MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

SOCIAL ZOMBIES
ROTTING PRIVACY, MOVING TARGET

Tom Eston, Veracode (@agent0x0)

Kevin Johnson, Secure Ideas (@secureideas)

ABOUT YOUR PRESENTERS

Tom Eston

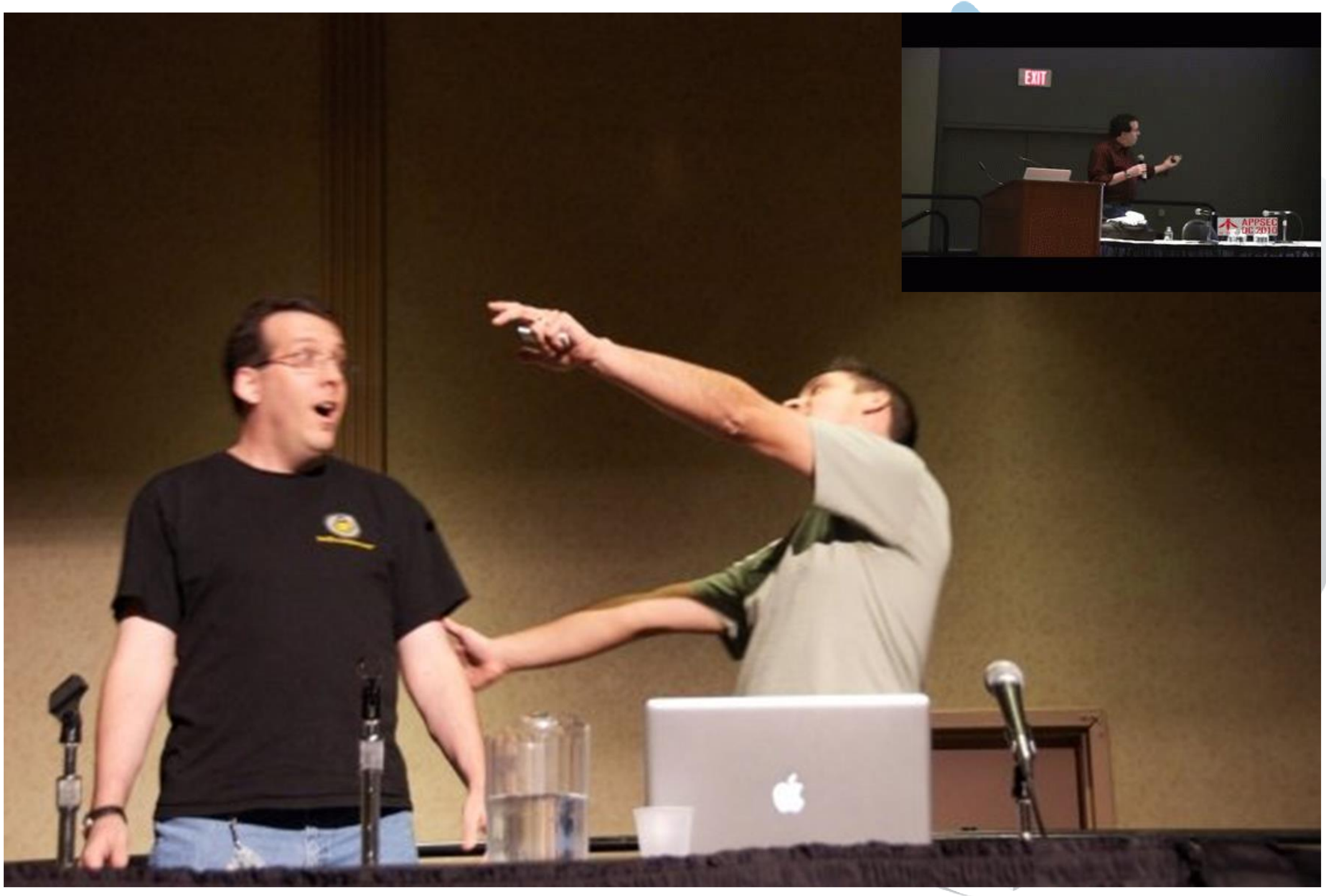
- Manager of Penetration Testing, Veracode
- Security/Privacy Researcher
- Co-host of the Shared Security Podcast

Kevin Johnson

- Professionally Evil
- Small Fan of Star Wars
- Secure Ideas CEO

AGENDA

- A historical reference (2009-2013)
- Where are we Today?
  - The Internet of Things (IoT)
  - Government Surveillance and Attacks
  - Privacy
- The Future
- Conclusions


EXIT
APPSEC
DC 2010

A HISTORICAL REFERENCE OF ZOMBIES (TALKS)

