

# Wait, this is about security *and* privacy?

Secure Systems Engineering Fall 2024

 EE G7701

October 30, 2024

Tushar Jois



# Recap

- The complexity of e-voting lends it to having several flaws
- E-voting requires the consideration of a strong adversary model
- The use of e-voting necessarily means confronting societal questions

## Lesson objectives

- Work through, step by step, the operation of the Signal protocol
- Describe how Tor uses onion routing to provide censorship resistance
- Understand the political and societal ramifications of privacy

# Defining privacy

- What are the goals of security?
  - What are the goals of privacy?
- } *(it's okay if some of them are the same!)*
- Order the following data types by how valuable privacy is to the data:
    - a. Browser history
    - b. Financial statements
    - c. Medical records
    - d. Text messages
    - e. Grade transcript

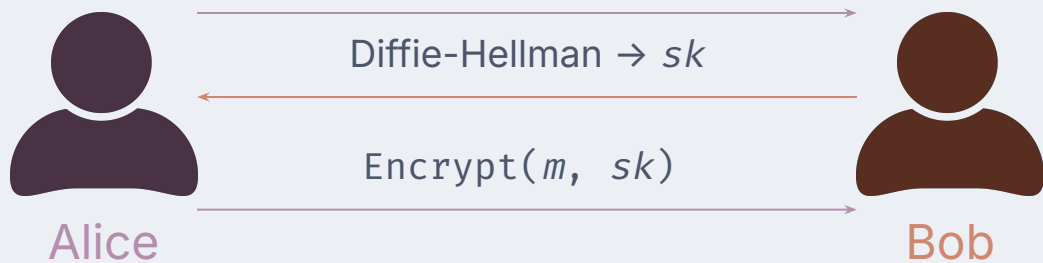
# The importance of secure messaging

- Facebook Messenger, Instagram are not “end-to-end”
  - Facebook reads the messages, delivers ads about them
  - Governments can subpoena Facebook for your messages, reconstruct your digital life
- “Surveillance capitalism”
  - The person is the product
  - “Free” services provided by Big Tech powered by the selling of your data
- Data sharing agreements
  - Seen ads for things you’ve talked about on Amazon?

*“But I have nothing to hide!”*

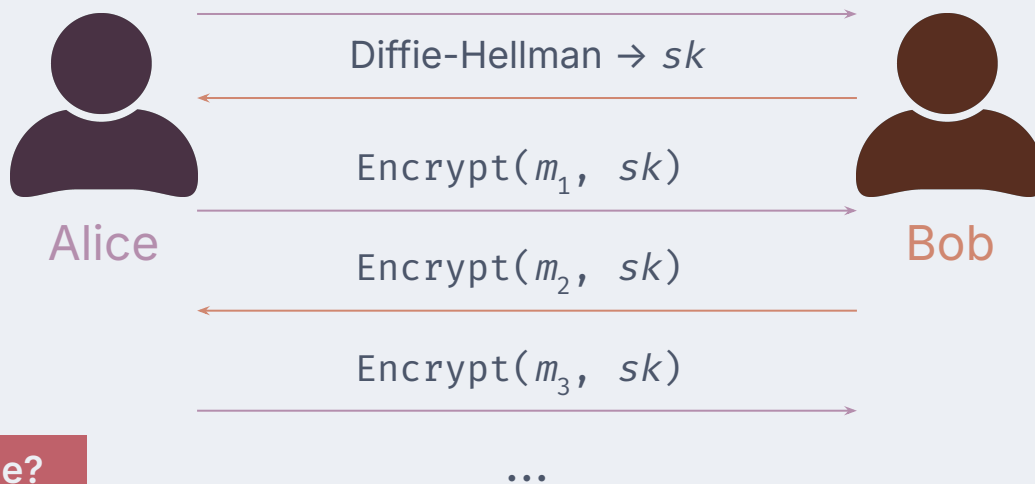
- Solidarity with those who do
  - Snowden/whistleblowers, but also “The Feeling of Being Watched” subjects
- You might not realize how much data is out there
  - “We kill people based on metadata”
- Data lasts forever, and you might have to someday
  - Data lasts *forever* -- and companies/banks/governments are looking

# Attempt 0



More than one  
message?

