CSE 484 / CSE M 584: Computer Security and Privacy

Emerging Tech + Wrap-Up

Autumn 2020

Franziska (Franzi) Roesner
franzi@cs.washington.edu

Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, Yoshi Kohno, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Admin

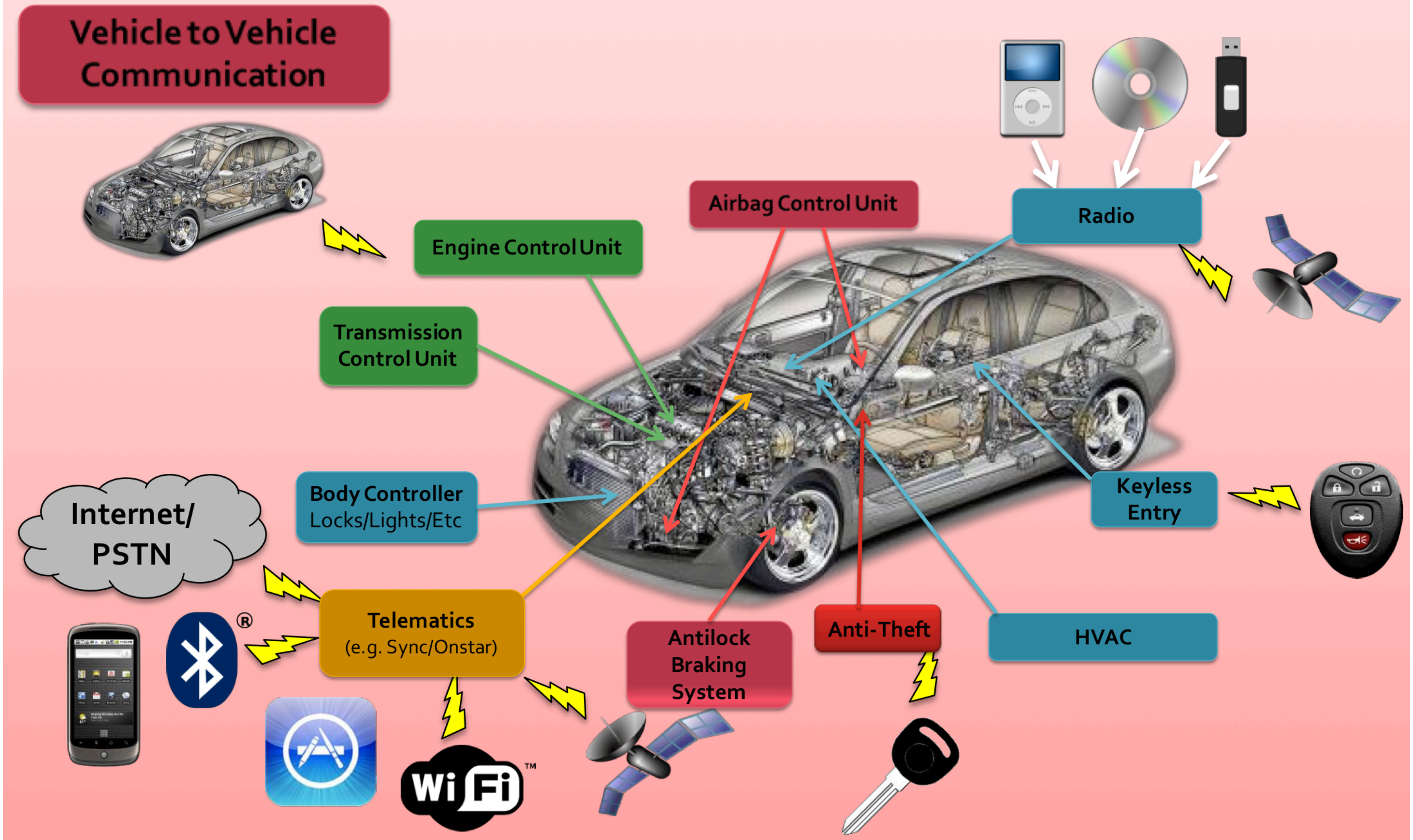
- **Lab 3** due today
  - OK to use late days
- Final **project due** Mon, Dec 14 @ 11:59pm
  - No late days
- Please let us know asap if your late days seem incorrect

SECURITY AND PRIVACY FOR EMERGING TECHNOLOGIES

(1) Connected Automobiles

- Already emerged by now, but a fun story ☺
- Automobiles were only just being connected to the internet when we (UW+UCSD) studied them (~2009)
  - Had not faced significant adversarial pressure
  - Won a “Test of Time” Award this year

www.autosec.org



Vehicle to Vehicle Communication

Engine Control Unit

Airbag Control Unit

Radio

Transmission Control Unit

Internet/ PSTN

Body Controller Locks/Lights/Etc

Keyless Entry

Telematics (e.g. Sync/Onstar)

