What's the worst that could happen?

Petra Smith

Aura Information Security

OWASP NZ Day 2020

This talk includes discussion of death, physical violence, torture and abuse that may be distressing or traumatic.

Hi. I’m Petra.

I’m an inoffensive security consultant
at Aura Information Security.

I catastrophise for a living.

These are not the views of my employer.

What’s the worst that could happen?

Oh, I didn’t see you there.

What’s the worst that could happen?

Uber’s autonomous vehicle killed Elaine Herzberg.

Mistakes were made.

“If they catch me, they will kill me.”

Jamal Khashoggi to his friend Khaled Saffuri

May 2018

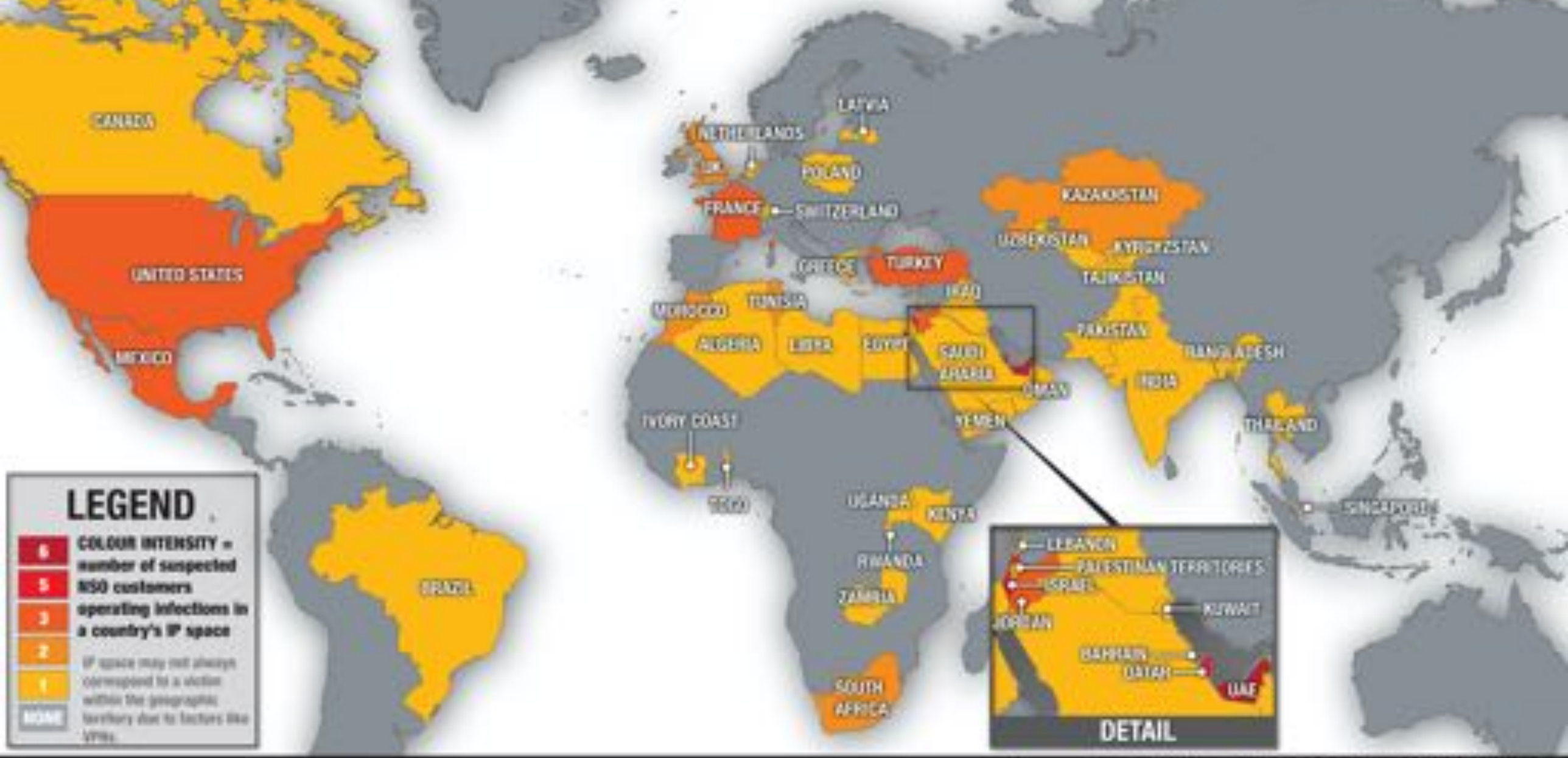
What's the worst that could happen?