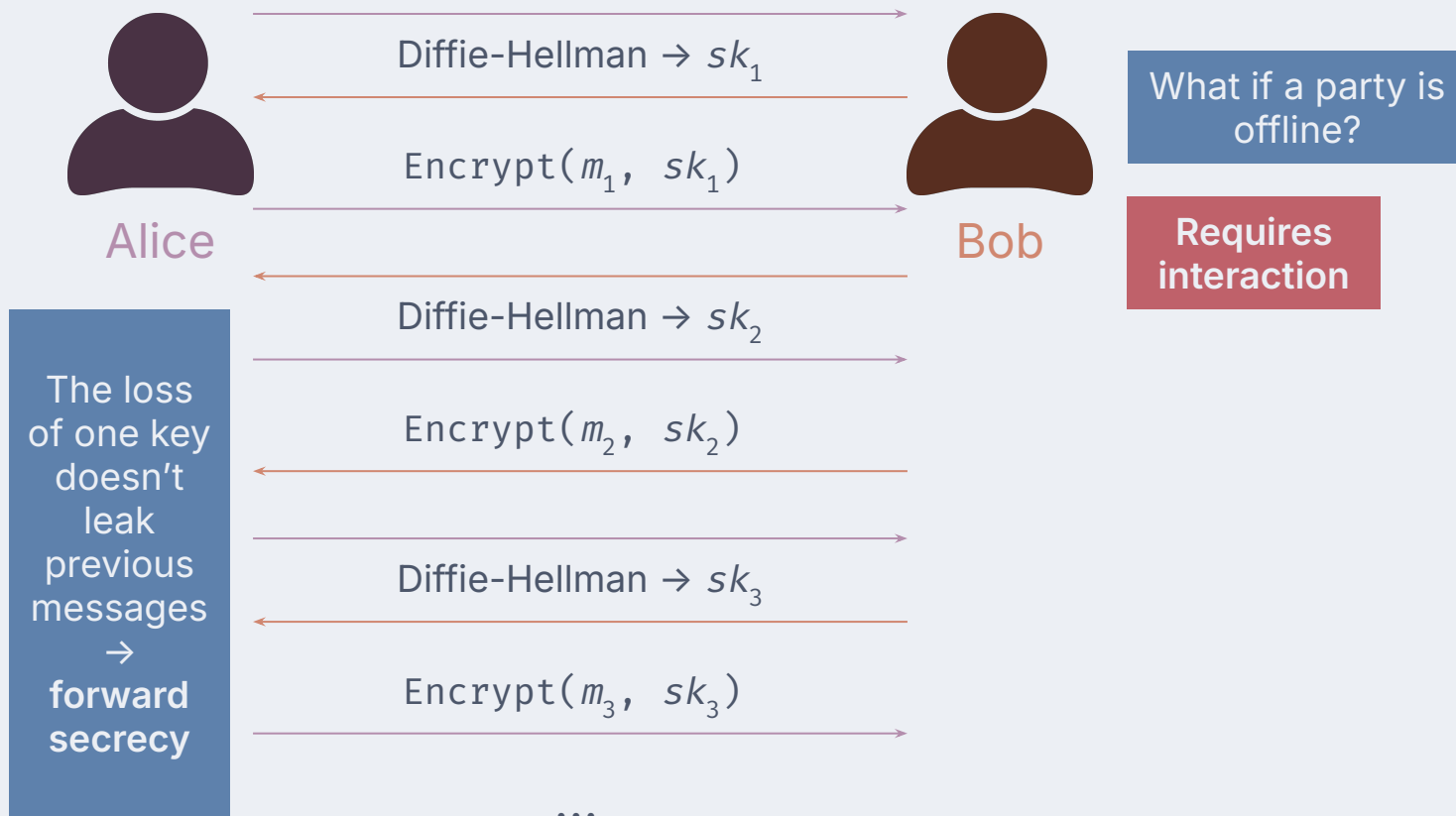
# Attempt 1



## Key compromise?

- If Alice loses  $sk$ , the entire message history is disclosed
  - Phone loss
  - Forensic extraction
- Can we do better?

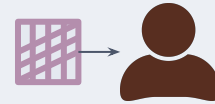
# Attempt 2



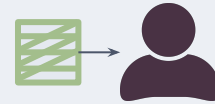
*public channel color* 



$$\begin{array}{|c|} \hline \text{red vertical lines} + \text{blue diagonal lines} = \text{purple grid} \\ \hline \end{array}$$



$$\begin{array}{|c|} \hline \text{yellow horizontal lines} + \text{blue diagonal lines} = \text{green grid} \\ \hline \end{array}$$