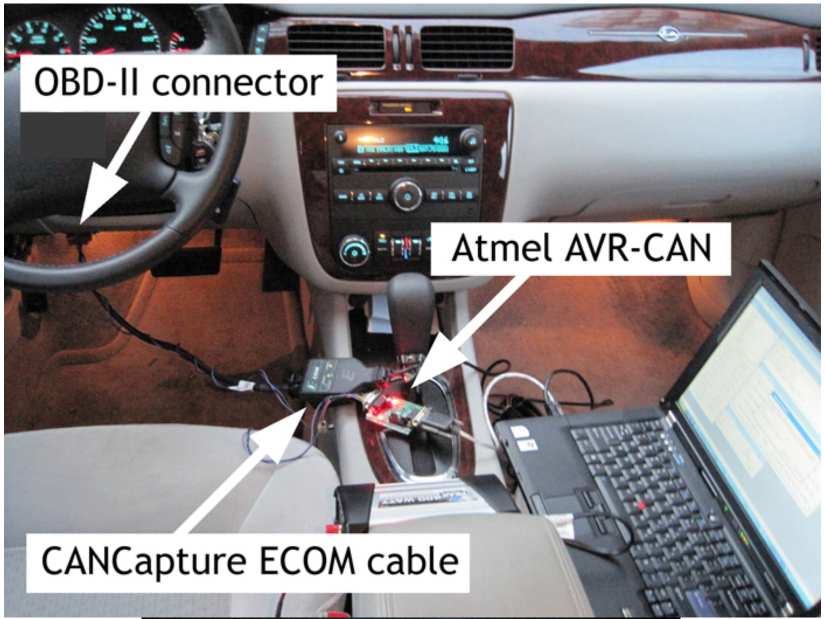
Antilock Braking System

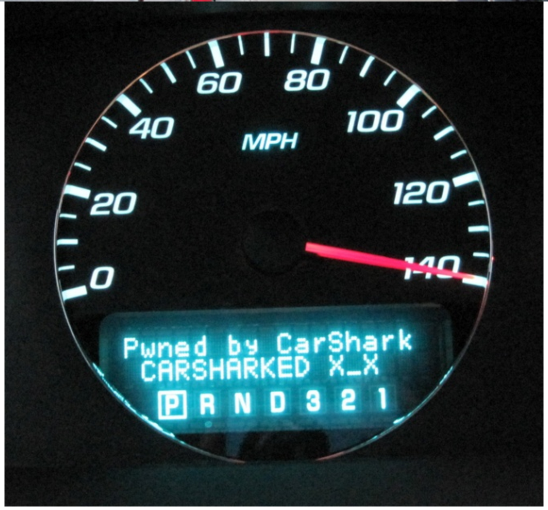
Anti-Theft

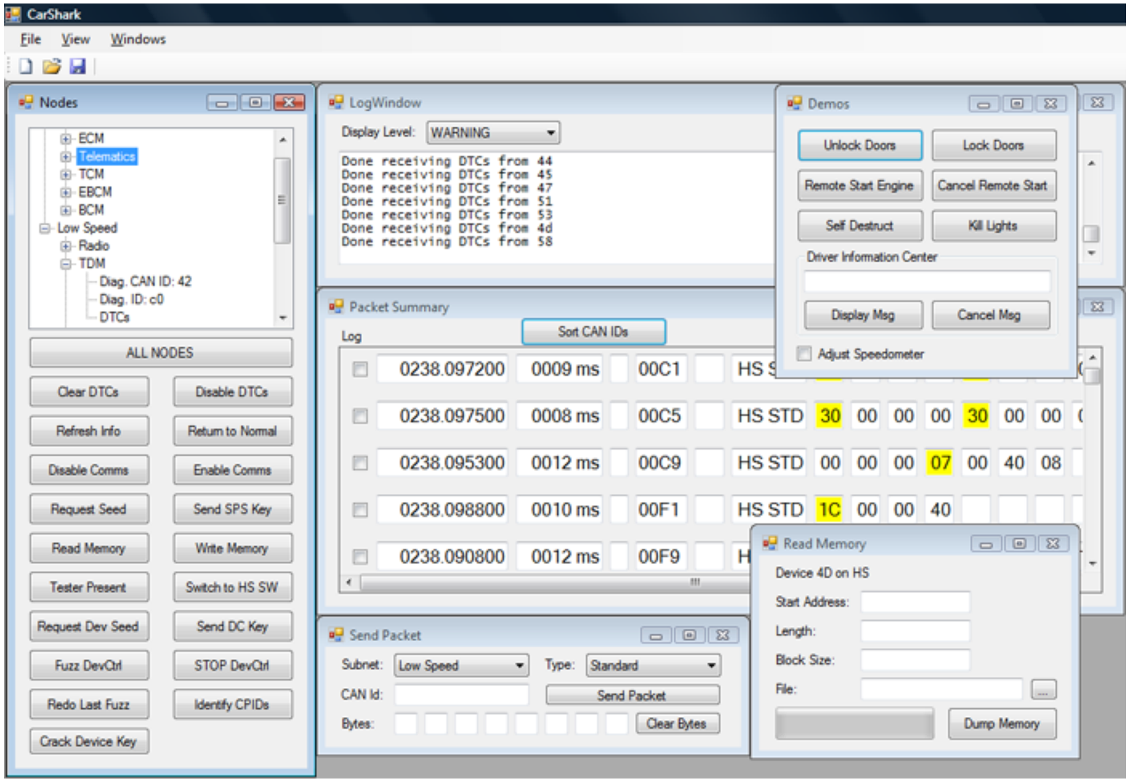
HVAC

Computers in a modern automobile

Experiments with a Real Car







Display Level: WARNING

```
Done receiving DTCs from 44
Done receiving DTCs from 45
Done receiving DTCs from 47
Done receiving DTCs from 51
Done receiving DTCs from 53
Done receiving DTCs from 4d
Done receiving DTCs from 58
```

```
□ 0238.097200  0009 ms  00C1  HS S
□ 0238.097500  0008 ms  00C5  HS STD  30  00  00  00  30  00  00
□ 0238.095300  0012 ms  00C9  HS STD  00  00  00  07  00  40  08
□ 0238.098800  0010 ms  00F1  HS STD  1C  00  00  40
□ 0238.090800  0012 ms  00F9  H
```

Subnet: Low Speed

Type: Standard

CAN Id:

Bytes:

Device 4D on HS

Start Address:

Length:

Block Size:

File:

Experiments with a Real Car

Example: Force Brakes On/Off

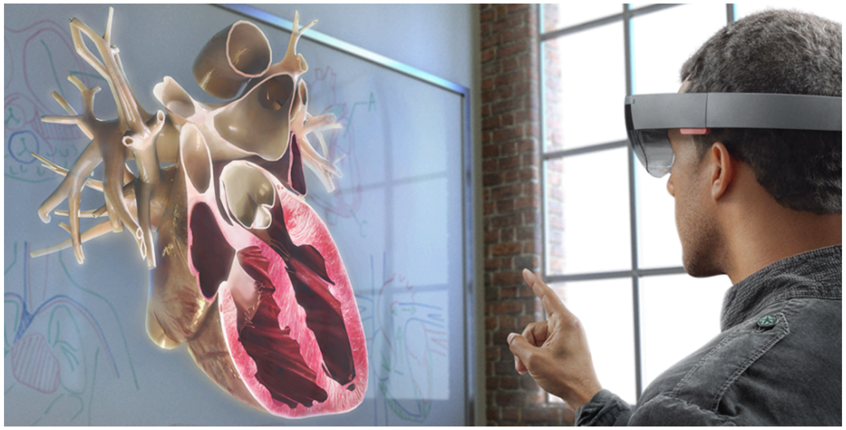
https://www.youtube.com/watch?v=H6oozuid1K4

