THE GOOD & EVIL OF THE INTERNET AND WHY YOU SHOULD KNOW ABOUT THEM

WEEK 4

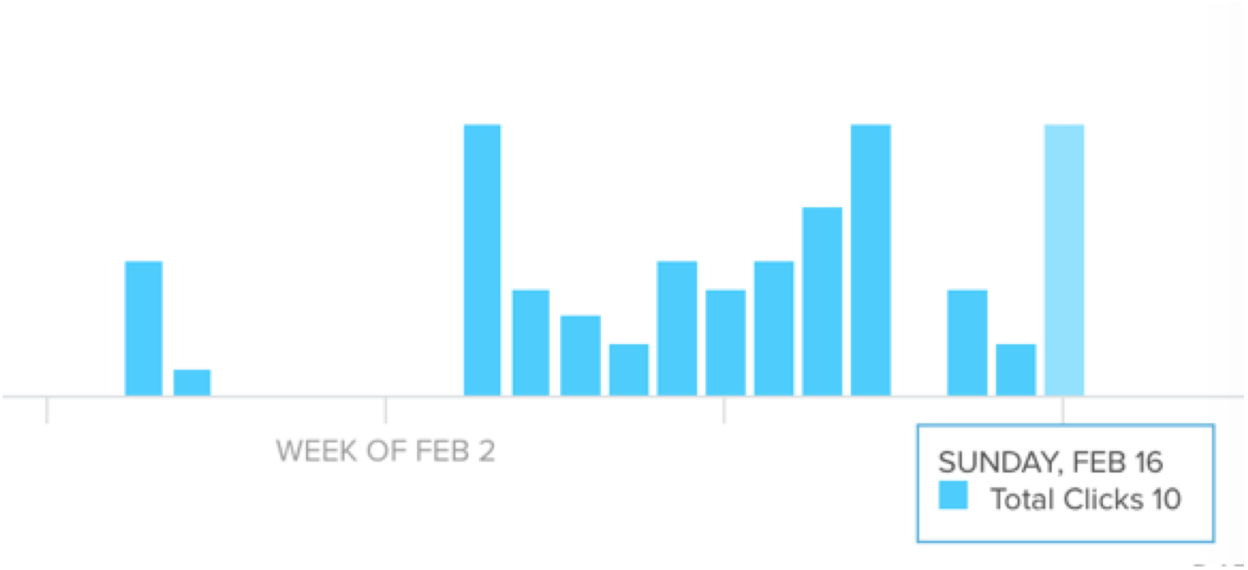
- OLLI WINTER 2020 COURSES
- Mondays, January 27—March 2
- 9:30—11:30 a.m.
- @Cooperage

OSHER
LIFELONG
LEARNING
INSTITUTE

- Dr. Farid Farahmand

A Quick Check-in…..

- Thank you for completing the survey



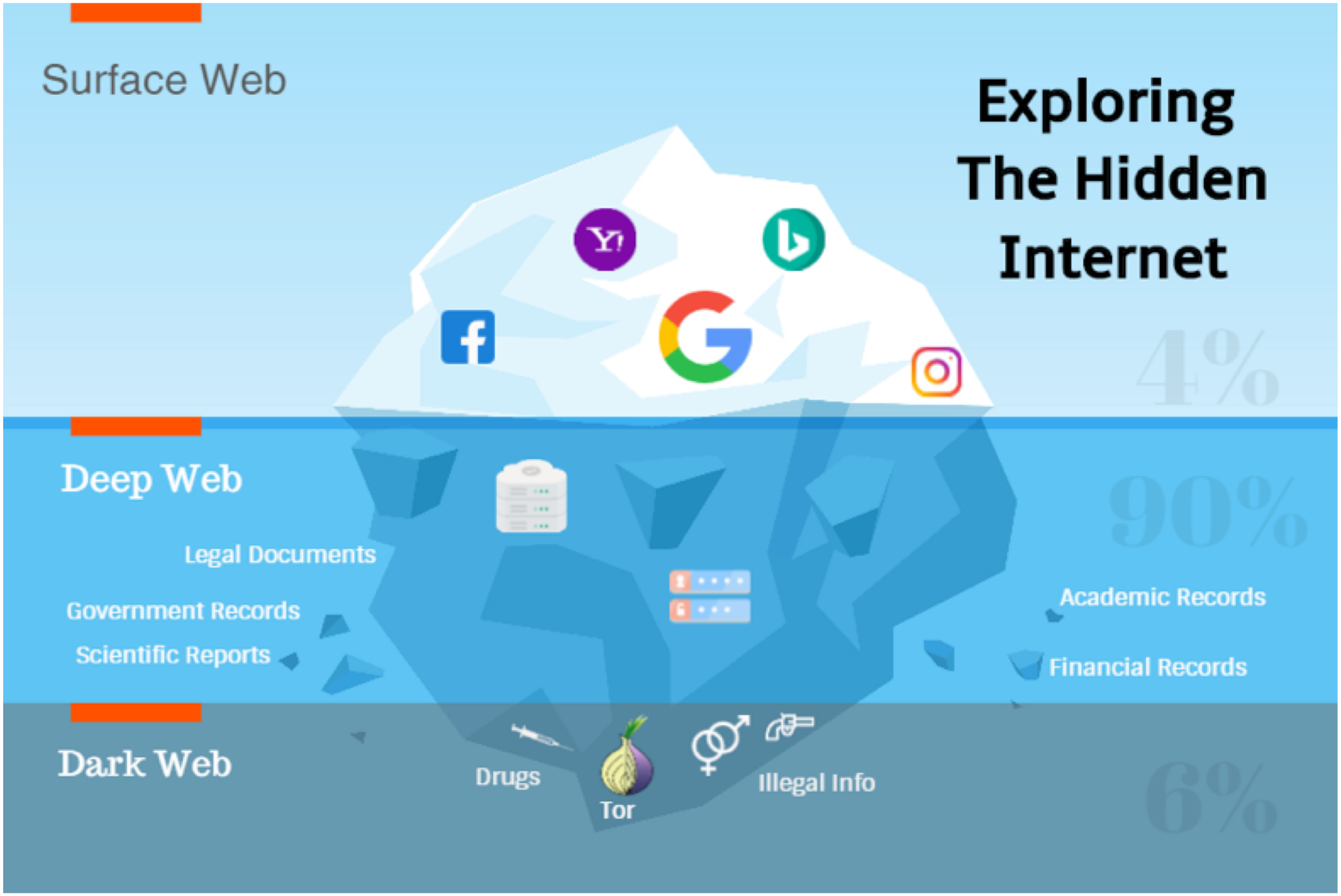
- Uploaded the slides
- Let's hold on to your questions for the first 45 min