$$\text{red vertical lines} + \text{green grid} = \text{brown grid}$$

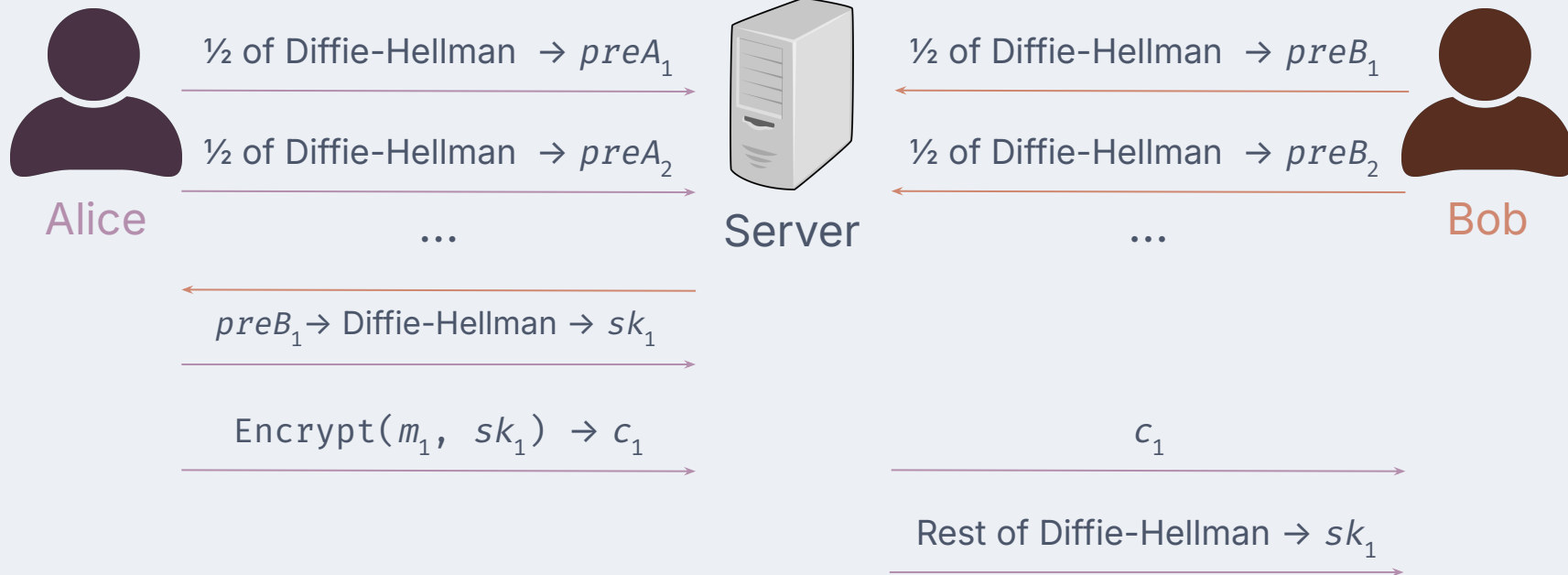


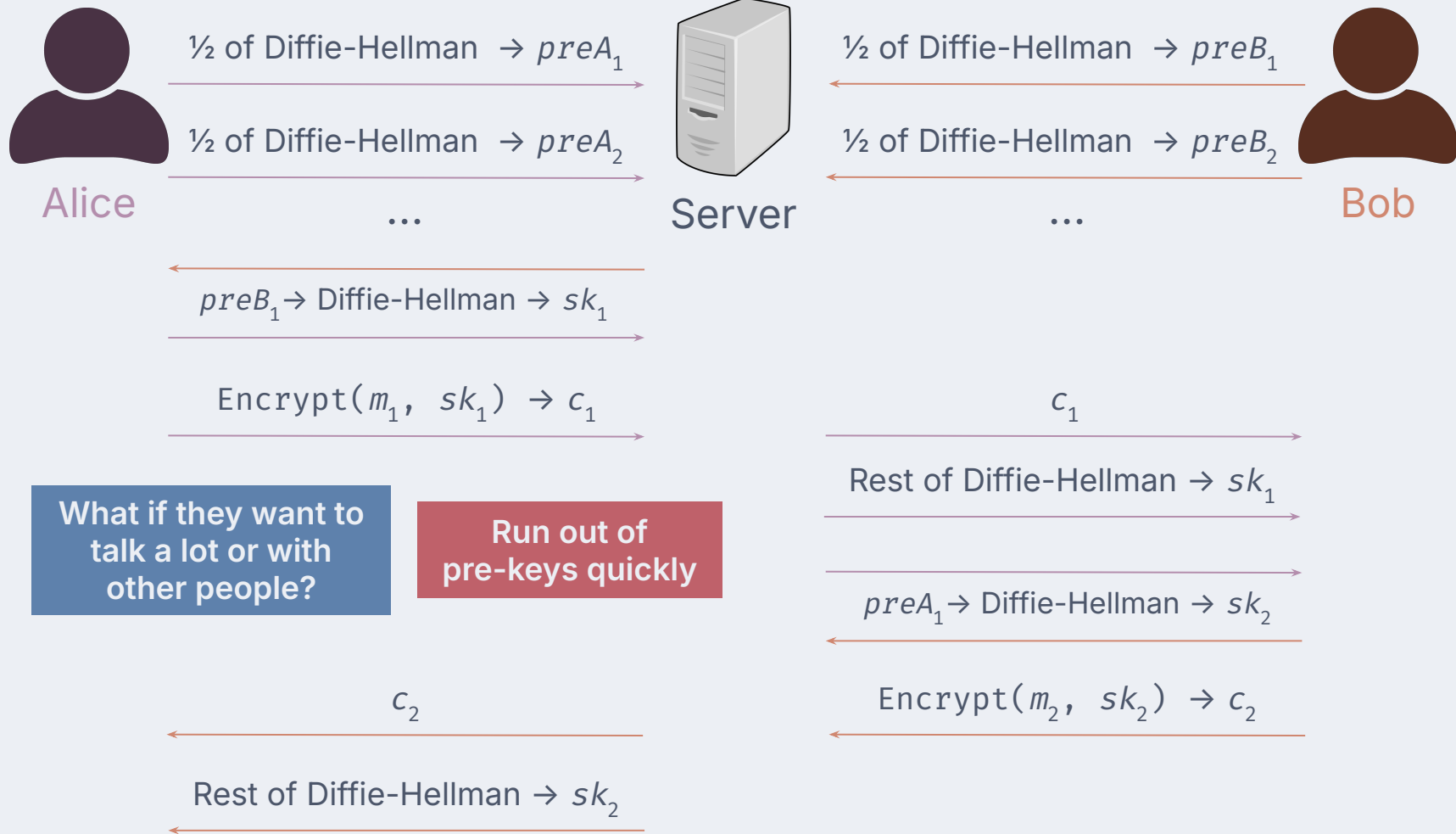
$$\text{yellow horizontal lines} + \text{purple grid} = \text{brown grid}$$

