



digital defense fund

# Digital Surveillance, Encryption, & Your Nonprofit

Adapted from Netroots Nation 2020

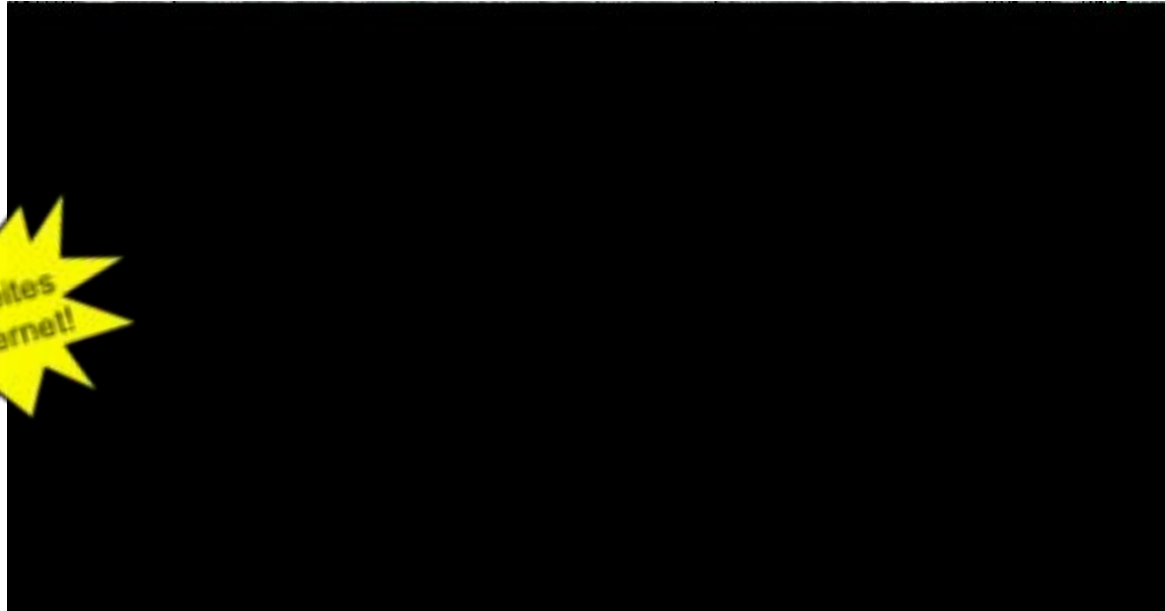
Amanda Bennett (she/her) & Rachael Lorenzo (they/them)

Last updated 2/25/21

# Understanding the Internet in 5 Minutes



# The internet is not a cloud...it's cables & computers



Source: [https://www.youtube.com/watch?v=ts7v5dkQs\\_w](https://www.youtube.com/watch?v=ts7v5dkQs_w)

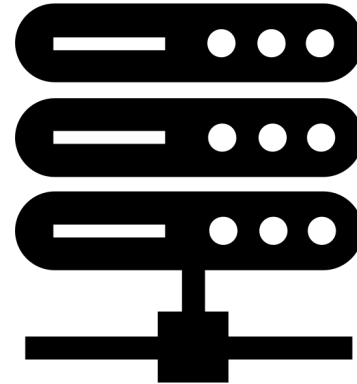
The internet is a bunch of computers talking to other computers, and those computers are (mostly) owned by companies.



# What's "The Cloud?"

"The Cloud" is someone else's servers.

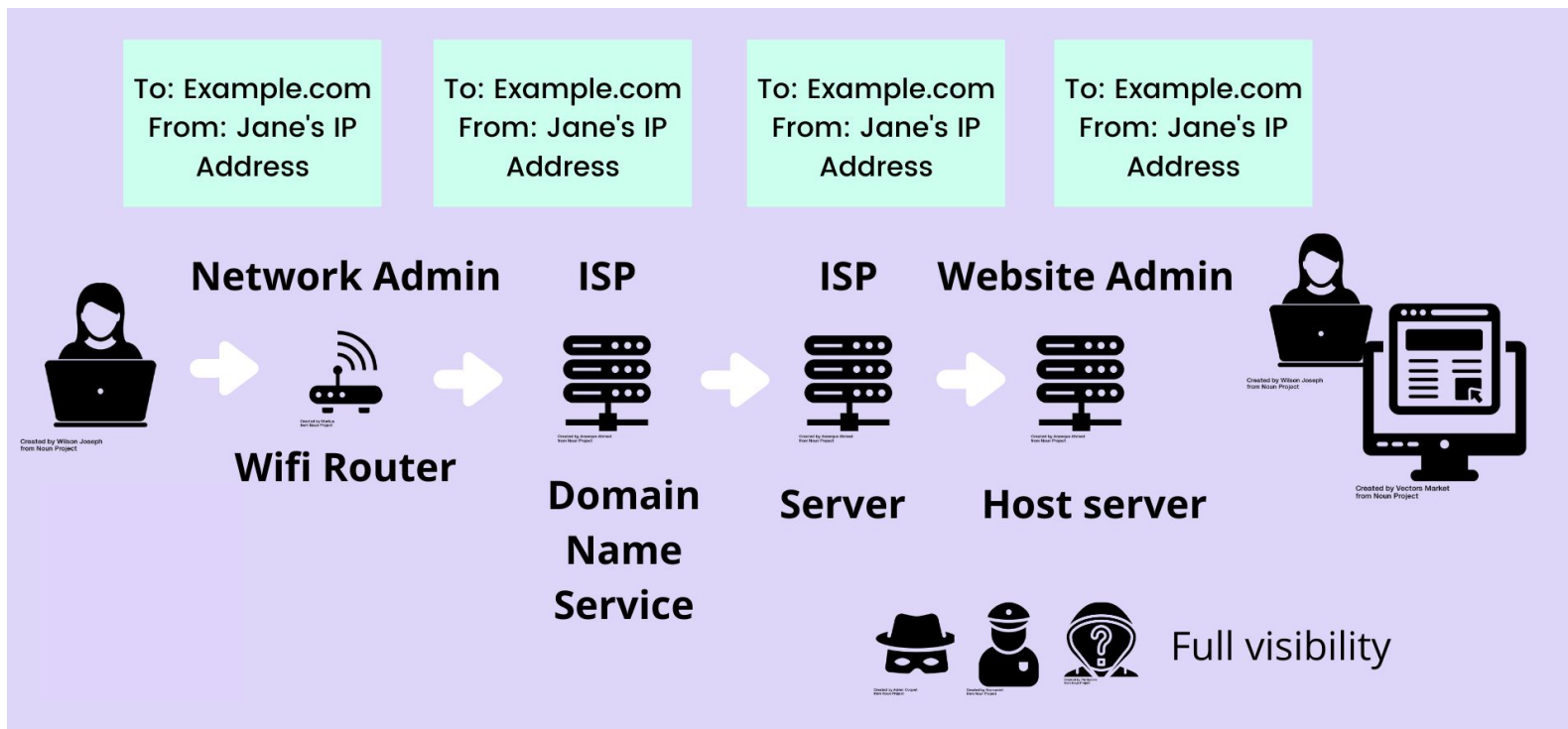
(Servers are just a kind of computer.)