2009 – DEF CON 17

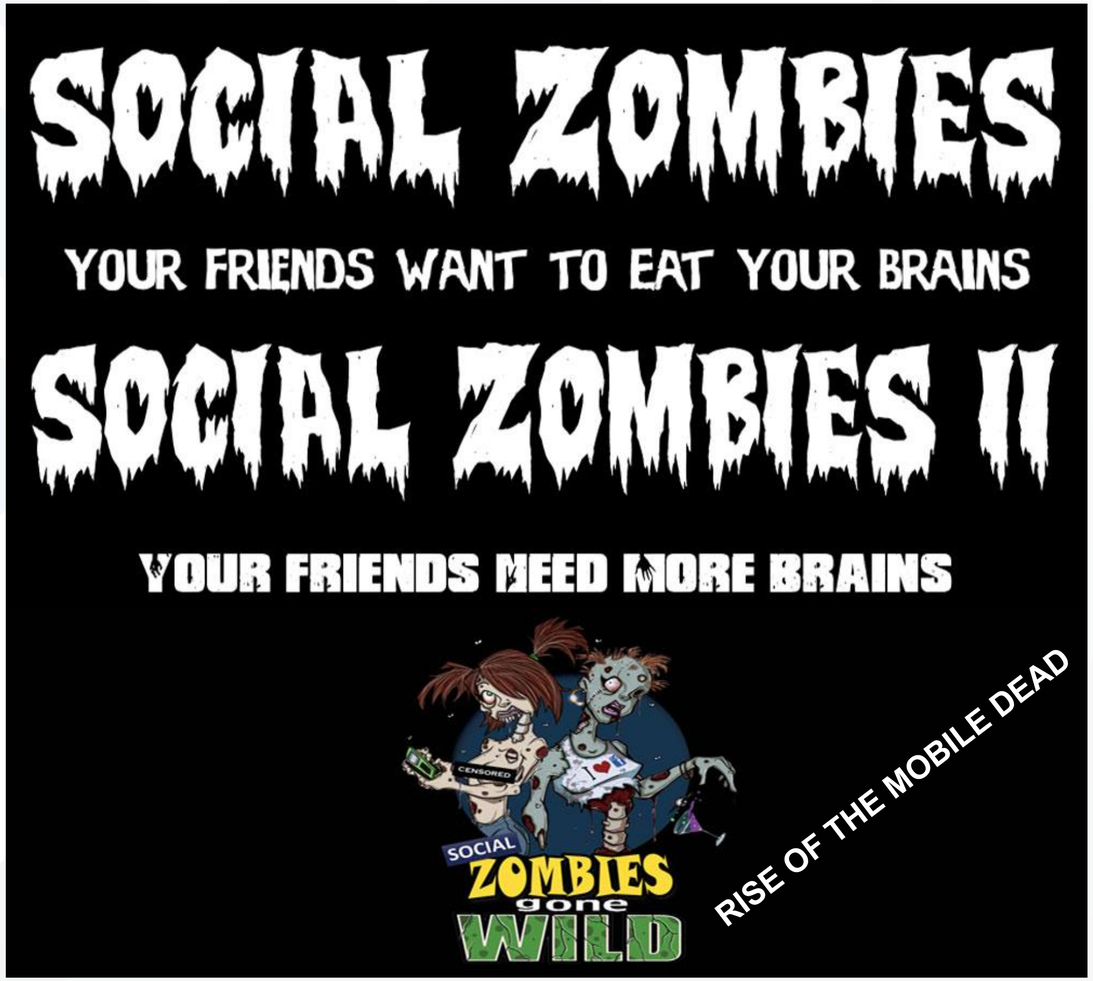
- Your friends really wanted to eat your brains
- You posted everything on social media
- Facebook developers thought we were crazy (Kevin, to be specific)

2010 – ShmooCon

- Your friends were bots (still are?)
- We showed how socnets could be used to send malware

2011-2013 – Notacon 8 / OWASP AppSec / SANS

- Abuse of location based services (geolocation)
- Mobile apps (it was 2009/1999 all over again)
- Lots of new tech (Facial Recognition/NFC)
- Little or no government privacy regulations (at least in the United States)



TODAY?

It’s worse than we’ve ever imagined!

(Laughing all the way to the bank…)

STATE OF SOCIAL MEDIA

We’re consumed with social media
How many times a day do you check Facebook?

Recent court cases in Europe have ruled that it’s illegal for Facebook to track non-Facebook users (as in everyone!)

“Facebook collects information about us all when we surf the Internet”

“…pervasive background surveillance of internet activity for digital ad targeting purposes which is enabled by a vast network of embedded and at times entirely invisible tracking technologies”

