APPSEC - CALIFORNIA 2018 OWASP

Unpoisoned Fruit:

Seeding Trust into a Growing World of Algorithmic Warfare

Davi Ottenheimer

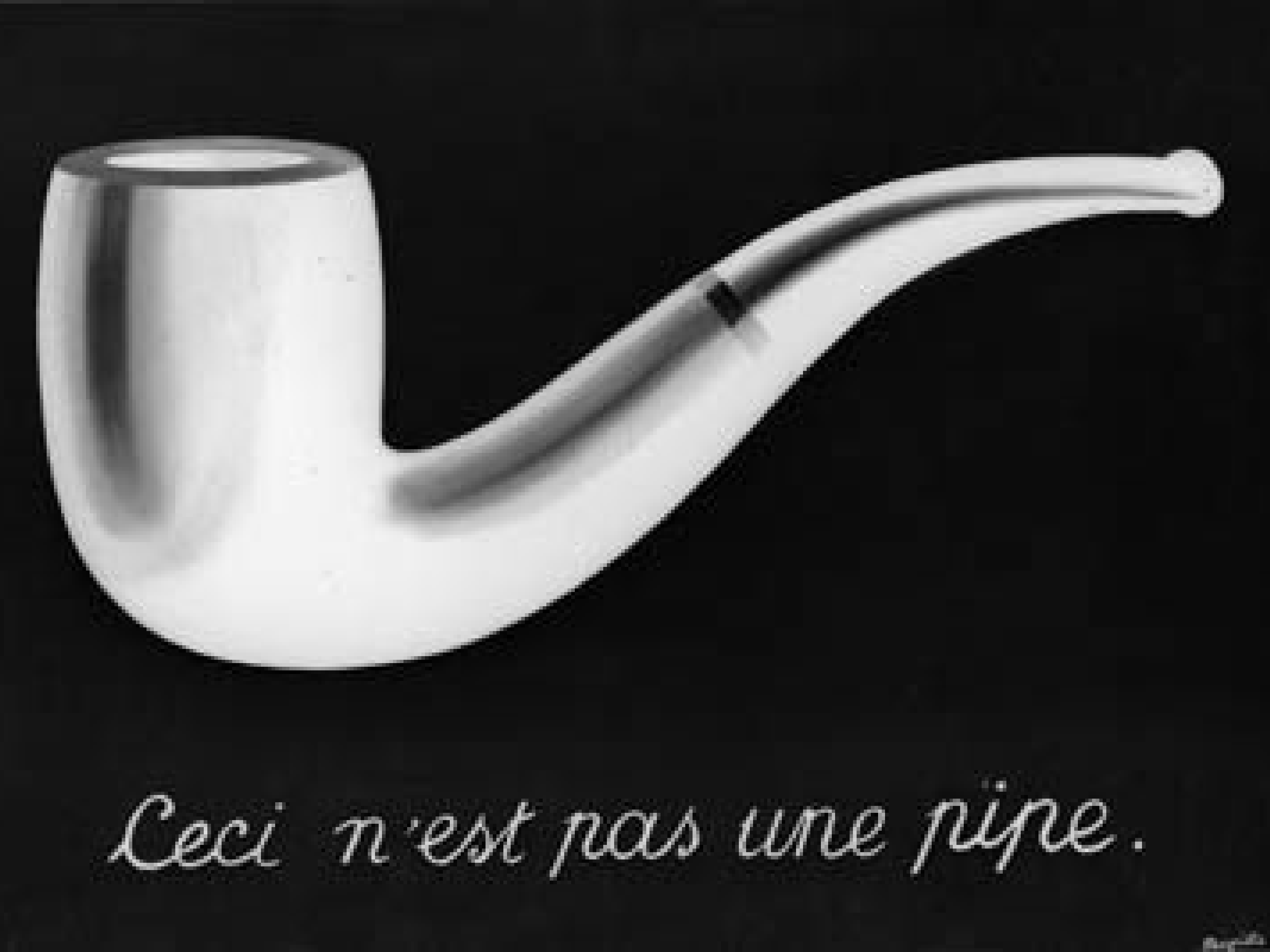
mongoDB

Agenda

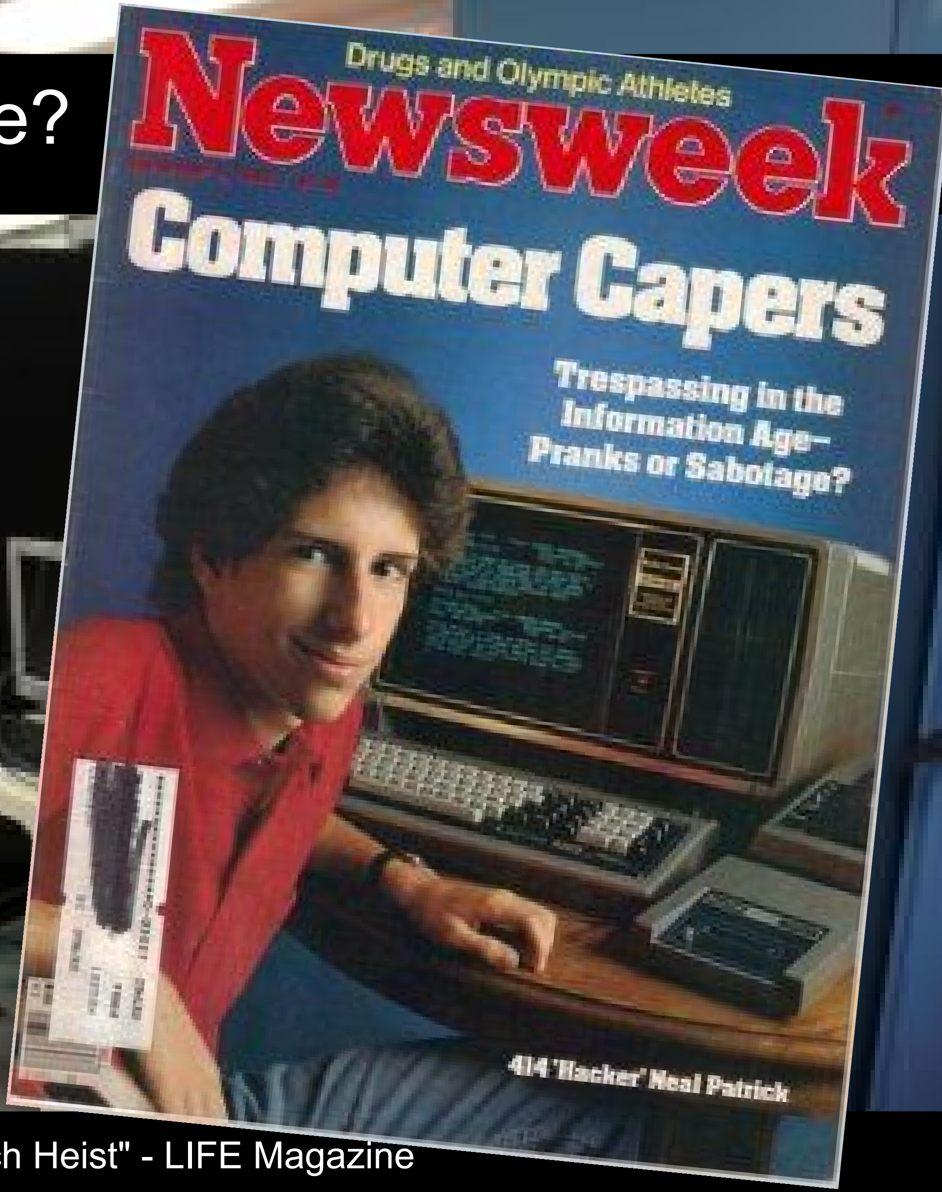
1. Whoami
2. Defensive concepts for algorithmic warfare based on intl history
3. Nearly all digital life influenced by AI
4. Can delegated automation agents (cyber soldiers) be trusted?
    - ○ History shows absence of regulation (integrity breach) ends in humanitarian disasters
    - ○ Yet platform infosec slow to regulate after breaches (social inequalities and conflict)
    - ○ Algorithm security increasingly raises need to avert, or win, kinetic conflict
5. How and why to seed security into big data rather than unpoison its fruit

1. whoami

(ode to BlackHat)


Ceci n'est pas une pipe.

1980s Pranks or Sabotage?


Drugs and Olympic Athletes
Newsweek
Computer Capers
Trespassing in the Information Age—Pranks or Sabotage?
414 'Hacker' Neal Patrick

Internet, Email, BBS, Laptop (T1000), Self-built 286, Commodore, Amiga, VAX/VMS, SunOS, Macintosh

'83

- **April**: "Russians Steal Our Secrets...High-Tech Heist" - LIFE Magazine
- **June**: WarGames Movie
- **August**: “Computer Capers” by 414 “Hacker” - Newsweek

https://blogs.k-state.edu/it-news/2009/07/07/k-state-bids-farewell-to-central-ibm-computer-mainframe/

1990s Ethics of Humanitarian Intervention

- 1993 BA on Somalia

NATURA ET REVELATIO CŒLI GEMINI.
MACALESTRI COLL.

SOAS
University of London

- 1994 MSc on Ethiopia

RERUM CAUSAS COGNOSCERE

http://www.flyingpenguin.com/?p=5349

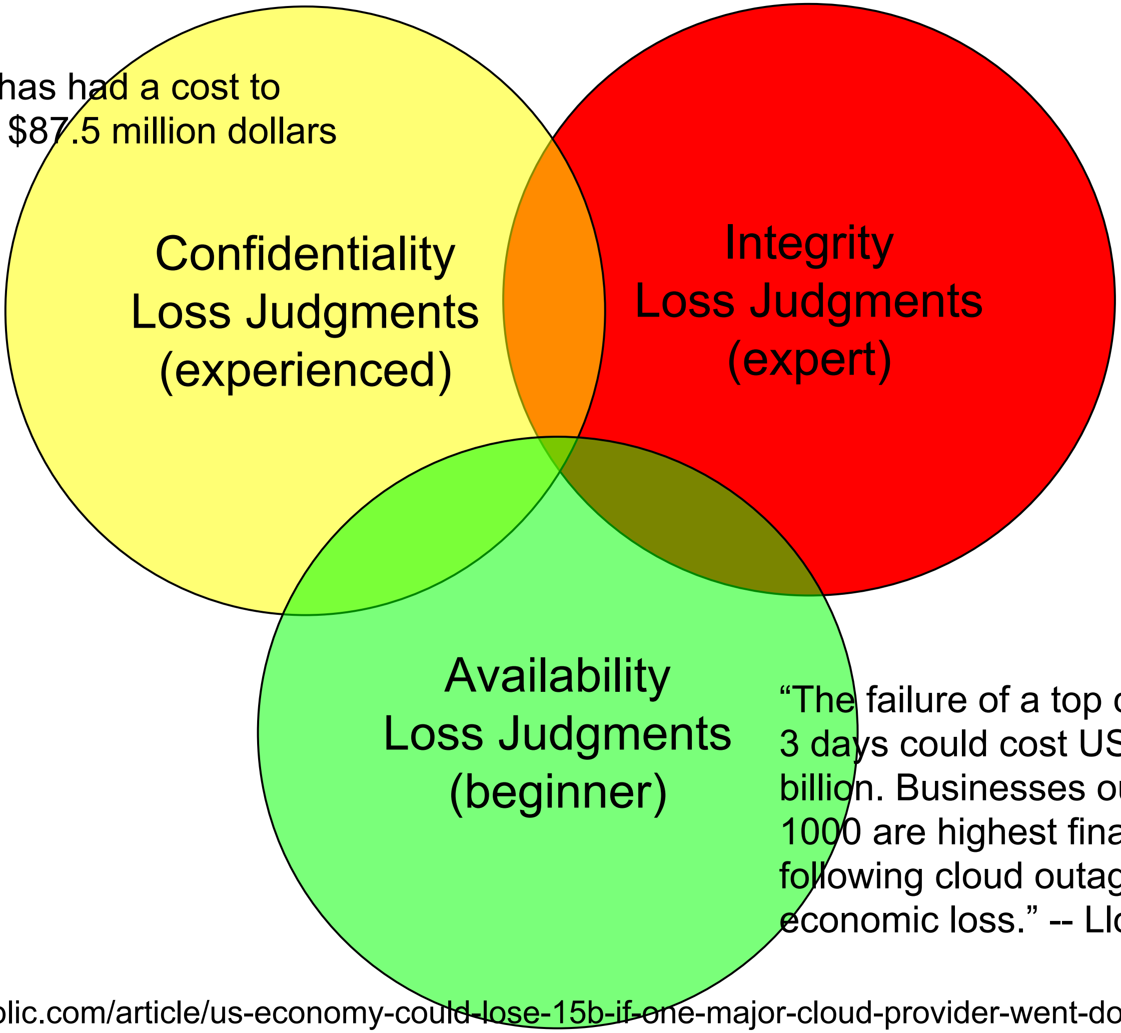
2. defensive concepts for algowar...

“data changes our judgment and that’s what the modern world is about”

(hat tip to bayes and fisher)

and so after 2+ decades of infosec...here we are

"...breach has had a cost to Equifax of $87.5 million dollars so far..."



Confidentiality
Loss Judgments
(experienced)

Integrity
Loss Judgments
(expert)

?

Availability
Loss Judgments
(beginner)

"The failure of a top cloud service for 3 days could cost US economy $15 billion. Businesses outside Fortune 1000 are highest financial risk following cloud outage, with 63% of economic loss." -- Lloyd's, 2018

https://www.techrepublic.com/article/us-economy-could-lose-15b-if-one-major-cloud-provider-went-down-for-a-few-days/
https://www.sec.gov/cgi-bin/viewer?action=view&cik=33185&accession_number=0000033185-17-000032&xbrl_type=v#

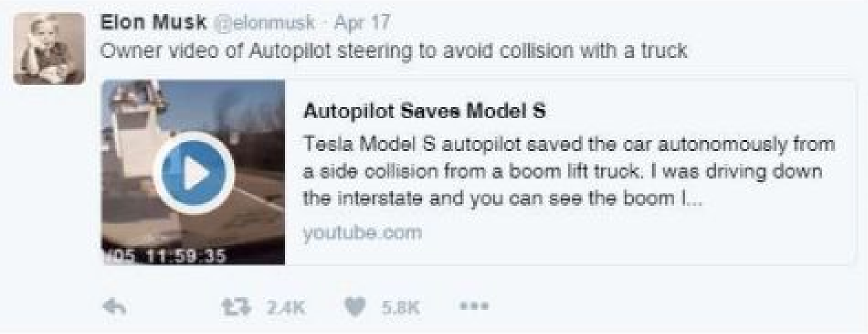
...based on international history perspective of data integrity

(ethical judgments)

Iran 1980

Tesla 2016 - Did not see until too late

"human far earlier detects what ***Tesla blind*** to"



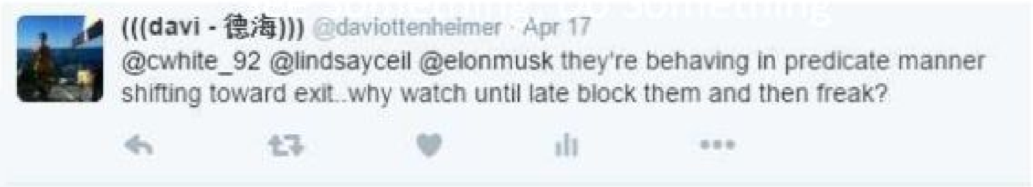
Elon Musk @elonmusk · Apr 17

Owner video of Autopilot steering to avoid collision with a truck

Autopilot Saves Model S

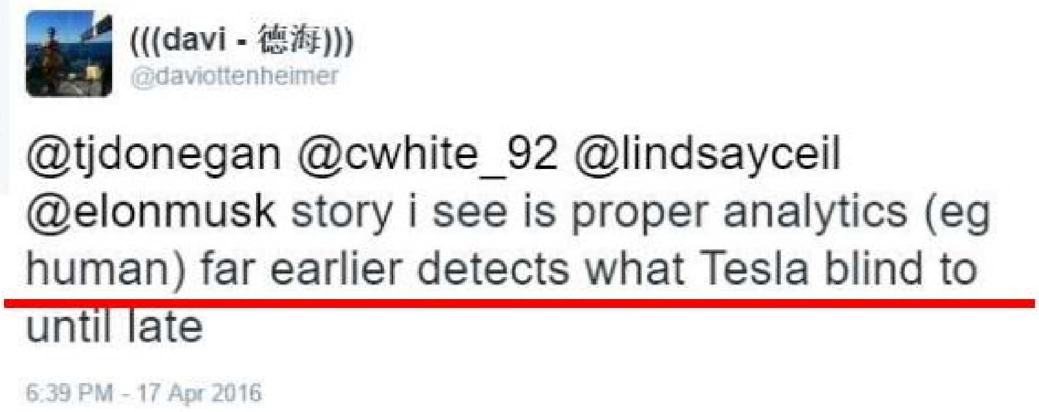
Tesla Model S autopilot saved the car autonomously from a side collision from a boom lift truck. I was driving down the interstate and you can see the boom l...

youtube.com



(((davi - 德海))) @daviottenheimer · Apr 17

@cwhite_92 @lindsayceil @elonmusk they're behaving in predicate manner shifting toward exit..why watch until late block them and then freak?



(((davi - 德海)))
@daviottenheimer

@tjdonegan @cwhite_92 @lindsayceil @elonmusk story i see is proper analytics (eg human) far earlier detects what Tesla blind to until late

6:39 PM - 17 Apr 2016

https://twitter.com/daviottenheimer/status/721875721946202112

flyingpenguin

http://www.flyingpenguin.com/?p=22441

Seychelles 1981

"[Kenya President] Moi either had been duped by intelligence or was playing politics.

He insisted persons who hired Beechcraft aircraft from Sunbird Aviation were 'American tourists'.