https://www.youtube.com/watch?v=917VOx6tBKA

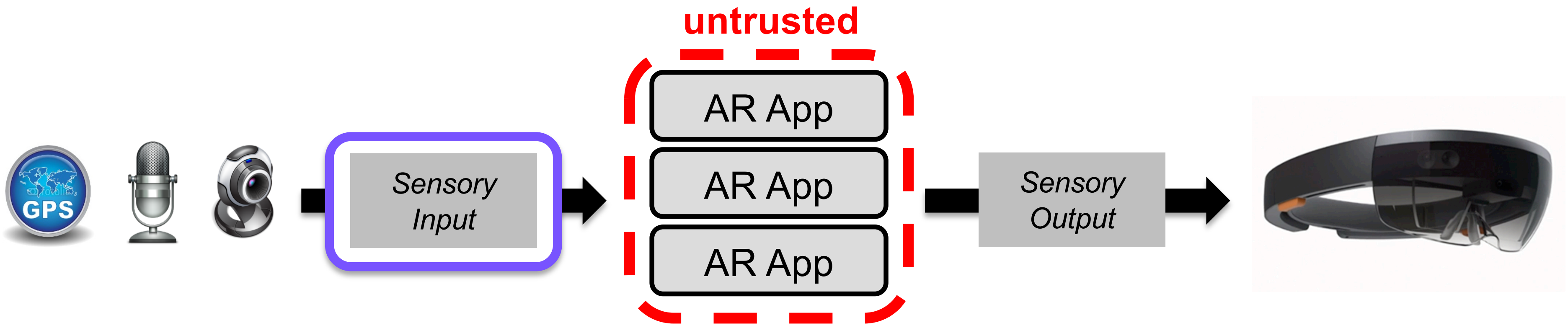
Impacts

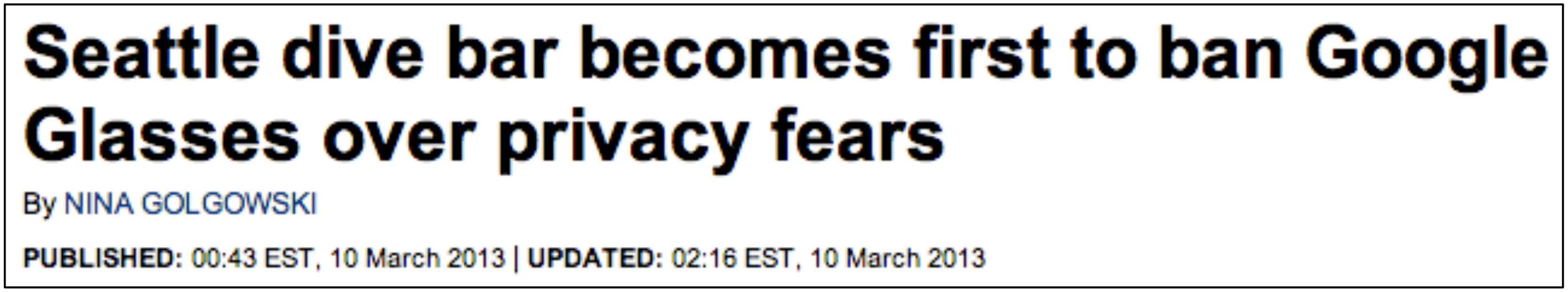
- Impact on automotive industry
  - Significant investment by automotive companies
  - Spurred vendor industry around automotive security
- Impact on standards, regulation, and legislation
  - SAE International (de facto standards body for the U.S. automotive industry) created committee and standards
  - Resources committed by NHTSA
  - U.S. bills on automotive cybersecurity
- Impact on research
  - New subfield of automotive security and significant DARPA and other funding efforts