Pegasus gave up Jamal Khashoggi's location to the men who killed him.

“Why should anyone harm you physically? They try to drown your voice with smear campaigns and put pressure on your family, but you are under the protection of the United States.”

Nihad Awad to Jamal Khashoggi

September 2018



SUSPECTED PEGASUS INFECTIONS

A GLOBAL MAP MADE WITH DNS CACHE PROBING

Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak & Ron Deibert

CITIZEN LAB 2018

“I like to be able to read the news and not think somebody’s holding a gun to a reporter’s head, deciding what he writes”

Former Black Cube contractor Igor Ostrovskiy to reporter and surveillance target Ronan Farrow

“Our technology is not designed or licensed for use against human rights activists and journalists. We consider any other use of our products than to prevent serious crime and terrorism a misuse, which is contractually prohibited”

Statement from NSO Group

What's the worst that could happen?

Twitter engineers used their privileged access to spy on political targets.

Don’t worry, it’s just metadata.

Private internet access for nonprofit organizations

The NordVPN Nonprofits program offers eligible organizations a discount on a VPN subscription.

Who qualifies

We welcome applications from journalists, human rights advocat and other nonprofit organizations that need to access informatio securely, communicate with their sources, and report the news without the fear of being watched. NordVPN is happy to help nonprofits fulfill their mission by providing safe and private acces the internet.

Server Incident Timeline

Incident Scope - March 2018

Affected servers (1)

Secure servers
(over 3,300)


SERGEANT
LOS ANGELES POLICE
714
DRAGNET

What’s the worst that could happen?

London Metropolitan Police successfully use AI to identify hundreds of criminals.

What's the worst that could happen?

London Metropolitan Police "successfully" use AI to falsely identify hundreds of young black men as criminals.

“We are using a tried-and-tested technology.”

Statement from London Metropolitan Police

What's the worst that could happen?

Law enforcement agencies rely on technology that routinely misidentifies people of colour.


SHAPING INTELLIGENCE
2018 AI CLOUD WORLD SUMMIT, HANGZHOU
少数民族
Ethnic Minority
这套系统同时可以对特定游客进行定位
This system can also track specific visitors to monitor

What's the worst that could happen?

iOS zero-days were exploited in a probable nation-state attack on China's Uyghur people.

“we take the safety and security of all users extremely seriously”

Statement from Apple

Don’t worry, it’s anonymised.

What’s the worst that could happen?

Grindr shared users’ HIV status and location data.

What's the worst that could happen?

Up to 40% of cases of intimate partner abuse involve technology to stalk, harass or intimidate.

What’s the worst that could happen?

Trolls harassed children by hacking into Ring cameras.

We take your security. Seriously.