Andrew Cole later ... would admit Sunbird flew Mad Mike Hoar into Seychelles. 'We did, but we didn't know (they were mercenaries) …

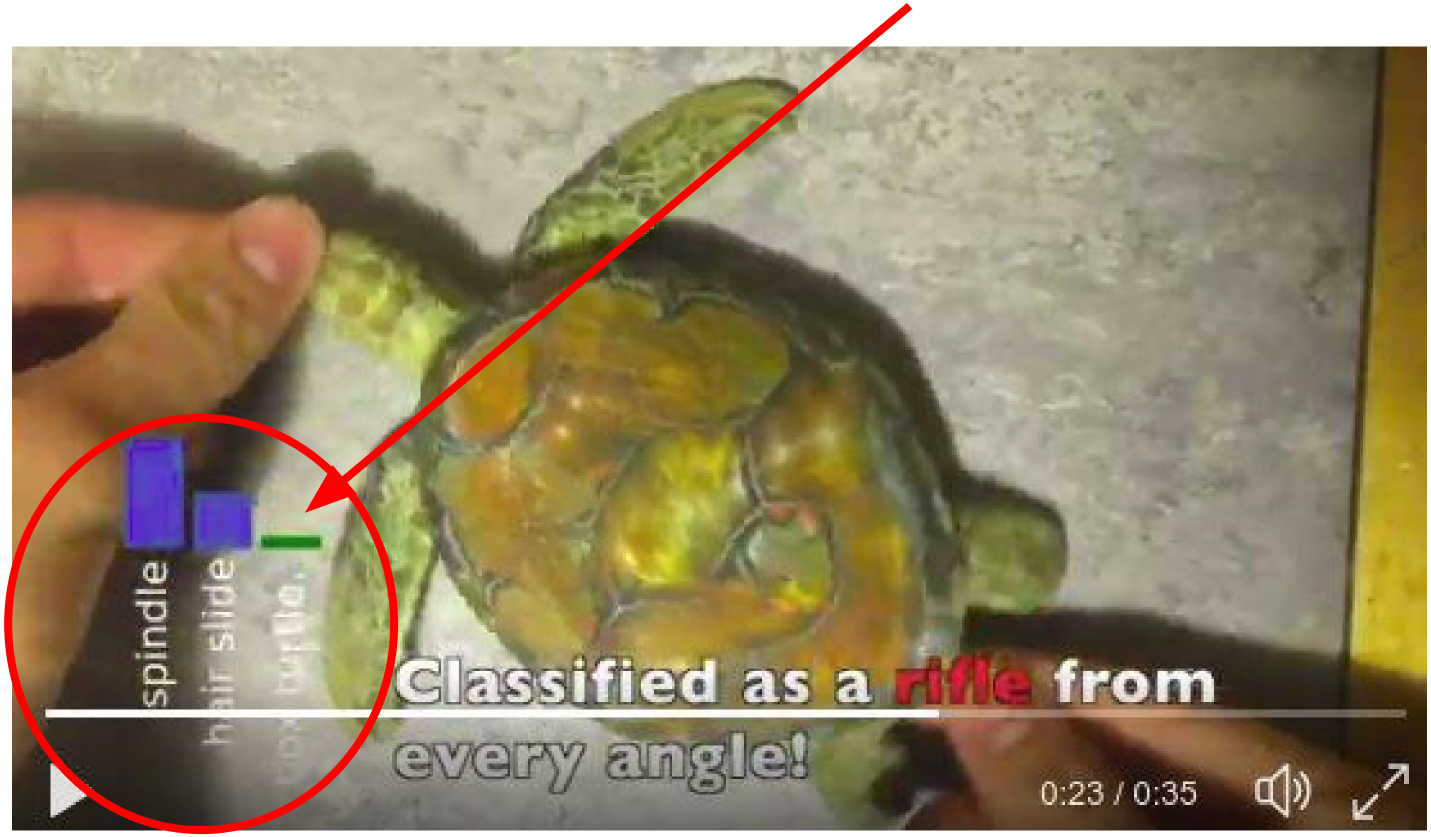
They registered as a rugby team.'"

https://www.nation.co.ke/news/politics/How-Njonjo-Gethi-were-embroiled-in-Seychelles-coup-plot/-/1064/2937724/-/hijdu0/-/index.html

MIT/LabSix 2017 - Easily exposed

- Researchers: "**Classified as a rifle from every angle!**"
- Reality: It’s still classified as a turtle. Rifle not listed

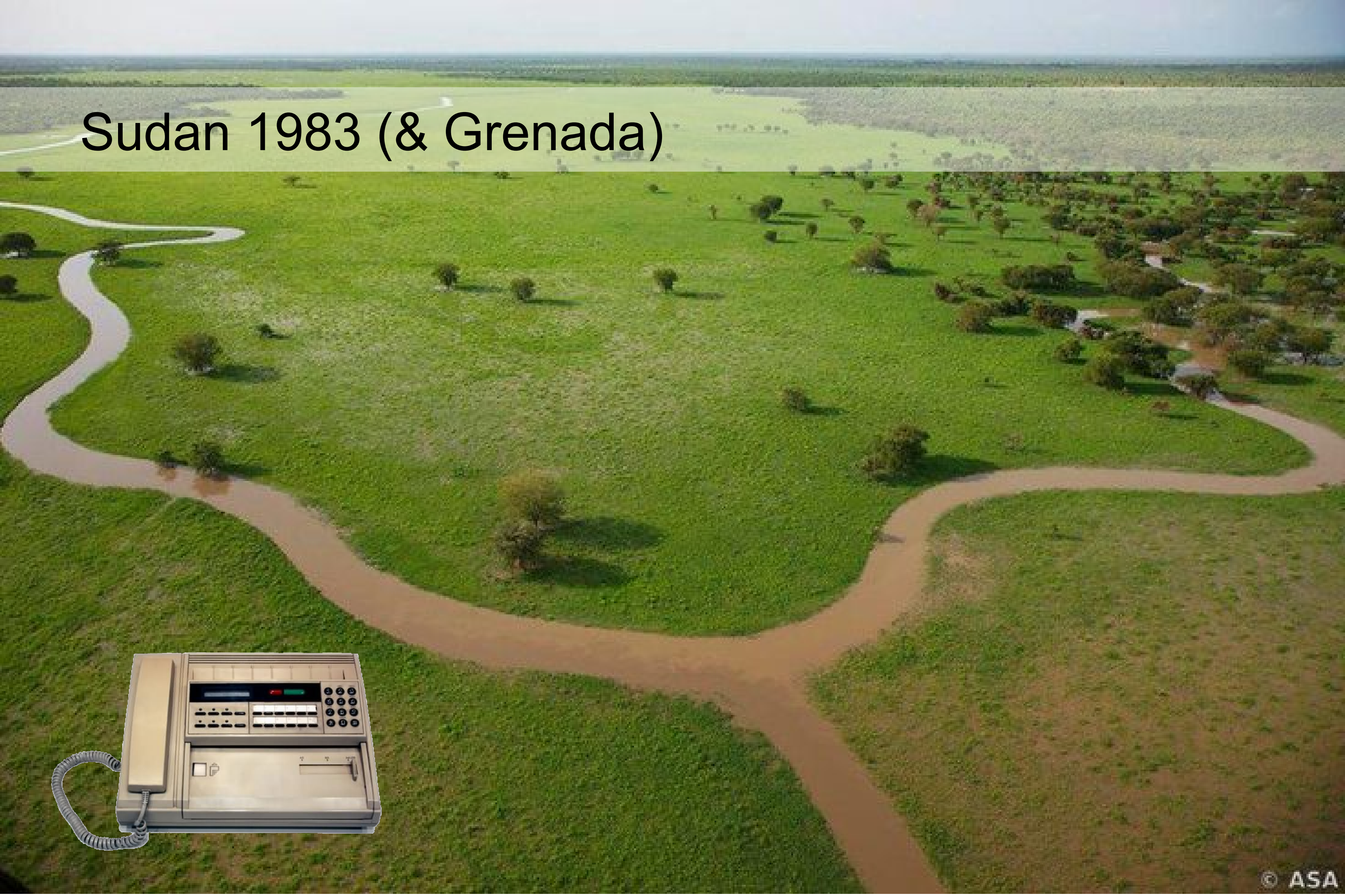
NOT RIFLES



Classified as a rifle from every angle!

https://twitter.com/daviottenheimer/status/925550016378343424
https://arxiv.org/pdf/1707.07397.pdf

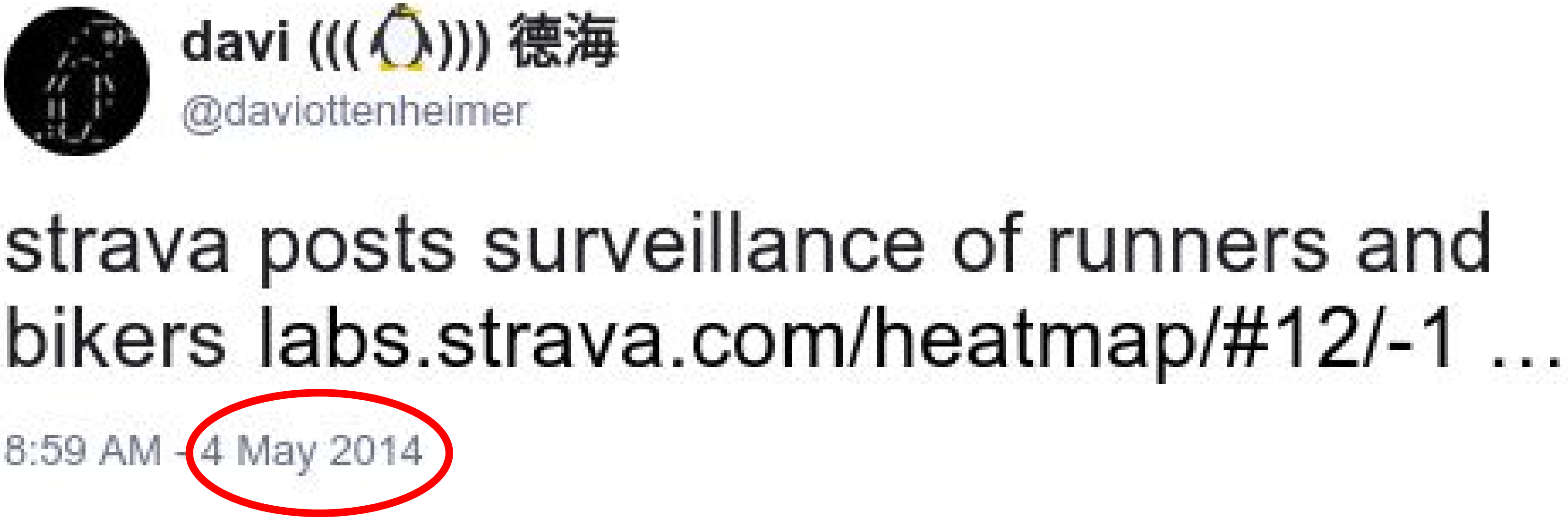
Sudan 1983 (& Grenada)



© ASA

https://www.upi.com/Archives/1983/07/09/Hostages-clean-up-mess-from-bloody-rescue/3923426571200/

Strava 2014



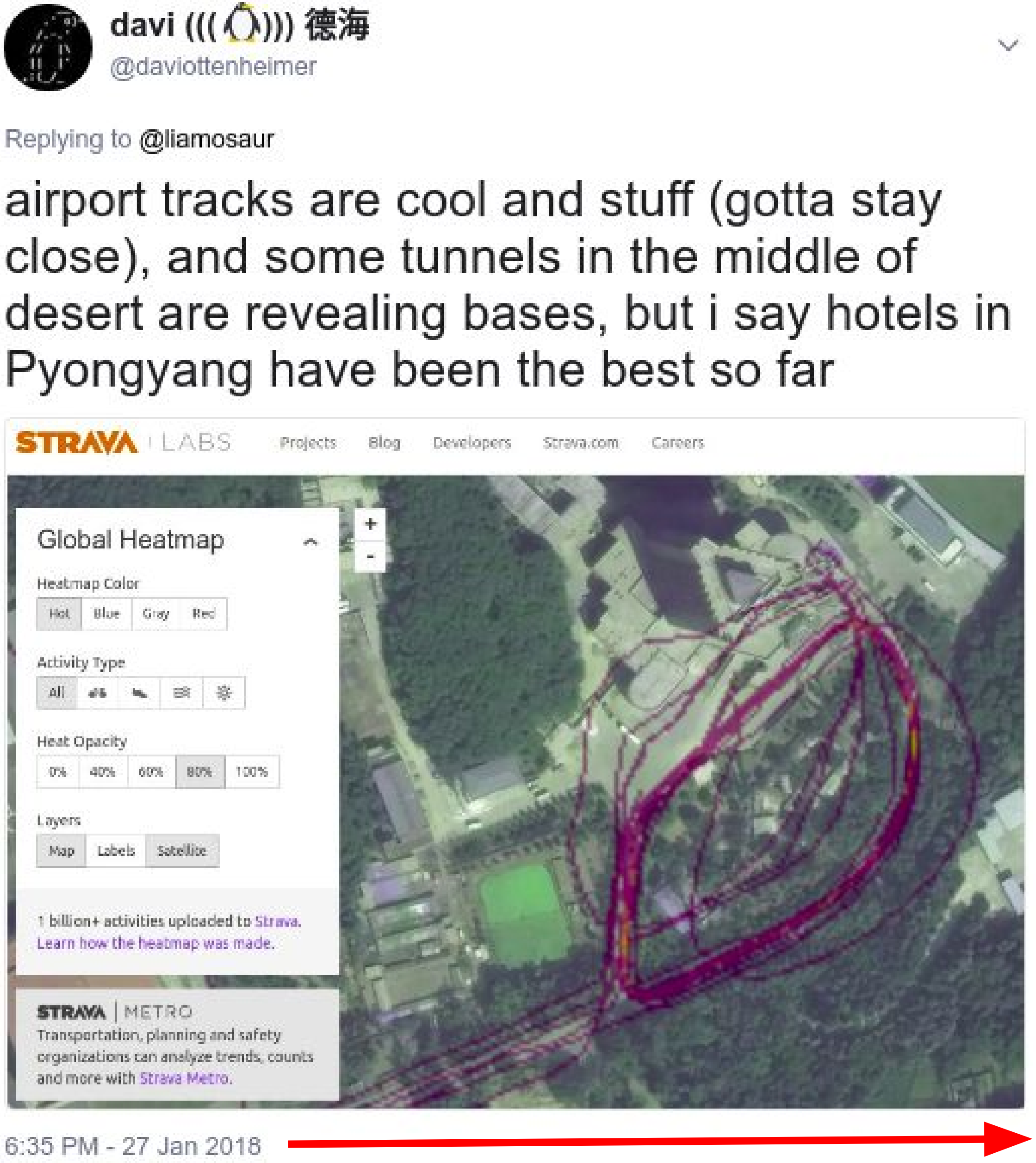
davi (((🐧))) 德海
@daviottenheimer

strava posts surveillance of runners and bikers labs.strava.com/heatmap/#12/-1 ...

8:59 AM - 4 May 2014

https://twitter.com/daviottenheimer/status/462984852803833856

Strava 2018



davi (((🐧))) 德海
@daviottenheimer

Replying to @liamosaur

airport tracks are cool and stuff (gotta stay close), and some tunnels in the middle of desert are revealing bases, but i say hotels in Pyongyang have been the best so far

Global Heatmap

Heatmap Color: Hot | Blue | Gray | Red

Activity Type: All

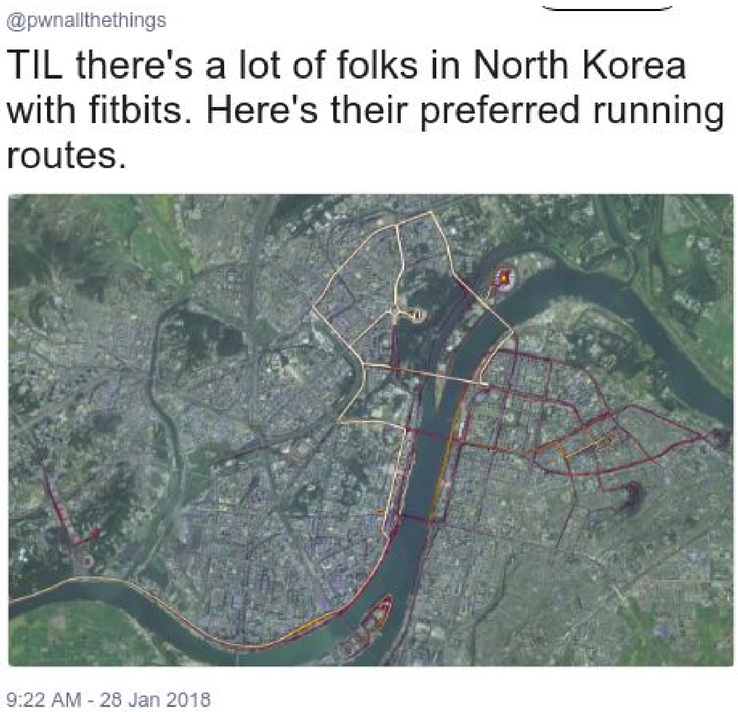
Heat Opacity: 0% | 40% | 60% | 80% | 100%

Layers: Map | Labels | Satellite

1 billion+ activities uploaded to Strava.
Learn how the heatmap was made.

STRAVA | METRO
Transportation, planning and safety organizations can analyze trends, counts and more with Strava Metro.

6:35 PM - 27 Jan 2018



@pwnallthethings

TIL there's a lot of folks in North Korea with fitbits. Here's their preferred running routes.

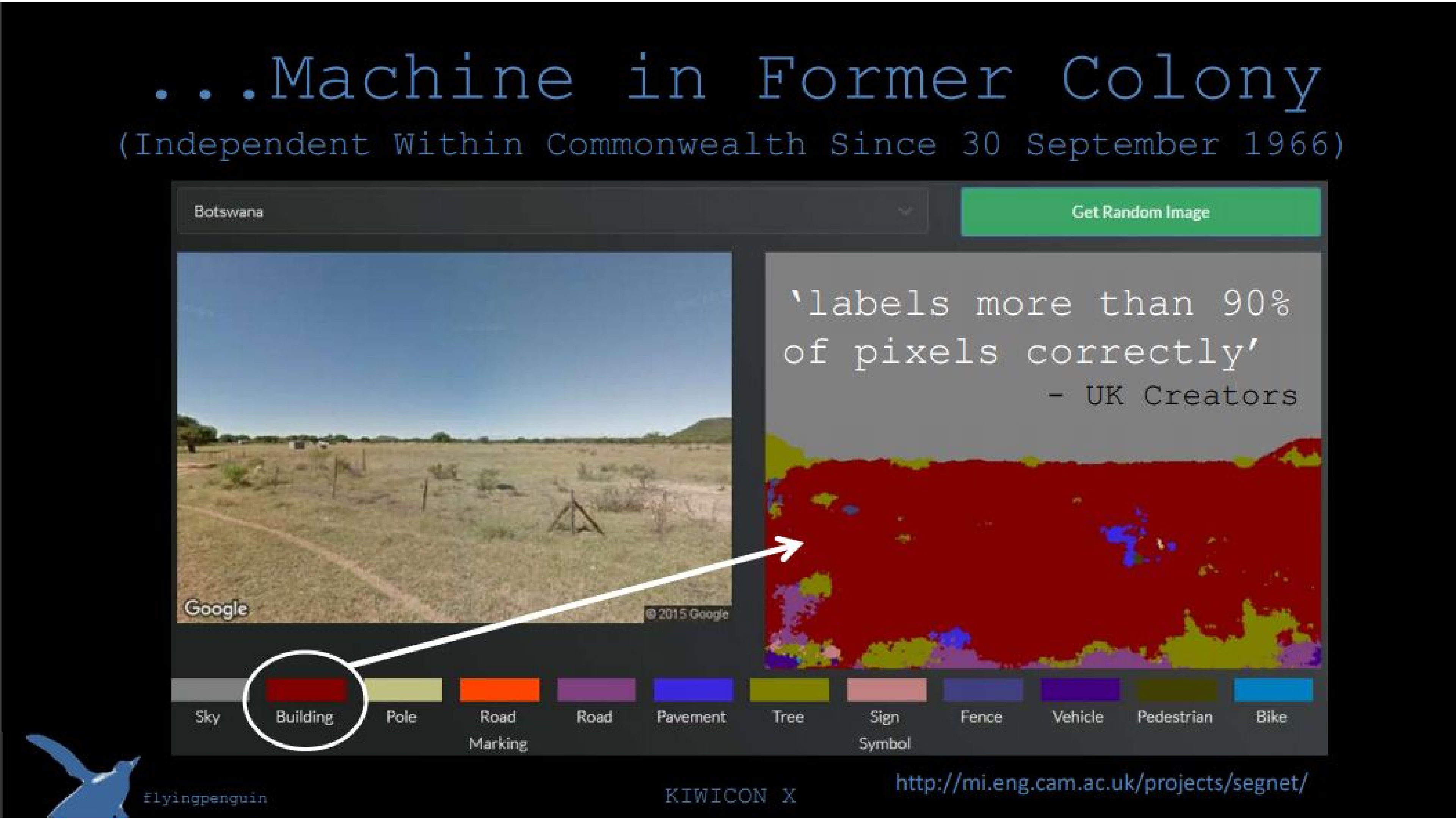
9:22 AM - 28 Jan 2018

https://labs.strava.com/heatmap/#17.88/125.69248/39.00986/hot/all
https://twitter.com/Nrg8000/status/957318498102865920

Panama 1989

https://history.army.mil/html/books/070/70-85-1/cmhPub_70-85-1.pdf

Cambridge 2016



...Machine in Former Colony

(Independent Within Commonwealth Since 30 September 1966)

'labels more than 90% of pixels correctly'
- UK Creators

http://mi.eng.cam.ac.uk/projects/segnet/

http://www.flyingpenguin.com/?p=22429

Fast Forward to...Niger 2017

"That special forces team did not have a true picture of the environment that they were in...did not understand how close the terrorists were to their operation."

https://www.cnn.com/2018/01/11/politics/niger-ambush-final-investigation/index.html

