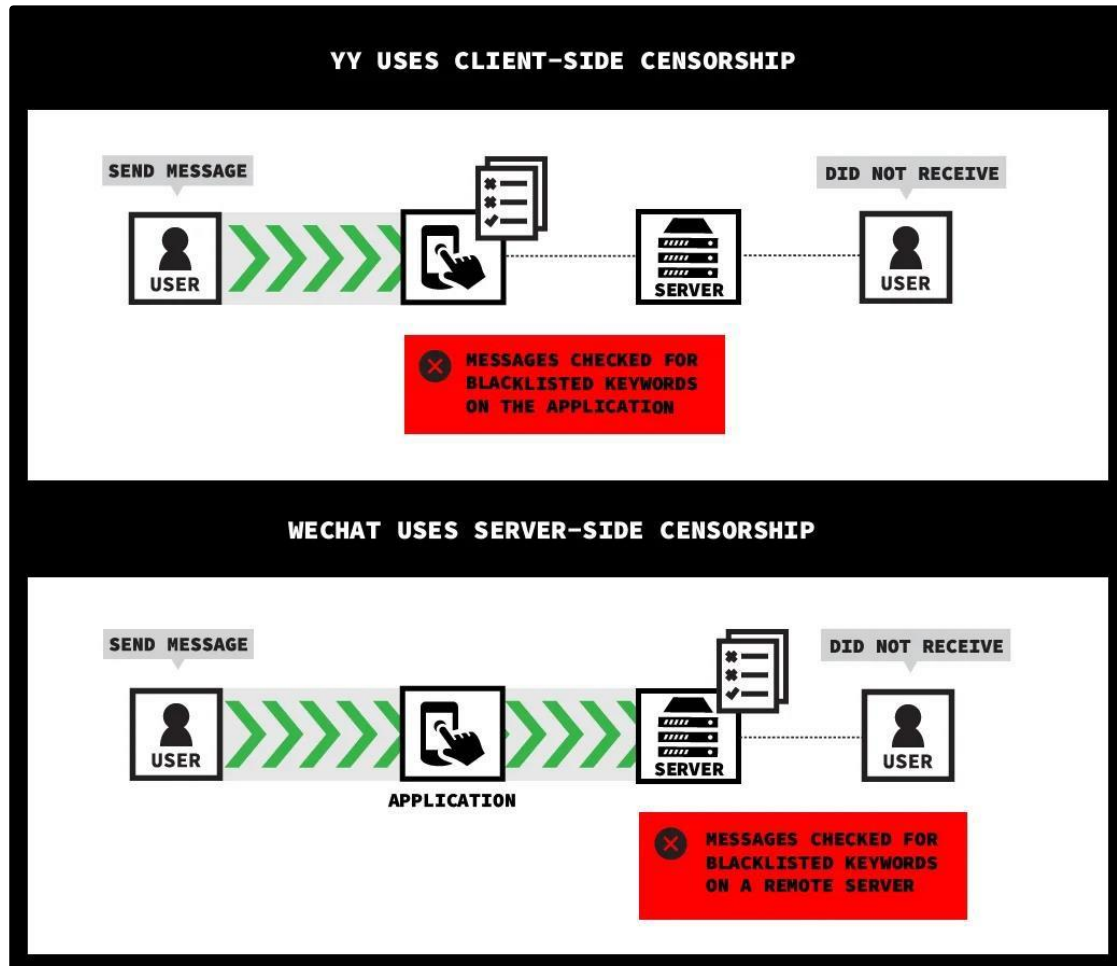
Comment



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



# Censorship on WeChat



# 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/1224444444)

**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/1224444444)

# 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.**