} Doesn't  
require the  
other party



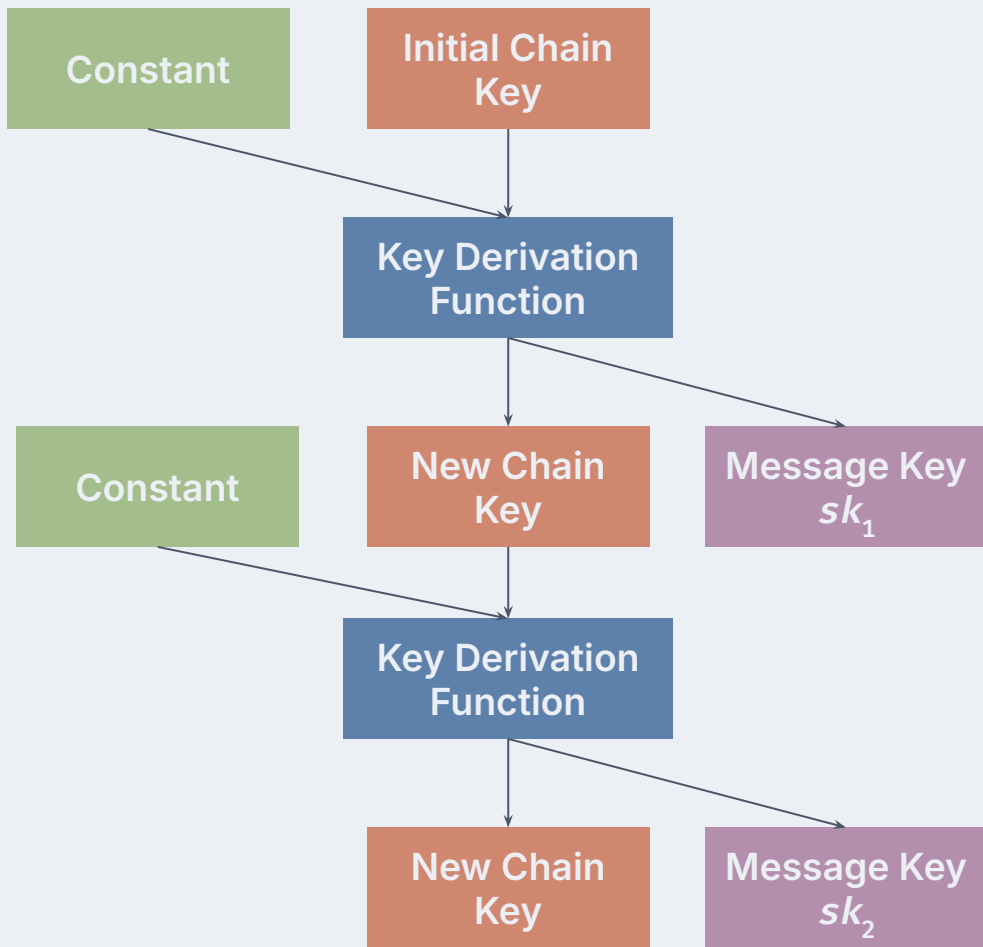
# Attempt 3





# KDF chain

- Special cryptographic construct that generates new keys from old keys
  - We can use the new keys for subsequent messages
  - Requires both parties to be in the same "state" of the ratchet
- Send a message, Alice encrypts with a key, and then "ratchets it forward"
  - Bob receives the message, decrypts it, and then "ratchets it forward"
  - Forward secrecy without significant interaction
  - Both have to keep in sync



# Symmetric ratcheting

"The parties derive new keys for every Double Ratchet message so that earlier keys cannot be calculated from later ones... [giving] some protection to earlier or later encrypted messages in case of a compromise of a party's keys."

*Perrin and Marlinspike, "The Double Ratchet Algorithm" (2016)*

# Signal protocol\*

\*abridged

(signed)



Alice

$\frac{1}{2}$  of Diffie-Hellman  $\rightarrow preA_1$

$\frac{1}{2}$  of Diffie-Hellman  $\rightarrow preA_2$

...

$preB_1 \rightarrow$  Diffie-Hellman  $\rightarrow sk_1$

Encrypt( $m_1, sk_1$ )  $\rightarrow c_1$

Ratchet forward  $sk_1 \rightarrow sk_2$



Server

$\frac{1}{2}$  of Diffie-Hellman  $\rightarrow preB_1$

$\frac{1}{2}$  of Diffie-Hellman  $\rightarrow preB_2$

...

$c_1$

Rest of Diffie-Hellman  $\rightarrow sk_1$

Ratchet forward  $sk_1 \rightarrow sk_2$



Bob



Alice

$\frac{1}{2}$  of Diffie-Hellman  $\rightarrow preA_1$

$\frac{1}{2}$  of Diffie-Hellman  $\rightarrow preA_2$

...



Server

$\frac{1}{2}$  of Diffie-Hellman  $\rightarrow preB_1$

$\frac{1}{2}$  of Diffie-Hellman  $\rightarrow preB_2$

...