Created by Aneeqe Ahmed  
from Noun Project



# These are some of those computers:



# Lots of actors want our information!



Image credit: Electronic Frontier Foundation

# The responsibility of blocking those actors is shared between platforms and users

## What they control:

- Security of our data in transit
- Security of our data storage
- What and how they share our data with other services, or entities

## What we control:

- Our login
- What and how we share with other services
- What and how we share with other users
- Our devices we use to access those platforms





# What's surveillance & who is surveilling us?

# Why do we care about surveillance?

From Lucy Parsons Lab:

Even if you "aren't doing anything wrong", surveillance alters people's state of mind.

Similar to the state you enter when there's a police cruiser behind you.



# Biased Algorithms Built by Biased People in an Oppressive Society!

## Why facial recognition's racial bias problem is so hard to crack

Good luck if you're a woman or a darker-skinned person.



Queenie Wong  March 27, 2019 5:00 AM PDT



### I'm a trans woman – here's why algorithms scare me

SCIENCE & TECH - INFINITE IDENTITIES

We want to live our truth in the present and define our own future – not be algorithmically chained to false identities

12th February 2019

Text Janus Rose  
Illustration Marianne Wilson



# Surveillance is dangerous when it's inaccurate and scary if it's accurate!

The New York Times

## *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*

A New Jersey man was accused of shoplifting and trying to hit an officer with a car. He is the third known Black man to be wrongfully arrested based on face recognition.

<https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html>

**THE VERGE**

## NYPD used facial recognition to track down Black Lives Matter activist

*Mayor Bill de Blasio says standards need to be "reassessed"*

By James Vincent | Aug 18, 2020, 5:26am EDT





Surveillance techniques are tested on already oppressed communities.

## The Government Is Testing Mass Surveillance on the Border Before Turning It on Americans

Almost every technology developed at the border in the last two decades now exists in local police departments



Jack Herrera [Follow](#)

Oct 17, 2019 · 5 min read ★



# Non-profits are monitored even if we aren't doing anything "wrong".

A student volunteer was recruiting lawyers who might be willing to provide representation to protestors who were arrested while exercising First Amendment rights

Name: [REDACTED]

Email Address: [REDACTED]

Phone: [REDACTED]

Brief description of your legal issue:  
Hello! I hope this email finds you in good regards.

My name is [REDACTED] I am from [REDACTED] and I attend the University of Oregon, studying Political Science. I am a long time activist and ally of the Black Lives Matter movement. I am emailing you today regarding the ongoing events in our country. Due to the killing of George Floyd, and many unjust deaths inflicted by corrupt law enforcement officials before hand, large protests and riots have broken out within the largest cities in America.

I am currently working on a list of resources for myself, my friends, and other individuals who are protesting, to refer to if they were to be arrested while protesting. I am mostly catering toward areas in which most of the students who attend my college are from. I am worried that Trump's latest remarks, regarding the new designation naming Antifa as terrorists, will allow for law enforcement to arrest peaceful protesters under the guise of them, "terrorizing," as Antifa is not an actual organization with collective members and could easily be anyone.

Is there anyway that I could add your firm, or consenting lawyers under your firm, to a list of resources who will represent protesters pro bono if they were/are to be arrested? Thank you very much for your time.

[REDACTED]

How would you like to be contacted?:  
email



One of the lawyers the student contacted sent this letter to local law enforcement, accusing the student of being a “terrorist”.

PLEASE SEE THE ATTACHED SOLICITATION I RECEIVED FROM AN ANTIFA TERRORIST WANTING MY HELP TO BAIL HER AND HER FRIENDS OUT OF JAIL, IF ARRESTED FOR RIOTING.