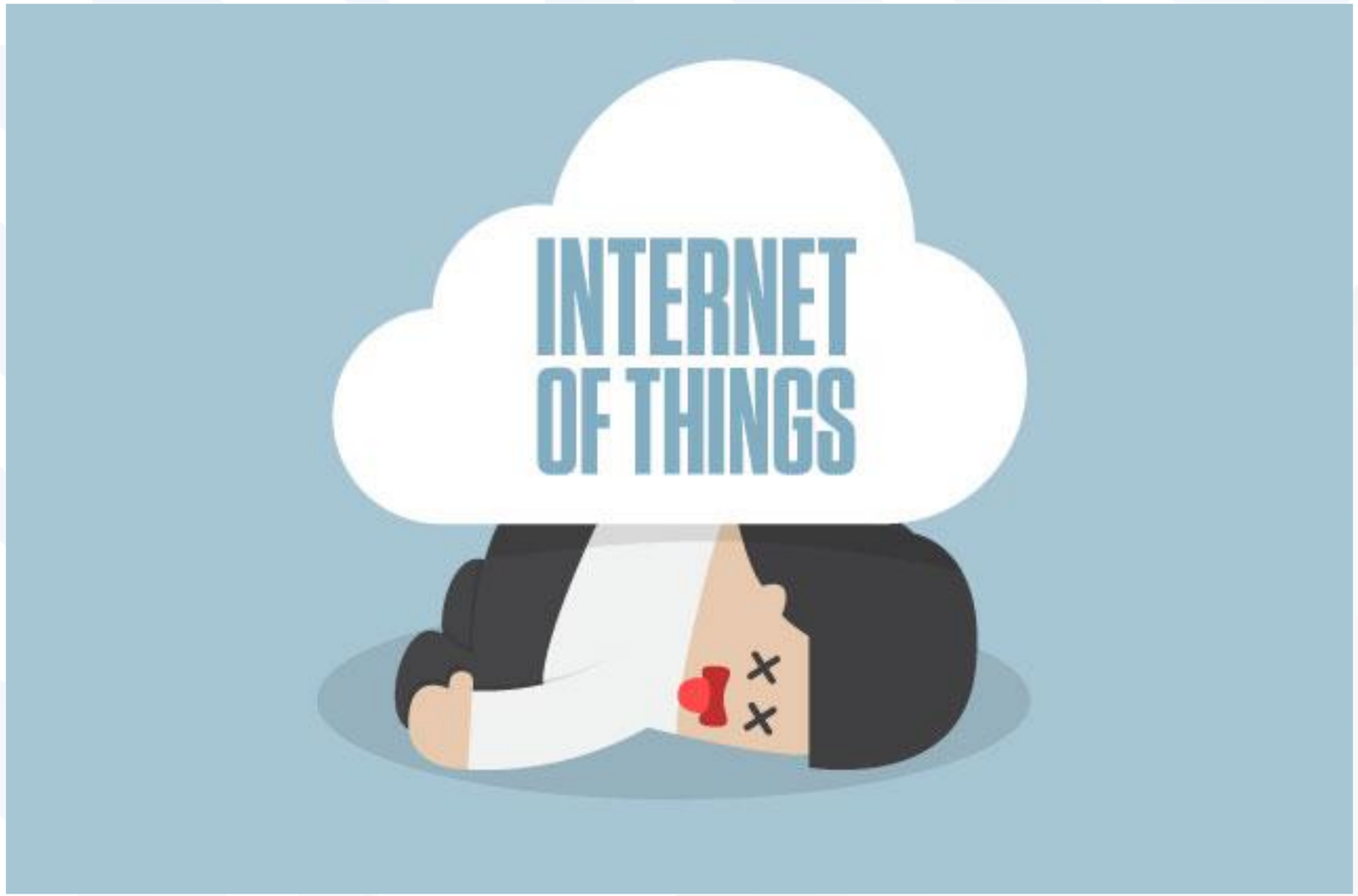
WHAT'S THE DEAL WITH THE INTERNET OF THINGS?

Does everything need to connect to the Internet?
(why does Kevin's toaster have an IP address??)

- Anyone read about the journalist who replaced everything in her home with "smart" devices?
- Are our lives really that much better?
- Does it have to be? (What level of invasion is ok?)

Mass market adoption has led to thousands of insecure devices with little regard for privacy

THE HORROR OF THE INTERNET OF THINGS



Connected devices may be the end of us all!

WINK HUB

Wink Hub for smart homes

- Manage multiple devices

Connects to a cloud service

- Via HTTPS

Certificate was updated

- Broke cert-pinning
- Devices needed to be mailed back

AMAZON KEY

Amazon Key is useful for deliveries

- And guests

Application unlocks door

- And activates camera

Simple wireless attacks

- Blocking the lock command

What could possibly go wrong??

ST. JUDE MEDICAL DEVICES

Connected Medical devices

- Pacemakers and such

MedSec discovered a large number of flaws

- Unencrypted communications
- Authentication Issues
- Replay attacks

GOVERNMENT SURVEILLANCE

State sponsored

- ISPs under government or local law enforcement control

Local sponsored

- Surveillance cameras, local communication tracking systems (IMSI catchers)

Targeted

- Can be state sponsored, local or other organization
- Threats are focused on an individual or group
- Open Source Intelligence (OSINT) often used in attacks

GOVERNMENT SPONSORED ATTACKS

The last several years have seen a dramatic increase in “sponsored” attacks across the world…

We all know about the NSA and WikiLeaks/Snowden disclosures

But what about what’s going on in the rest of the world?