Bob

$preB_1 \rightarrow$  Diffie-Hellman  $\rightarrow sk_1$

Encrypt( $m_1, sk_1$ )  $\rightarrow c_1$

Ratchet forward  $sk_1 \rightarrow sk_2$

$c_2$

Ratchet forward  $sk_2 \rightarrow sk_3$

$c_1$

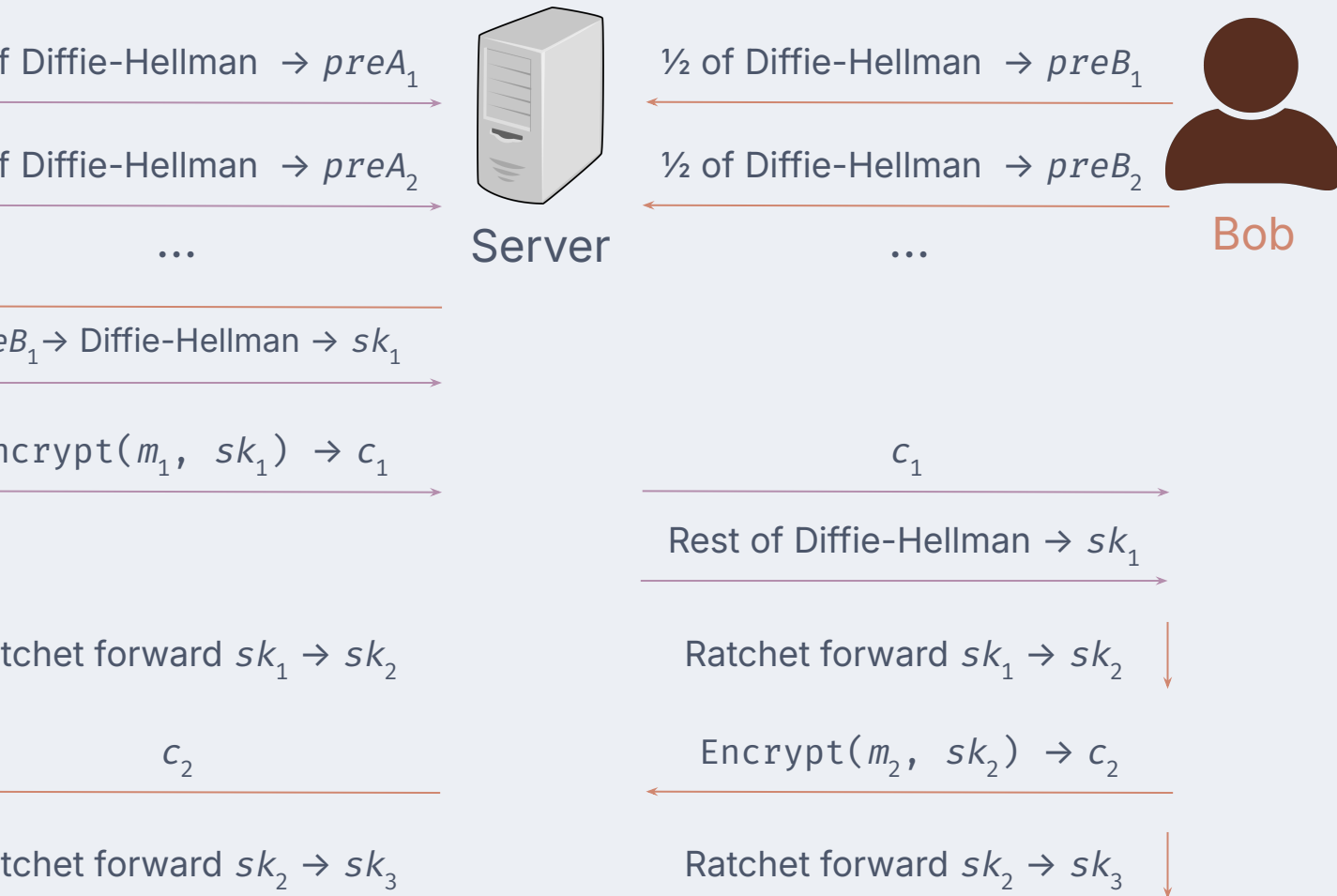
Rest of Diffie-Hellman  $\rightarrow sk_1$

Ratchet forward  $sk_1 \rightarrow sk_2$

Encrypt( $m_2, sk_2$ )  $\rightarrow c_2$

Ratchet forward  $sk_2 \rightarrow sk_3$

The loss  
of one  
key  
doesn't  
leak  
previous  
ones  
 $\rightarrow$   
forward  
secrecy