MY APOLOGIES FOR NOT PROVIDING MY RETURN E-MAIL AND IDENTITY. I AM AN ATTORNEY AND CANNOT RISK THIS PIECE OF SHIT ANTIFA – SEE ATTACHED – FILING A BAR COMPLAINT AGAINST ME. AS YOU CAN CLEARLY SEE IN THE E-MAIL SHE SENT ME, SHE WAS CLEARLY CROSSING STATE LINES FOR THE PURPOSES OF RIOTING.

SHE TOLD ME – WHEN I SPOKE WITH HER & AT NO TIME DID I TELL IT WAS A CONFIDENTIAL CONVERSATION – THAT SHE HAD CONTACTED HUNDREDS OF BAY AREA LAWYERS FOR ASSEMBLE THIS LIST.

I NEED YOU TO UNDERSTAND THAT THE SAN FRANCISCO PUBLIC DEFENDERS WILL VIGOROUSLY DEFEND THESE TERRORISTS.

SO YOU WANT TO COORDINATE WITH THE SFPD AND D.A. OFFICE TO SIT IN ON COURT DOCKETS WITH LOOTING AND OTHER RIOTING RELATED CASES BECAUSE YOU WILL THEN FIND MANY OF THESE OUT OF STATE ASSHOLES. HAPPY HUNTING.

**I AM DOING THIS BECAUSE I LOVE THE U.S.A. AND I MEANT IT.**





As reported below in the Intercept, the local DA's office logged this ludicrous report as potentially legitimate, and the student's name was logged in the regional intelligence center database.

An investigator in the Marin County DA's office considered this useful intelligence. She logged into the Northern California Regional Intelligence Center's CMS and created a new Suspicious Activity Report, or SAR, under the category "Radicalization/Extremism" and typed the student's name as the subject. "The attached letter was received via US Postal Service this

<https://theintercept.com/2020/07/15/blueleaks-anonymous-ddos-law-enforcement-hack/>



We experience an immense amount of data and surveillance - we can't possibly cover it all.

## DNA from cigarette leads to Dakota Access arrest 3 years on

*North Dakota authorities relying on DNA collected from a cigarette butt have charged a man with engaging in a riot for his part in a Dakota Access pipeline protest three years ago*

By **The Associated Press**

September 6, 2019, 3:21 PM • 2 min read

## Five Concerns about Amazon Ring's Deals with Police

DEEPLINKS BLOG

BY **MATTHEW GUARIGLIA**

AUGUST 30, 2019

*The New York Times*

## *She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database.*

With little oversight, the N.Y.P.D. has been using powerful surveillance technology on photos of children and teenagers.



What state surveillance exists near you?

Navigate to <https://atlasofsurveillance.org/>



So...what can we do?



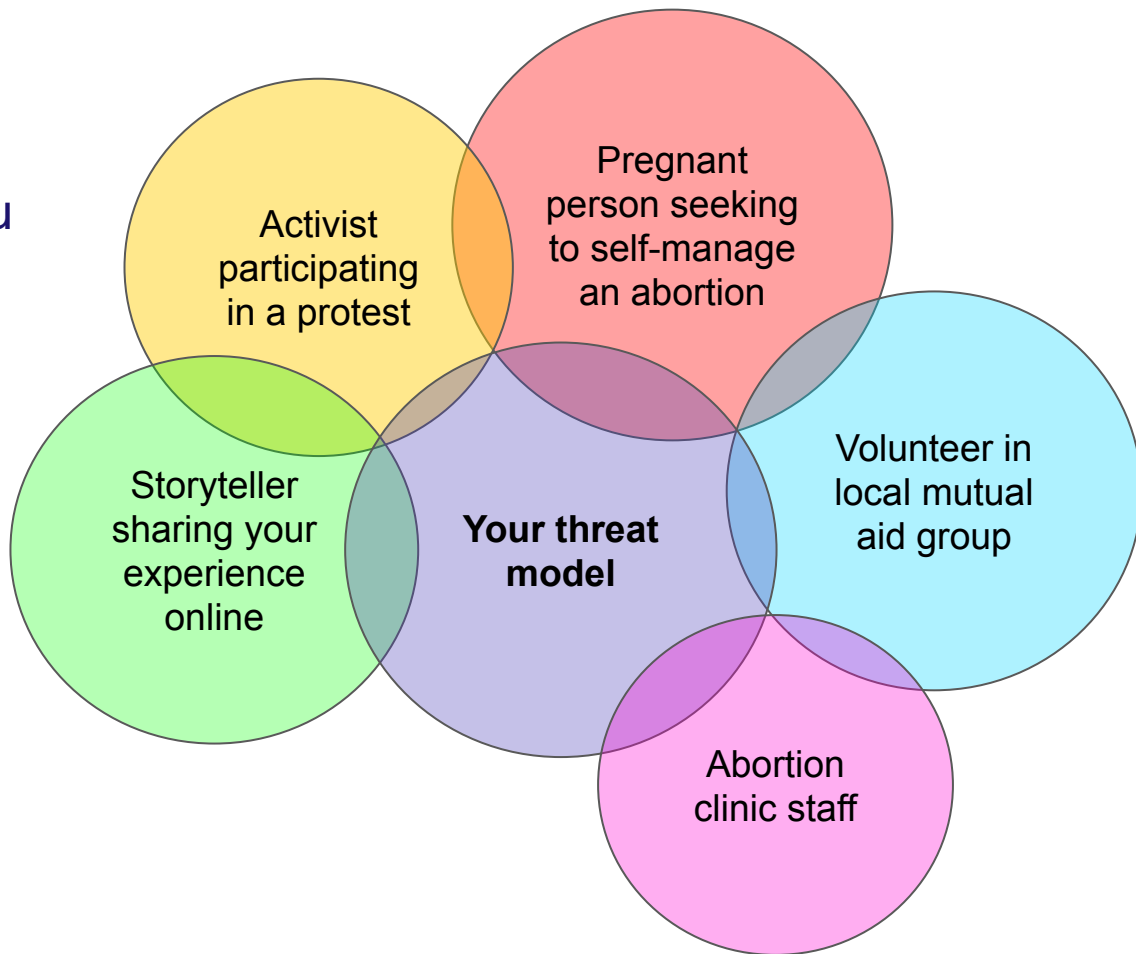
# Take control of what affects you!