(2) Security and Privacy for Augmented Reality



AR Input Privacy



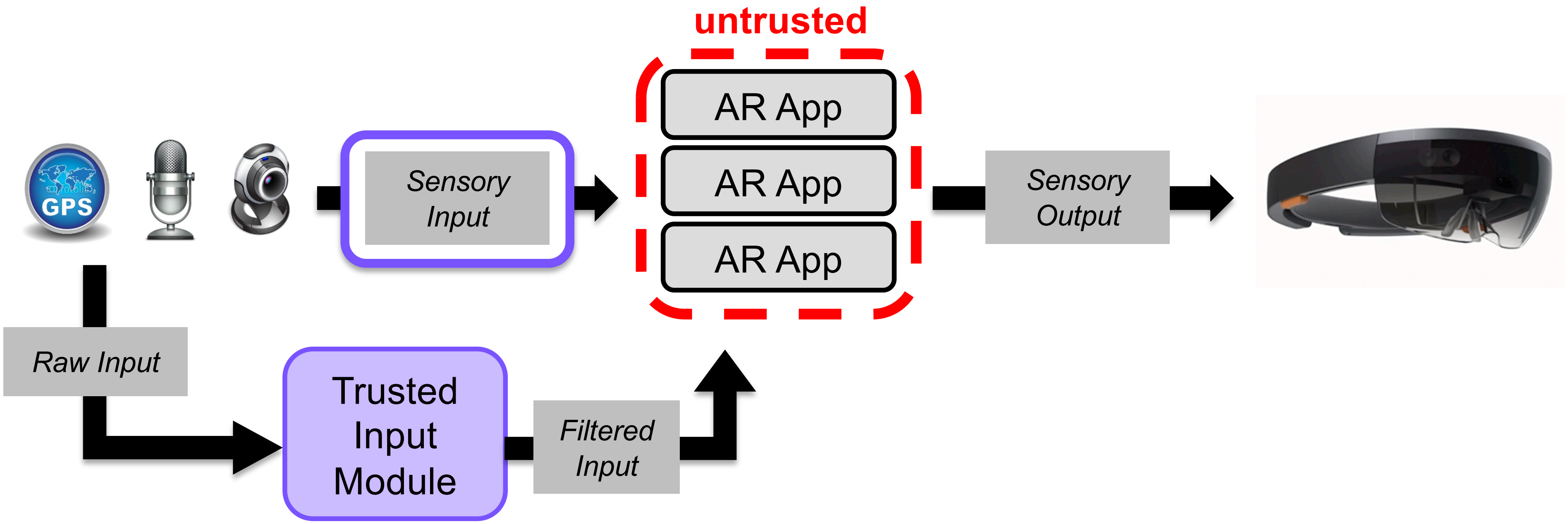


Seattle dive bar becomes first to ban Google Glasses over privacy fears

By NINA GOLGOWSKI

PUBLISHED: 00:43 EST, 10 March 2013 | **UPDATED:** 02:16 EST, 10 March 2013

AR Input Privacy



untrusted

AR App

AR App

AR App

Sensory Input

Sensory Output

Raw Input

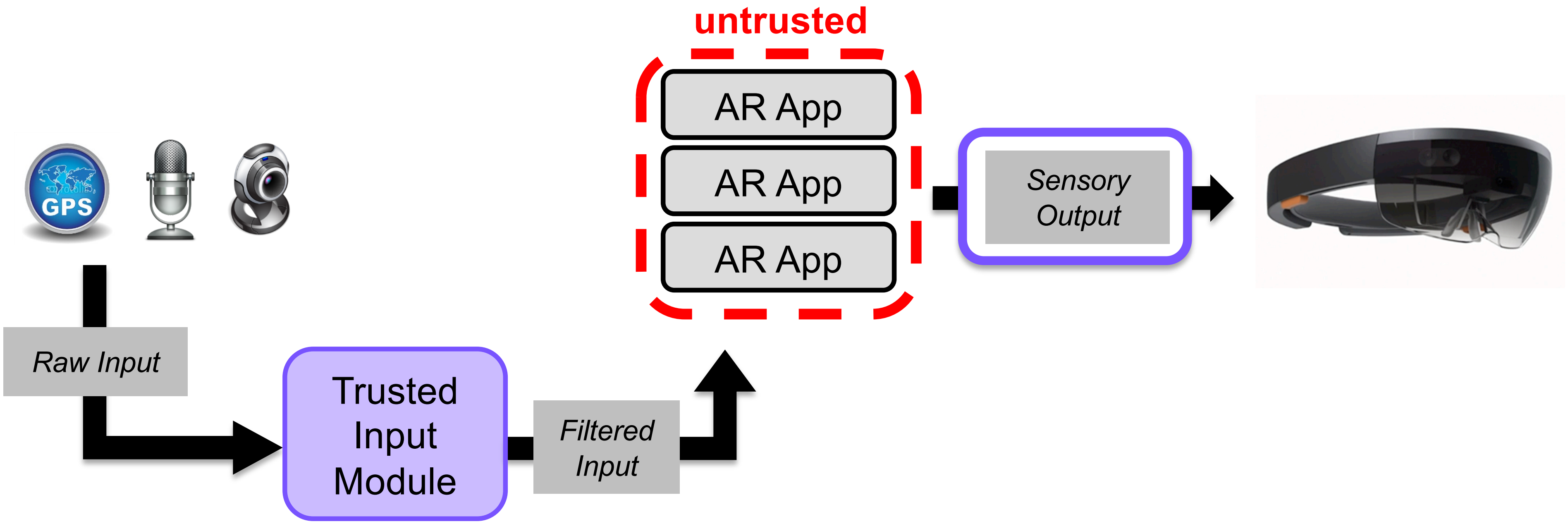
Trusted Input Module

Filtered Input

Input Privacy

- Jana et al., USENIX Security ’13
- **Roesner et al., CCS ’14**
- Templeman et al., NDSS ’14
- Raval et al., MobiSys ’16

AR Output Security



untrusted

AR App

AR App

AR App

Sensory Output

Raw Input

Trusted Input Module

Filtered Input

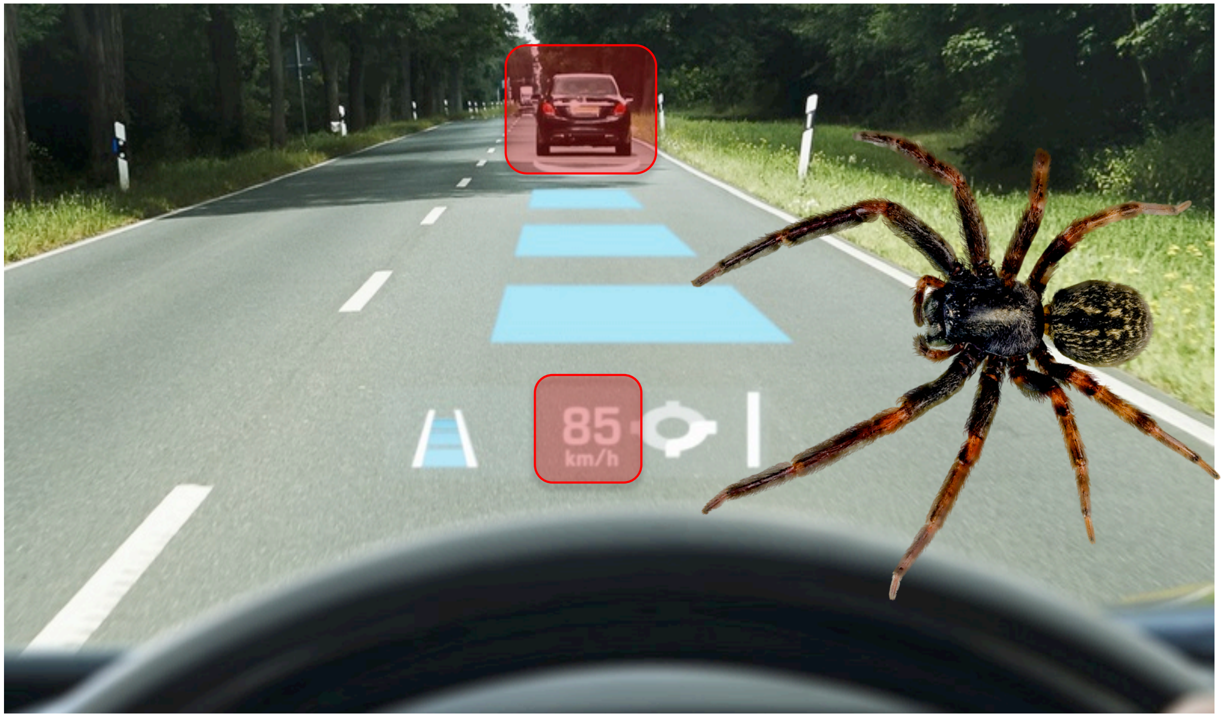
SYSTEM UPDATES AVAILABLE
3 NEW MESSAGES
Marly Lopez
Camilo Alvarez
push here to open your inbox
COOTRASANA
THE NEXT STOP
HERNAN ORTIZ
SEXY BEACH
GET
JOB MONKEY
URGENT
HURRY!
BUY GROCERIES FOR MR D. JURADO
GET OFF AT DOWNTOWN
DOWNTOWN
EXITO
EL POBLADO
shopping list
- pineapple
- yoghurt
7 MONKEYPOINTS
BONUS JOB
MASCOT
8 MONKEYPOINTS
BONUS JOB
PROOF READING
premium only
BONUS JOB
ELDERLY CARE
special offer on now!
5 MONKEYPOINTS
NEXT
USER TESTING FOR DOGS
Google
Ask a question
POINTS MANAGER
JOB MONKEY LEVEL 4
LEVEL 23
medellin

Hyper Reality (https://www.youtube.com/watch?v=YJg02ivYzSs)