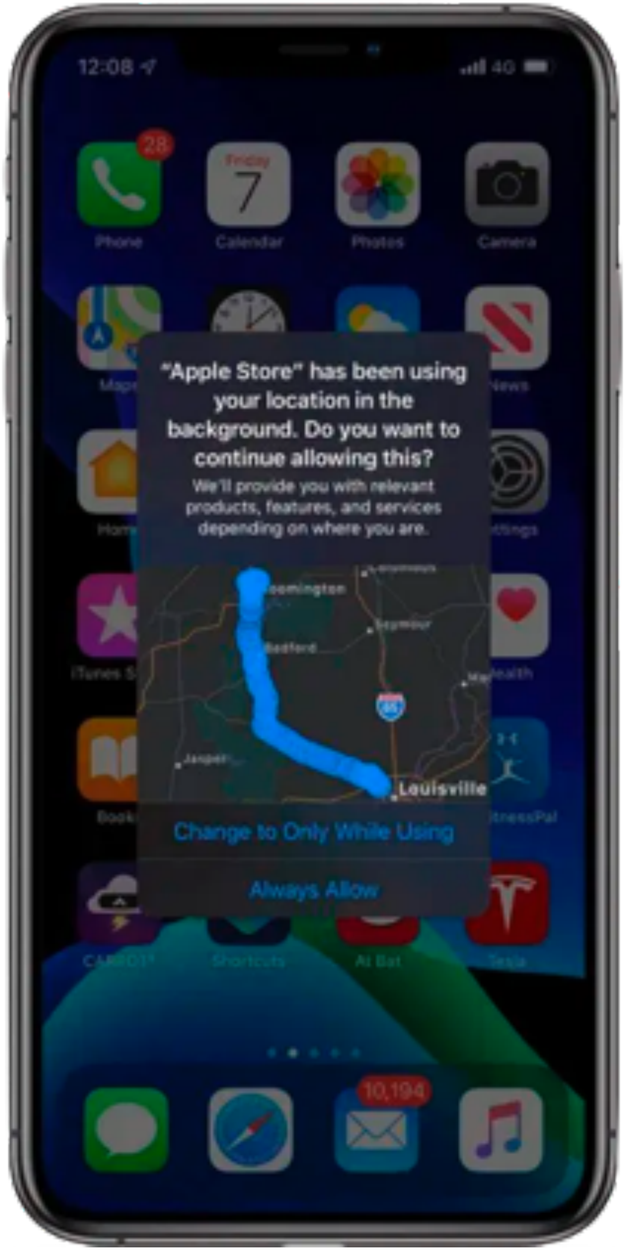
79% are concerned over how companies use their data

81% say they don’t have enough control over their data

79% aren't confident companies will admit misuse or breaches

81% say the potential risks outweigh the potential benefits

Source: *Americans and Privacy,* Pew Research Centre, 2019


12:08
4G
28
Phone
Friday
7
Calendar
Photos
Camera
"Apple Store" has been using your location in the background. Do you want to continue allowing this?
We'll provide you with relevant products, features, and services depending on where you are.
Louisville
Change to Only While Using
Always Allow
10,194

What you don’t know can hurt you.


- IT'S VERY EASY TO CRITICIZE.
- FUN, TOO!

thaddeus e. grugq
@thegrugq

Your threat model is not my threat model.

7:42 PM · May 15, 2017 · Tweetbot for iOS

What are you building?

What can go wrong?

What should you do about those things that can go wrong?

Did you do a decent job of analysis?

Source: Adam Shostack, *Threat Modeling: Designing for Security*

What are you building?

What can go wrong?

What should you do about those things that can go wrong?

Did you do a decent job of analysis?

Source: Adam Shostack, *Threat Modeling: Designing for Security*

What are you building?

What can go wrong?

What should you do about those things that can go wrong?

Did you do a decent job of analysis?

Source: Adam Shostack, *Threat Modeling: Designing for Security*

Spoofing – threats against authentication

Tampering – threats against integrity

Repudiation - threats against non-repudiation

Information Disclosure - threats against confidentiality

Denial of Service - threats against availability

Elevation of Privilege - threats against authorisation

Source: Adam Shostack, *Threat Modelling: Designing for Security*

What are you building?

What can go wrong?

What should you do about those things that can go wrong?

Did you do a decent job of analysis?

Source: Adam Shostack, *Threat Modeling: Designing for Security*

To protect our app’s users from spoofing attacks, we

- Give them the option to turn on 2FA
- Let them paste into the password box
- Remind them we’ll never ask for their password
- TODO: add “never ask for passwords” to Support’s induction manual

What are you building?

What can go wrong?

What should you do about those things that can go wrong?

Did you do a decent job of analysis?