SMS text messages received by Ahmed Mansoor (Reads: “New secrets about torture of Emiratis in state prisons”). Clicking the link would have installed malware via a 0-day exploit on his fully updated iPhone 6

DARK CARACAL

Recent malware espionage campaign

Traced back to the Lebanese government

Android and Windows affected

Installs trojanized versions of popular messaging apps like WhatsApp and Signal

Uses text, WhatsApp and Facebook Group posts to install malware on the device

WHAT'S COMMON ABOUT THESE ATTACKS?

Phishing and social engineering attack vectors

Mobile devices and apps are being targeted

Common communication methods like text and social media are used to distribute malware

Think only specific individuals would be targeted? Think again! Businesses and anyone else can be a target

NET NEUTRALITY

Net Neutrality is a hot button topic

- No matter your side

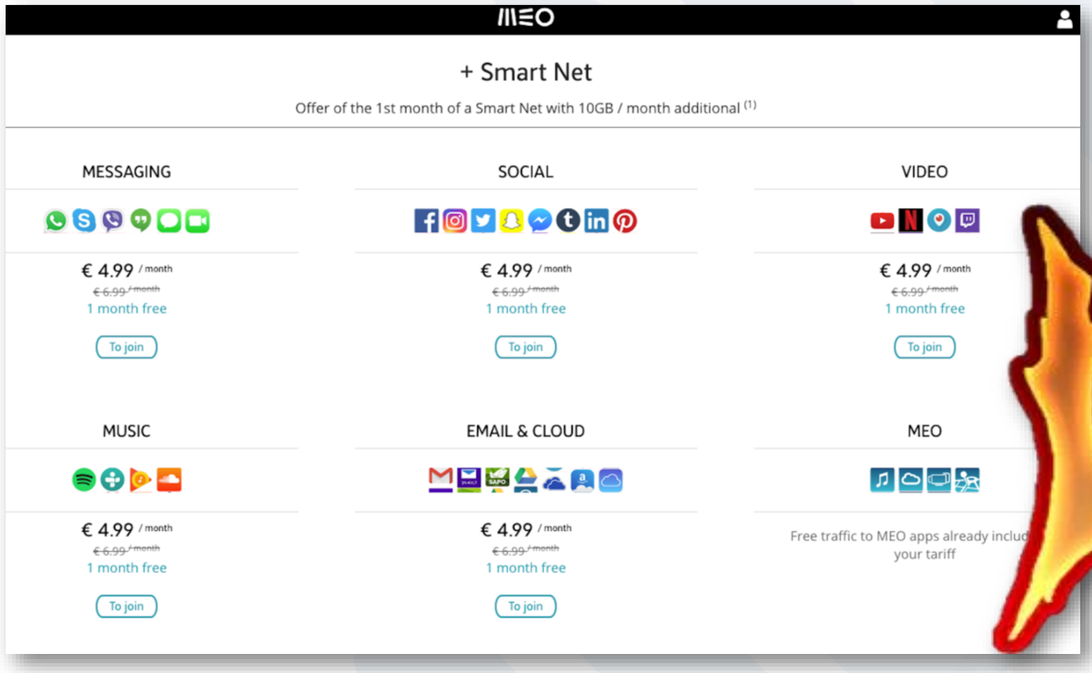
Example where privacy collides with wants