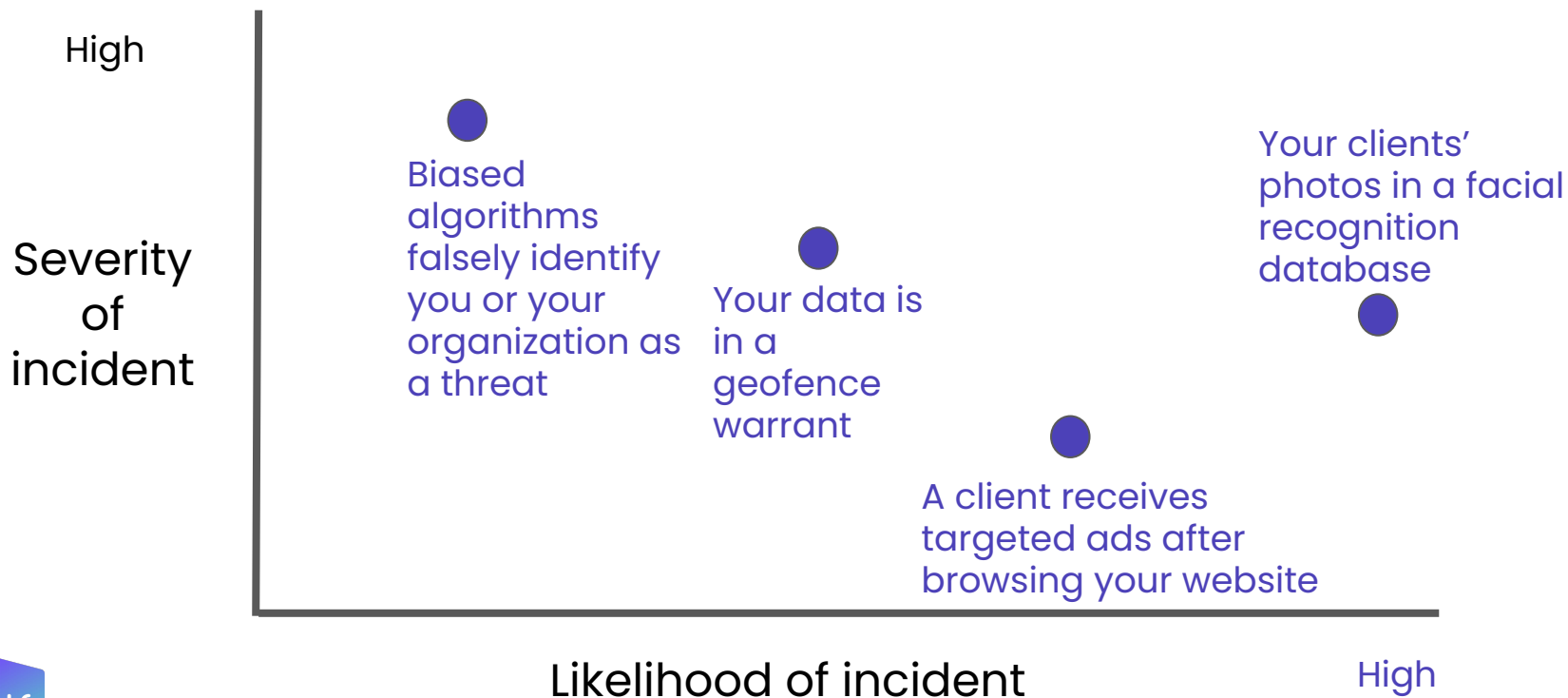
# Context is key!

What type of work are you doing?

This affects the type of threat you'll face.