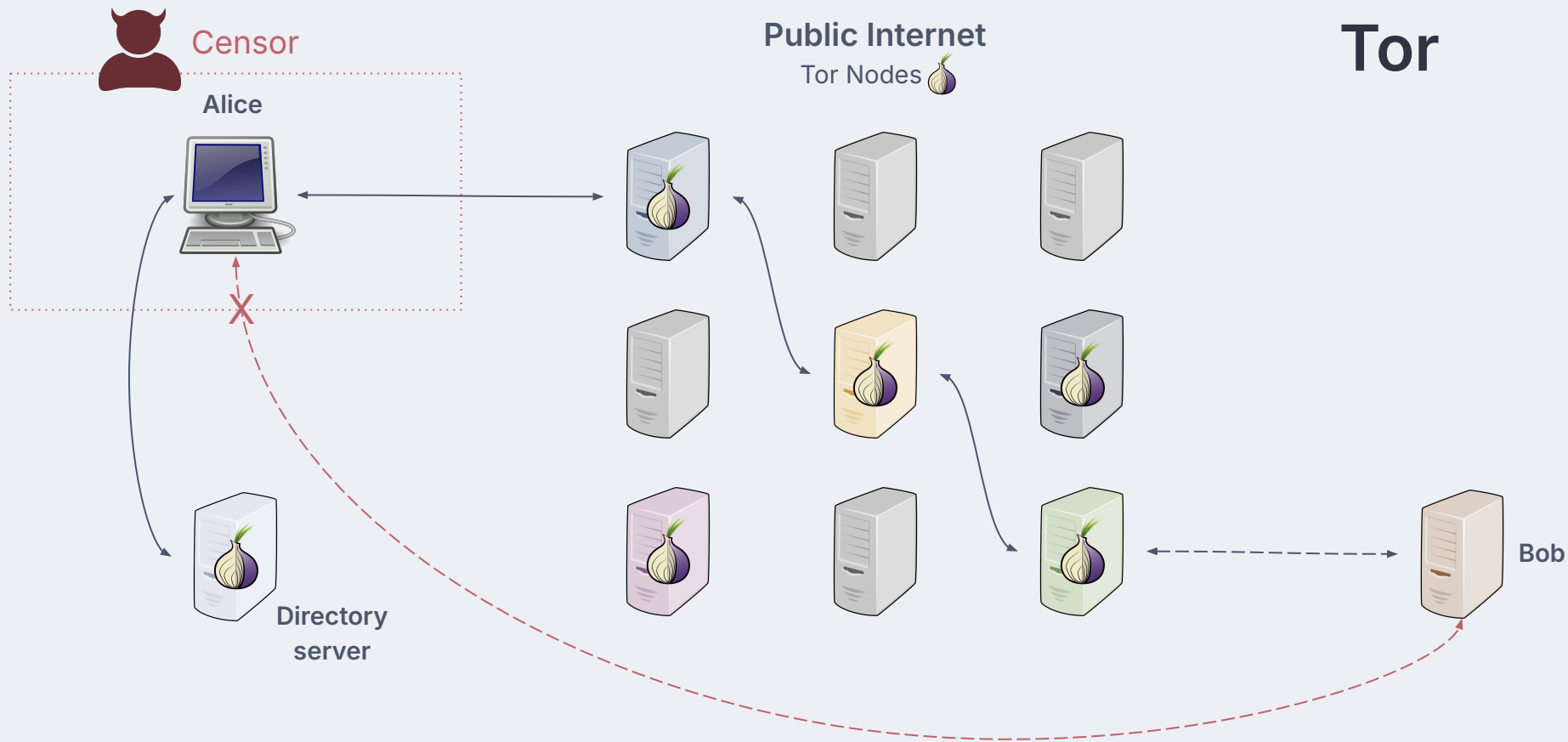
## Sidebar

- Not a trivial protocol
- Complicated to provide forward secrecy, limited interaction, and efficiency
- Good example of security engineering in practice
- Needs to be usable in practice

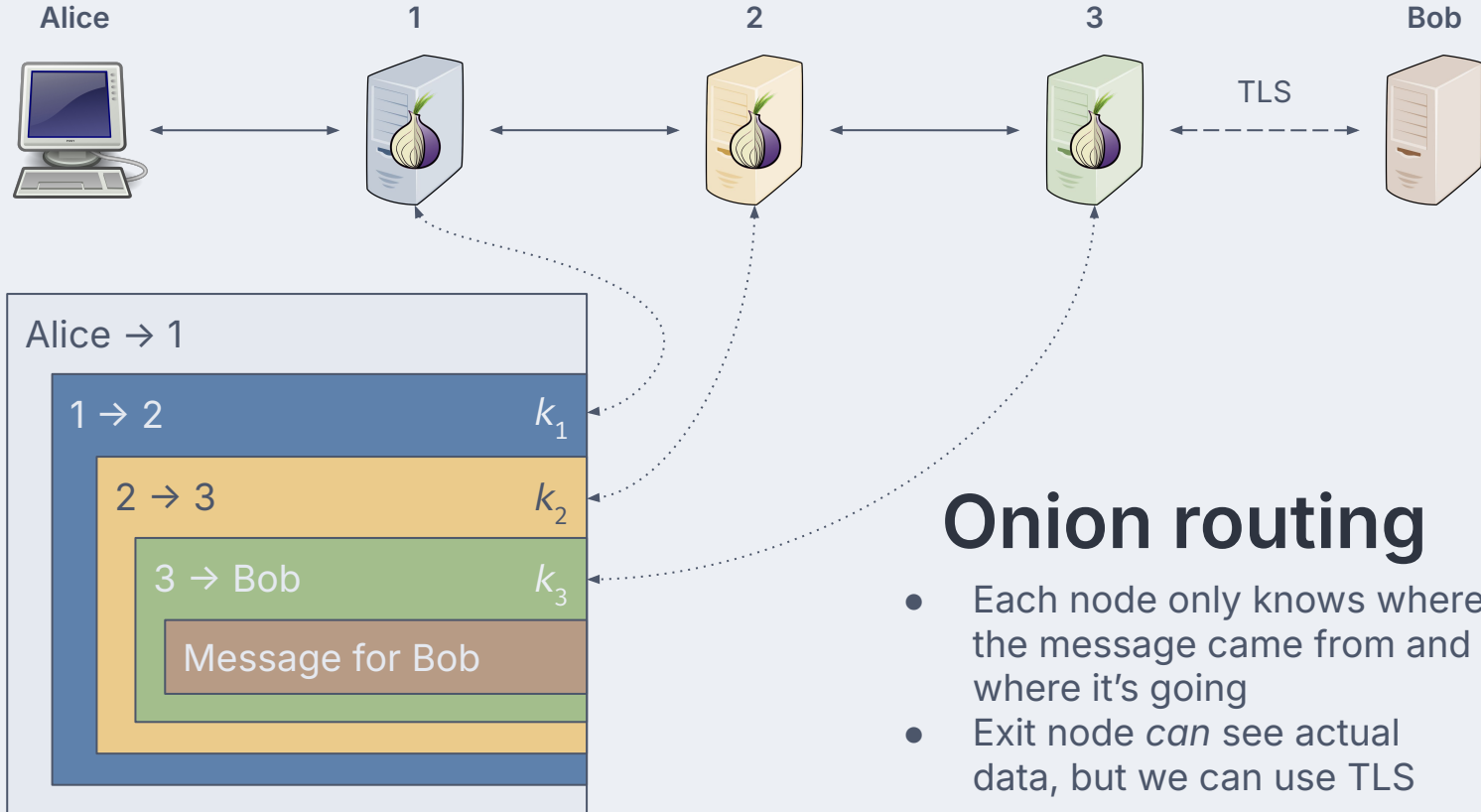
# Censorship resistance

- Some users live under regimes with authoritarian Internet policies
- They are forbidden from accessing content that the government deems subversive
  - A government's "subversive content" could be a group's "civil rights protest"
- A system like Signal prevents direct observation of content by governments
  - So, the Signal server is blocked by an authoritarian government
- What if we decided that *all* users should be able to access any content?
  - This choice lies in opposition to the existence of censorship
  - Society gets to decide which values we keep
- So, there's a valid use case for technology that combats censorship