- Which becomes more important

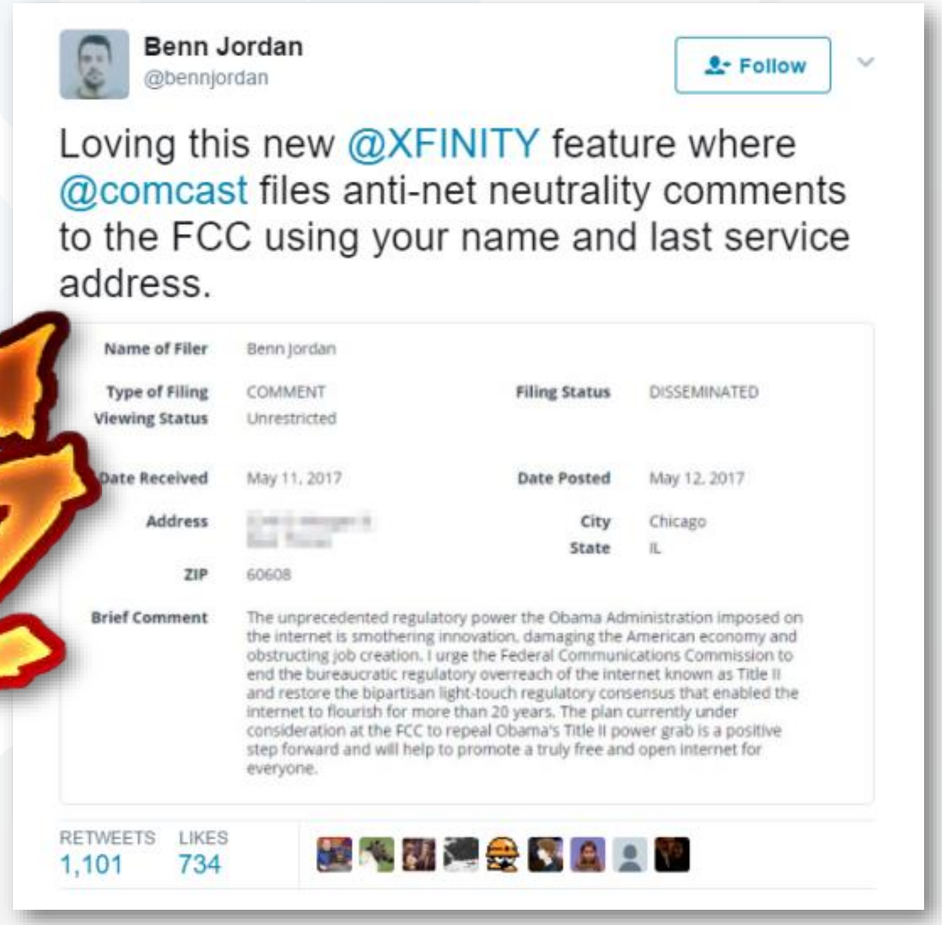
ELECTRONIC FRONTIER FOUNDATION

Federal Communications Commission

NET NEUTRALITY



VS.



PRIVACY

More products and services are taking a “all or nothing” approach to privacy

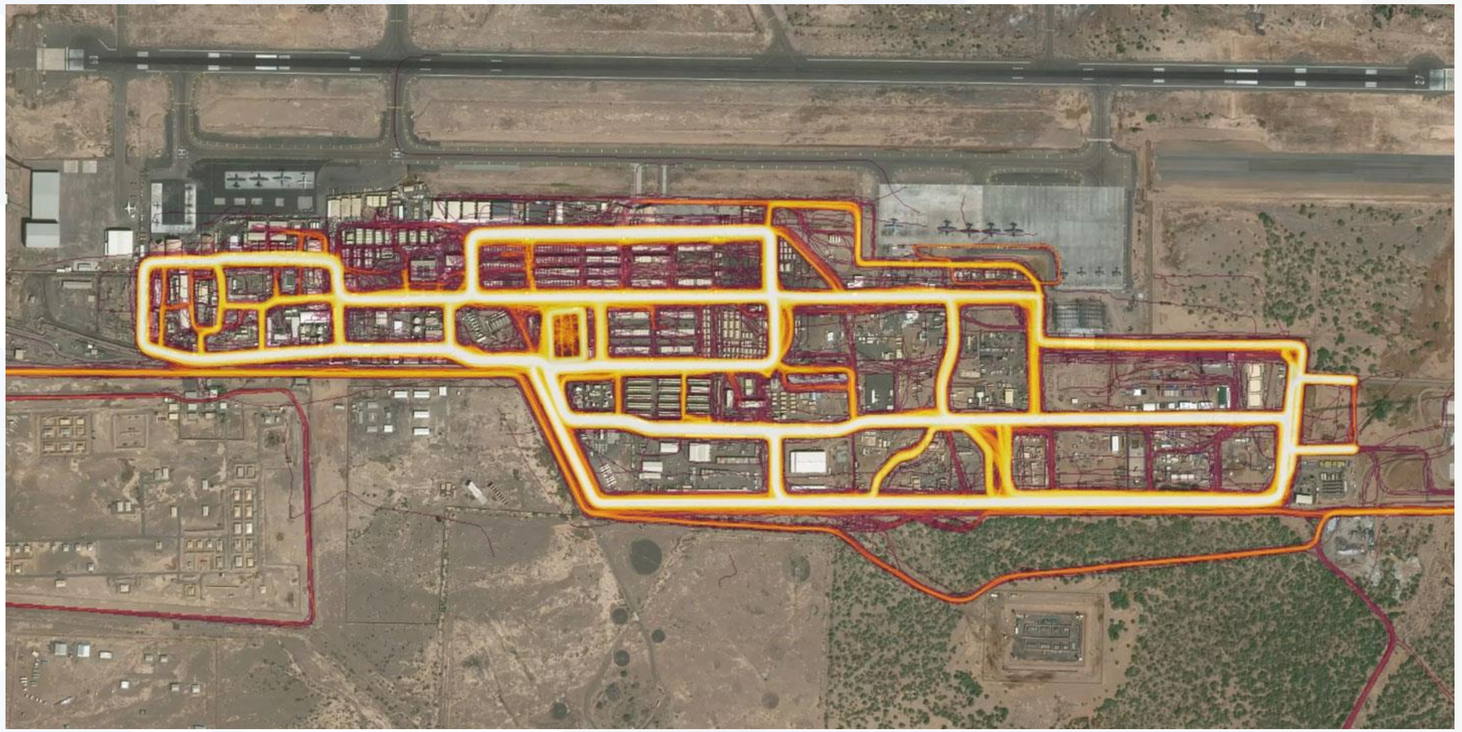
- Vizio was fined $1.5 in 2017 from the FTC for collecting users viewing habits without their knowledge
- Most new TVs you now have to “opt in” but that comes with a cost
- You want to stream Netflix?
  Accept our policy to collect your viewing habits.