OSHER
LIFELONG
LEARNING
INSTITUTE

What We Cover Today

- Quick review…..
  - VPN
  - Darknet
- Bitcoin (video)
- Malwares & viruses
- Face recognition
- Algorithms & and Data collection (next week)

Dark Net (Watch Video)



OSHER LIFELONG LEARNING INSTITUTE

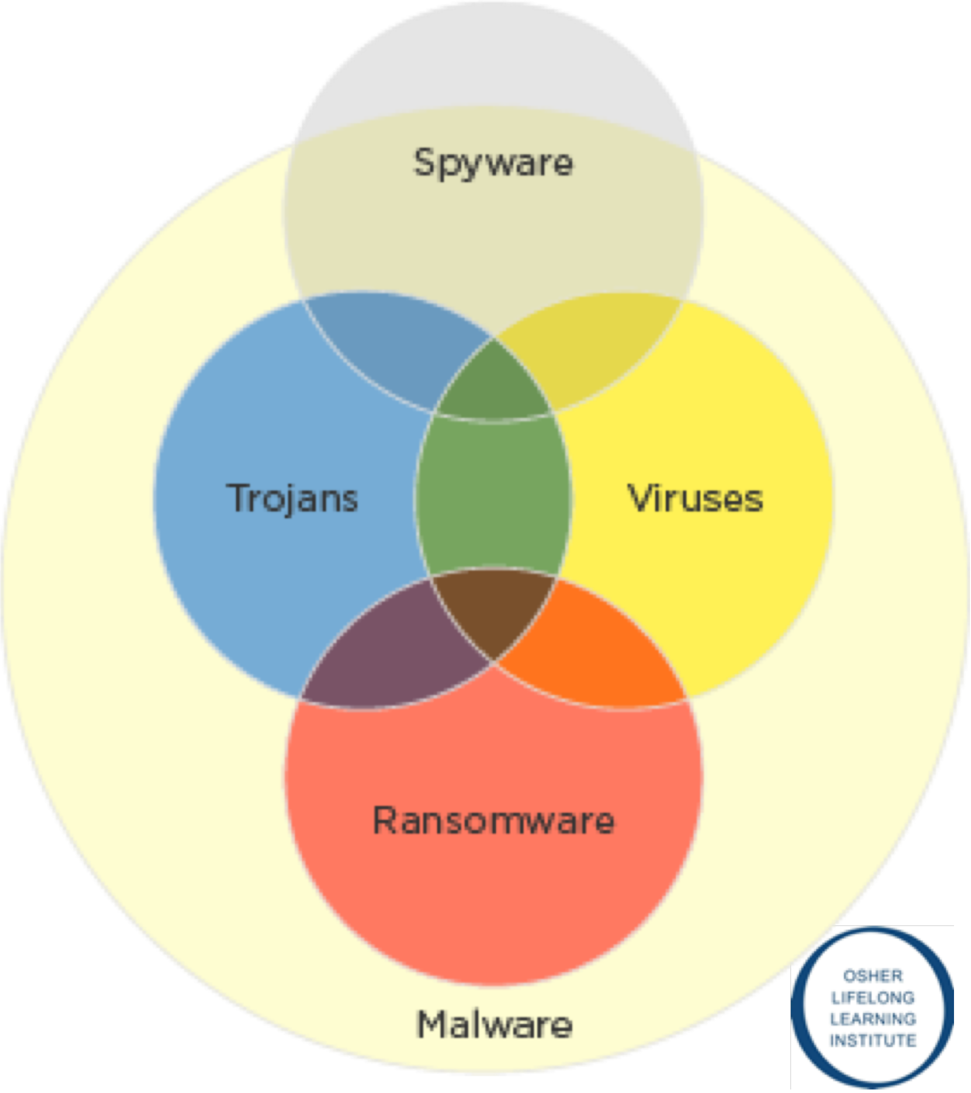
What is Cryptocurrency or Bitcoin!

…Let’s remove the bank as the central organization!

- Watch the Video!

Computer Threat Classification

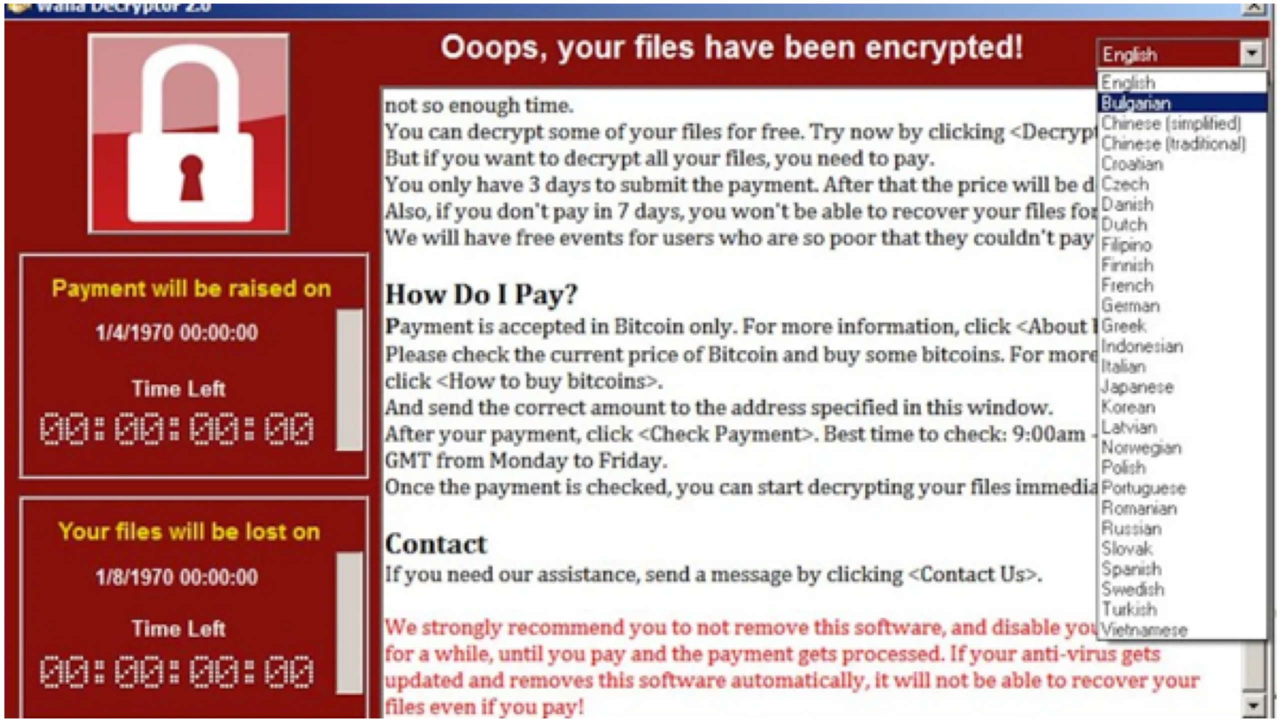
- Malware is the umbrella term for any type of **malicious software**
- Email attachments are the #1 **delivery method** for malware
- They are highly sophisticated and can take many different **shapes** and forms
  - Spyware
  - Trojans
  - Viruses
  - Ransomware
- Each can **affect**
  - Hardware
  - Software



OSHER LIFELONG LEARNING INSTITUTE

Malware Types

- **Viruses** damage your hard drive and system performance. They are designed to spread from one computer to another.
- **Ransomwares** prevent you from accessing your PC, either by locking your screen or your files until you pay money to an anonymous hacker.