## Tor Circuit



## Onion routing

- Each node only knows where the message came from and where it's going
- Exit node *can* see actual data, but we can use TLS

Tor Project | Anonymity Online

https://www.torproject.org

Site Information for www.torproject.org

Connection

Secure Connection

Tor Circuit

This browser

Lithuania 195.189.96.148 Guard

Germany 131.188.40.188

Austria 109.70.100.7

torproject.org

New Circuit for this Site

Your Guard node may not change. Learn more

Permissions

You have not granted this site any special permissions.

rt Community Blog Donate English (En) Download Tor Browser

Privately.  
Freely.

and surveillance. Circumvent censorship.

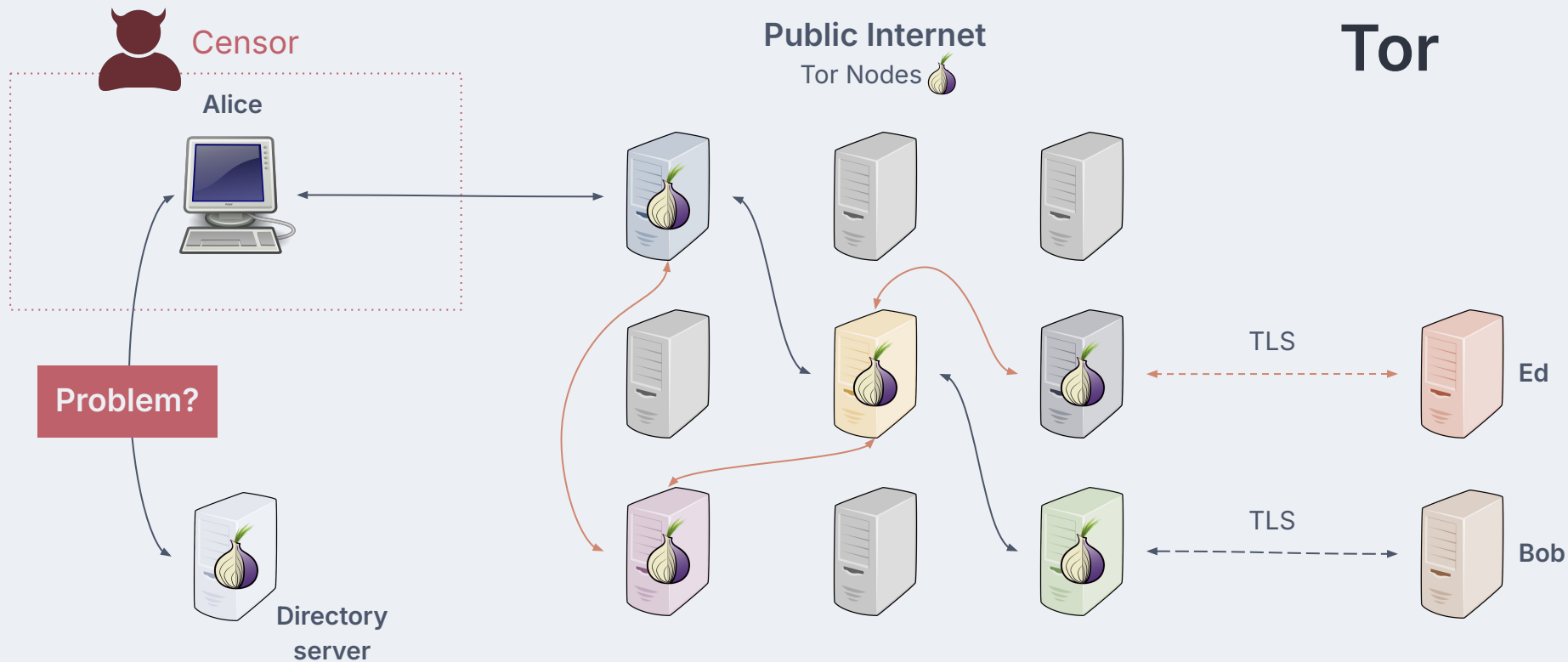
Download Tor Browser

BLOCK TRACKERS

Tor Browser isolates each website you visit so third-party trackers and ads can't follow you. Any cookies