  Don’t accept? Enjoy your “dumb TV”.

INADVERTENT PRIVACY DISCLOSURE

Anyone use Strava to track their runs?

Release of Strava's "global heatmap" showed secret locations of military bases and CIA outposts (oops!)



PRIVACY NOTICES

98% of people don’t read privacy notices for the services and technology that they use

- In one study* people unwillingly allowed data sharing with the NSA and employers, and agreed to provide a first-born child as payment for access (this was a fake social network used in the study)

The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465)

PRIVACY NOTICES

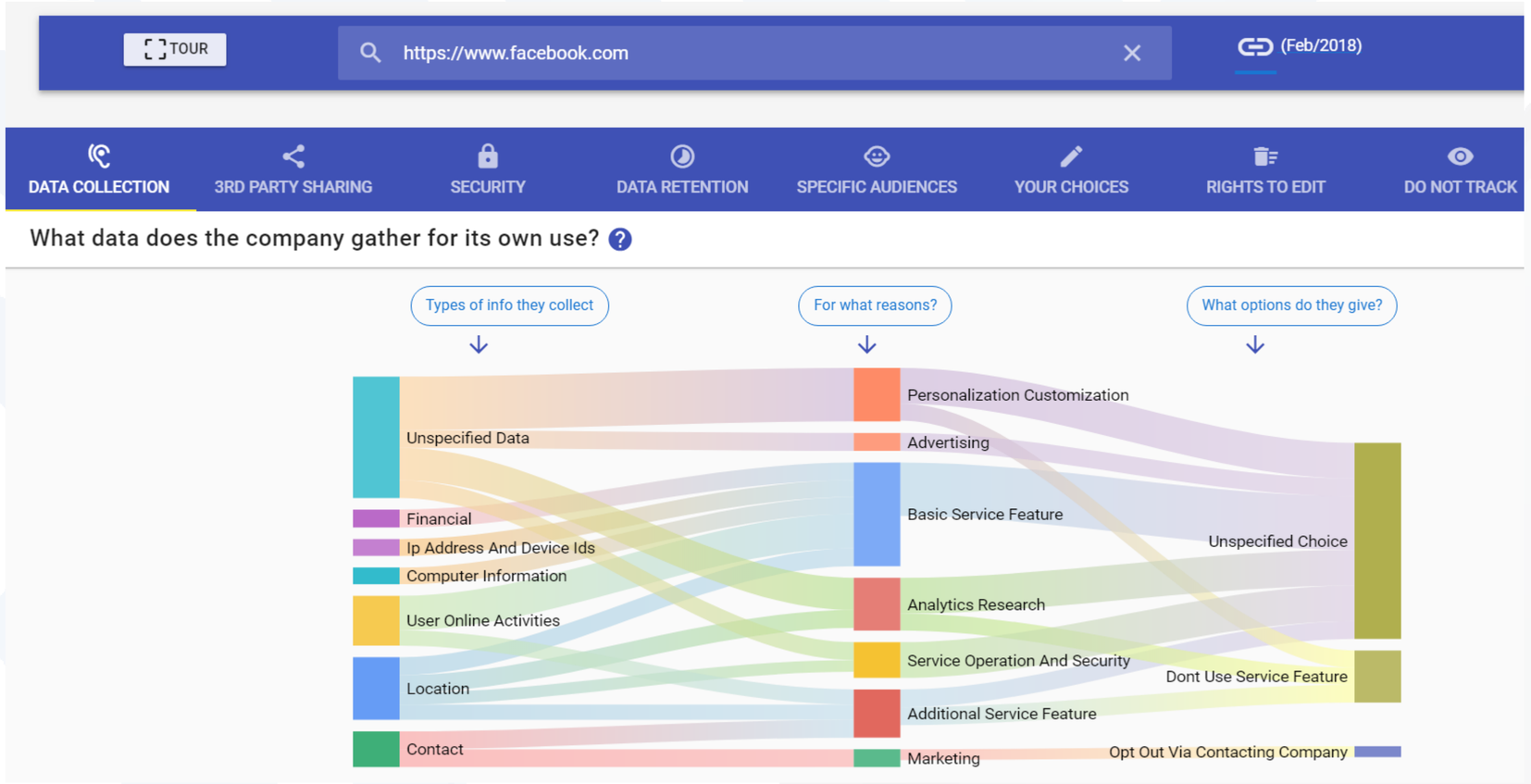
Can you blame us?

According to another study*…it would take the average person 250 working hours (30 full working days) to read all the privacy notices of the websites they visit in a year!