Source: Adam Shostack, *Threat Modeling: Designing for Security*

“Now he had learned that a machine simple in its design, could produce results of infinite complexity.”

Neal Stephenson, *Cryptonomicon*

Why do bad things still happen?

What are you scared of?

- credit card skimming
- identity theft
- sensitive data exposure

Here’s what I’m scared of

- stalker knowing where to find me
- getting hacked by the scary ex
- outed to an anti-LGBTIA+ government
- denied healthcare by an algorithm

“The future is here – it’s just not very evenly distributed.”

William Gibson

What's the worst that could happen?

The Washington Post's owner was blackmailed over photos extracted from his phone using Pegasus spyware.

What's the worst that could happen?

The Washington Post's owner was blackmailed over photos extracted from his phone using Pegasus spyware.

He told the blackmailers "no thanks".

Jeff Bezos Follow
Feb 8, 2019 · 9 min read

No thank you, Mr. Pecker

Something unusual happened to me yesterday. Actually, for me it wasn't just unusual — it was a first. I was made an offer I couldn't refuse. Or at least that's what the top people at the National Enquirer thought. I'm glad they thought that, because it emboldened them to put it all in writing. Rather than capitulate to extortion and blackmail, I've decided to publish exactly what they sent me, despite the personal cost and embarrassment they threaten.

AMI, the owner of the National Enquirer, led by David Pecker, recently entered into an immunity deal with the Department of Justice related to their role in the so-called "Catch and Kill" process on behalf of President Trump and his election campaign. Mr. Pecker and his company have also been investigated for various actions they've taken on behalf of the Saudi

“There are more things in heaven and earth, Horatio, than are dreamed of in your philosophy.”

William Shakespeare, *Hamlet*

The problem with threat modeling

The problem with threat modeling

- we don’t know what we don’t know

The problem with threat modeling

- we don’t know what we don’t know
- we don’t recognise our biases

The problem with threat modeling

- we don’t know what we don’t know
- we don’t recognise our biases
- we don’t recognise biases in technology

“Technology is neither good nor bad; nor is it neutral.”

Melvin Kranzberg’s first law of technology

The problem with threat modeling

- we don’t know what we don’t know
- we don’t recognise our biases
- we don’t recognise biases in technology (especially when they mirror our own)

“The model confuses parenting while poor with poor parenting.”

Virginia Eubanks, *Automating Inequality*

Algorithms disguise human biases and make them seem neutral and objective.

“Is it legal” isn’t a good yardstick for morality.

How can we do it better?

How can we do it better?

- involve people with a diverse range of perspectives

How can we do it better?

- involve people with a diverse range of perspectives
- listen to people with lived experience

Finally, some good news!

What's the worst that could happen?

A law meant to prevent sex trafficking and exploitation made it harder to prosecute trafficking and increased harm to survival sex workers.

How can we do it better?

- involve people with a diverse range of perspectives
- listen to people with lived experience

How can we do it better?

- involve people with a diverse range of perspectives
- listen to people with lived experience
- design for “stress cases” not “edge cases”

Ramona

As a ninja delivery driver who travels between dimensions, I need web apps that are mobile-friendly and work even when data coverage is patchy.

I don’t like having to commit to anything for too long.

I have seven evil exes.

How can we do it better?

- involve people with a diverse range of perspectives
- listen to people with lived experience
- think about “stress cases” not “edge cases”
- be transparent and let people make choices

How can we do it better?

- involve people with a diverse range of perspectives
- listen to people with lived experience
- think about “stress cases” not “edge cases”
- be transparent and let people make choices
- accept and listen to feedback

How can we do it better?

- involve people with a diverse range of perspectives
- listen to people with lived experience
- think about “stress cases” not “edge cases”
- be transparent and let people make choices
- accept and listen to feedback
- advocate for positive change

Takeaways

Technology can seriously harm people

Threat modeling can help us build safer software

We need to be more aware of our biases and limitations

thanks to

the team at Aura for the time and support

the OWASP NZ Day organisers and volunteers

and all of you for coming on this adventure