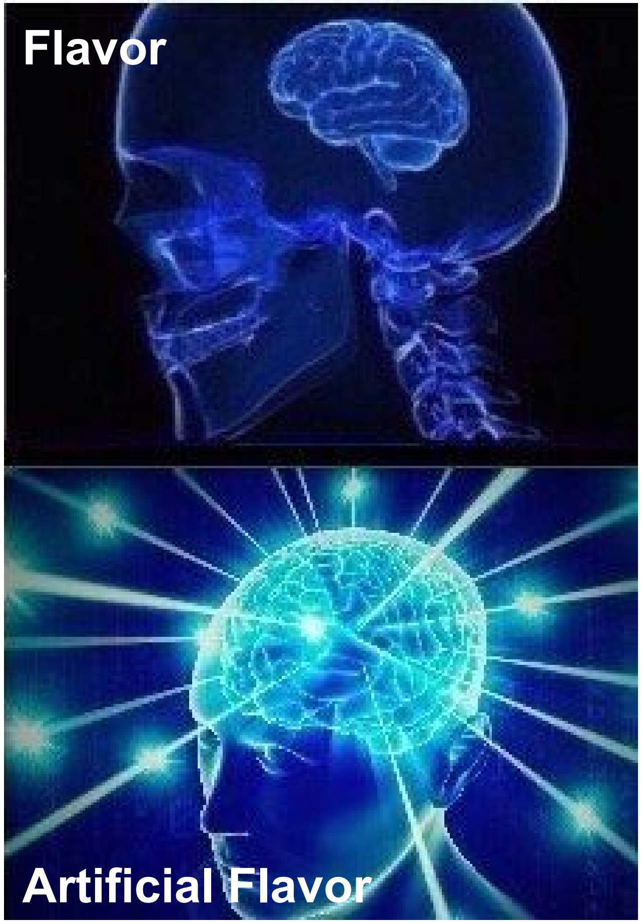
“Data Changes Our Judgment”

http://asc.army.mil/web/news-alt-jfm18-complex-environments-call-for-better-sensors/

3. AI/ML impact expanding fast:
all human “privileges” and rights
(authority transfer to pass judgment)

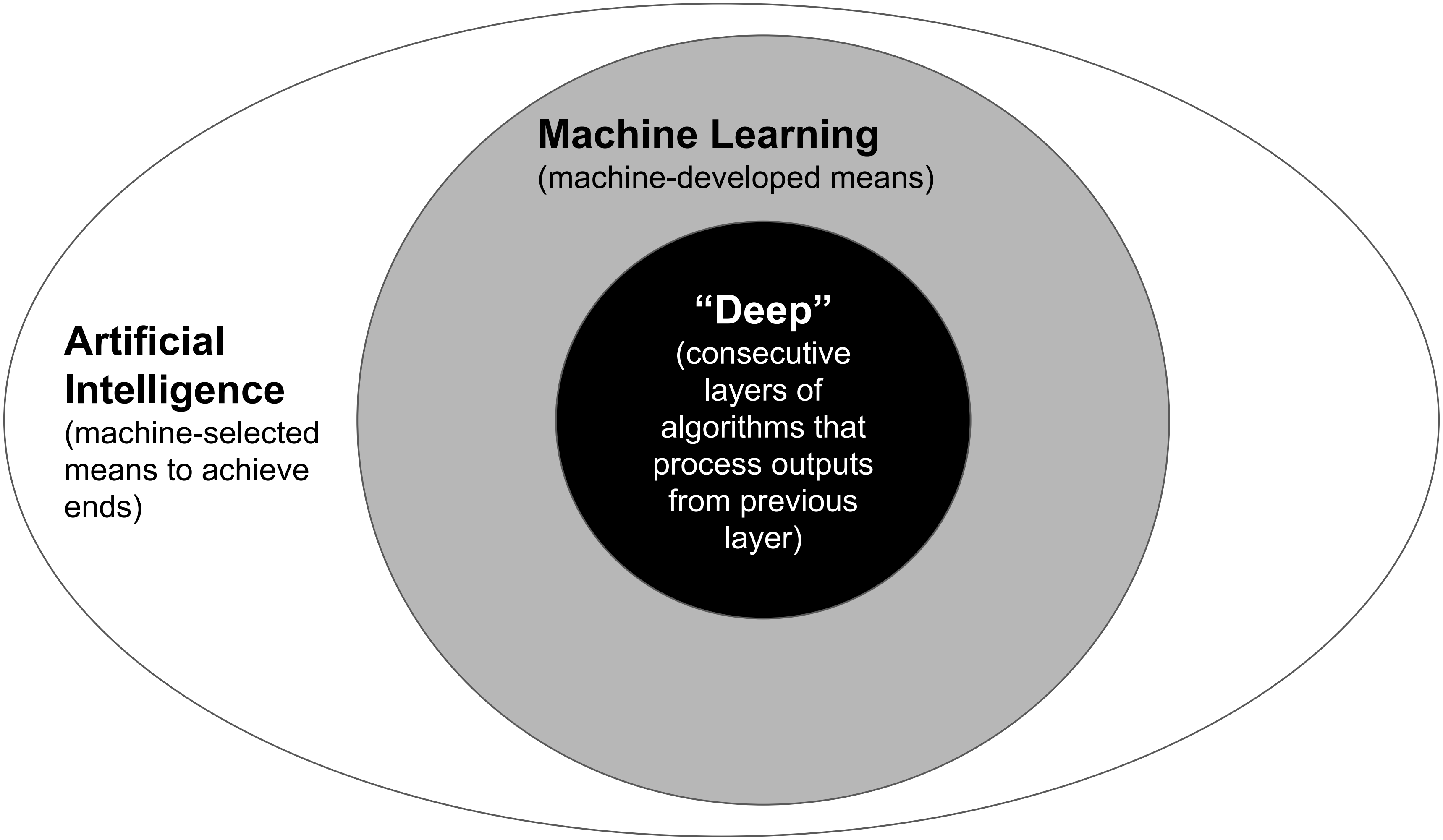
EVERY Industry Already “Smoking” Some AI/ML
(replacing organic/natural sensors/agents)

- Retail
- Ag
- Financial
- Health
- Education
- Energy
- Gov
- Transit



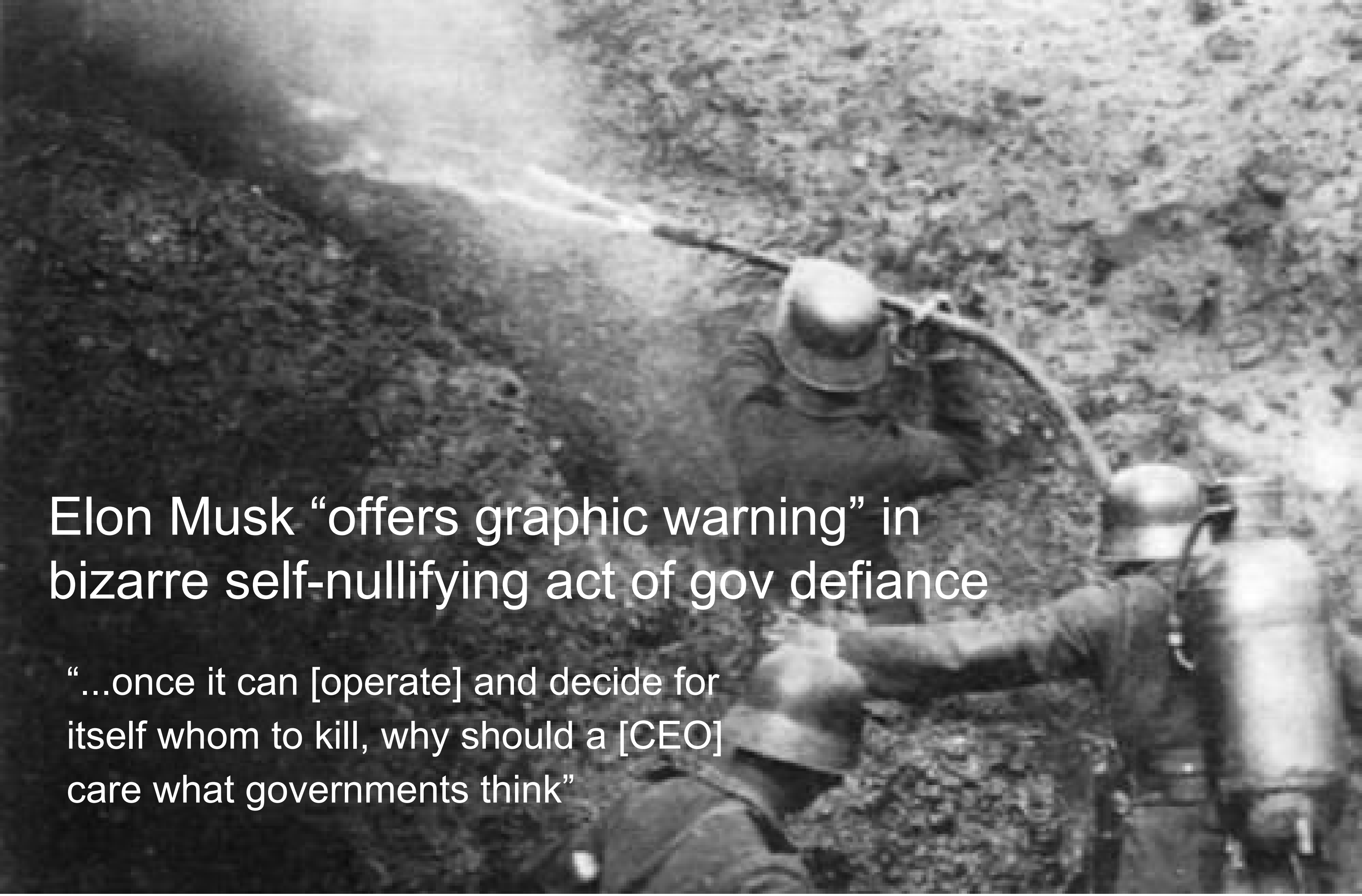
“AI is the Civil Rights Battle of Our Time”

-- @yeshican



Artificial Intelligence
(machine-selected means to achieve ends)
Machine Learning
(machine-developed means)
“Deep”
(consecutive layers of algorithms that process outputs from previous layer)

https://twitter.com/TheRundownBET/status/954352757661581313



Elon Musk “offers graphic warning” in bizarre self-nullifying act of gov defiance

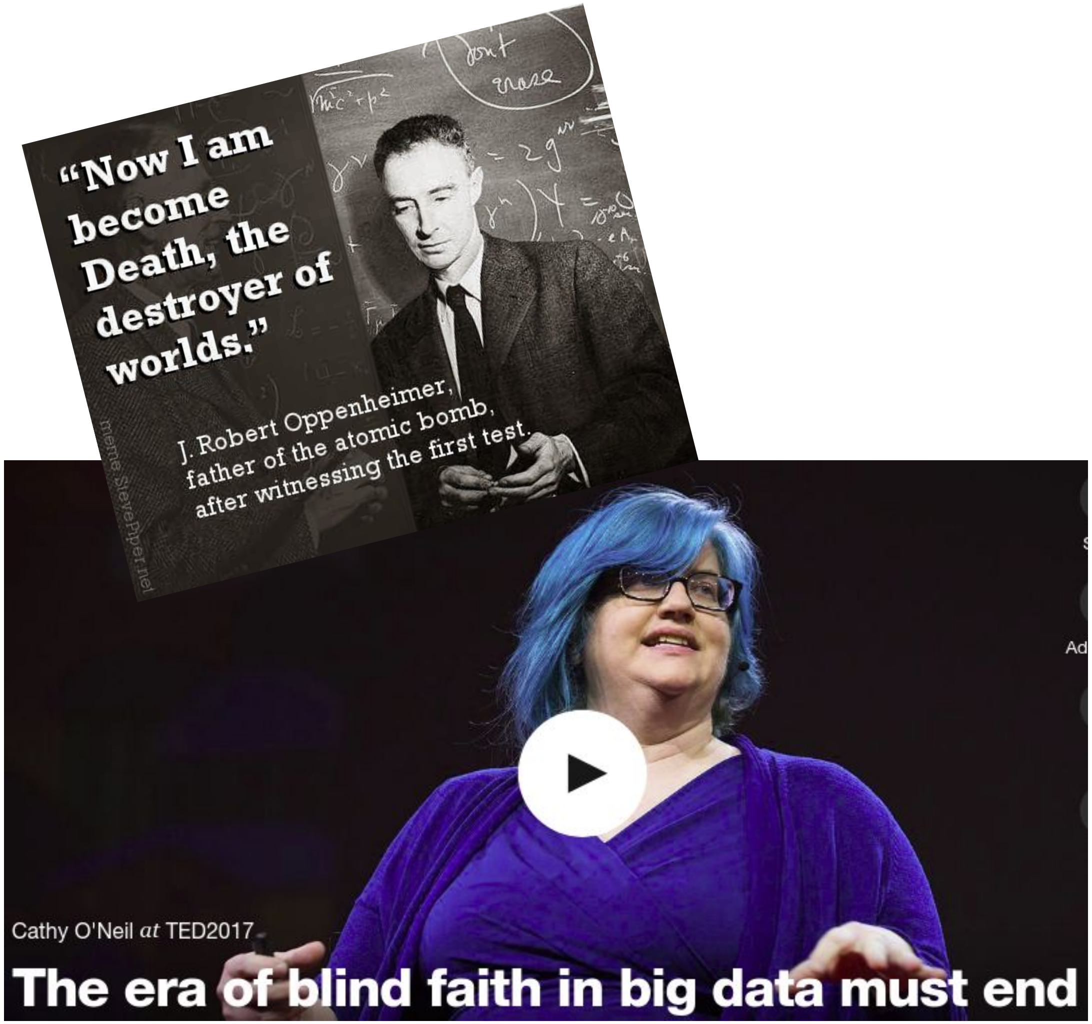
“...once it can [operate] and decide for itself whom to kill, why should a [CEO] care what governments think”

https://www.cnet.com/news/scary-slaughterbots-video-shows-danger-of-ai-powered-drone-weapons/

Even Math PhD is Woke, Worried Math = Weapons

- Campaigning to end “blind faith” in big data
- No replacements for faith, just says ***quit believing***
- Confusingly calls Netflix her example of safe AI

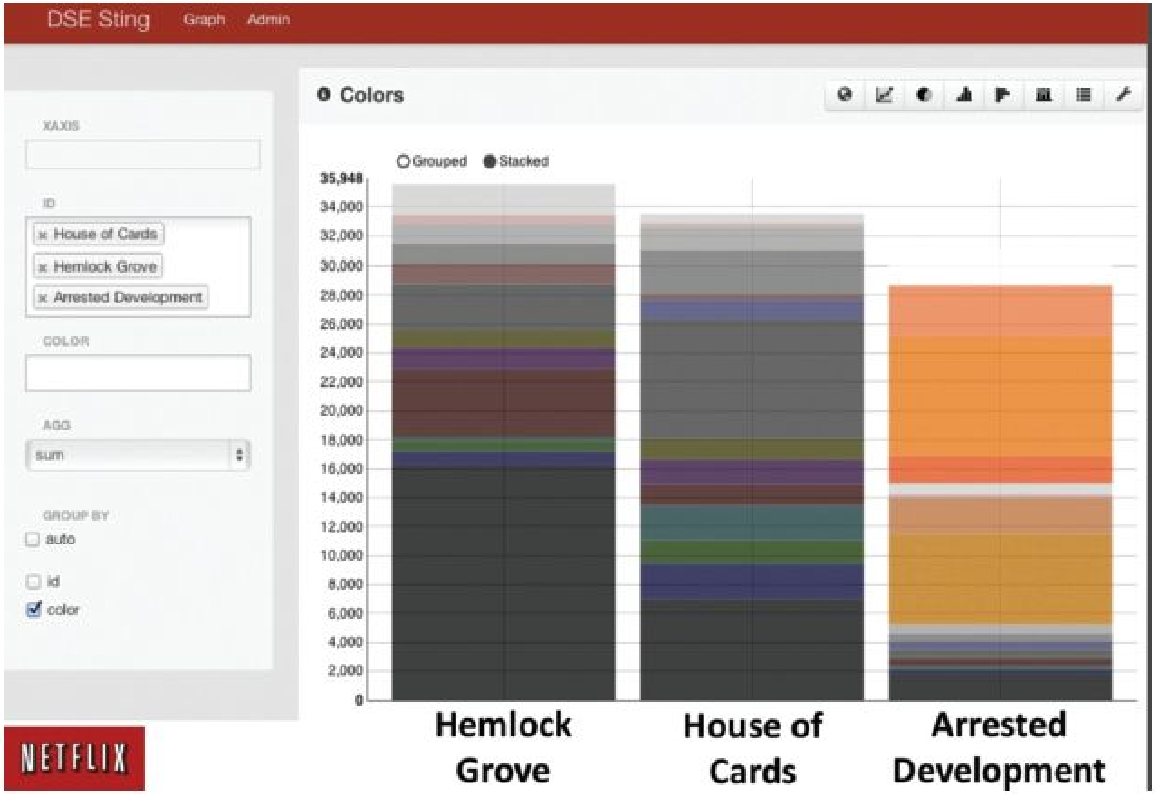
Does her abrupt destruction of faith invite greater instability, without a guide for how to be a professional skeptic? (hint: yes)


“Now I am become Death, the destroyer of worlds.”
J. Robert Oppenheimer, father of the atomic bomb, after witnessing the first test.
meme StevePiper.net
Cathy O'Neil at TED2017
The era of blind faith in big data must end

https://twitter.com/Abebab/status/902531251852251136

HEY CATHY: NetFlix NOT Good Example of Safe AI

1. Data accessible, easy to discover, and easy to process for ***everyone***
2. Whether large or small, able to ***visualize***
3. The longer to find data, less ***value***