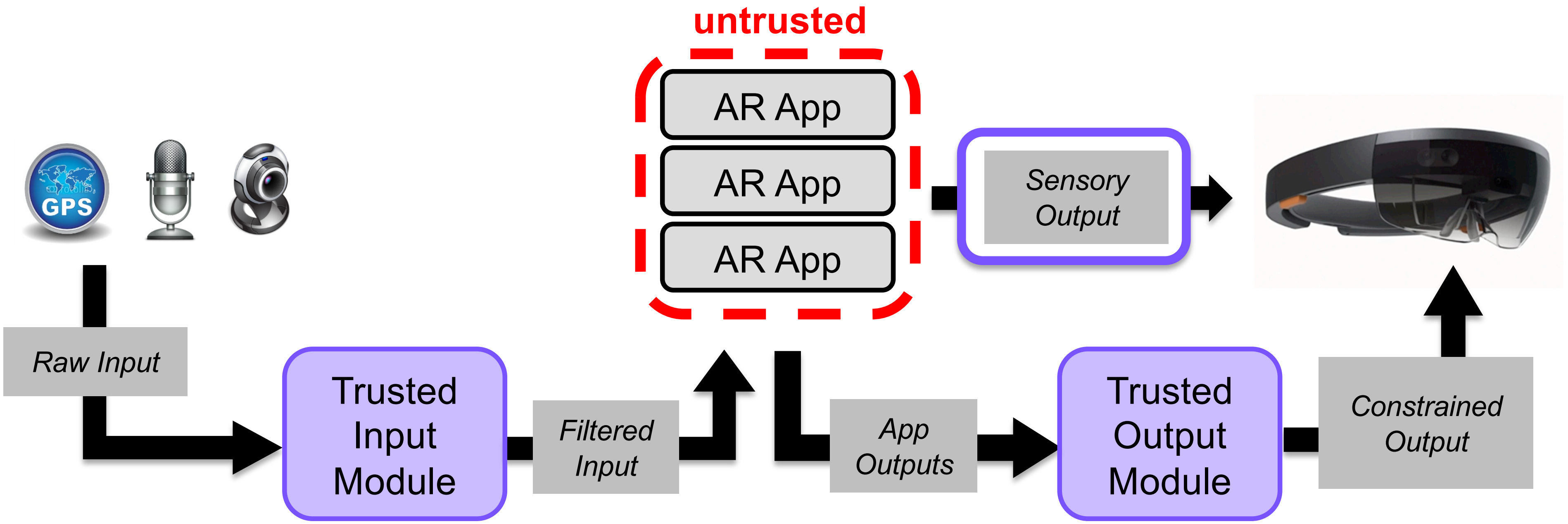
AR Output Security

A buggy or malicious app might…

- **Obscure another app's virtual content** to hide or modify its meaning
- **Obscure important real-world content,** such as traffic signs or cars
- **Disrupt the user physiologically,** such as by startling them



AR Output Security



Output Security

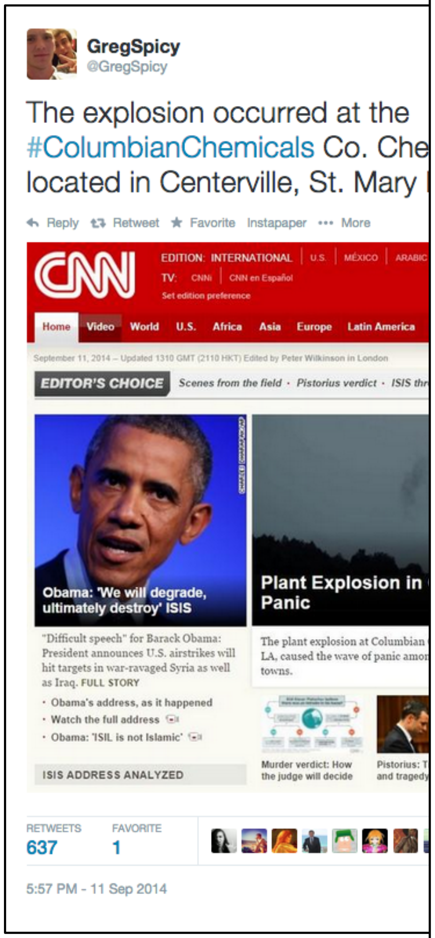
- Lebeck et al., HotMobile ’16
- Lebeck et al., IEEE S&P ’17
- Lebeck et al., HotMobile ‘19

Many Other Questions

- How to handle multiple apps augmenting reality at the same time?
  - **Lebeck et al., HotMobile ‘19**
- How to handle interactions between multiple users who may see different realities?
  - **Ruth et al., USENIX Security ‘19**

https://ar-sec.cs.washington.edu

(3) Technology-Enabled Disinformation



GregSpicy
@GregSpicy

The explosion occurred at the #ColumbianChemicals Co. Che
located in Centerville, St. Mary

Reply
Retweet
Favorite
Instapaper
More
CNN
EDITION: INTERNATIONAL | U.S. | MÉXICO | ARABIC
TV: CNNi | CNN en Español
Set edition preference
Home Video World U.S. Africa Asia Europe Latin America
September 11, 2014 – Updated 1310 GMT (2110 HKT) Edited by Peter Wilkinson in London
EDITOR'S CHOICE
Scenes from the field · Pistorius verdict · ISIS thr
Obama: 'We will degrade, ultimately destroy' ISIS
Plant Explosion in Panic

"Difficult speech" for Barack Obama: President announces U.S. airstrikes will hit targets in war-ravaged Syria as well as Iraq. FULL STORY

- Obama's address, as it happened
- Watch the full address
- Obama: 'ISIL is not Islamic'

ISIS ADDRESS ANALYZED

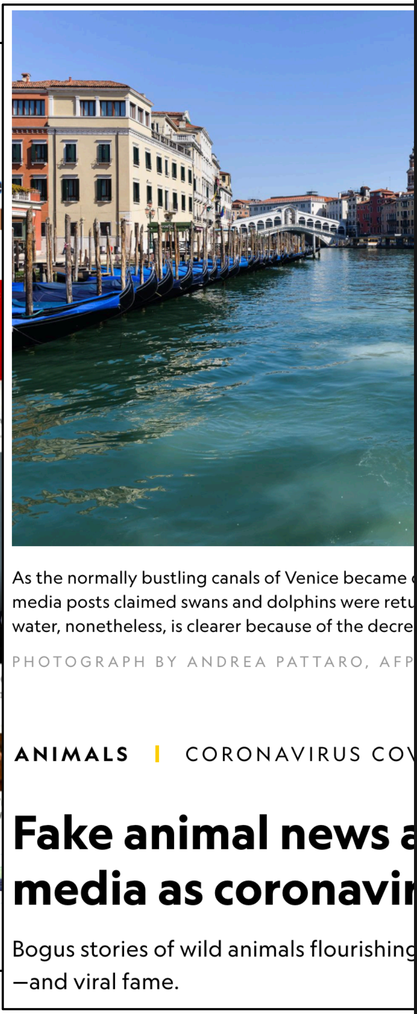
The plant explosion at Columbian LA, caused the wave of panic amon towns.