Ooops, your files have been encrypted!

Payment will be raised on

1/4/1970 00:00:00

Time Left

00:00:00:00

Your files will be lost on

1/8/1970 00:00:00

Time Left

00:00:00:00

not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be d
Also, if you don't pay in 7 days, you won't be able to recover your files fo
We will have free events for users who are so poor that they couldn't pay

How Do I Pay?

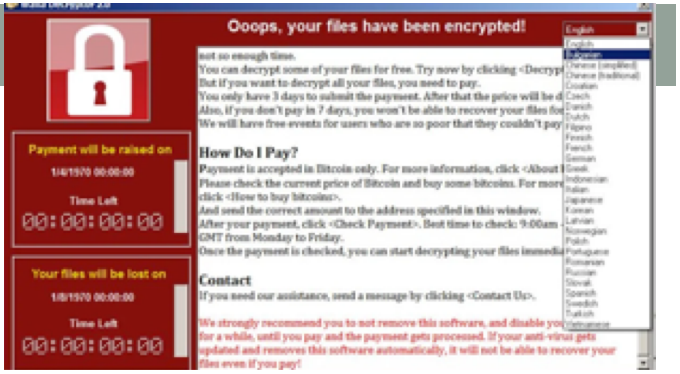
Payment is accepted in Bitcoin only. For more information, click <About
Please check the current price of Bitcoin and buy some bitcoins. For more
click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am -
GMT from Monday to Friday.
Once the payment is checked, you can start decrypting your files immedia

Contact

If you need our assistance, send a message by clicking <Contact Us>.

We strongly recommend you to not remove this software, and disable yo
for a while, until you pay and the payment gets processed. If your anti-virus gets updated and removes this software automatically, it will not be able to recover your files even if you pay!

Malware Types



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

Payment will be raised on
1/4/1970 00:00:00
Time Left
00:00:00:00

Your files will be lost on
1/8/1970 00:00:00
Time Left
00:00:00:00

not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be d
Also, if you don't pay in 7 days, you won't be able to recover your files fo
We will have free events for users who are so poor that they couldn't pay

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About B
Please check the current price of Bitcoin and buy some bitcoins. For more
click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am -
GMT from Monday to Friday.
Once the payment is checked, you can start decrypting your files immedia

Contact
If you need our assistance, send a message by clicking <Contact Us>.

We strongly recommend you to not remove this software, and disable you
for a while, until you pay and the payment gets processed. If your anti-virus gets
updated and removes this software automatically, it will not be able to recover your
files even if you pay!

- **Spyware** is invasive software that hides on your PC and monitors your online activity, collecting keystrokes, passwords, and even internet surfing habits. It adds illicit backdoor components to your programs and sites.
- **Trojans** masquerade as benign files or applications and then create digital backdoors that allow hackers to steal your personal data, files, and even use your computer to send out spam

OSHER
LIFELONG
LEARNING
INSTITUTE

Malware Types

- **Worms –** A type of malware that spreads copies of itself from computer to computer. A worm can replicate itself without any human interaction. They can modify and delete files, and they can even inject additional malicious software onto a computer.
- **Adware**—Are you redirected to a particular page or see unexpected pop-up ads when you start your browser
- **Rootkits** are software packages that allow malware to hide on your computer so you can't remove it. Rootkits keep malware from even showing up on your computer's list of active processes

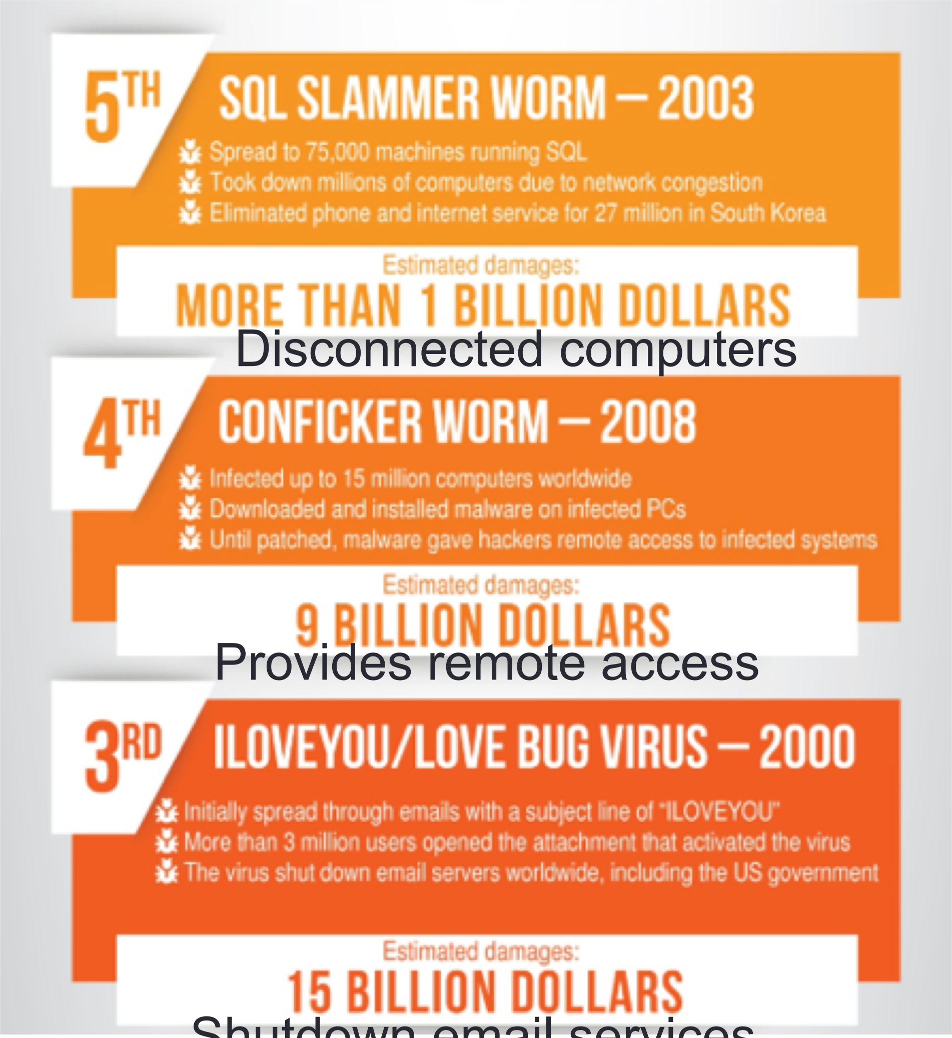
In 2010 the United States used a computer worm as a cyber weapon against Iranian facility in Natanz - Dubbed "Stuxnet,"