XAXIS

ID
× House of Cards
× Hemlock Grove
× Arrested Development

COLOR

AGG
sum

GROUP BY
☐ auto
☐ id
☑ color

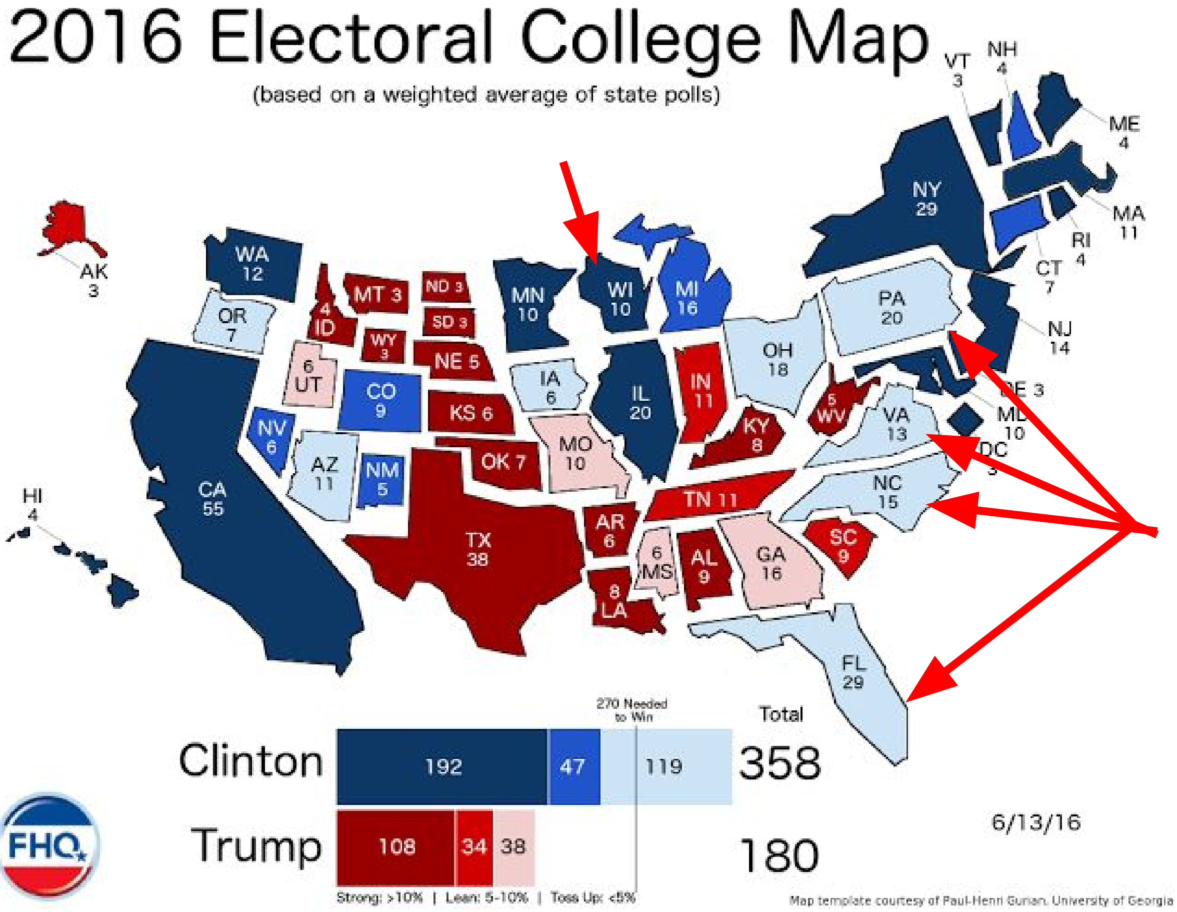
Figure 3.2 Detailed Color Comparison of *Hemlock Grove*, *House of Cards*, and *Arrested Development*
Source: Netflix Technology Blog (techblog.netflix.com)

https://www.wired.com/insights/2014/03/big-data-lessons-netflix/

Courts Manually Found GOP Guilty of Killing Votes

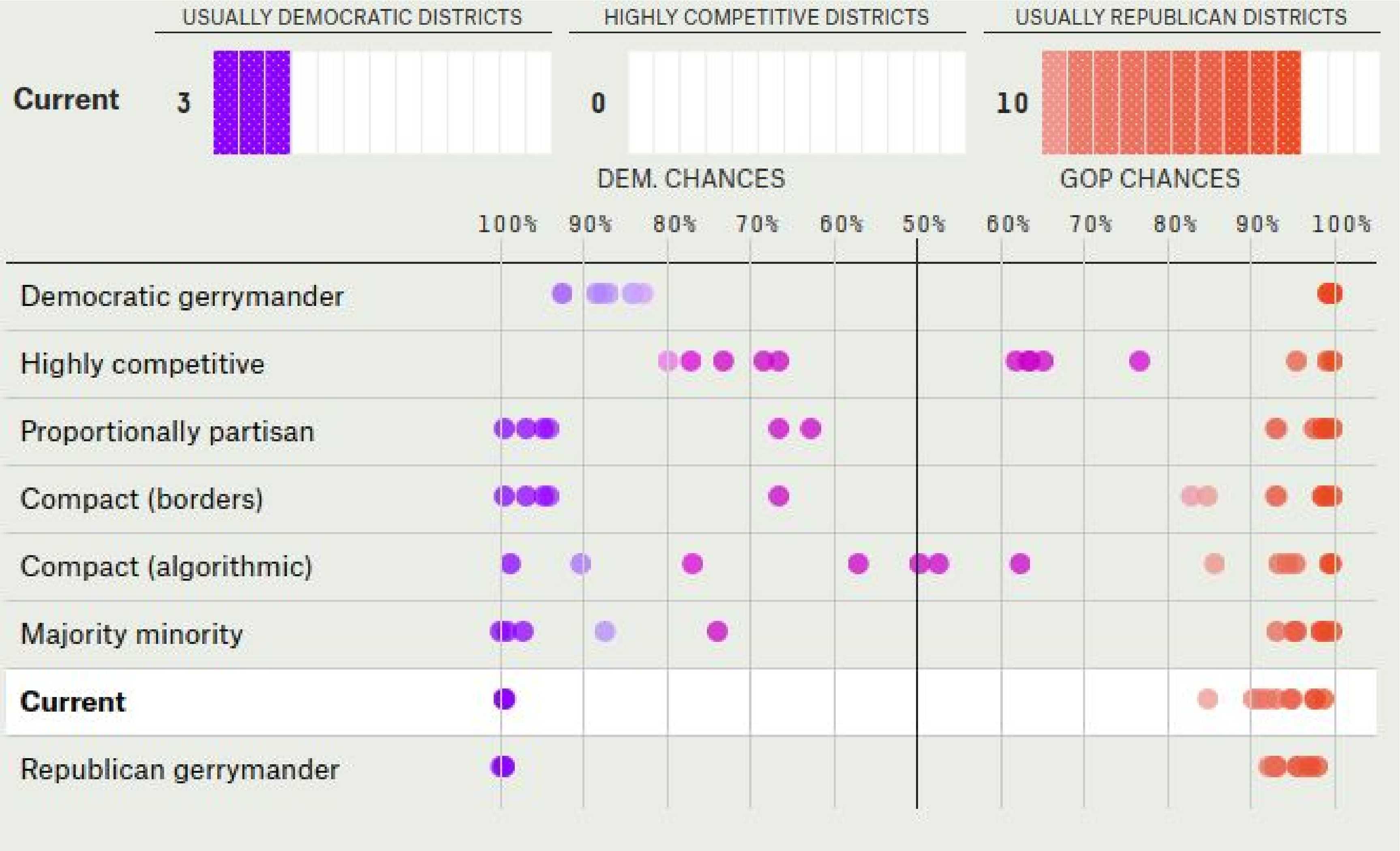
129 Electoral College Votes out of 270 Needed to Win (48%)

- **TX - 34**
- **FL - 27**
- **PA - 21**
- **NC - 15**
- **VA - 13**
- **WI - 10**
- **AL - 9**



https://frontloading.blogspot.com/2016/06/the-electoral-college-map-61316.html

Machines Reveal Pervasive GOP Gerrymandering



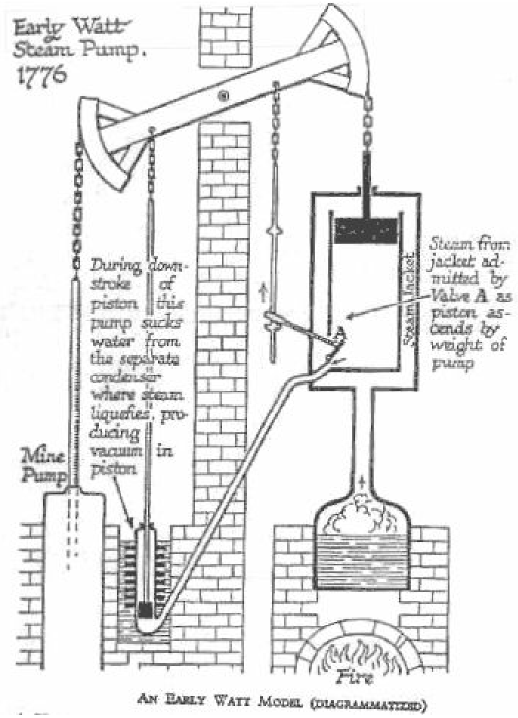
https://projects.fivethirtyeight.com/redistricting-maps/north-carolina/

History Time: Let’s Not Repeat Errors of Past

Automation Machines...The “Gilded Age” of 1880s

1. Piston Engine:

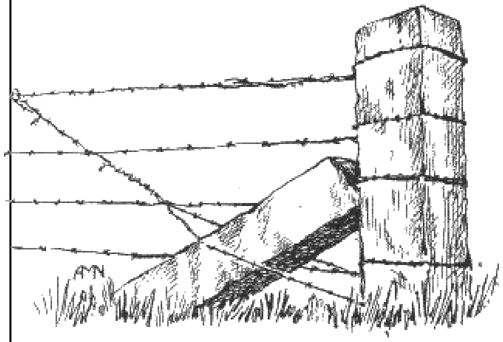
Horsepower


Early Watt Steam Pump. 1776
During down-stroke of piston this pump sucks water from the separate condenser where steam liquefies, producing vacuum in piston
Mine Pump
Steam Jacket
Steam from jacket admitted by Valve A as piston ascends by weight of pump
Fire

An Early Watt Model (diagrammatized)

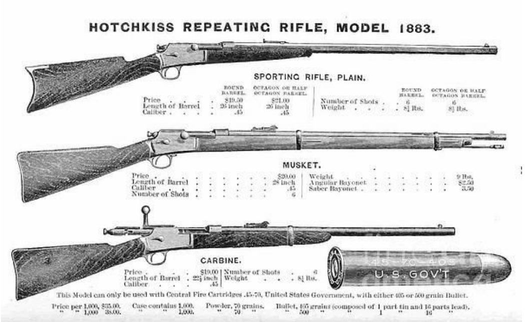
2. Barbed Wire:

Asset Management



3. Repeat Rifle:

Law and Order



HOTCHKISS REPEATING RIFLE, MODEL 1883.

SPORTING RIFLE, PLAIN.

	ROUND BARREL.	OCTAGON OR HALF OCTAGON BARREL.
Price	$19.50	$21.00
Length of Barrel	26 inch	26 inch
Caliber	.45	.45
Number of Shots	6	6
Weight	8¼ lbs.	8¼ lbs.

MUSKET.

Price	$20.00
Length of Barrel	28 inch
Caliber	.45
Number of Shots	6
Weight	9 lbs.
Angular Bayonet	$2.50
Saber Bayonet	3.50

CARBINE.

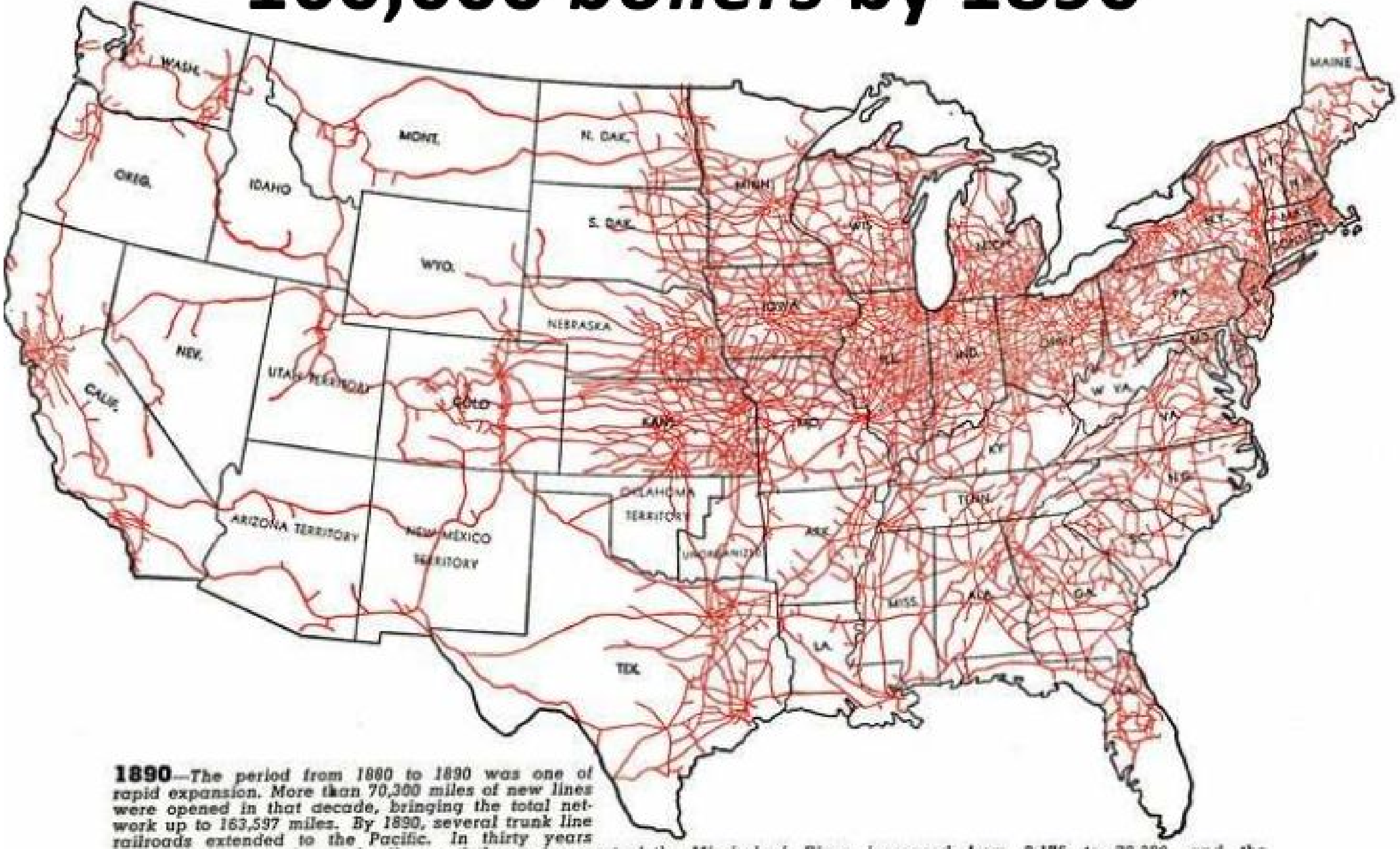
Price	$19.00
Length of Barrel	22½ inch
Caliber	.45
Number of Shots	6
Weight	8¼ lbs.

This Model can only be used with Central Fire Cartridges .45-70, United States Government, with either 405 or 500 grain Bullet.

Price per 1,000, $35.00. Case contains 1,000. Powder, 70 grains. Bullet, 405 grains (composed of 1 part tin and 16 parts lead).
" " 1,000 38.00. " " 1,000. " 70 " " 500 " " 1 " 16 "

1) Piston Engine Gives...Horsepower

100,000 *boilers* by 1890



1890—*The period from 1880 to 1890 was one of rapid expansion. More than 70,300 miles of new lines were opened in that decade, bringing the total network up to 163,597 miles. By 1890, several trunk line railroads extended to the Pacific. In thirty years from 1860 to 1890, the total mileage of the region west of the Mississippi River increased from 2,175 to 72,389, and the population of that area increased fourfold.*

2) Barbed Wire Gives...Asset Management

Inexpensive galvanized telegraph wire and simple twist for barbs.

Vast labor force unnecessary suddenly with inexpensive method to divide and allocate land to control livestock movements.

3) Repeat Rifle Gives...Law and Order

> Maxim, an egomaniacal draft dodger, gave the world the first true automatic weapon (Patent No 3493 1883). Used by British in Colonial Africa and by Germans in WWI to ***turn earth into hell.*** Died proud.
>
> – C. J. Chivers

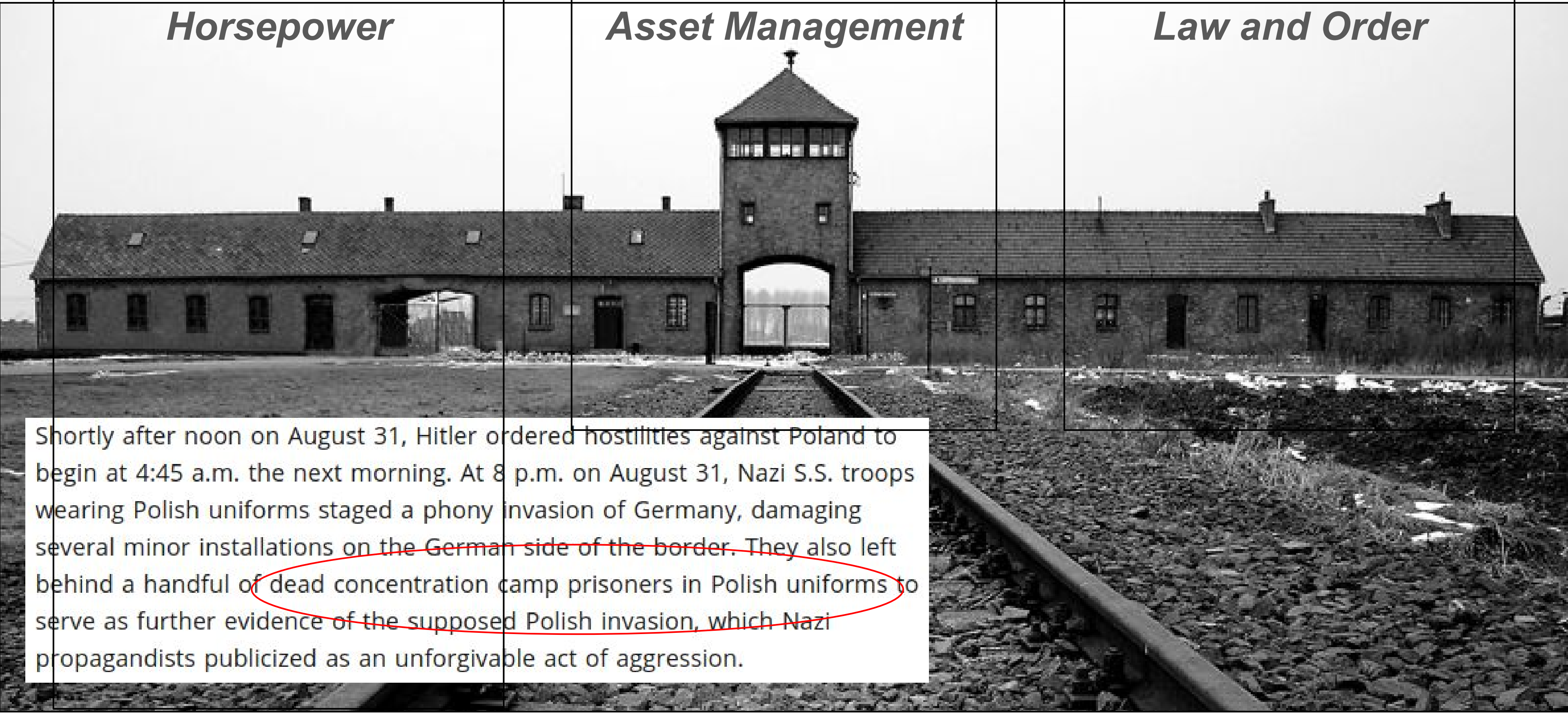
Never Forget: How/Why Automation Ends Here

INDUSTRIALIZED GENOCIDE IN DISGUISE

1. Piston Engine:
Horsepower

2. Barbed Wire:
Asset Management

3. Repeat Rifle:
Law and Order



Shortly after noon on August 31, Hitler ordered hostilities against Poland to begin at 4:45 a.m. the next morning. At 8 p.m. on August 31, Nazi S.S. troops wearing Polish uniforms staged a phony invasion of Germany, damaging several minor installations on the German side of the border. They also left behind a handful of dead concentration camp prisoners in Polish uniforms to serve as further evidence of the supposed Polish invasion, which Nazi propagandists publicized as an unforgivable act of aggression.

https://www.history.com/this-day-in-history/germans-invade-poland

Are Driverless Cars Just Disguised Private Missiles?