* The Cost of Reading Privacy Policies http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf

HOPE FOR PRIVACY NOTICES?

"AI and Machine Learning" is now able to analyze notices, visually*



* https://pribot.org/polisis

GDPR

GDPR stands for the General Data Protection Regulation

- Goes into effect May 25th and applies to organizations within the European Union but also to organizations outside of the EU that provide services to EU residents

- Will require individual consent before processing any personal data and requires said data to be erased within 72 hours when necessary

- Personal data includes: Name, location data, ID number, online IDs, specific identifiers of a person (i.e., physical)

GDPR – TIME TO FREAK OUT?

If organizations violate GDPR they can be fined **4 percent of annual global revenue, or 20 million Euros (whichever is higher).**

While a pain for organizations, overall GDPR will help.

But organizations should be doing good privacy already ☺

Everyone should have clear privacy policies for customer data, a data protection officer, a solid data breach plan and knowing where all this private data is, EASY RIGHT?

IS REALLY THAT BAD?

Yes! (but there is some hope…)

- There appears to be more movement towards people becoming more privacy aware due to high profile government surveillance and net neutrality

- Which have led to
  - Better privacy protection tools (and awareness of)
  - Better and easier ways of secure communication

PRIVACY TOOLS AT OUR DISPOSAL

Importance of end-to-end encryption

VPNs

Tor

Secure Communication Apps

Secure Email

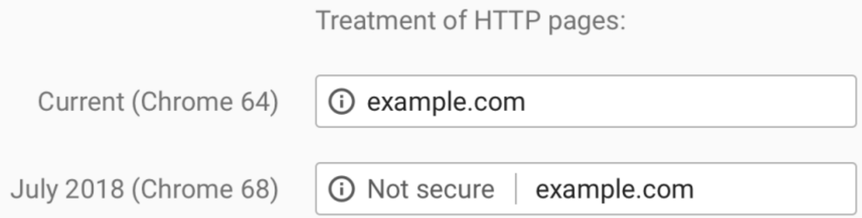
END-TO-END ENCRYPTION

Becoming more common and being pushed by major Internet companies

For example…

Google lowers the search rankings for non-HTTPS sites

Google Chrome will show non-HTTPS sites as “Not Secure”



VPN (VIRTUAL PRIVATE NETWORKS)

Pros

- Can be used to stay somewhat anonymous from your ISP (see cons below)
- Entire VPN session is encrypted
- All services on a system can utilize the VPN connection (i.e., email, chat and Internet)

Cons

- VPN providers can keep logs (even ones that say they don't could be convinced to keep logs)
- VPN providers can monitor your traffic
- VPN providers typically know who you are via your payment method

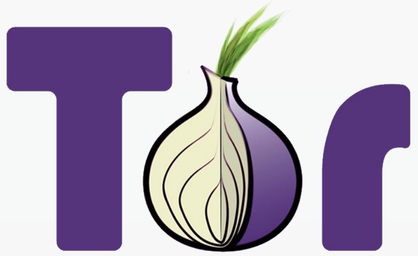
Research any potential VPN provider to see what their policy on logging is!

TOR (THE ONION ROUTER)