How To Block or Remove Malwares

- Windows 10 now includes a vast array of security and “threat mitigation” technologies
- There has also been a huge improvement in the security of web browsers
  - Including Google’s Chrome and Microsoft’s Edge.
- Google’s Chrome
  - Chrome protects the underlying operating system from web-based attacks
  - Google also runs a “**bug bounty**” program
    - The program pays researchers up to $100,000 for each exploitable hole they find in Chrome or Android.
    - It paid out more than $3 million last year, making Chrome even more secure.

OSHER LIFELONG LEARNING INSTITUTE

The Most Expensive Viruses….



5TH SQL SLAMMER WORM – 2003

- Spread to 75,000 machines running SQL
- Took down millions of computers due to network congestion
- Eliminated phone and internet service for 27 million in South Korea

Estimated damages:
MORE THAN 1 BILLION DOLLARS

Disconnected computers

4TH CONFICKER WORM – 2008

- Infected up to 15 million computers worldwide
- Downloaded and installed malware on infected PCs
- Until patched, malware gave hackers remote access to infected systems

Estimated damages:
9 BILLION DOLLARS

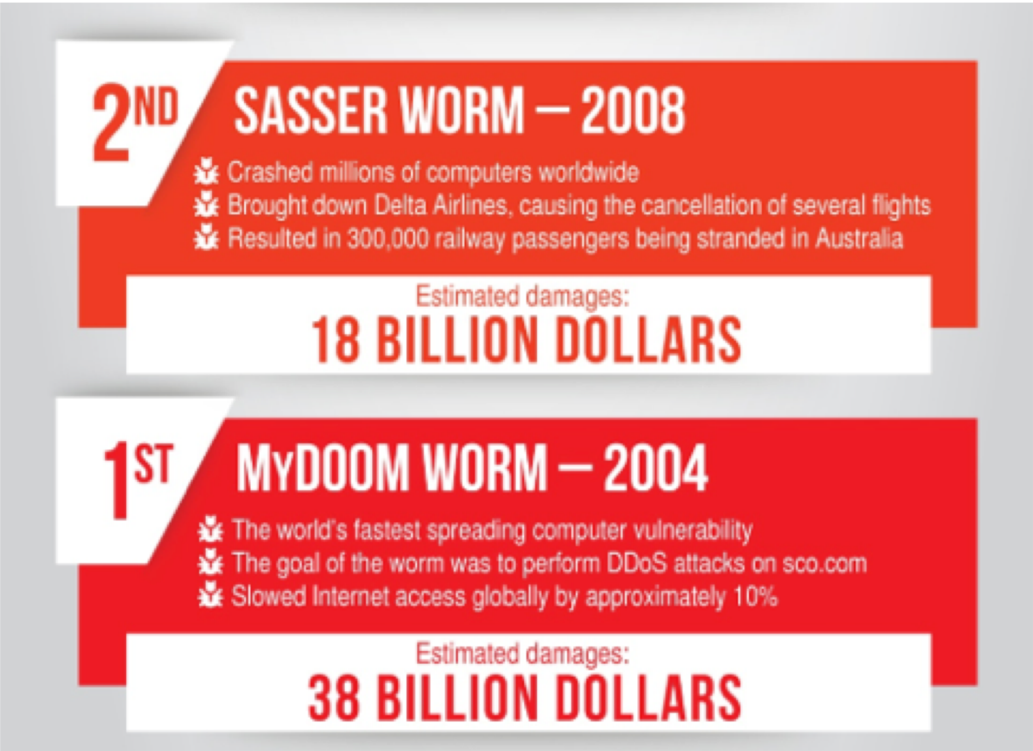
Provides remote access

3RD ILOVEYOU/LOVE BUG VIRUS – 2000

- Initially spread through emails with a subject line of "ILOVEYOU"
- More than 3 million users opened the attachment that activated the virus
- The virus shut down email servers worldwide, including the US government

Estimated damages:
15 BILLION DOLLARS

Shutdown email services



2ND SASSER WORM – 2008

- Crashed millions of computers worldwide
- Brought down Delta Airlines, causing the cancellation of several flights
- Resulted in 300,000 railway passengers being stranded in Australia