Murder verdict: How the judge will decide

Pistorius: T and tragedy

RETWEETS 637 FAVORITE 1

5:57 PM - 11 Sep 2014



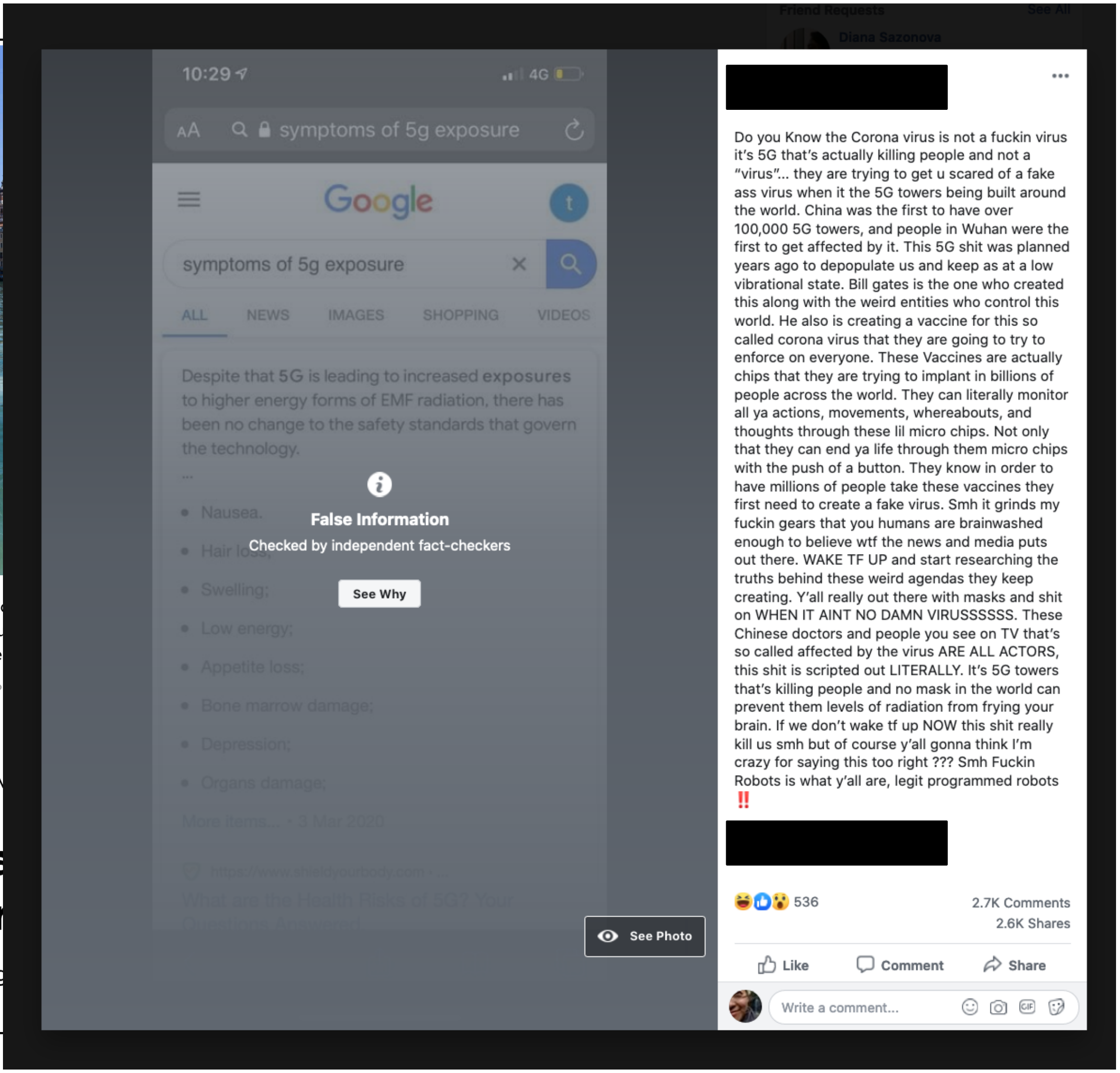
As the normally bustling canals of Venice became media posts claimed swans and dolphins were retu water, nonetheless, is clearer because of the decre

PHOTOGRAPH BY ANDREA PATTARO, AFP

ANIMALS | CORONAVIRUS COV

Fake animal news a media as coronavir

Bogus stories of wild animals flourishing —and viral fame.



Despite that 5G is leading to increased exposures to higher energy forms of EMF radiation, there has been no change to the safety standards that govern the technology.

...

- Nausea.
- Hair loss;
- Swelling;
- Low energy;
- Appetite loss;
- Bone marrow damage;
- Depression;
- Organs damage;

More items... • 3 Mar 2020

https://www.shieldyourbody.com › ...

What are the Health Risks of 5G? Your Questions Answered

False Information

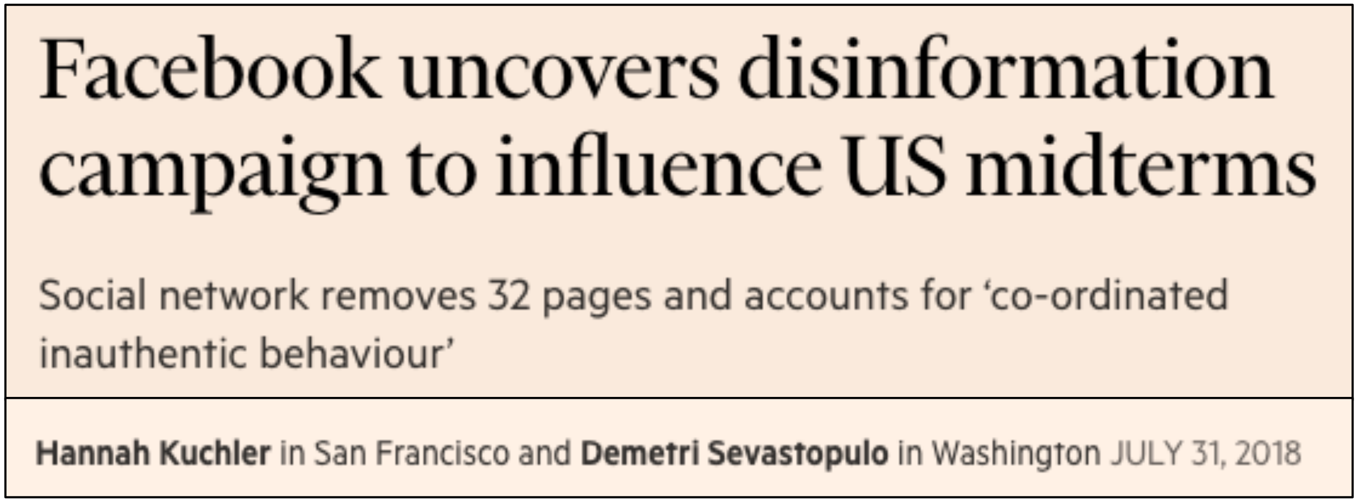
Checked by independent fact-checkers

[redacted]