TESLA WAITED NINE DAYS TO REPORT INCIDENT TO SAFETY REGULATORS

"...continue to find parts of the car in their yard eight weeks after the crash"

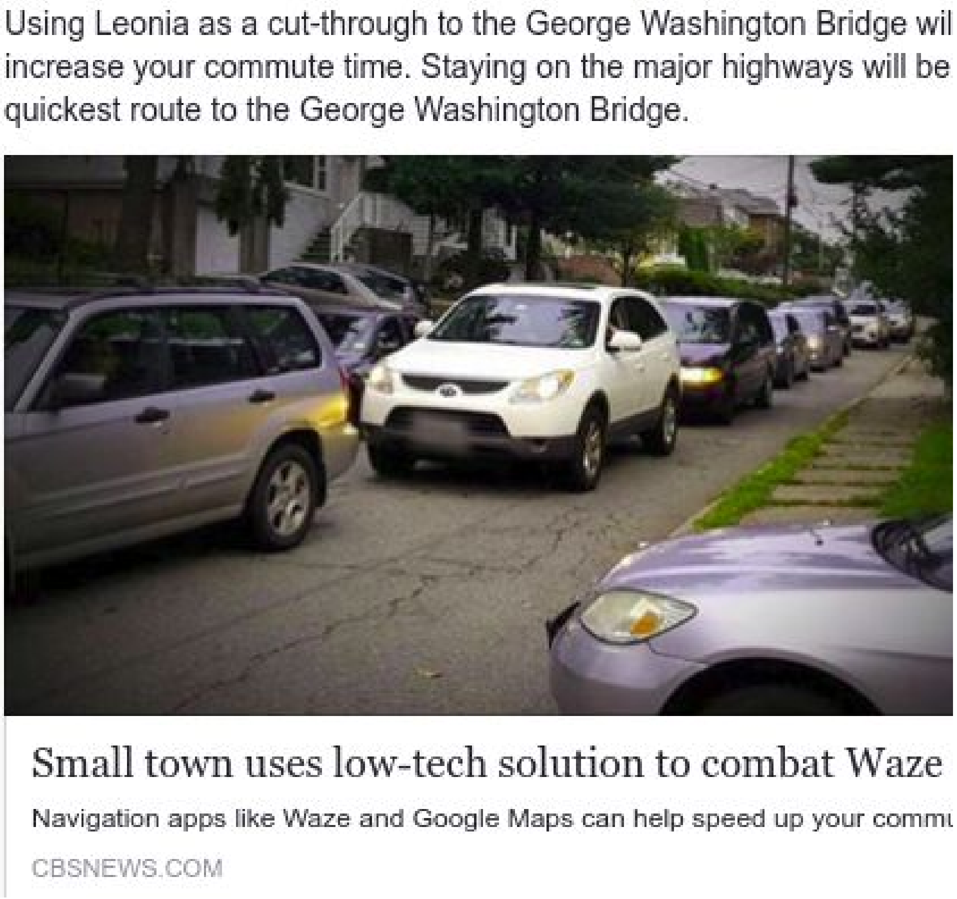
http://www.flyingpenguin.com/?p=22441

City Tires of Attack: Locals Combat Armored Drones

“Mayor Judah Zeigler said some streets get three times more traffic than the normal average.

‘We get about 4,000 vehicles that travel up the street that’s behind me on their way to the bridge,’ Zeigler said. ‘If the bridge is backed up we get about 12,000 vehicles that go up that street.”

Which Impacts Faster? Car Swarms or ICBMs



Using Leonia as a cut-through to the George Washington Bridge wil increase your commute time. Staying on the major highways will be quickest route to the George Washington Bridge.

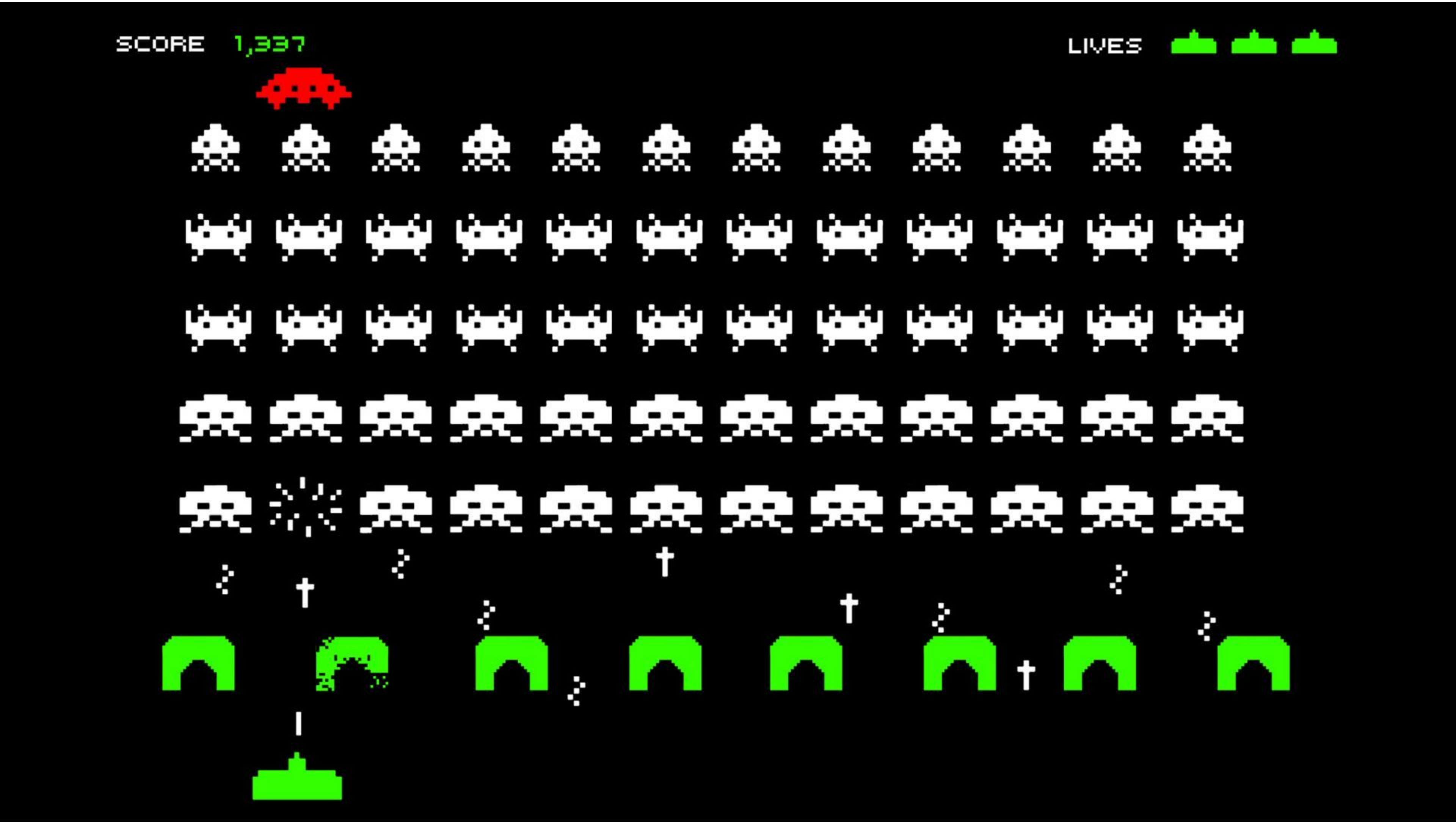
Small town uses low-tech solution to combat Waze

Navigation apps like Waze and Google Maps can help speed up your commu

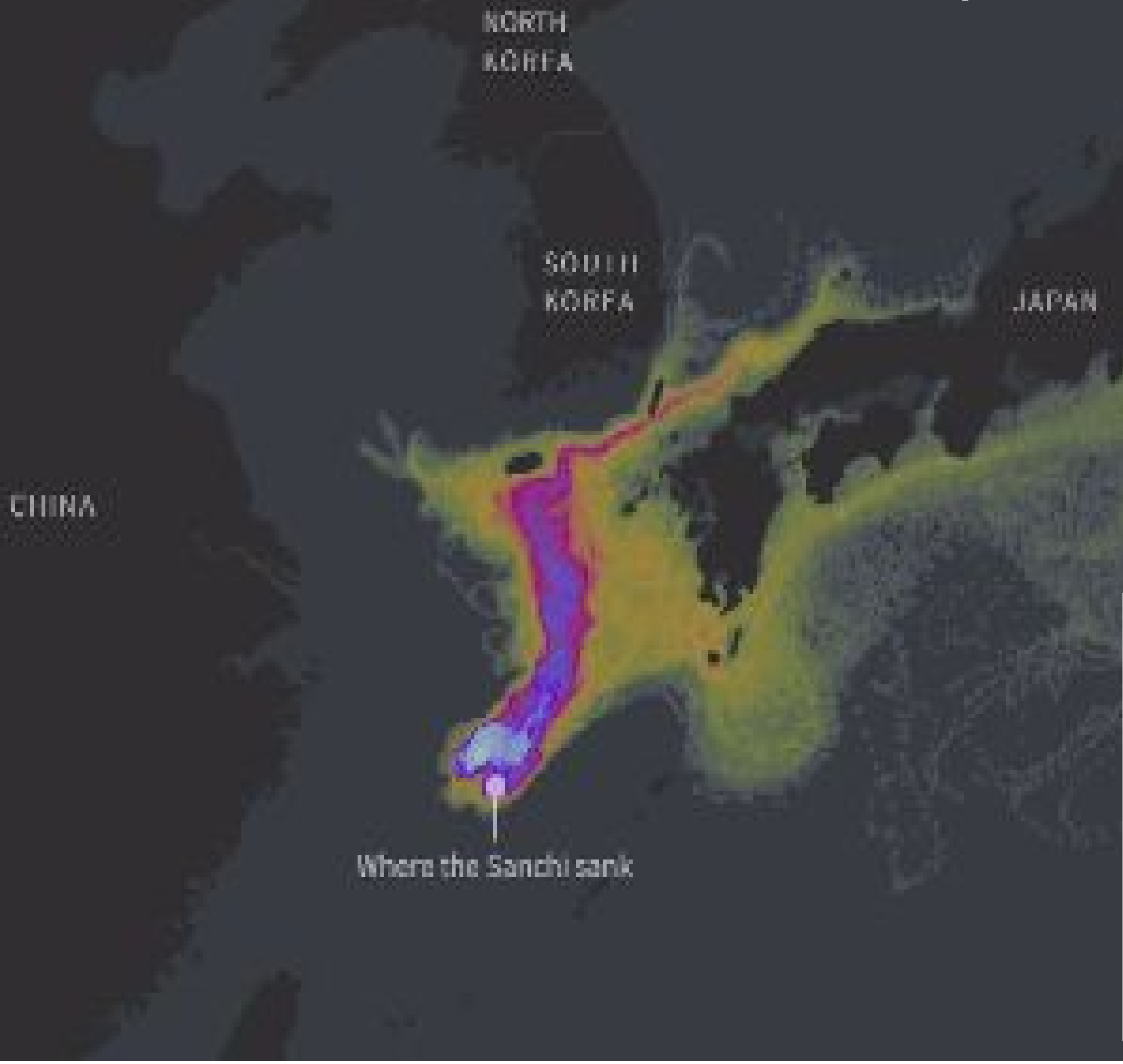
CBSNEWS.COM

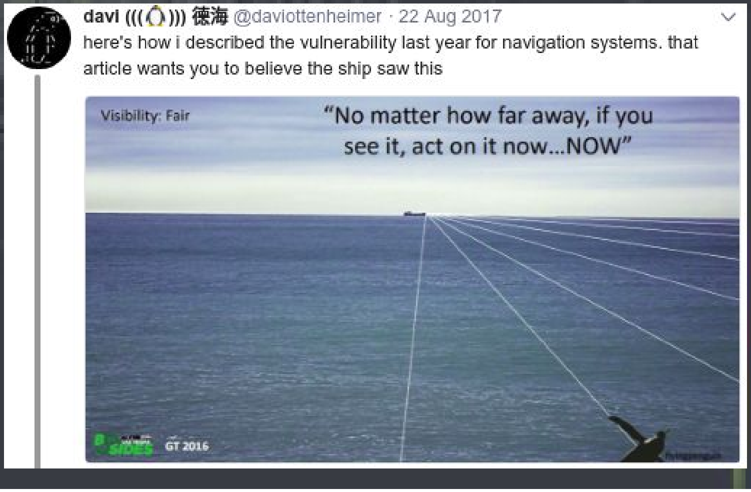
http://newyork.cbslocal.com/2018/01/22/leonia-gwb-traffic-ban/

"Waze Invaders"



Driverless Vehicles as Weapon of Mass Destruction




davi (((🐧))) 徳海 @daviottenheimer · 22 Aug 2017

here's how i described the vulnerability last year for navigation systems. that article wants you to believe the ship saw this

Visibility: Fair
"No matter how far away, if you see it, act on it now...NOW"
BSIDES
GT 2016

https://twitter.com/Reuters/status/957268697244229632
https://twitter.com/daviottenheimer/status/900065436506763265

4. can delegated automation agents (cyber soldiers) be trusted?

Compliance

A. standard-based ethical test

(value objective facts)

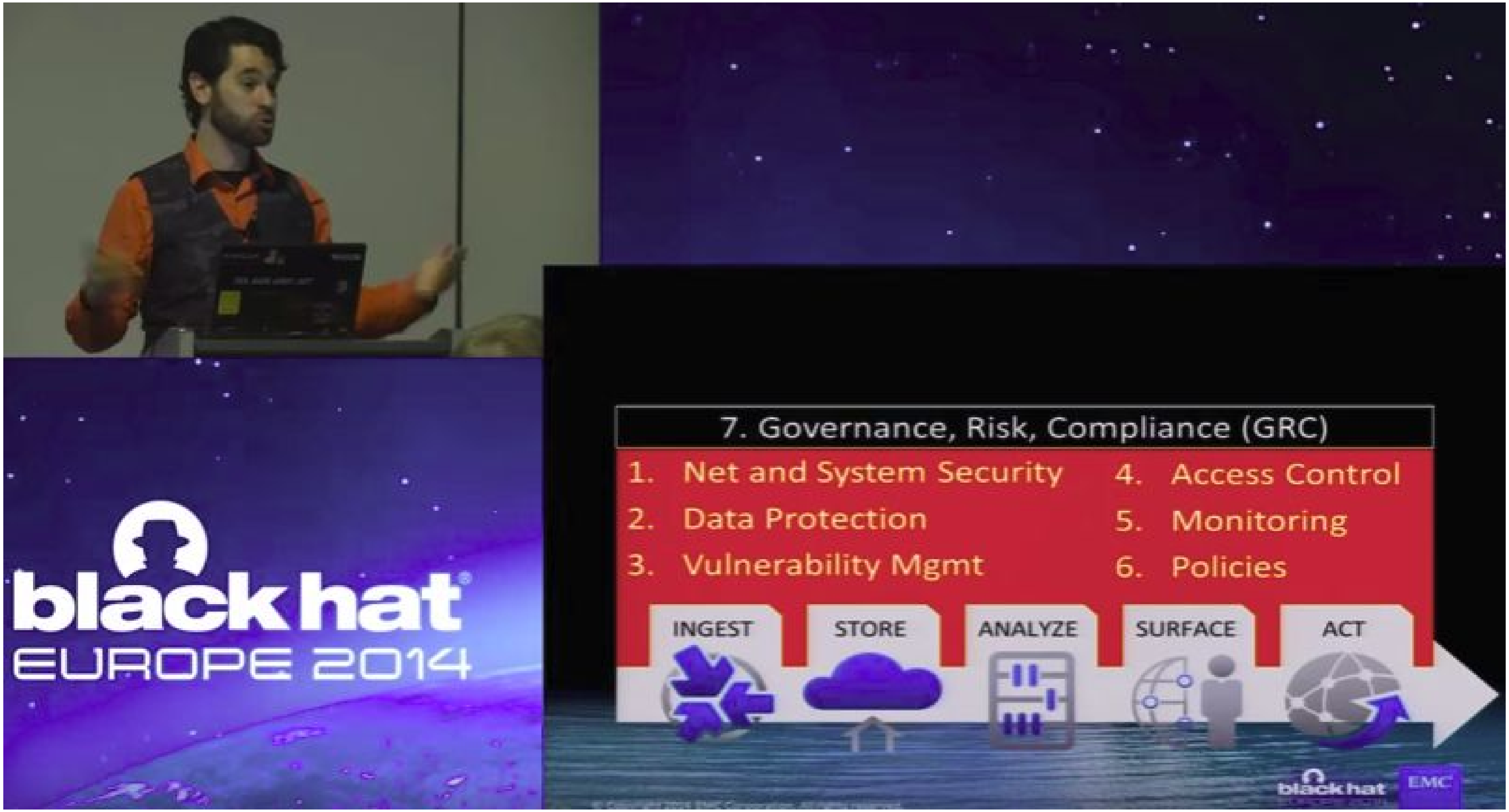
B. system transparency

(value getting consent)

Science

= reduced security breaches, and increased accountability

Formerly Step (7) in Reality of Securing Big Data



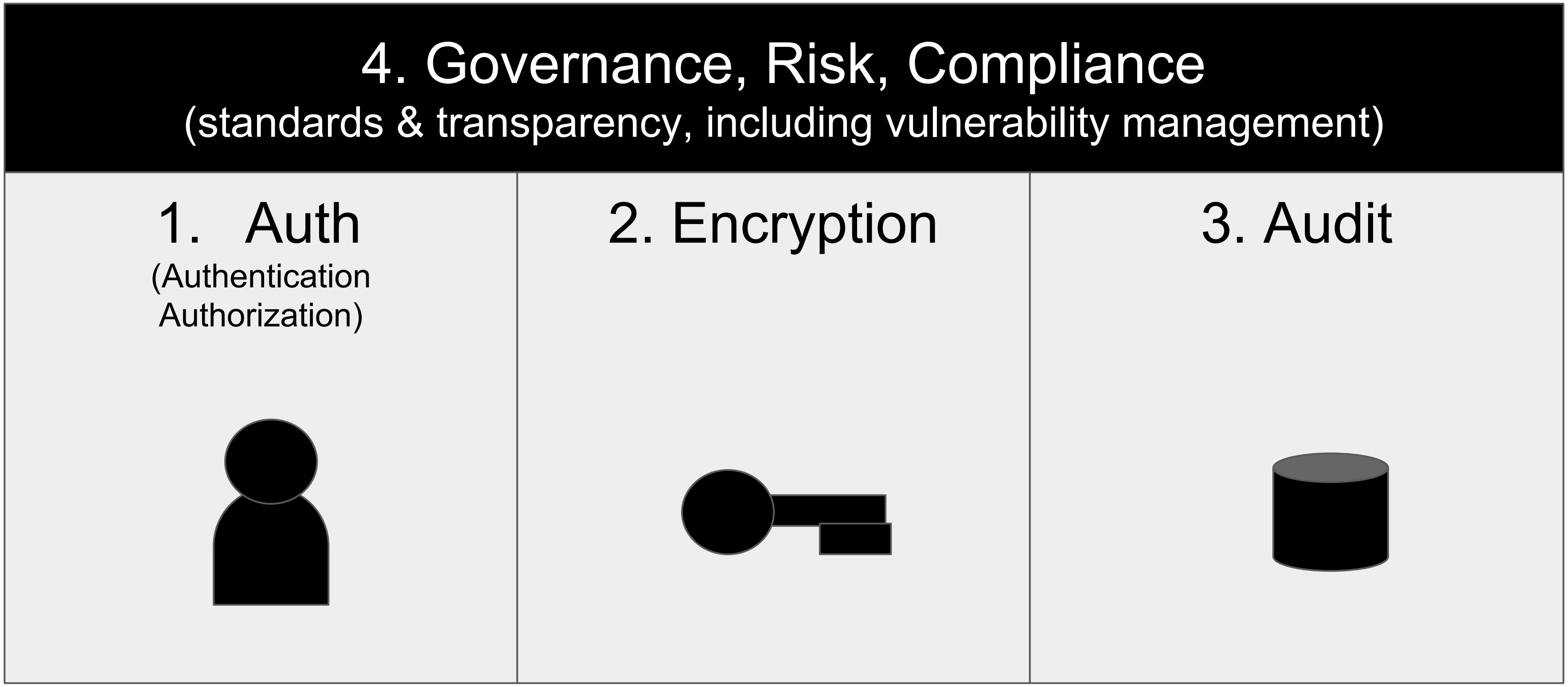
7. Governance, Risk, Compliance (GRC)

1. Net and System Security
2. Data Protection
3. Vulnerability Mgmt
4. Access Control
5. Monitoring
6. Policies

INGEST → STORE → ANALYZE → SURFACE → ACT

https://youtu.be/flUqDwVf6NQ

Now Step (4)