Estimated damages:
18 BILLION DOLLARS

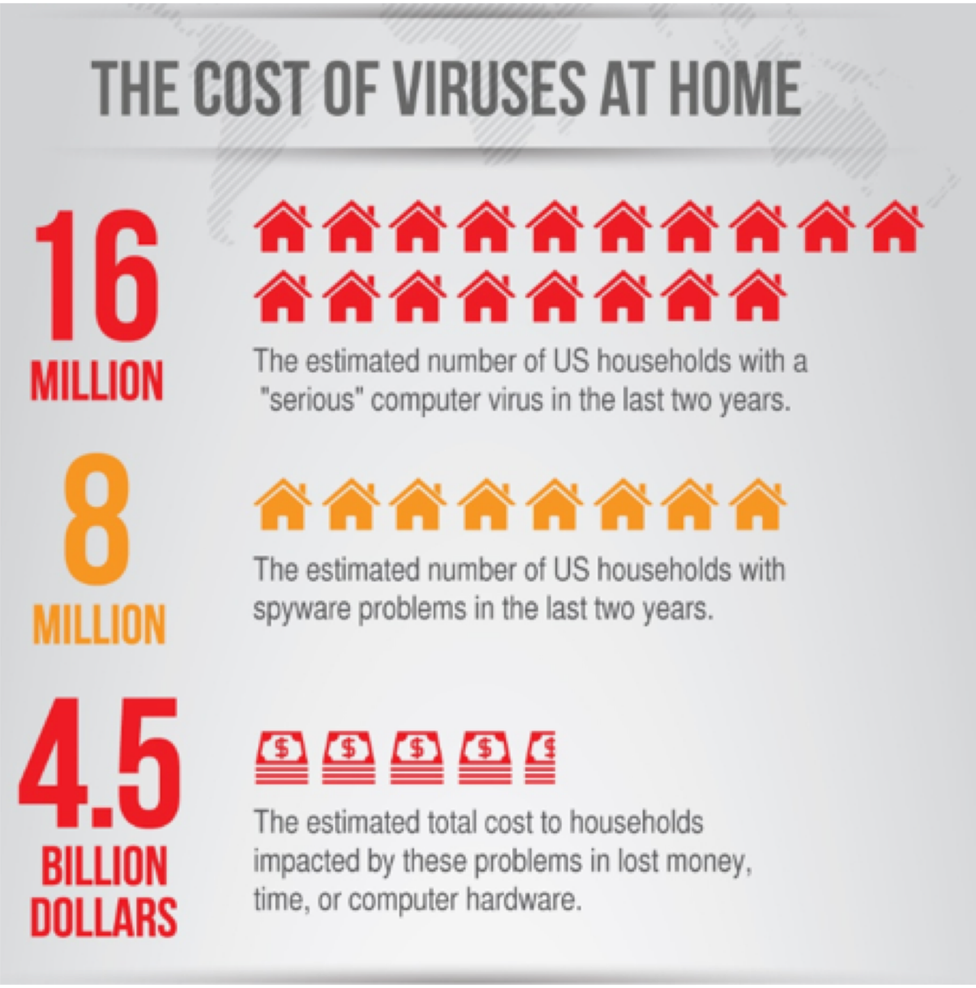
1ST MyDOOM WORM – 2004

- The world's fastest spreading computer vulnerability
- The goal of the worm was to perform DDoS attacks on sco.com
- Slowed Internet access globally by approximately 10%

Estimated damages:
38 BILLION DOLLARS

OSHER LIFELONG LEARNING INSTITUTE

Cost of Computer Viruses

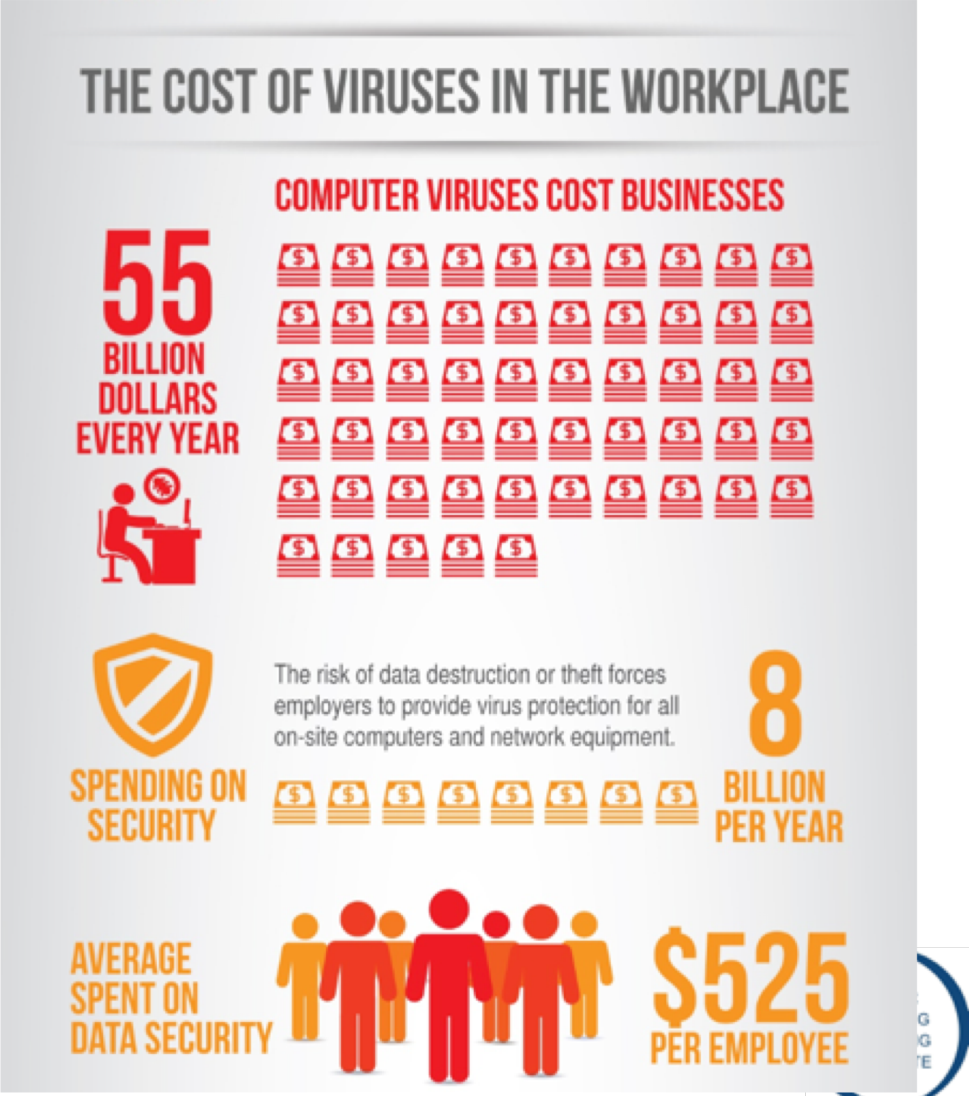


THE COST OF VIRUSES AT HOME

16 MILLION
The estimated number of US households with a "serious" computer virus in the last two years.

8 MILLION
The estimated number of US households with spyware problems in the last two years.

4.5 BILLION DOLLARS
The estimated total cost to households impacted by these problems in lost money, time, or computer hardware.