Do you Know the Corona virus is not a fuckin virus it's 5G that's actually killing people and not a "virus"... they are trying to get u scared of a fake ass virus when it the 5G towers being built around the world. China was the first to have over 100,000 5G towers, and people in Wuhan were the first to get affected by it. This 5G shit was planned years ago to depopulate us and keep as at a low vibrational state. Bill gates is the one who created this along with the weird entities who control this world. He also is creating a vaccine for this so called corona virus that they are going to try to enforce on everyone. These Vaccines are actually chips that they are trying to implant in billions of people across the world. They can literally monitor all ya actions, movements, whereabouts, and thoughts through these lil micro chips. Not only that they can end ya life through them micro chips with the push of a button. They know in order to have millions of people take these vaccines they first need to create a fake virus. Smh it grinds my fuckin gears that you humans are brainwashed enough to believe wtf the news and media puts out there. WAKE TF UP and start researching the truths behind these weird agendas they keep creating. Y'all really out there with masks and shit on WHEN IT AINT NO DAMN VIRUSSSSSS. These Chinese doctors and people you see on TV that's so called affected by the virus ARE ALL ACTORS, this shit is scripted out LITERALLY. It's 5G towers that's killing people and no mask in the world can prevent them levels of radiation from frying your brain. If we don't wake tf up NOW this shit really kill us smh but of course y'all gonna think I'm crazy for saying this too right ??? Smh Fuckin Robots is what y'all are, legit programmed robots ‼️

[redacted]

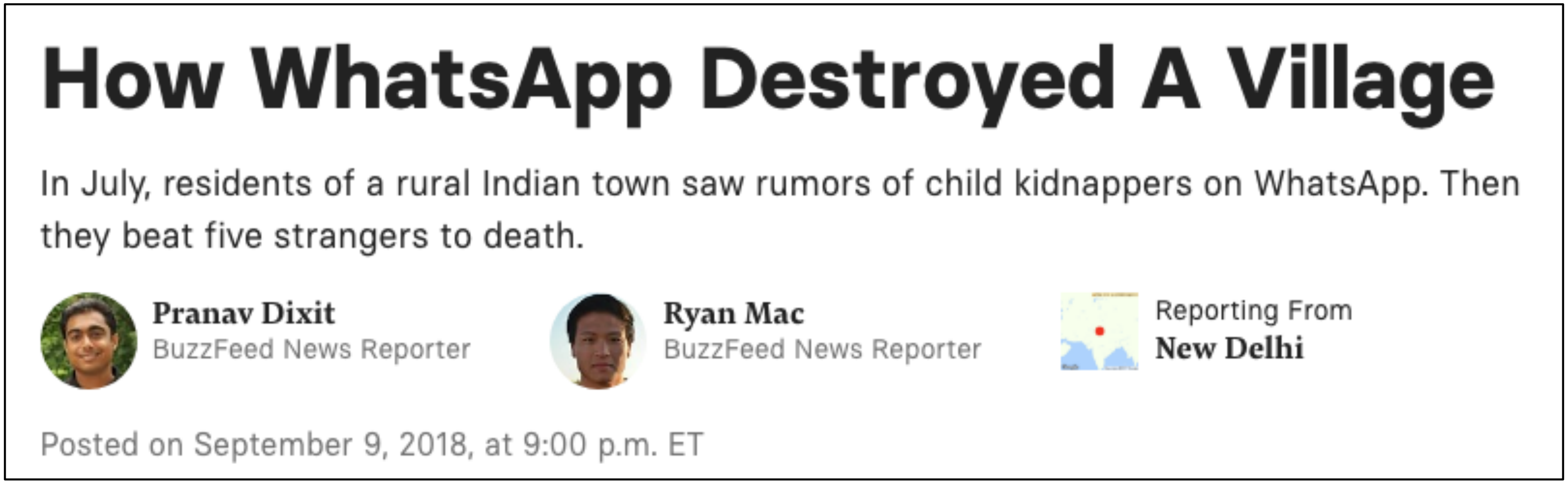
Serious Potential Consequences



Facebook uncovers disinformation campaign to influence US midterms

Social network removes 32 pages and accounts for 'co-ordinated inauthentic behaviour'

Hannah Kuchler in San Francisco and **Demetri Sevastopulo** in Washington JULY 31, 2018



How WhatsApp Destroyed A Village

In July, residents of a rural Indian town saw rumors of child kidnappers on WhatsApp. Then they beat five strangers to death.