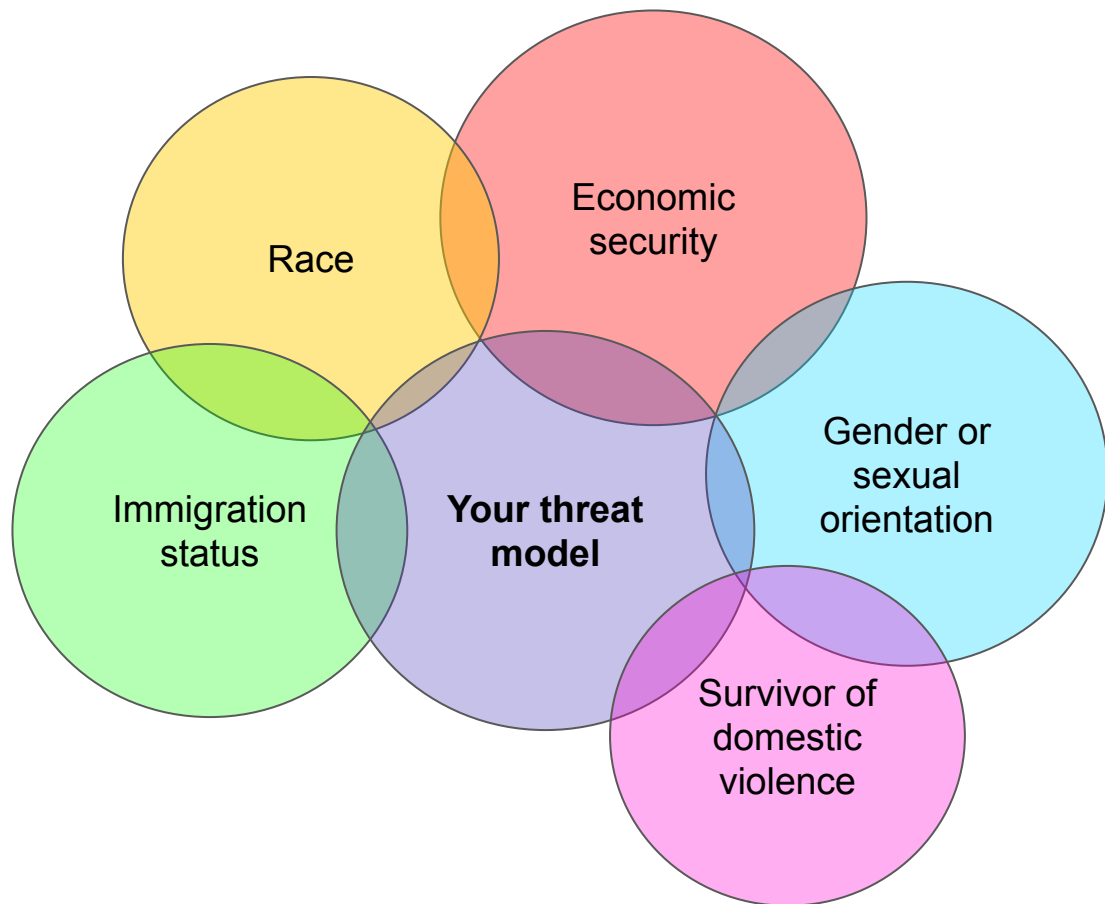
# Axis of risk: Surveillance



# Context is key!

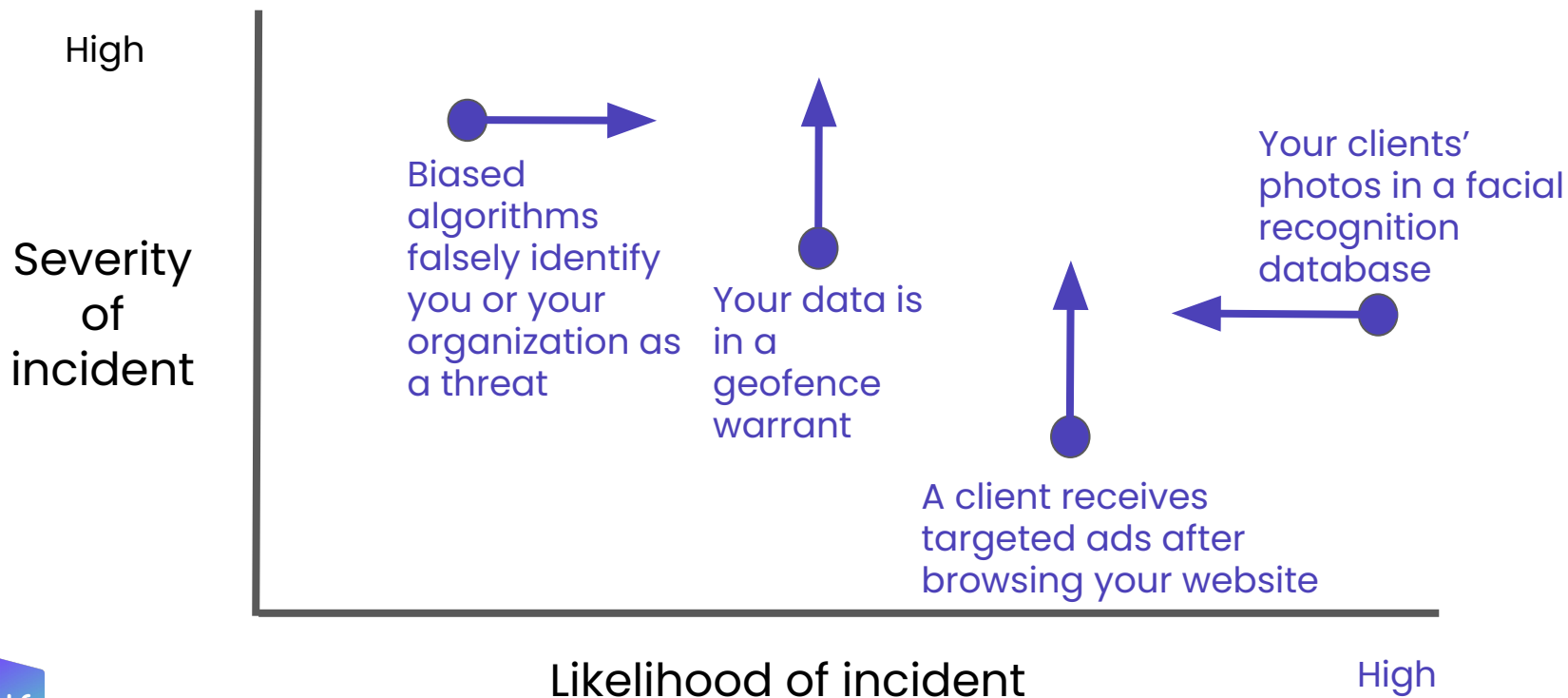
What about your identity affects how you move through the world?