THE COST OF VIRUSES IN THE WORKPLACE

COMPUTER VIRUSES COST BUSINESSES
55 BILLION DOLLARS EVERY YEAR

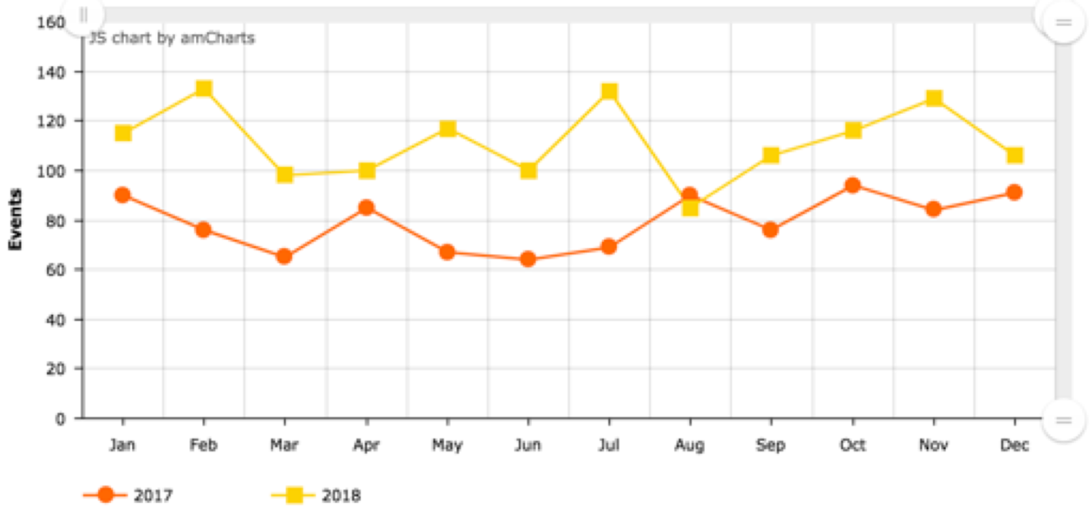
SPENDING ON SECURITY
The risk of data destruction or theft forces employers to provide virus protection for all on-site computers and network equipment.
8 BILLION PER YEAR

AVERAGE SPENT ON DATA SECURITY
$525 PER EMPLOYEE

Economic Cost

According to National Institute of Standards and Technology

- Economic costs that malicious cyber activity imposes on the U.S. economy [1] according to 2016 NIST report:
  - It is estimated that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016.
  - That's between 0.3 and 0.6 percent of the value of all the country's goods and services.
  - Cyberattacks against critical infrastructure sectors could be highly damaging to the U.S. economy.



[3] https://www.hackmageddon.com/2018-master-table/

[1] The Cost of Malicious Cyber Activity to the U.S. Economy: https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

[2] https://www.blue-pencil.ca/top-12-cyber-crime-facts-and-statistics/

OSHER LIFELONG LEARNING INSTITUTE

Government Sponsored Malwares…

“The Invisible Ware”

- In America, Iran’s cyberattacks have largely targeted the private sector.
  - **December 2009 – Twitter homepage hacked by** ‘Iranian Cyber Army’ defaced Twitter’s homepage
  - **August 2013 – Security Breach at Bowman Dam, New York:** Iranian hackers remotely took control of the command and control network of the Bowman Dam just outside New York.
  - **Sep. 2014,-** hacked into **Sands Hotel and Casino’s systems**, stealing and destroying data and ultimately costing the casino at least $40 million.
  - **Between 2011 and 2013,** seven Iranians allegedly working on the Iranian government’s behalf were accused of launching DoS attacks on **46 businesses, mostly financial institutions**,
- **August 2017 – Shamoon Virus attack on Saudi Aramco Oil Company:** The 2017 attack on the world’s largest oil company marked a shift in Iran’s cyberwarfare operations. Using Shamoon malware, the hackers were able to wipe **over 30,000 computers** and cost the company millions in damages.
  - Saudi Aramco was forced to go **offline for months** until it could rebuild its IT infrastructure, ultimately costing one of the most valuable companies in the world hundreds of millions of dollars.

https://www.metacompliance.com/blog/irans-cyber-attack-timeline-2009-2020/

Government Sponsored Malwares…

“The Invisible Ware”

- Organizations, companies, and governments in multiple countries have alleged incidents of hacking or espionage committed by China:
- **Australia:** In May 2013, ABC News claimed that China stole **blueprints to the headquarters** of the Australian Security Intelligence Organisation.
- **Canada:** Officials in the Canadian government claimed that Chinese hackers stole documents
- **USA**:
  - In February 2020, a US federal grand jury charged four members of China’s People's Liberation Army with the **2017 Equifax hack** - "one of the largest thefts of personally identifiable information by state-sponsored hackers ever recorded", **involving "145 million Americans”**
  - In 2019, a study showed continued attacks on the **US Navy** and its industrial partners.
  - In 2015, the **U.S Office of Personnel Management (OPM)** announced that it had been the target of a data breach targeting the records of as many as 21.5 million people.

https://en.wikipedia.org/wiki/Chinese_cyberwarfare

Government Sponsored Malwares…

“The Invisible Ware”

- Israel is leading the global cyberwarfare race
  - DF's 8200 unit is spearheading cyber efforts.
- Israel has become a powerhouse in cyberwarfare and security information
- It is said that the real Cyber threat for Israel is Iran

OSHER LIFELONG LEARNING INSTITUTE

Government Sponsored Malwares…
"The Invisible Ware"

- The United States Department of Defense recognizes the use of computers and the Internet to conduct warfare in cyberspace as a threat to national security, but also as a platform for attack.
- In June 2010, Iran was the victim of a cyber attack when its nuclear facility in Natanz was infiltrated by the cyber-worm 'Stuxnet',
  - said to be the most advanced piece of malware ever discovered and significantly increases the profile of cyberwarfare.
  - It destroyed perhaps over 1,000 nuclear centrifuges and, according to a Business Insider article, "
- In 2013, Edward Snowden, a former systems administrator for the CIA revealed:
  - The United States government had hacked into Chinese mobile phone companies to collect text messages and
  - U.S. spied on Tsinghuka University, one of China's biggest research institutions, as well as home to one of China's six major backbone networks, the China Education and Research Network (CERNET), from where internet data from millions of Chinese citizens could be mined.

https://en.wikipedia.org/wiki/Cyberwarfare_in_the_United_States

OSHER LIFELONG LEARNING INSTITUTE

Government Sponsored Malwares…

"The Invisible Ware"

- NSA infiltrated the servers in the headquarters of Huawei, China's largest telecommunications company and the largest telecommunications equipment maker in the world.
- In June 2019, Russia conceded that it is "possible" its electrical grid is under cyber-attack by the United States. The *New York Times* reported that American hackers from the United States Cyber Command planted malware potentially capable of disrupting the Russian electrical grid.