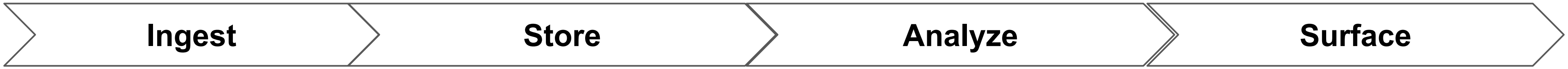


4. Governance, Risk, Compliance
(standards & transparency, including vulnerability management)

1. Auth
(Authentication
Authorization)

2. Encryption

3. Audit



Ingest

Store

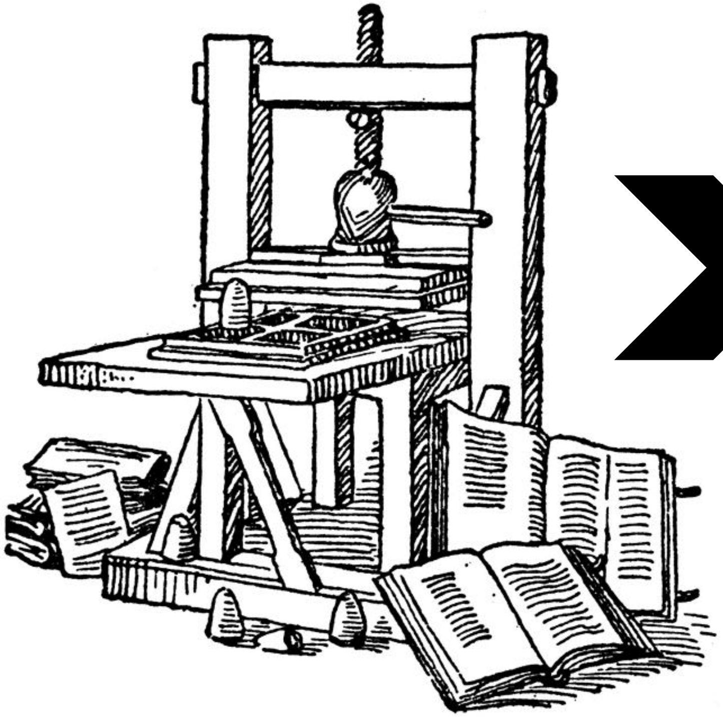
Analyze

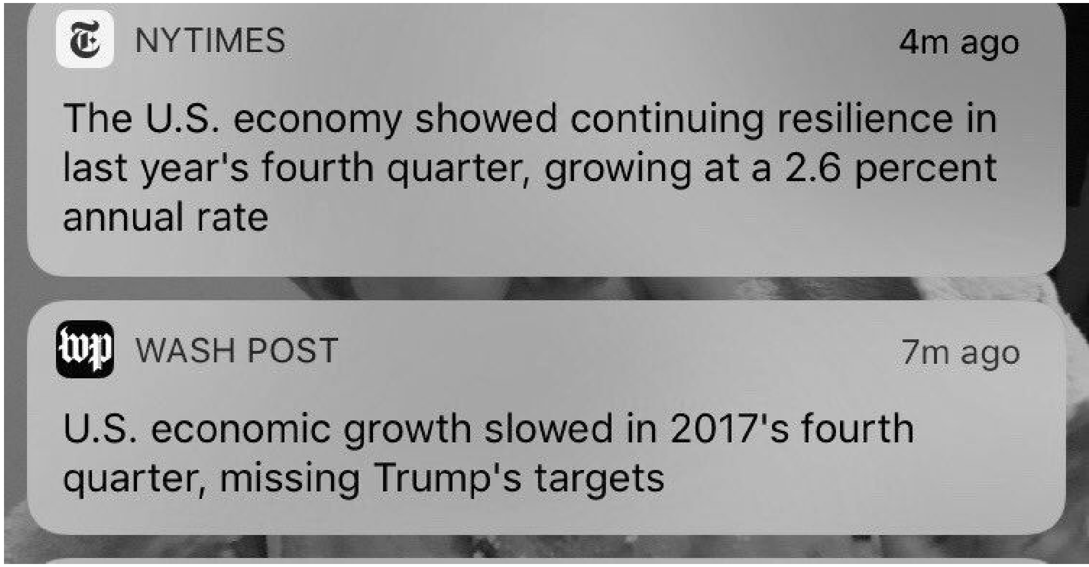
Surface

“New Tech” Challenges to GRC are Very Old Game

Don’t get too hooked on motives. Consider means / opportunity / **consequence (harm)** given commodity econ:

1. Is it more dangerous when “nation-state” gets into computers?
2. Is it more dangerous when “non-nation state” gets into drones?





NYTIMES 4m ago

The U.S. economy showed continuing resilience in last year's fourth quarter, growing at a 2.6 percent annual rate

WASH POST 7m ago

U.S. economic growth slowed in 2017's fourth quarter, missing Trump's targets

https://twitter.com/samstein/status/956885096480608256

I Think, Therefore I...Must Learn How to Avert Harm

Rene Descartes
(1596-1650)

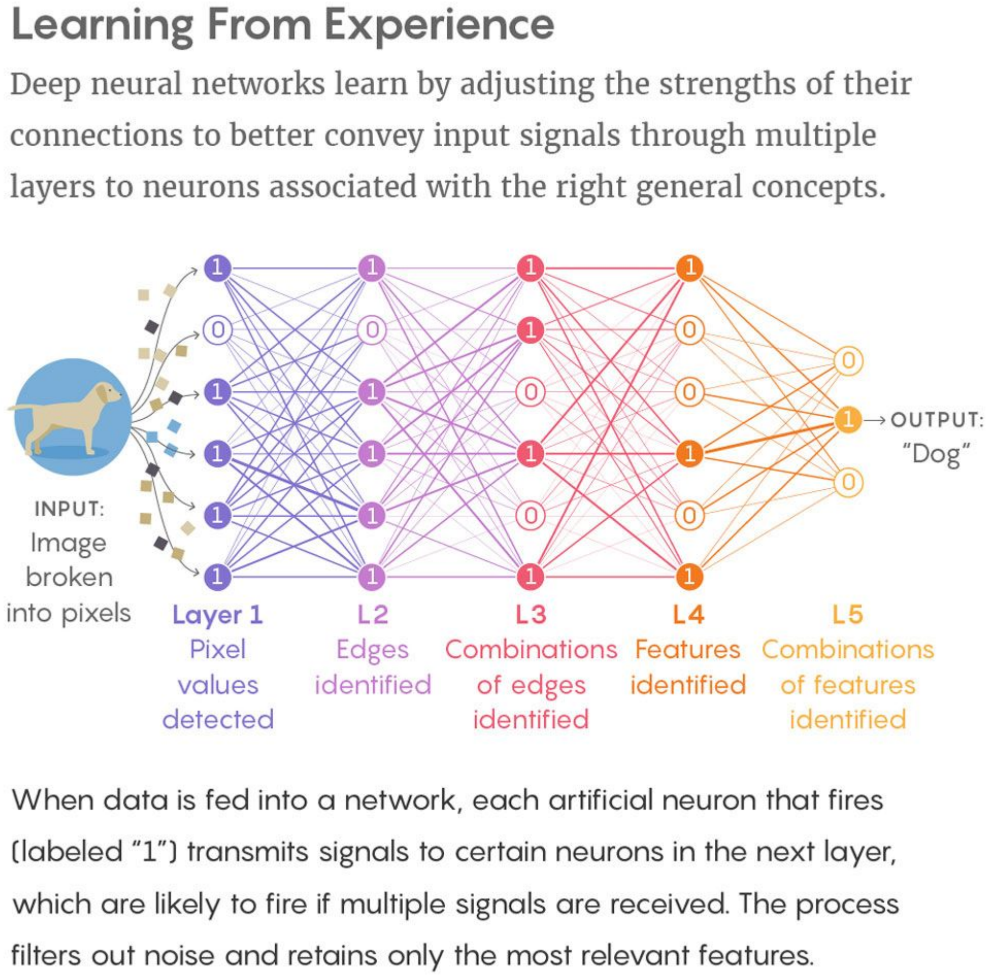
1637: 'Cogito, ergo sum'

John Locke
(1632-1704)

1693: Reflective Process, Articulated Steps

OWASP Open Web Application Security Project http://www.flyingpenguin.com/?p=22429 mongoDB.

Is it the Empiricism Era (1700s) of AI Yet?



Learning From Experience

Deep neural networks learn by adjusting the strengths of their connections to better convey input signals through multiple layers to neurons associated with the right general concepts.

When data is fed into a network, each artificial neuron that fires (labeled "1") transmits signals to certain neurons in the next layer, which are likely to fire if multiple signals are received. The process filters out noise and retains only the most relevant features.

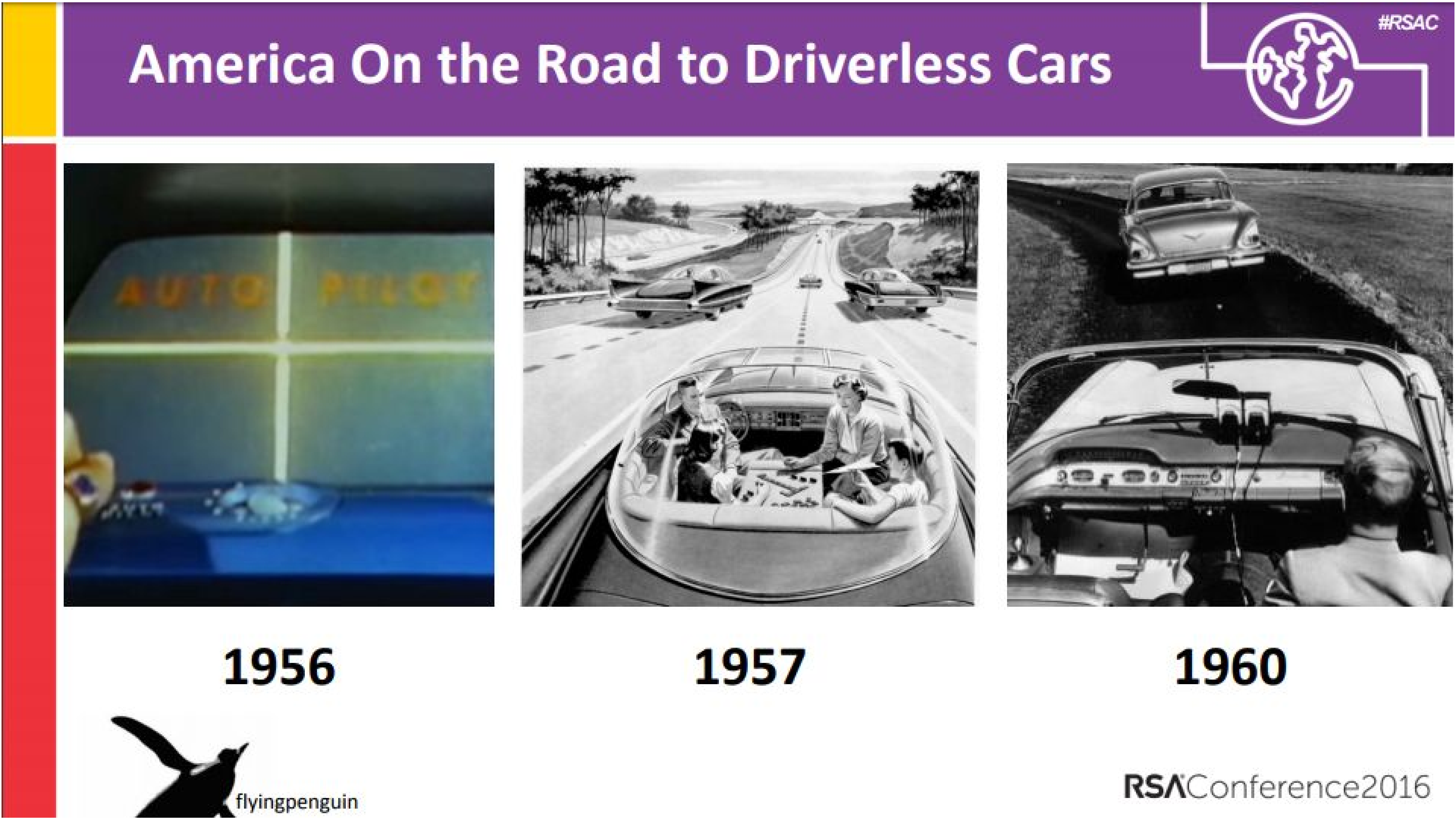
"The most important part of learning is forgetting [noise unnecessary to remember]"

David Hume

(1711-1776)

https://www.quantamagazine.org/new-theory-cracks-open-the-black-box-of-deep-learning-20170921/

2016 “Missile Crisis” Talk Explained Road Ahead



America On the Road to Driverless Cars

#RSAC

1956

1957

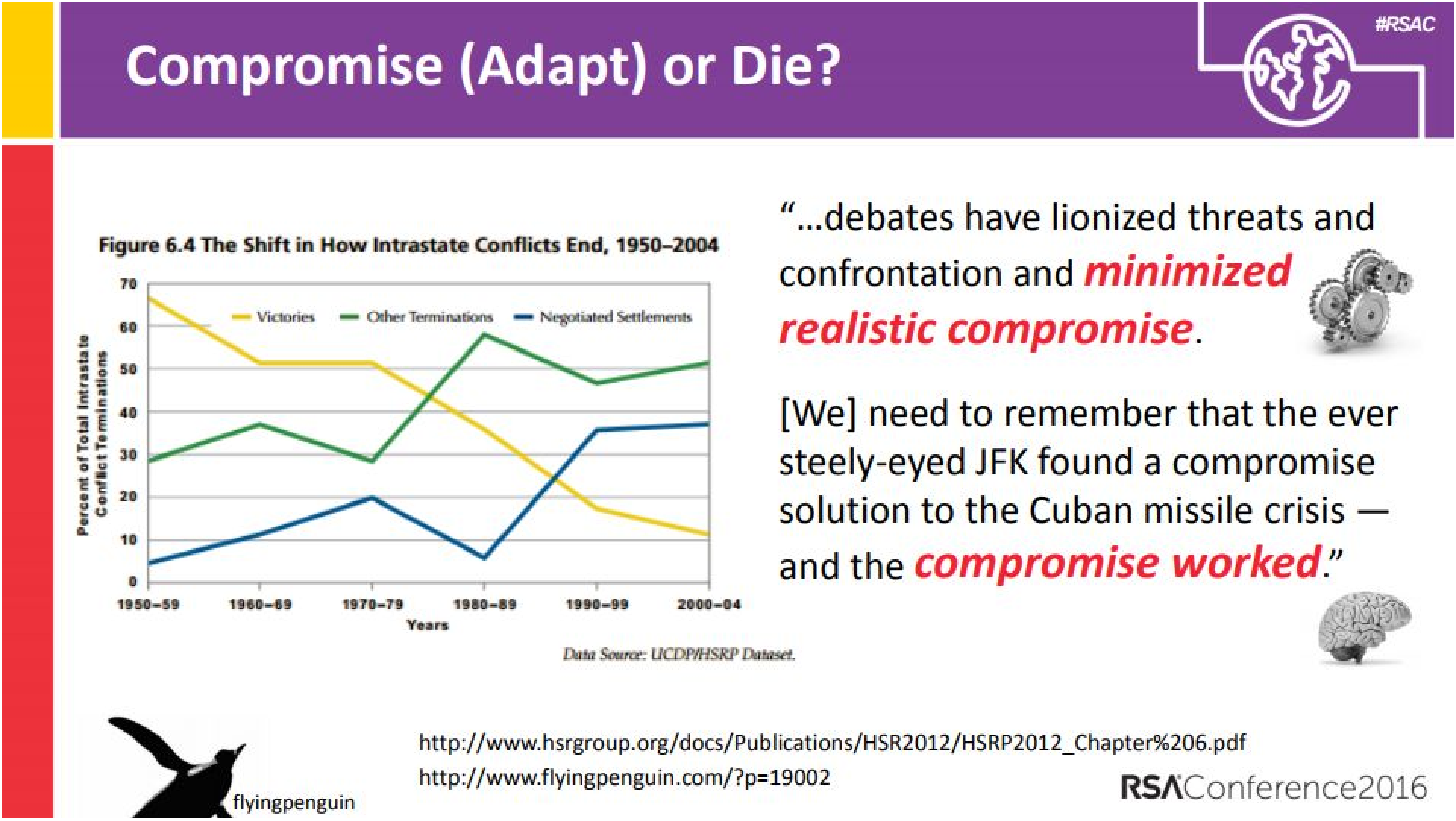
1960

flyingpenguin

RSAConference2016

https://www.youtube.com/watch?v=q9DEzqFW6jU

Experience (history) tells us self-interested (rational) behavior won't save us from automation holocaust



Compromise (Adapt) or Die?

Figure 6.4 The Shift in How Intrastate Conflicts End, 1950–2004

Data Source: UCDP/HSRP Dataset.

"...debates have lionized threats and confrontation and ***minimized realistic compromise***.

[We] need to remember that the ever steely-eyed JFK found a compromise solution to the Cuban missile crisis — and the ***compromise worked***."

http://www.hsrgroup.org/docs/Publications/HSR2012/HSRP2012_Chapter%206.pdf

http://www.flyingpenguin.com/?p=19002

https://www.youtube.com/watch?v=q9DEzqFW6jU

Newest Tech = Tax People Without Representation

“Acting in own interests against the public good”

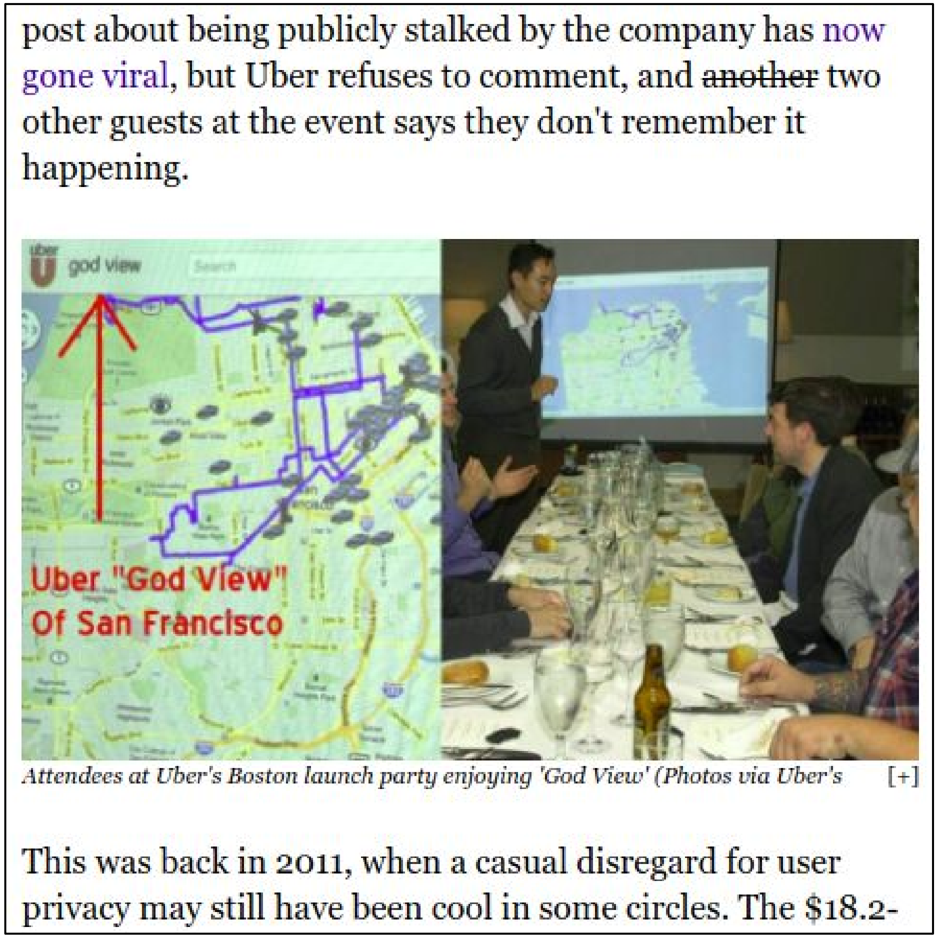
Governance, Risk, Compliance

1. Establishing Standards Based Testing: Users have right take/extract data *from* any platform

2. Transparency: Users have right to representation (safe from harm, opposite of blind) if algorithms extract value from them (taxation)

Newest Tech = Tax People Without Representation

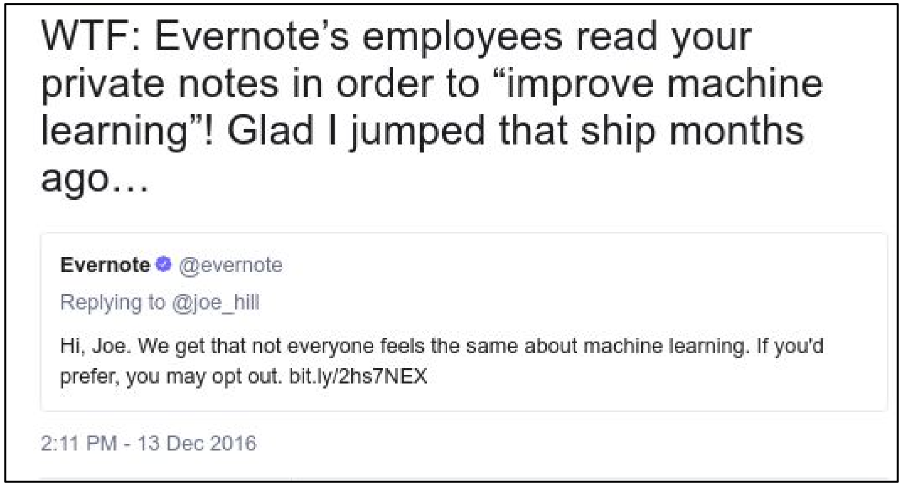
“Acting in own interests against the public good”



post about being publicly stalked by the company has now gone viral, but Uber refuses to comment, and ~~another~~ two other guests at the event says they don't remember it happening.