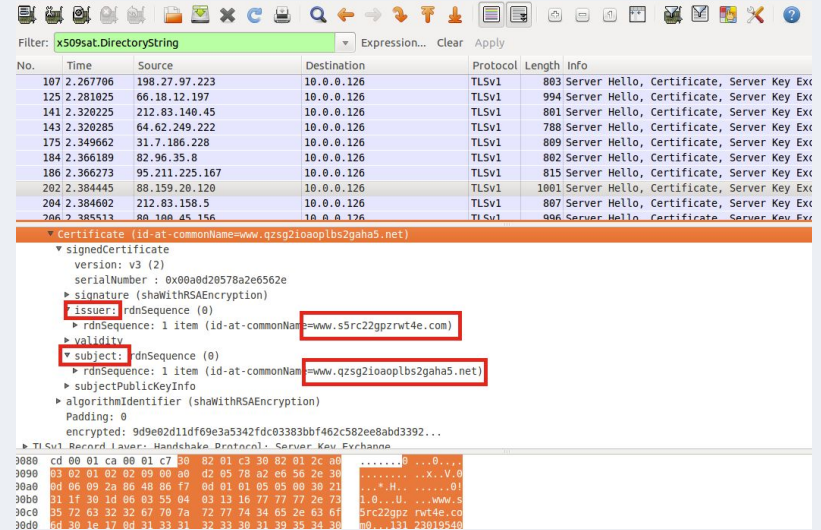
# Some thoughts on Tor

- Trusting Tor
  - Tor is another system we have to trust
  - Funded by lots of people (incl. US) but mostly written by volunteers (open source)
- Virtual Private Networks and Tor
  - VPNs are similar to Tor (having another computer request traffic for you)
  - No guarantees that a VPN will not read/store/log your actions
    - VPNs claim terms of use, audits, etc but no formal promises
    - Tor has cryptographic guarantees (encrypted traffic)
- Exit nodes on Tor
  - Exit node needs to see your data to perform a web request
  - Can potentially break your privacy, but also can use TLS
- But, there's a more fundamental problem...



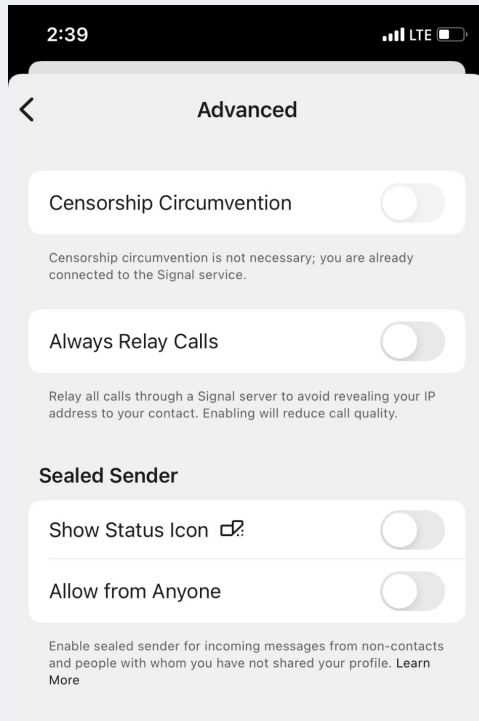
# Censoring censorship resistance

- Censor can clearly identify traffic that's going to a Tor network
  - Single point of failure: directory server
  - Block access to directory server → block access to Tor
  - China's "Great Firewall" does this
- Use of Tor could endanger your life
  - Protestors/dissidents/whistleblowers
  - Still need to access free communication



# Society

- Signal and Tor banned in several countries
  - Brittle censorship circumvention
  - Make messages look like other messages -- steganography
- "Going Dark"
  - FBI's initiative to reduce prevalence of end-to-end encryption
- EARN IT Act (2020)
  - Providers that provide end-to-end encrypted messaging must monitor messages for CSAM
  - Defeats end-to-end protections in the name of detecting abuse
  - Horrible, abusive content -- but universal scanning might not be the answer
- The debate rages on

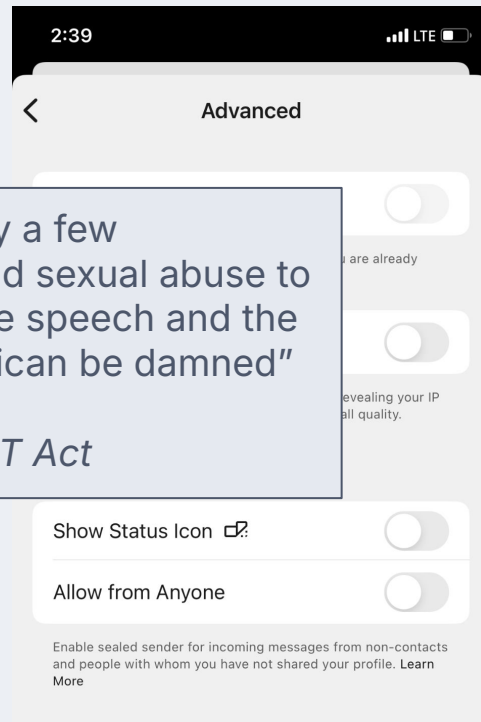


# Society

- Signal and Tor banned in several countries
  - Brittle censorship circumvention
  - Make messages look like other messages -- steganography
- "Going Dark"
  - FBI's initiative to use child sexual abuse to their political advantage, the impact to free speech and the security and privacy of every single American be damned"
- EARN IT Act
  - Providers of messaging services
  - Defeats end-to-end protections in the name of detecting abuse
  - Horrible, abusive content -- but universal scanning might not be the answer
- The debate rages on

"a transparent and deeply cynical effort by a few well-connected corporations ... to use child sexual abuse to their political advantage, the impact to free speech and the security and privacy of every single American be damned"

*Senator Ron Wyden (D-OR) on the EARN IT Act*





# Looking ahead

- Be reflective about your progress, and reach out if you need help
  - Key dates for the remainder of the semester
    - Nov 13: Exam 2
    - Nov 19: Project code due
    - Dec 4: Project demo day
    - Dec 11: Project presentations
  - Send an email with the subject "EE G7701 Exam 1 [LastName]" to get your exam back
  - New course! EE G7702 Research Topics in Cybersecurity
- **Today's activity:** personal privacy check-up lab

## Lesson objectives

- Work through, step by step, the operation of the Signal protocol
- Describe how Tor uses onion routing to provide censorship resistance
- Understand the political and societal ramifications of privacy