This can affect how severe impact of a threat will be.





# Axis of risk: Surveillance



Does your organization contribute  
to surveillance?

# People bring their (negative) experiences with surveillance to their interactions with your organization.

- Do people you work with understand how you got their information?
- Are you able to explain to the people you work with why you collect the information you do?
- Could the information you store about people be dangerous if it fell into the wrong hands?



# Solutions: Encryption

# Platforms choose what encryption protocols they use to protect our data.

What platforms control:

- **Security of our data in transit**
- **Security of our data storage**
- What and how they share our data with other services, or entities

What we control:


- Our login
- What and how we share with other services
- What and how we share with other users
- Our devices we use to access those platforms





**Bob**  
Bob writes a message to Alice.

Hello Alice!



Bob uses Alice's **PUBLIC KEY** to encrypt the message which can only be decrypted by the corresponding private key.

**Server**  
The server never sees plain text messages.

AN83D&!0A?  
%A%)20DJ8?



Alice uses her **PRIVATE KEY** to decrypt Bob's message.

**Alice**  
Alice reads the message from Bob.

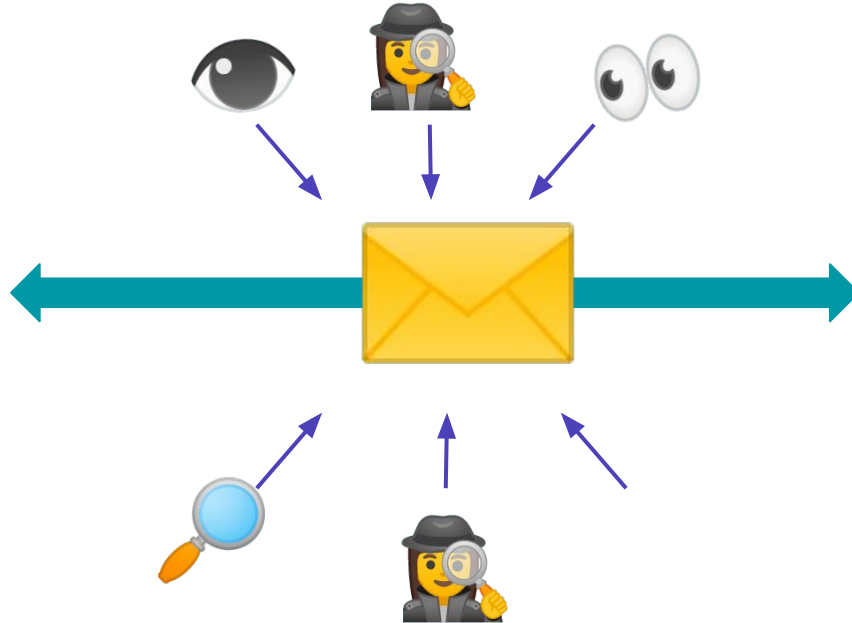
Hello Alice!



Source:  
ProtonMail

# Encrypt Your Messages

This keeps your communications out of the eyes of your phone carrier and protects from surveillance by bad actors!