Attendees at Uber's Boston launch party enjoying 'God View' (Photos via Uber's [+]

This was back in 2011, when a casual disregard for user privacy may still have been cool in some circles. The $18.2-



WTF: Evernote’s employees read your private notes in order to “improve machine learning”! Glad I jumped that ship months ago…

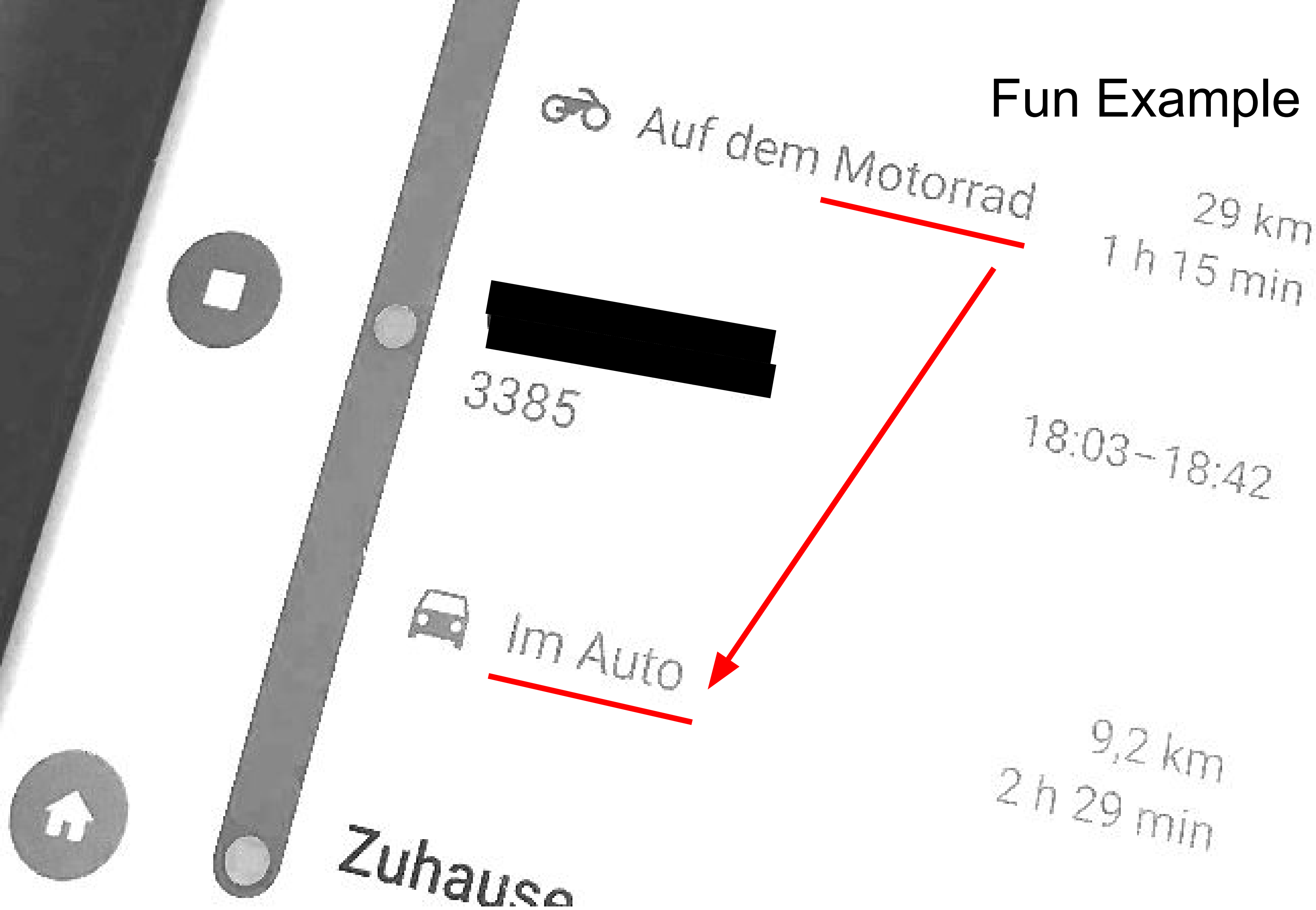
Evernote @evernote
Replying to @joe_hill

Hi, Joe. We get that not everyone feels the same about machine learning. If you'd prefer, you may opt out. bit.ly/2hs7NEX

2:11 PM - 13 Dec 2016

https://www.forbes.com/sites/kashmirhill/2014/10/03/god-view-uber-allegedly-stalked-users-for-party-goers-viewing-pleasure/
https://twitter.com/ragso/status/808796392747663364

Fun Example



Auf dem Motorrad

29 km

1 h 15 min

[redacted]

3385

18:03–18:42

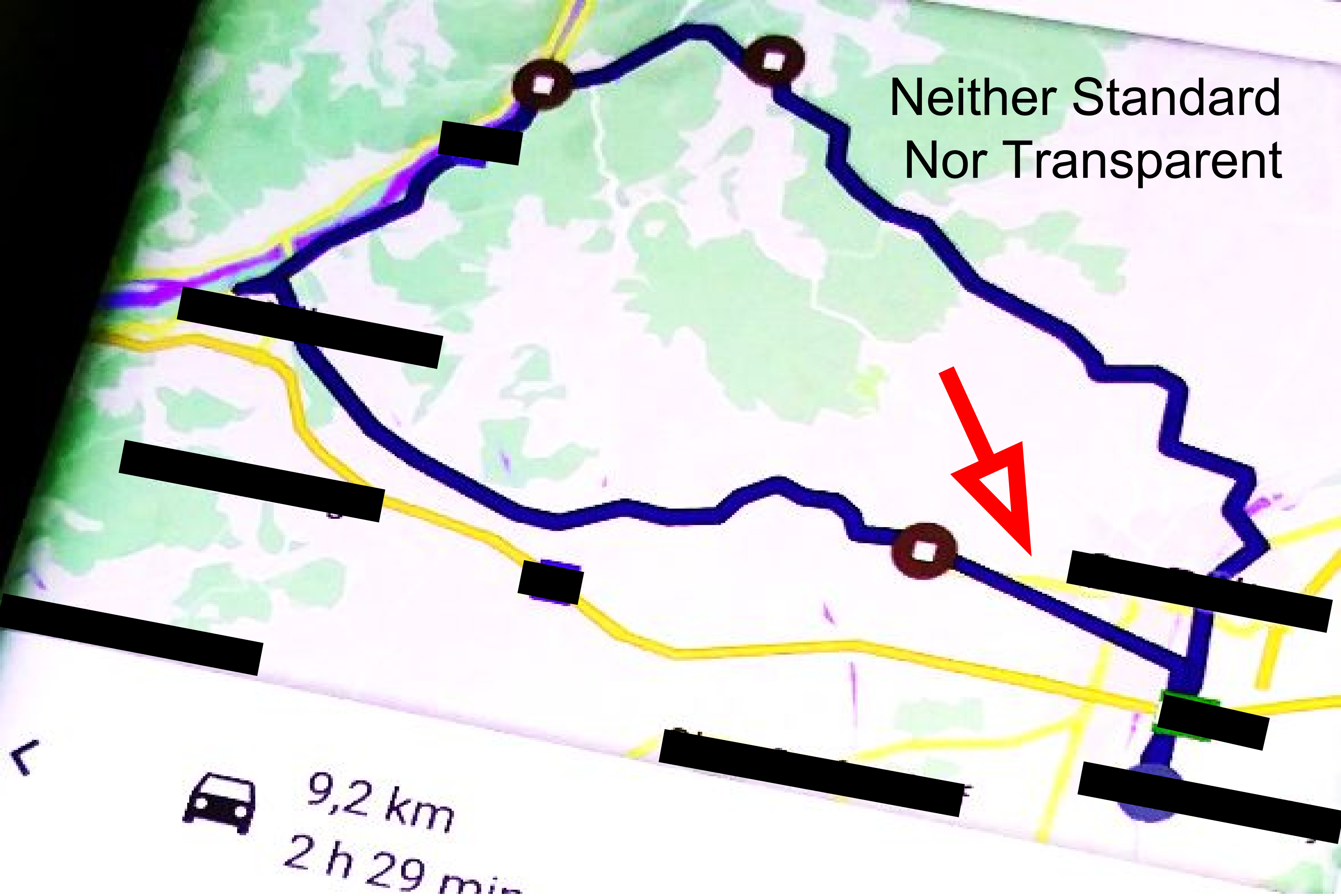
Im Auto

9,2 km

2 h 29 min

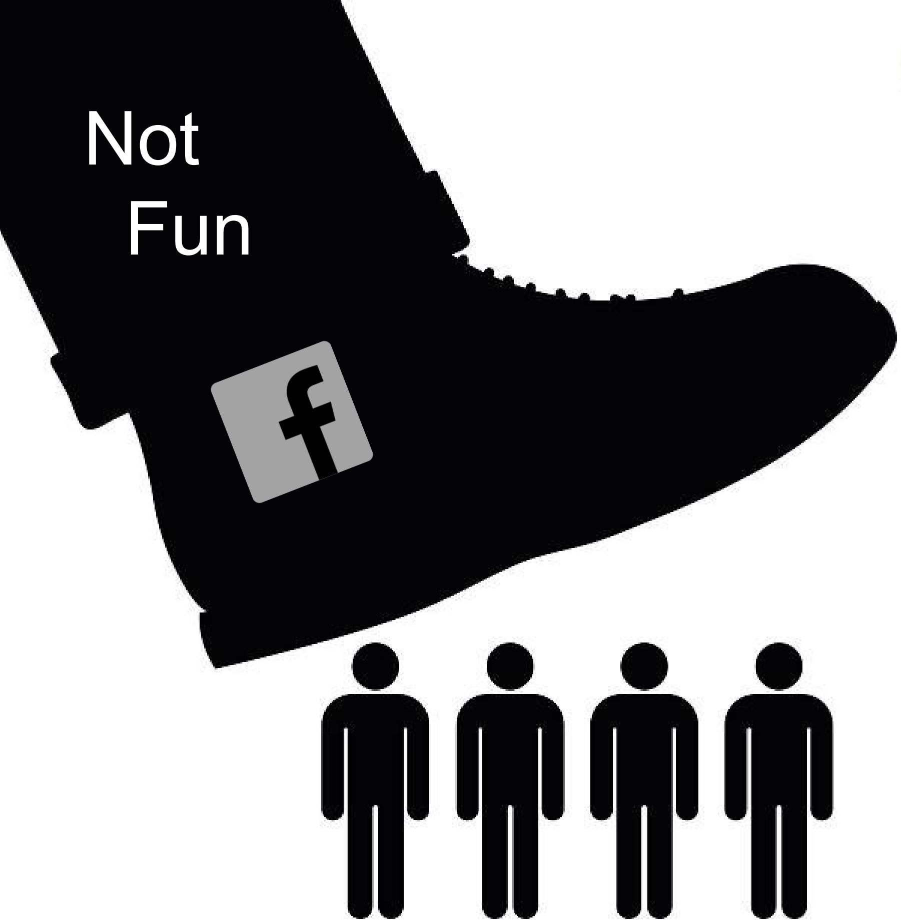
Zuhause

Neither Standard Nor Transparent



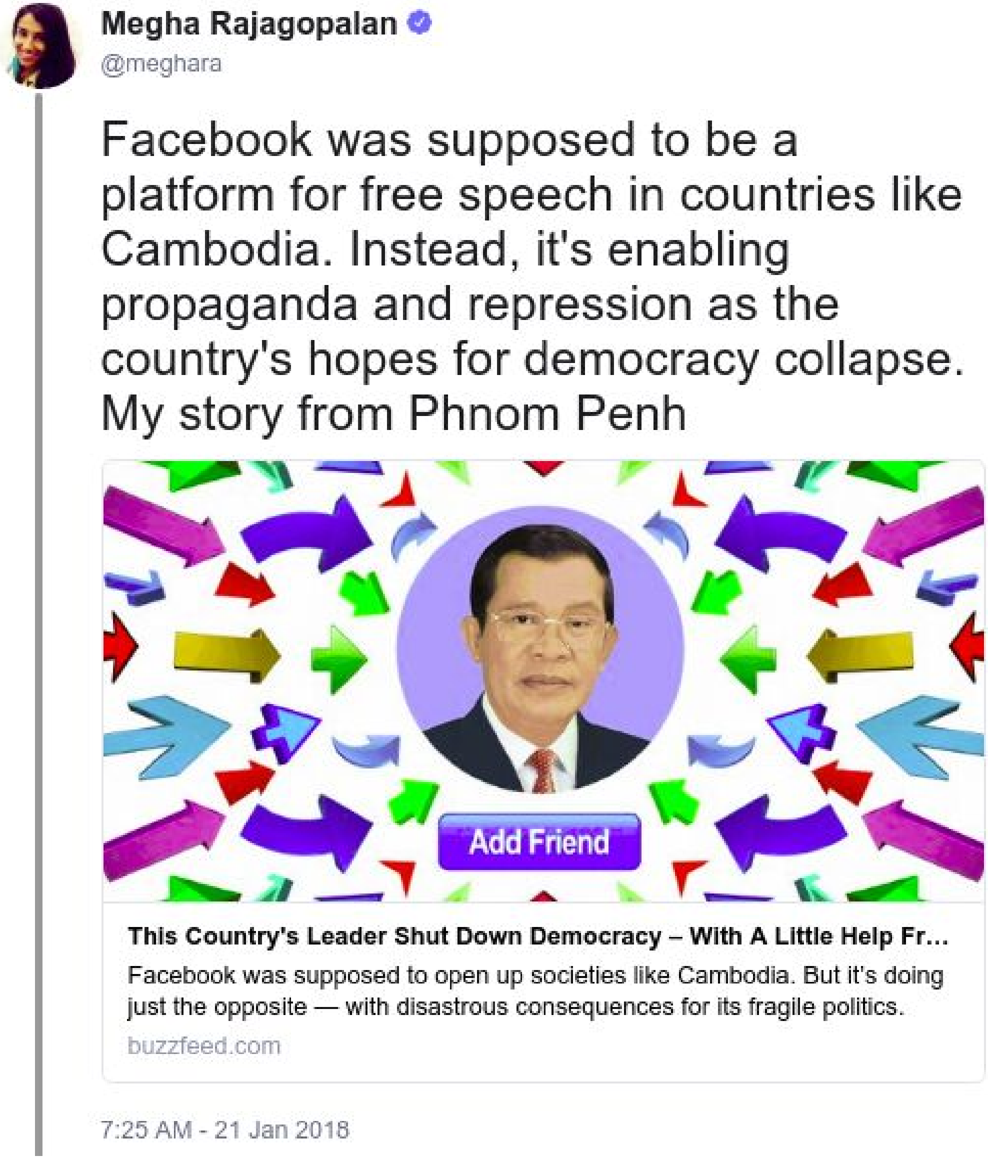
9,2 km

2 h 29 min



Not
Fun

Lack of Standards,
Lack of Transparency:
“Democracy Collapse”



Megha Rajagopalan
@meghara

Facebook was supposed to be a platform for free speech in countries like Cambodia. Instead, it's enabling propaganda and repression as the country's hopes for democracy collapse. My story from Phnom Penh

This Country's Leader Shut Down Democracy – With A Little Help Fr...
Facebook was supposed to open up societies like Cambodia. But it's doing just the opposite — with disastrous consequences for its fragile politics.
buzzfeed.com

7:25 AM - 21 Jan 2018

https://twitter.com/meghara/status/955099036259790854

CSO Failed to Disclose Massive Breach...AGAIN

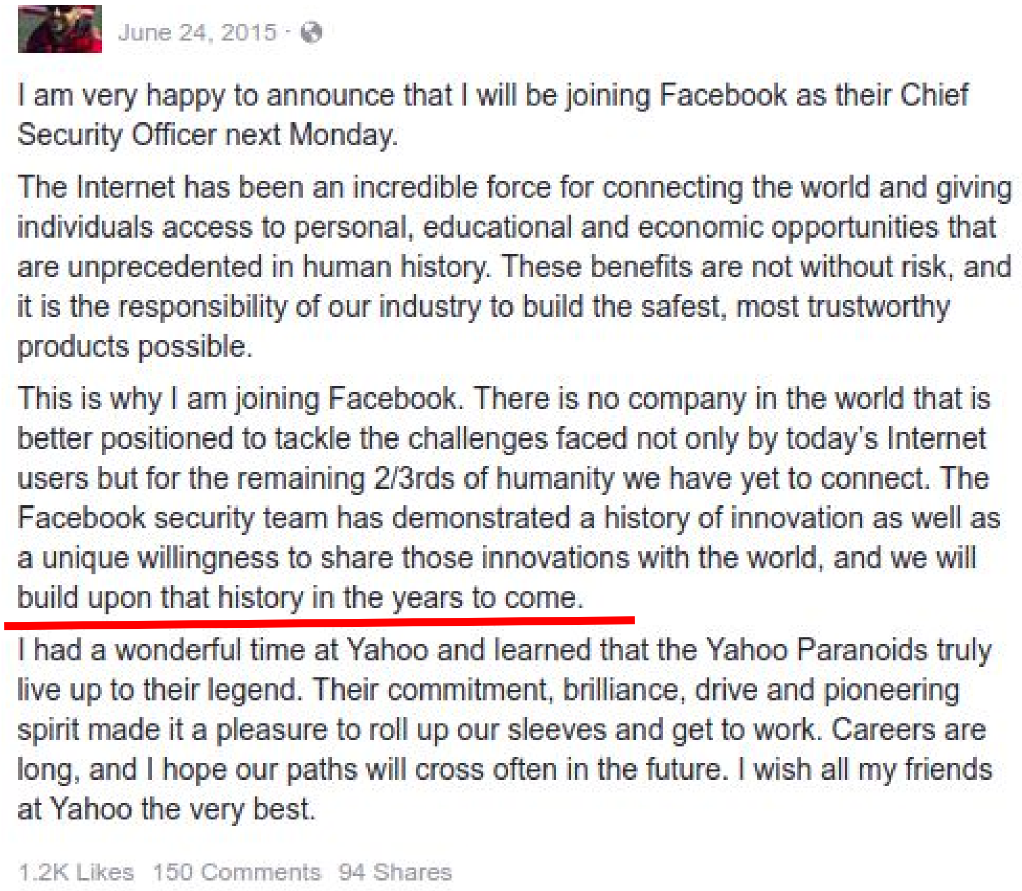
2015 Facebook

- Hire novice CSO from Yahoo
- RU Campaign Starts
- Receives external warnings (Ukraine) of RU Attacks

2016 CEO says no signs

2018 Senate Intelligence Committee Report

- 129 troll factory events
- 338,000 views
- 62,500 users confirm going



June 24, 2015 ·

I am very happy to announce that I will be joining Facebook as their Chief Security Officer next Monday.