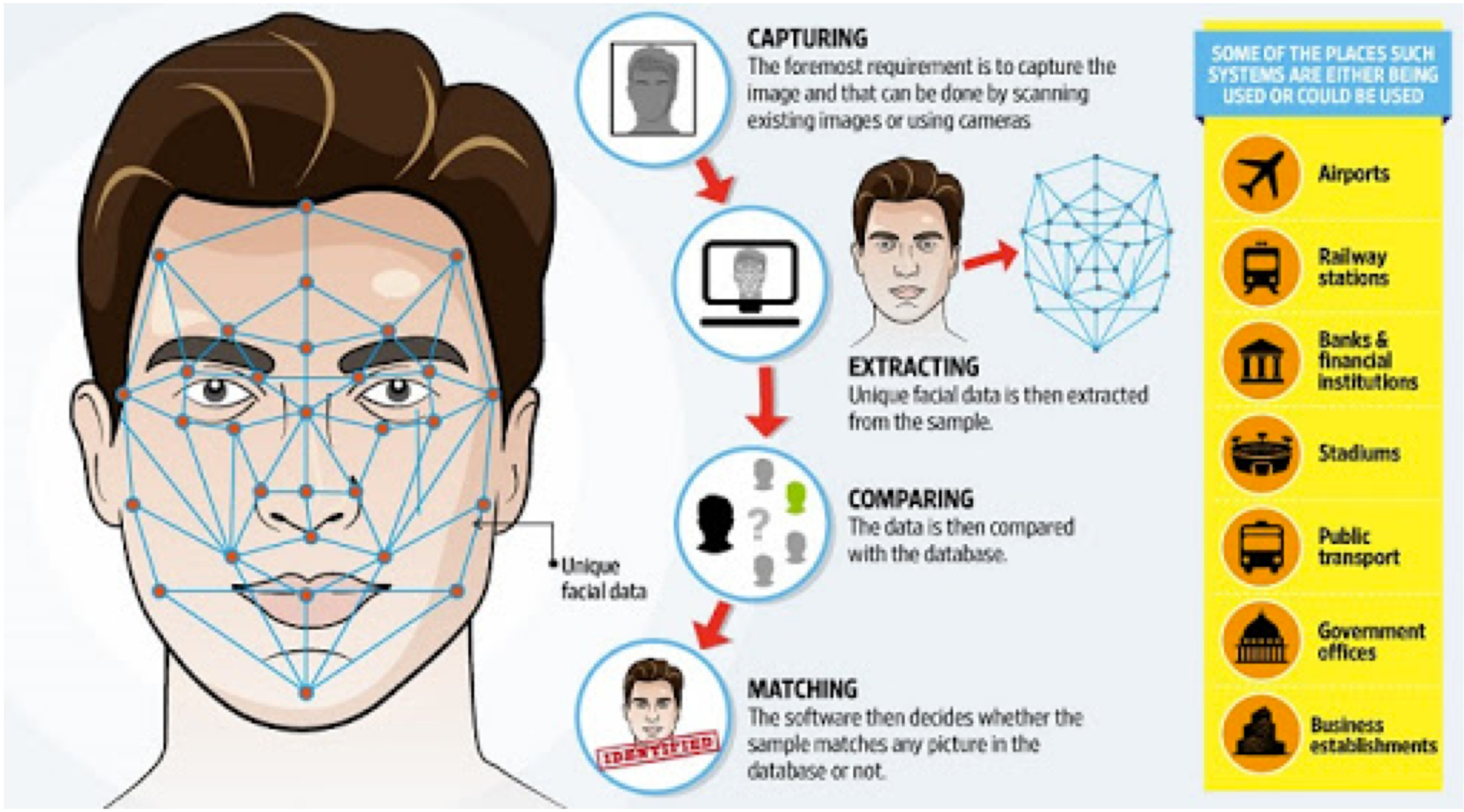
https://en.wikipedia.org/wiki/Cyberwarfare_in_the_United_States

OSHER LIFELONG LEARNING INSTITUTE

video

Facial Recognition Technology

- A facial recognition system is a technology capable of identifying or verifying a person from a digital image or a video frame from a video source



CAPTURING

The foremost requirement is to capture the image and that can be done by scanning existing images or using cameras

EXTRACTING

Unique facial data is then extracted from the sample.

COMPARING

The data is then compared with the database.

MATCHING

The software then decides whether the sample matches any picture in the database or not.

SOME OF THE PLACES SUCH SYSTEMS ARE EITHER BEING USED OR COULD BE USED

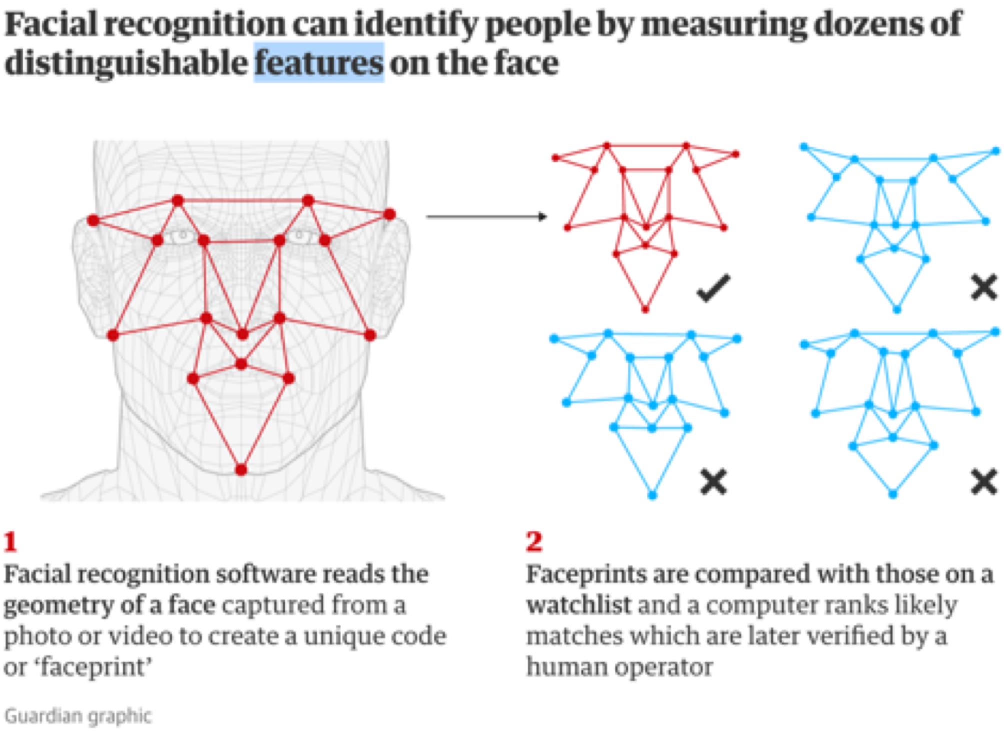
OSHER LIFELONG LEARNING INSTITUTE

Facial Recognition Technology

- The algorithms came from a range of major tech companies and surveillance contractors

- The systems are developed by companies inside or outside the U.S.:

- Intel,
- Microsoft,
- IBM,
- Face++
- Panasonic,
- SenseTime,
- Vigilant Solutions,
- Amazon,
- And more….