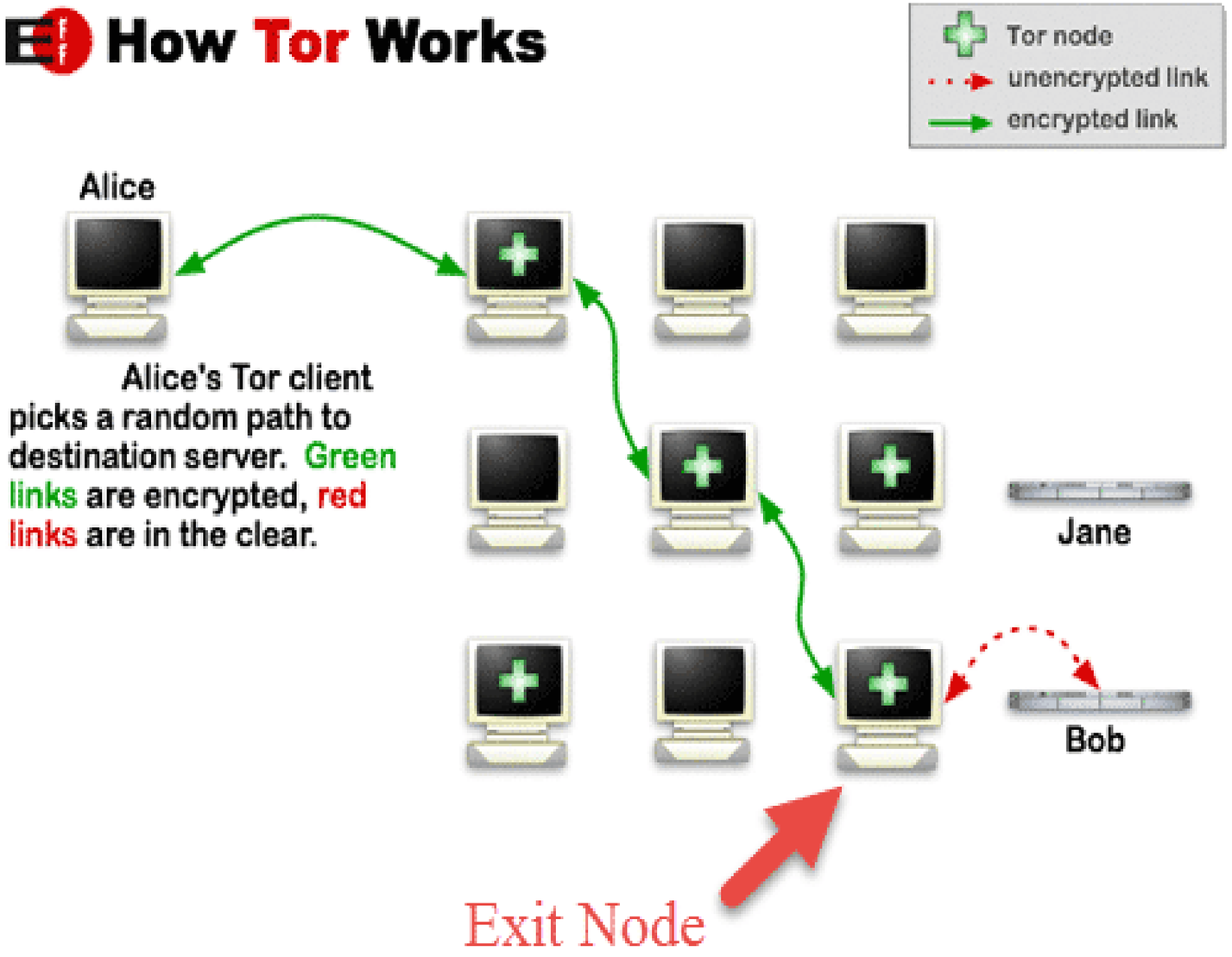
Tor is free software for enabling **anonymous** communication.

Tor uses a volunteer network of nodes (servers) which conceal a user's location **circumventing censorship** and making network surveillance and traffic analysis much more difficult.

Tor is typically used via a “Tor browser” that connects to nodes that route traffic randomly to other nodes...



HOW DOES TOR WORK?



TOR PROS AND CONS

Pros

- Easy to use on any operating system via the Tor browser package
- Free and open source software that's actively being developed and improved
- The only way to access .onion domains and hidden services (aka the Darknet)
- Ability to use **bridge servers** and **pluggable transports** to circumvent censorship if Tor is blocked

Cons

- Tor exit relays can eavesdrop on communications
- Man-in-the-middle attacks are possible, even with HTTPS
- Possible for people monitoring your Internet connection (ISP or global adversary) to know that you are using Tor
- Slow speed

SIGNAL

Signal is an **encrypted communications application** for Android, Apple iOS and desktops (Linux, Mac, Windows).

It uses the Internet to send text and group messages, which can include files, voice notes, images and videos, and make voice and video calls.

Signal uses uses **end-to-end encryption** and users can verify the identity of their contacts and the integrity of the data channel.

Signal is developed by Open Whisper Systems (Moxie Marlinspike) and is free and **open-source software**.

OTHER SECURE MESSAGING APPS

WhatsApp

- Uses Signal's end-to-end encryption protocol but the rest of the app is proprietary
- Many more features and users (over 1 billion) than Signal
- Some metadata is kept (i.e., location, device info, cookies)
- Whatsapp is owned by Facebook Inc. so metadata is shared for ads

OTHER SECURE MESSAGING APPS

Facebook Messenger

- You have to encrypt conversations individually by turning on the "Secret Conversations" option. App is proprietary including its end-to-end encryption.
- Very feature rich and integrates with existing Facebook contacts
- It’s a Facebook application so metadata and more is used for ad targeting

SECURE EMAIL COMMUNICATION

PGP (Pretty Good Privacy)

- PGP is used for signing, encrypting emails (and can also be used to encrypt files, disks and messages). Uses public and/or symmetric key cryptography
- GnuPG is the free and open source version that most people use today
- You can use normal email with PGP to send secure communications

Third-Party Secure Email Services

- Services like Protonmail provide secure third-party email (no logs, open source, end-to-end encryption)

WHAT ARE SOME SOLUTIONS?

IT STARTS WITH EDUCATION

Educate you and your business on how to identify:

- Social engineering attempts
- Phishing

Social engineering and phishing are the most common attack vectors

- Can come from email, text or even phone calls and voicemail

Familiarize yourself with privacy notices (yes, really)

CONCLUSIONS

Privacy is critical

- Understanding the gaps and weaknesses

Work with your developers and people

- Build and deploy securely

Know YOUR boundaries

- Before you are forced to figure it out

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Tom Eston, Veracode (@agent0x0)

Kevin Johnson, Secure Ideas (@secureideas)