# Encryption protects your information as it travels from computer to computer

- Only the people or computers with the encryption keys can read it

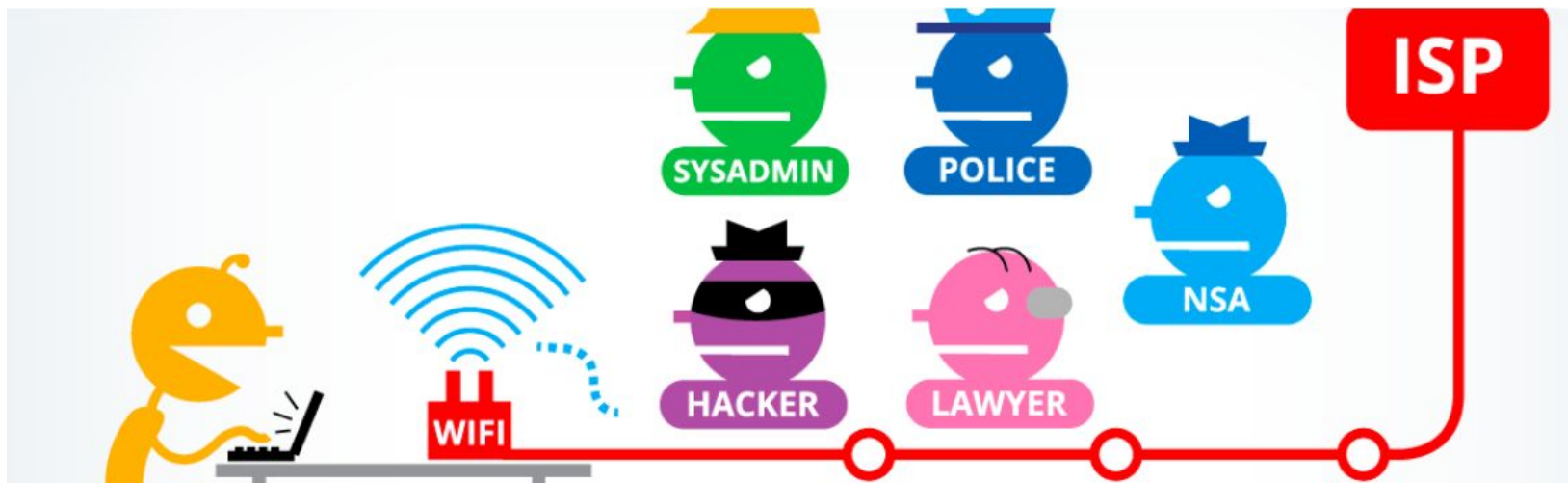


Image credit: Electronic Frontier Foundation



# We can choose platforms that encrypt our data.

When data is encrypted, only the people with the encryption key can read it!

There are two main ways that companies can encrypt our data:

- In transit & at rest
- End-to-end

## In transit/at rest

- The company owns the keys
- Company can see your data if they want to or if they are asked to show it (for example, when you call customer service or if they get a subpoena)

Examples: Snapchat, Wufoo, Gmail

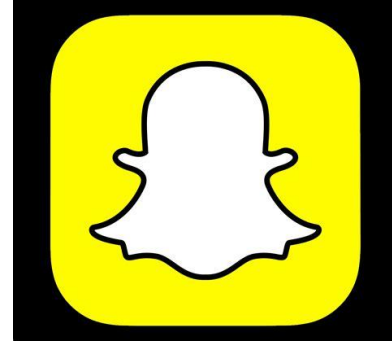
## End-to-end encryption

- Aka “zero knowledge”
- You own the keys!
- The company cannot see your data

Examples: Signal, Tresorit, Protonmail



# Encryption in transit & at rest



Slack, Snapchat, Gmail...

- Data encrypted in transit and at rest, **but not end-to-end**
- This means records can be subpoena-ed, but not intercepted by an unauthorized party
- The company holds the encryption keys

# End-to-End Encryption (E2EE)



## ProtonMail

- Email provider
- End-to-end encryption on open source protocol
- Doesn't log metadata
- Sign up with username & password
- Subject lines are not E2EE



## Signal

- Messaging app
- End-to-end encryption on open source protocol
- Doesn't log metadata
- Disappearing messages feature
- Sign up with phone number

# End-to-end encryption doesn't guarantee total security!

Both WhatsApp & iMessage use end-to-end encryption for chat messages, but collect metadata & backups that are NOT protected with E2EE



## WhatsApp

- End-to-end encryption on Signal protocol
- Owned by Facebook
- Very popular
- Collects metadata
- Can store unencrypted chat backups



## iMessage

- End-to-end encryption
- Owned by Apple
- Collects metadata
- If you backup to iCloud, Apple can access those unencrypted chat backups



# Whatsapp

## App Privacy

[See Details](#)

The developer, WhatsApp Inc., indicated that the app's privacy practices may include handling of data as described below. For more information, see the [developer's privacy policy](#).



### Data Linked to You

The following data may be collected and linked to your identity:

- Purchases
- Location
- Contacts
- Identifiers
- Diagnostics
- Financial Info
- Contact Info
- User Content
- Usage Data

Privacy practices may vary, for example, based on the features you use or your age. [Learn More](#)



# Signal

## App Privacy

[See Details](#)

The developer, Signal Messenger, LLC, indicated that the app's privacy practices may include handling of data as described below. For more information, see the [developer's privacy policy](#).



### Data Not Linked to You

The following data may be collected but it is not linked to your identity:

- Contact Info

Privacy practices may vary, for example, based on the features you use or your age. [Learn More](#)