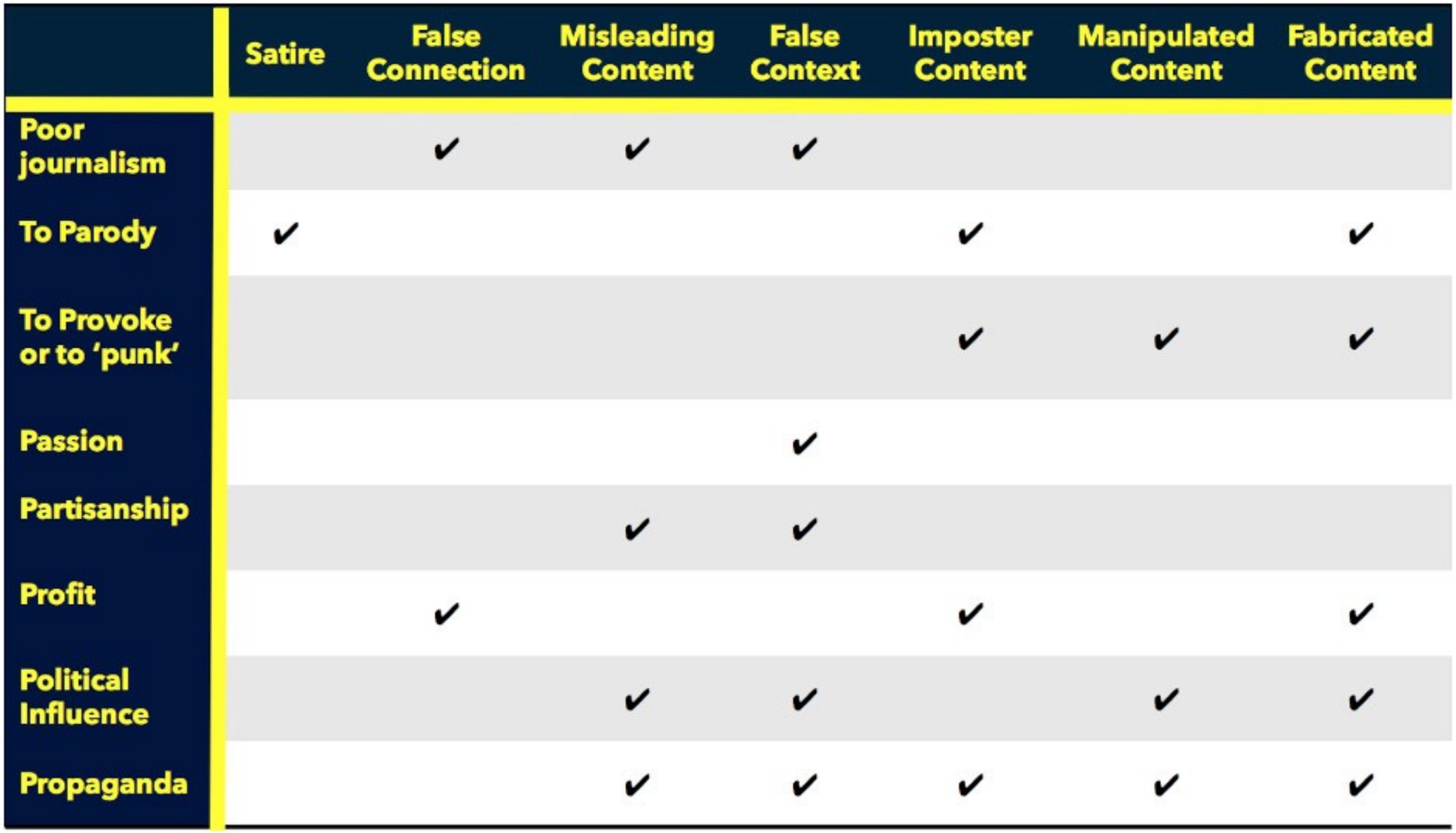
Pranav Dixit
BuzzFeed News Reporter

Ryan Mac
BuzzFeed News Reporter

Reporting From
New Delhi

Posted on September 9, 2018, at 9:00 p.m. ET

Many Types of “False News”



	Satire	False Connection	Misleading Content	False Context	Imposter Content	Manipulated Content	Fabricated Content
Poor journalism		✔	✔	✔			
To Parody	✔				✔		✔
To Provoke or to ‘punk’					✔	✔	✔
Passion				✔			
Partisanship			✔	✔			
Profit		✔			✔		✔
Political Influence			✔	✔		✔	✔
Propaganda			✔	✔	✔	✔	✔

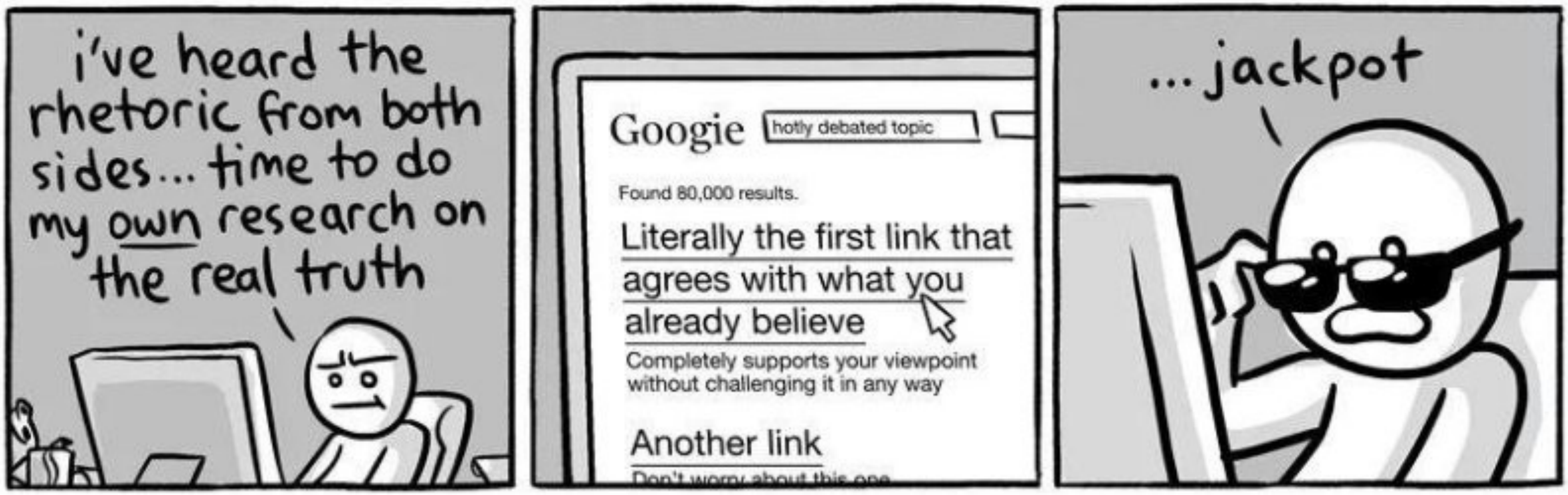
From Claire Wardle, https://medium.com/1st-draft/fake-news-its-complicated-d0f773766c79

What's New?

The Technology, Not the Incentives

- How content is created
  - Scale and democratization
  - Automated fake content creation
    - Video: https://grail.cs.washington.edu/projects/AudioToObama/
    - Text: https://rowanzellers.com/grover/
- How content is disseminated
  - Scale and democratization
  - Tracking and targeting
  - Algorithmic curation
  - Anonymity and bots
  - Immediate reach and feedback
- How content is consumed
  - Attention economy
  - Filter bubbles

Not Just a Technical Problem: Human Cognitive Vulnerabilities


i've heard the rhetoric from both sides... time to do my own research on the real truth
Googie
hotly debated topic
Found 80,000 results.
Literally the first link that agrees with what you already believe
Completely supports your viewpoint without challenging it in any way
Another link
Don't worry about this one
...jackpot

CHAINSAWSUIT.COM

(e.g., confirmation bias, backfire effect)

WRAP-UP

This Quarter

- Overview of:
  - Security mindset
  - Software security
  - Cryptography
  - Web security
  - Web privacy
  - Authentication
  - Mobile platform security
  - Usable security
  - Physical security
  - Anonymity
  - Smart home security
  - Side channels
  - Adversarial ML
  - Security for emerging tech

Lots We Didn't Cover…

- Really deep dive into any of the above topics
- (Most) Network security
- (Most) Traditional OS security
- (Most) Recent attacks/vulnerabilities
- (Most) Specific protocols (e.g., SSL/TLS, Kerberos)
- Access control
- Spam
- Malware / Bots / Worms
- Social engineering
- Cryptocurrencies (e.g., Bitcoin)
- Other emerging technologies
- …

Thanks for a great (even if strange) quarter! Hang in there.

- Stay in touch
  - Come say hi when we are back on campus ☺
- Not ready to be done?
  - CSE 490 Cryptography
  - CSE 481S Security Capstone in the winter
  - CSE 564 Graduate Computer Security
  - TAing for 484
- Please fill out course evaluation: https://uw.iasystem.org/survey/232765