Facial recognition can identify people by measuring dozens of distinguishable features on the face

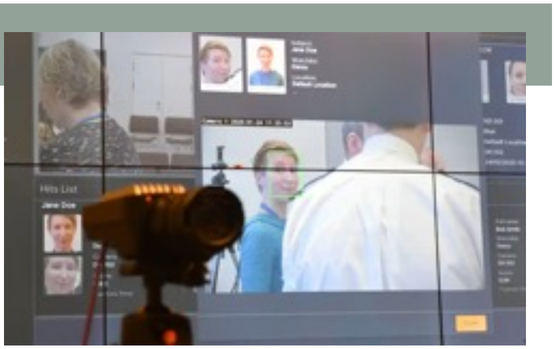
1
Facial recognition software reads the geometry of a face captured from a photo or video to create a unique code or 'faceprint'

2
Faceprints are compared with those on a watchlist and a computer ranks likely matches which are later verified by a human operator

Guardian graphic

OSHER LIFELONG LEARNING INSTITUTE

A City Covered by Cameras

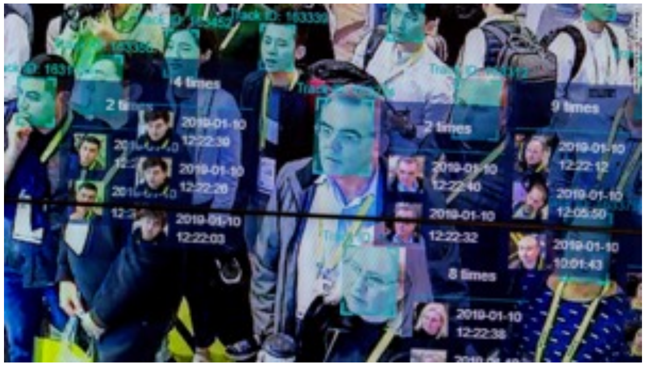


- In 2020 London’s Metropolitan Police announced it is ready to implementing facial recognition systems
- The biometric system is being provided to the Met by Japanese IT and electronics giant, NEC.
- London has seen a rise in violent crime in recent years, with murder rates hitting a 10-year peak last year.
- The number of security cameras in London is set to reach 627,000 this year, and could top 1 million cameras in 2025, according to a new estimate.
- With an estimated one CCTV camera for every 14 people currently in London, the total number in the city is approximately 627,707, according to CCTV.co.uk.

OSHER LIFELONG LEARNING INSTITUTE

Facial Recognition

- Amazon’s most audacious attempt to shake up the retail world, the cashless, cashier-less Go store.
  - Mainly the system is made up of dozens and dozens of camera units mounted to the ceiling, covering and recovering every square inch of the store
- More than 200 airports in China use facial recognition for passengers to check-in
  - Watch video: https://www.youtube.com/watch?v=IH2gMNrUuEY



Federal Governments and FR Systems

- Washington Post: ICE, FBI use state driver's license photos for facial-recognition scans
  - The FBI alone has logged more than 390,000 facial-recognition searches of state driver’s license records and other federal and local databases since 2011,
- Facebook notes that they only discloses records after a “formal and valid legal process.”

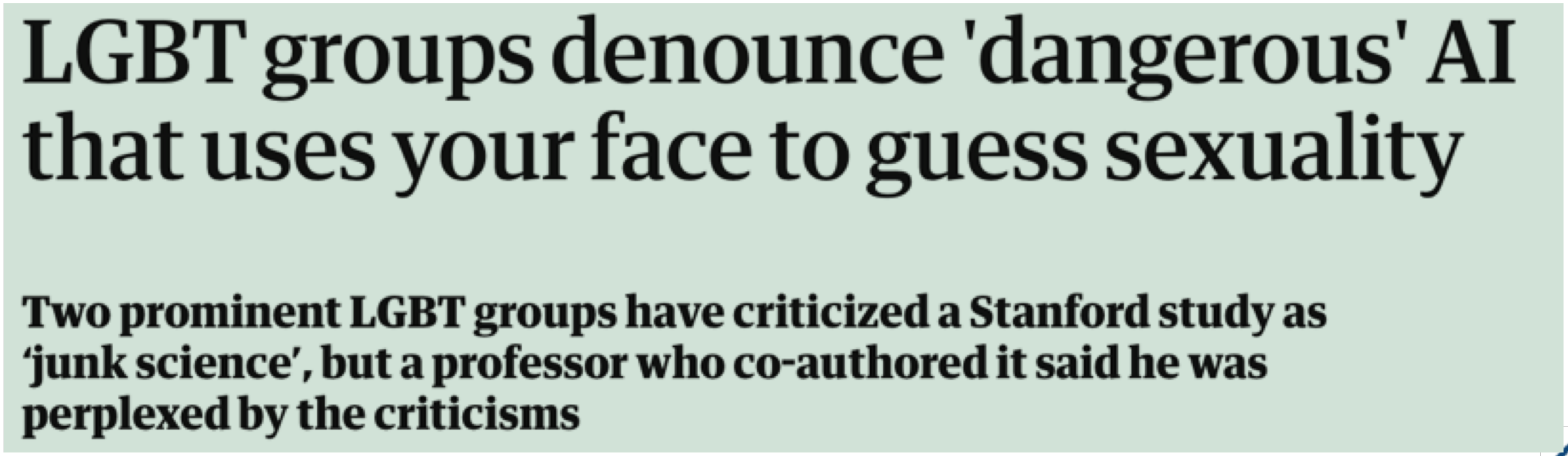
https://www.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html

Issues with Facial Recognition Systems According to National Institute of Standards and Technology (NIST),

- The system is widely used by **law enforcement across the United States**.
- Facial-recognition systems **misidentified people of color** more often than white people, a landmark federal study has released
- Asian and African American people were up to **100 times more likely to be misidentified** than white men,
- **Native Americans had the highest false-positive rate** of all ethnicities, according to the study, which found that systems varied widely in their accuracy.
- Algorithms developed in the United States also showed high error rates for “one-to-one” searches of Asians, African Americans, Native Americans and Pacific Islanders.
- NIST said Amazon did not submit its algorithm for testing.

Solution to Facial Recognition Systems

- **Debiasing:** Is the solution here to correct the bias in the AI system by ensuring that plenty of trans people are included in its training data?
- Some say the justice system is biased!
- There is a growing recognition among scholars and advocates that some biased AI systems should not be "fixed," but abandoned.



LGBT groups denounce 'dangerous' AI that uses your face to guess sexuality

Two prominent LGBT groups have criticized a Stanford study as 'junk science', but a professor who co-authored it said he was perplexed by the criticisms

https://www.vox.com/future-perfect/2019/4/19/18412674/ai-bias-facial-recognition-black-gay-transgender