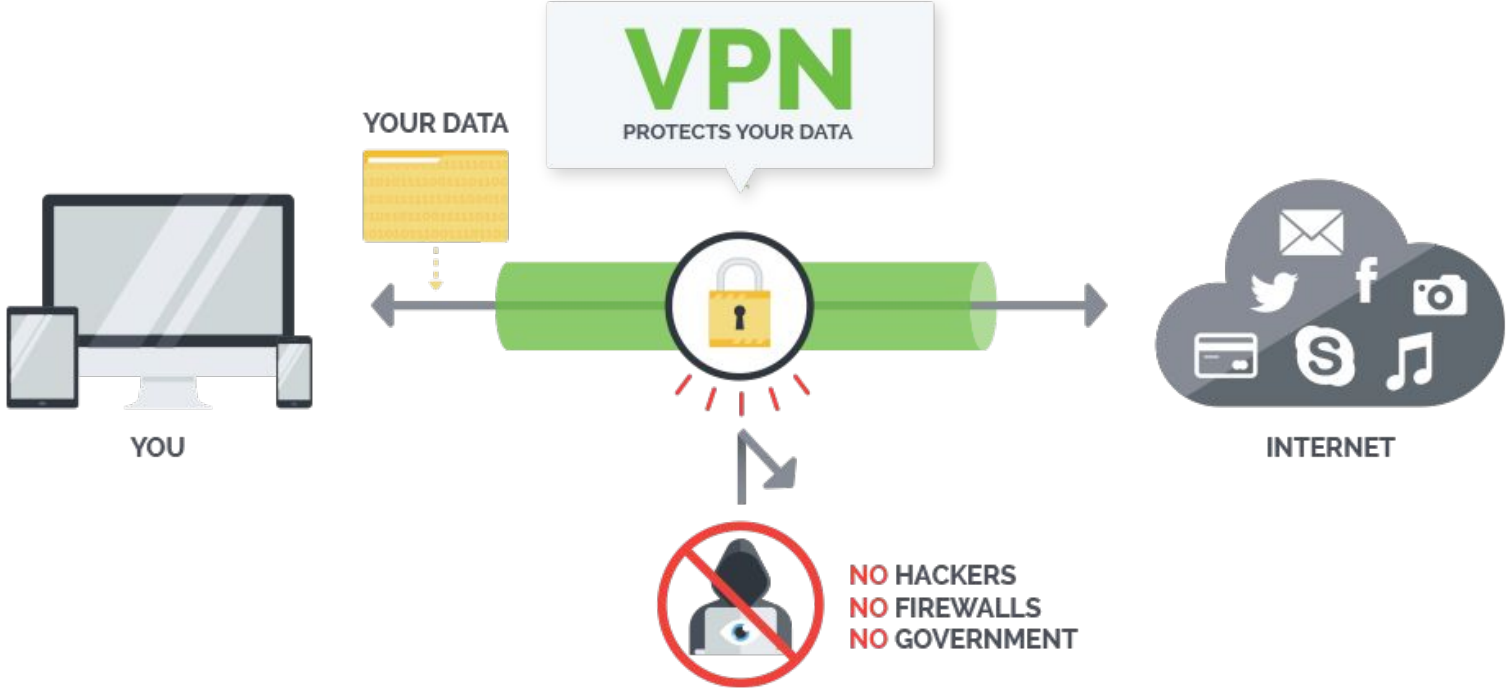
Screenshots from Apple's App Store



# Encrypt your internet traffic



# Encrypt your internet traffic

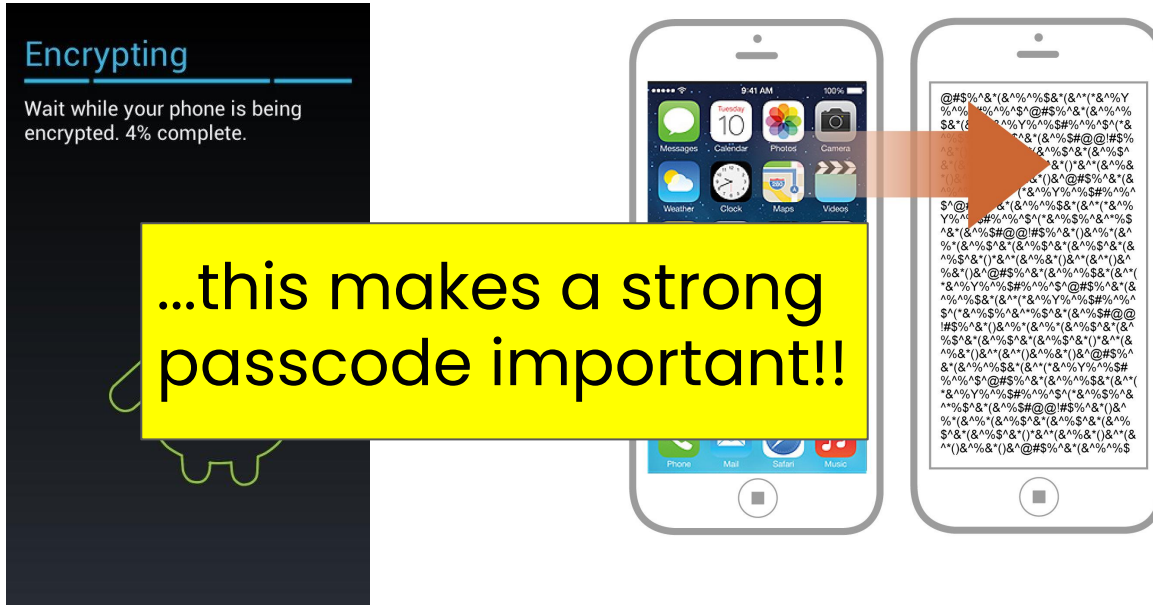


Credit: IPVanish



# Encrypt Your Devices

- iPhones & newer Androids encrypted by default with passcode or PIN



Remember:  
encryption does  
not mean you  
are 100%  
anonymous or  
secure!



SwiftOnSecurity  
@SwiftOnSecurity



When you reuse your MySpace  
password on your ProtonMail  
account



5:45 AM · 2/23/19 · [Twitter for iPhone](#)



# Encryption doesn't protect against all threats

## Safety

- Usually for people
- Depends on relationships
- Relies on trust and respect

*Ex: Knowing the person getting your Signal message is a trusted comrade*

## Security

- Usually for property or data
- Depends on the technology & using it correctly

*Ex: Knowing the message you send via Signal is protected with end-to-end encryption*



“Encryption is love.”

-@cyberdoula



# FYI: Keep an eye on legislation that seeks to make end-to-end encryption illegal.

In 2020, we kept an eye on the EARN IT Act and the Lawful Access to Encrypted Data Act. To stay up to date on that legislation and future bills, follow these groups:

- The Electronic Frontier Foundation (@EFF)
- Hacking/Hustling (@hackinghustling)
- Access Now (@accessnow)