The Internet has been an incredible force for connecting the world and giving individuals access to personal, educational and economic opportunities that are unprecedented in human history. These benefits are not without risk, and it is the responsibility of our industry to build the safest, most trustworthy products possible.

This is why I am joining Facebook. There is no company in the world that is better positioned to tackle the challenges faced not only by today's Internet users but for the remaining 2/3rds of humanity we have yet to connect. The Facebook security team has demonstrated a history of innovation as well as a unique willingness to share those innovations with the world, and we will build upon that history in the years to come.

I had a wonderful time at Yahoo and learned that the Yahoo Paranoids truly live up to their legend. Their commitment, brilliance, drive and pioneering spirit made it a pleasure to roll up our sleeves and get to work. Careers are long, and I hope our paths will cross often in the future. I wish all my friends at Yahoo the very best.

1.2K Likes 150 Comments 94 Shares

https://www.washingtonpost.com/news/the-switch/wp/2018/01/25/russians-got-tens-of-thousands-of-americans-to-rsvp-for-their-phony-political-events-on-facebook/

Do You See a Reflective Process, Articulated Steps?

"I write articles arguing that banning bump stocks, which enable semi-automatic guns to fire more rapidly, won't prevent mass shootings and that the left skews statistics. I believe the opposite to be true. I vehemently disagree with what I write…**contributing to an atmosphere of hatred...pays well**."

1) Automatic gun = potential to save lives
2) ???
3) Profit!

https://www.theguardian.com/lifeandstyle/2018/jan/26/experience-i-write-fake-news

AI Researchers Like to Say: "Explainability" of Learning

1) Automatic auto has potential to save lives
2) ???
3) Profit!

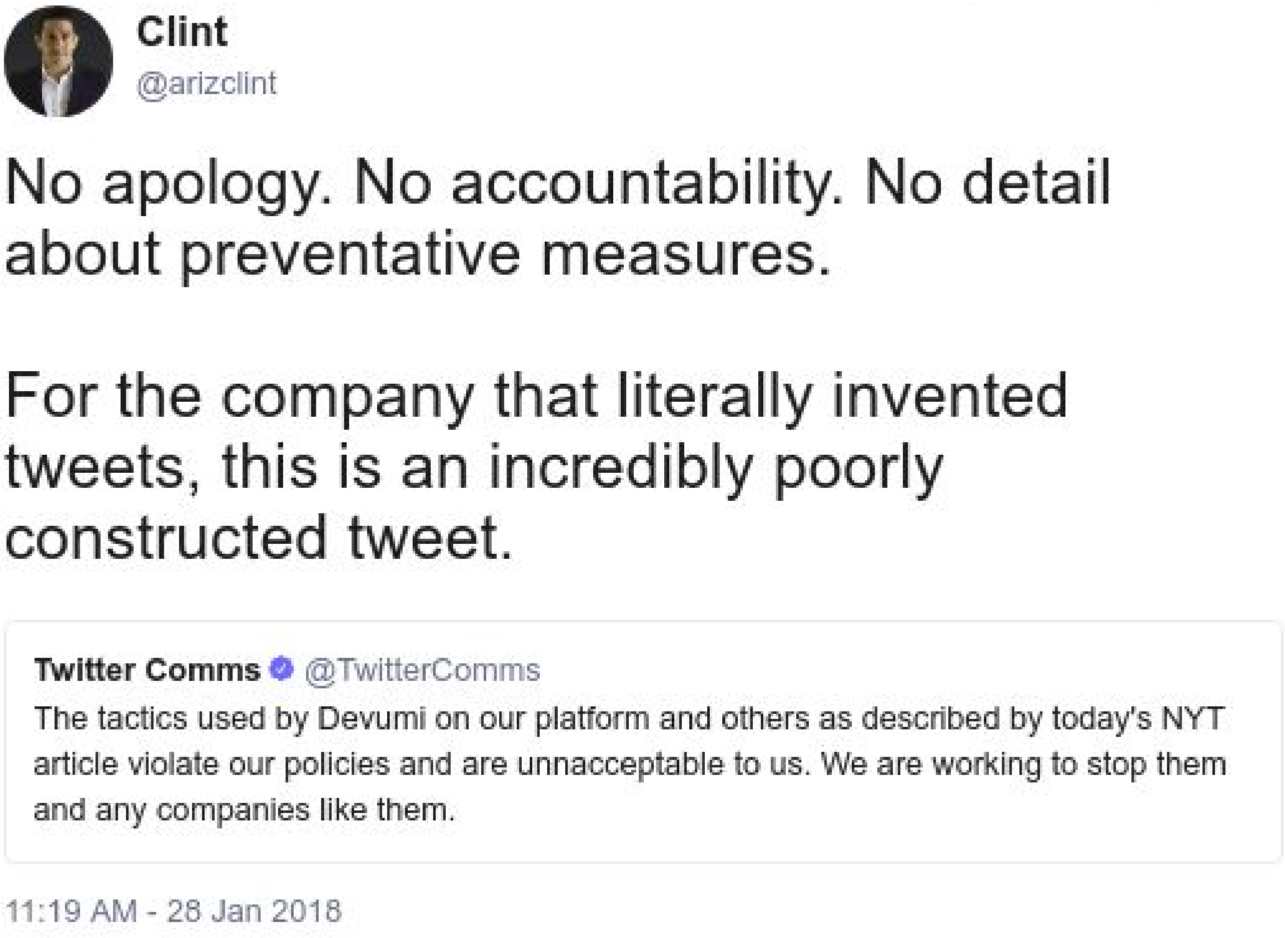
Decompose decisions into sub-decisions then organize into hierarchy of concepts to weigh decisions, and see how chosen.

Given Car drove below a trailer between wheels, the *most lethal* decision possible:

- Did AI merge right because simple algo avoidance (moving bridge)?
- Did AI not hit brakes because "good enough" engineering means decapitated human?

http://money.cnn.com/2016/07/28/technology/elon-musk-tesla-autopilot/index.html

A CSO “Working to Stop Them” is not Transparency



Clint
@arizclint

No apology. No accountability. No detail about preventative measures.

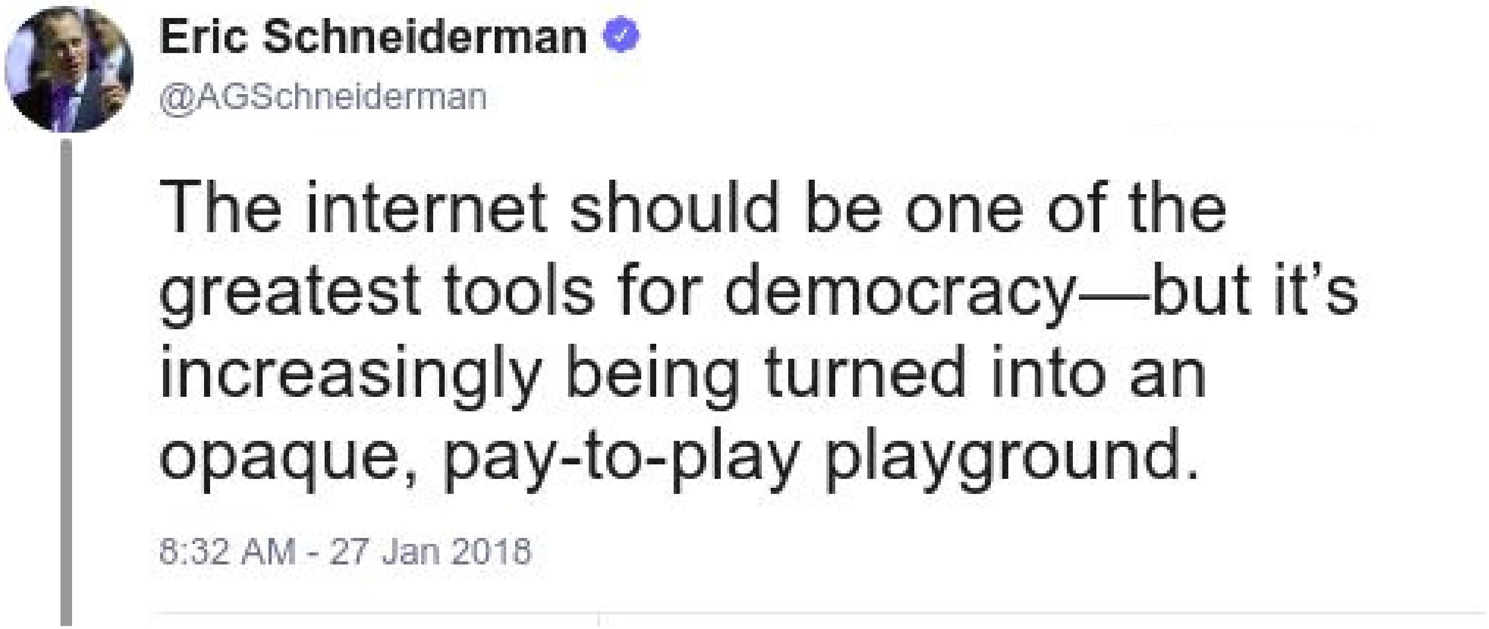
For the company that literally invented tweets, this is an incredibly poorly constructed tweet.

Twitter Comms @TwitterComms
The tactics used by Devumi on our platform and others as described by today's NYT article violate our policies and are unnacceptable to us. We are working to stop them and any companies like them.

11:19 AM - 28 Jan 2018

https://twitter.com/arizclint/status/957694570074030080

A CSO Opaque Playground is not Transparency



Eric Schneiderman
@AGSchneiderman

The internet should be one of the greatest tools for democracy—but it's increasingly being turned into an opaque, pay-to-play playground.

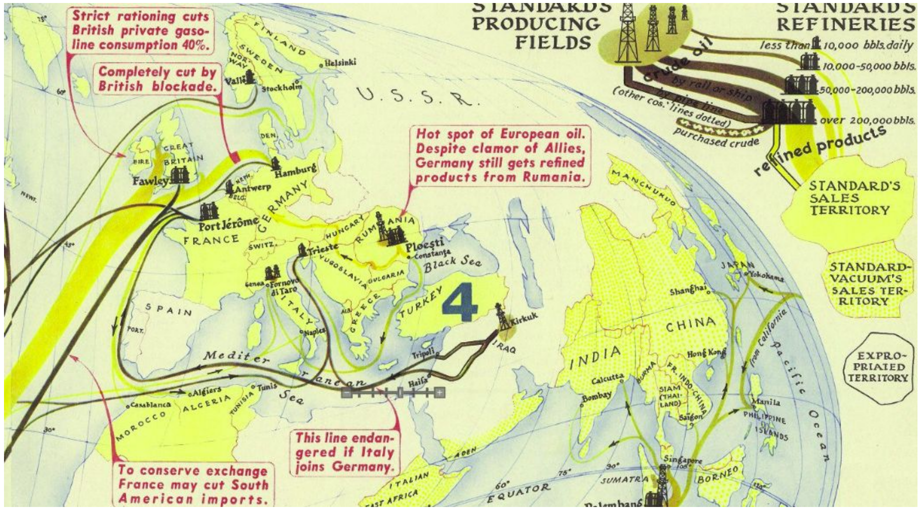
8:32 AM - 27 Jan 2018

https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html
https://twitter.com/AGSchneiderman/status/957290102715281408

Culpability of Executives Remaining Neutral While Watching Abuse on Their Platform

“We at Facebook Were Too Slow to Recognize”

“Russian posters had created 80,000 Facebook posts which had reached 126 million people in the US over a two-year period. [...] We at Facebook were far too slow to recognise how bad actors were abusing our platform.”

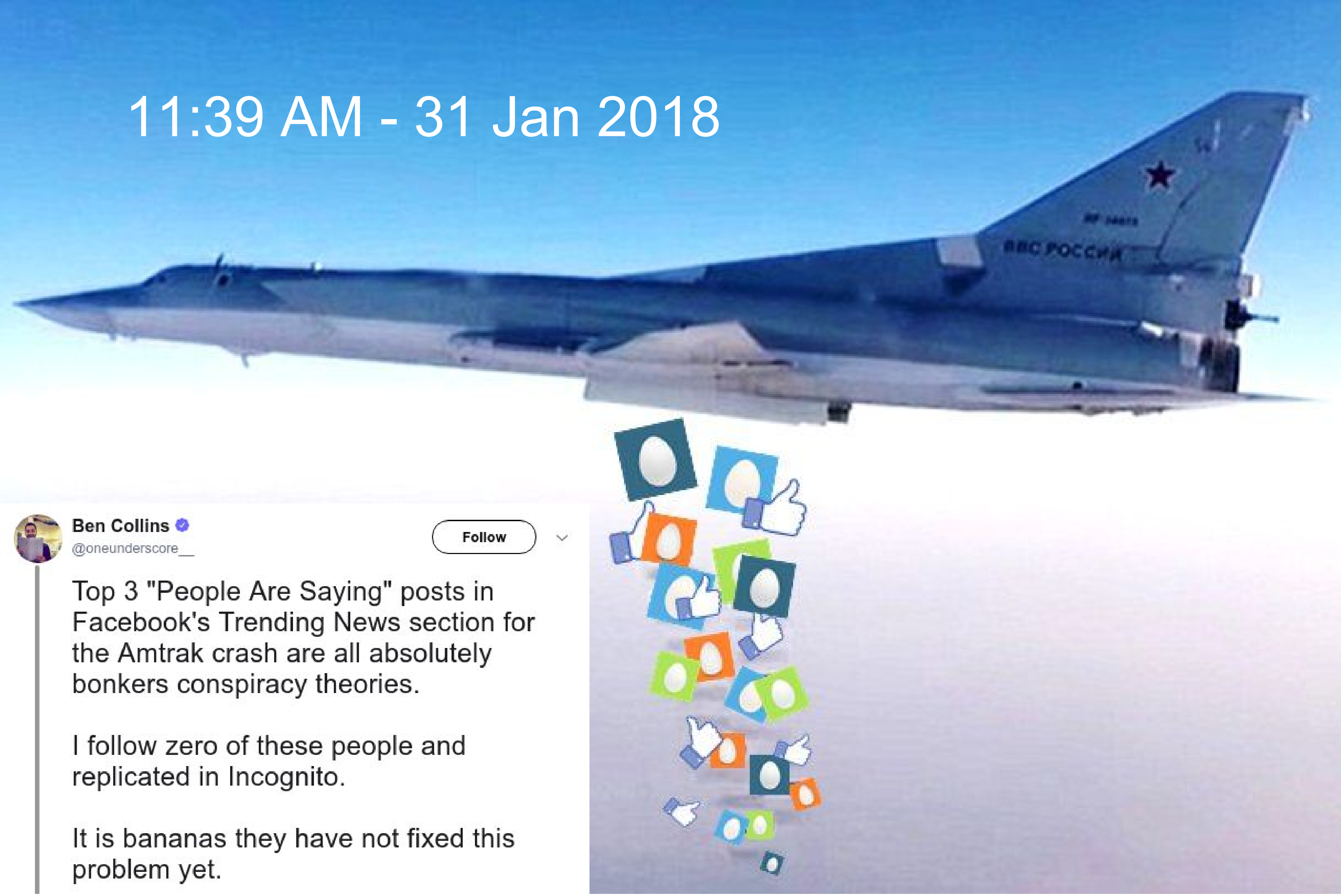


German bombers in skies over London by afternoon of September 7, 1940 while US Standard Oil management reporting: "*despite Allies, Nazis still get our refined products*"

https://www.theguardian.com/technology/2018/jan/28/tech-backlash-facebook-google-fake-news-business-monopoly-regulation

https://twitter.com/daviottenheimer/status/661453199723753473

11:39 AM - 31 Jan 2018



Ben Collins @oneunderscore__

Top 3 "People Are Saying" posts in Facebook's Trending News section for the Amtrak crash are all absolutely bonkers conspiracy theories.

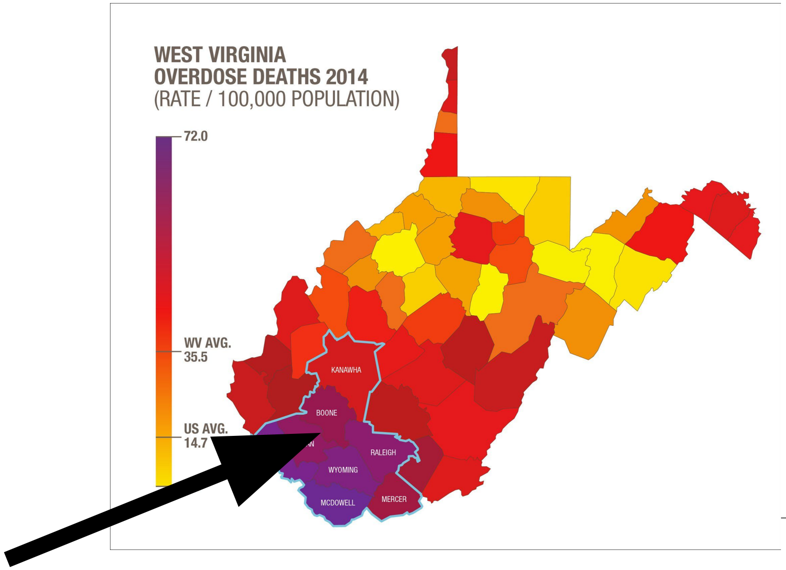
I follow zero of these people and replicated in Incognito.

It is bananas they have not fixed this problem yet.

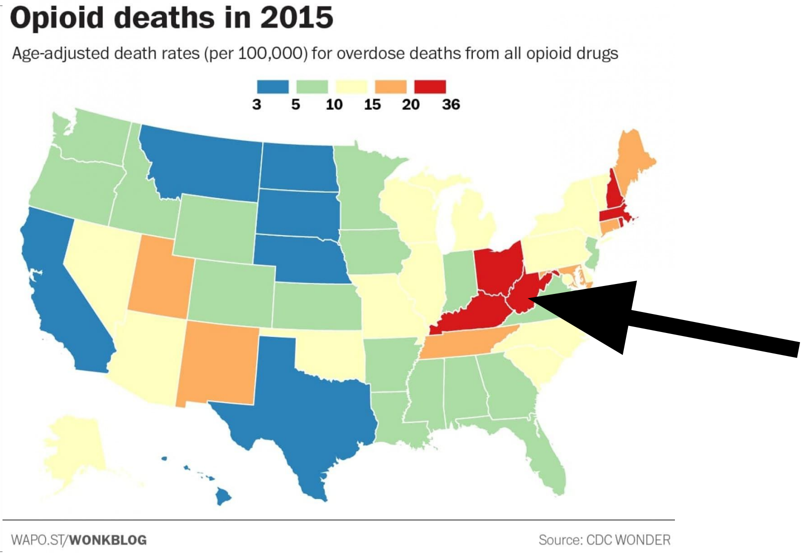
https://twitter.com/oneunderscore__/status/958786714562105345

Drug firms drop 20.8M pain pills on 2,900 Americans

- Pharma industry carefully tracks distribution of pills
- 20 million pills to 2 pharmacies of tiny town **obviously harmful**
- Knew harms and continued dropping. **They knew**



WEST VIRGINIA OVERDOSE DEATHS 2014 (RATE / 100,000 POPULATION)



Opioid deaths in 2015

Age-adjusted death rates (per 100,000) for overdose deaths from all opioid drugs

WAPO.ST/**WONKBLOG** Source: CDC WONDER

“The state has the highest drug overdose death rate in the nation. More than 880 people fatally overdosed in West Virginia in 2016.”

https://www.wvgazettemail.com/news/health/drug-firms-shipped-m-pain-pills-to-wv-town-with/article_ef04190c-1763-5a0c-a77a-7da0ff06455b.html

5. how to seed security rather than unpoison fruit

advanced
misinformation
persistence
threats
(AMPT)

2013 RU Army (Gerasimov Doctrine):

The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations

"The very 'rules of war' have changed. The role of **nonmilitary means of achieving political and strategic goals** has grown, and, in many cases, they have **exceeded the power of force of weapons** in their effectiveness. … All this is supplemented by military means of a concealed character."

http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf

2013 “Big Data Security” Warnings/Presentations

“On a Friendster social network consisting of 5.6 million nodes and 28 million edges we found a seed set in under 3.6 hour”

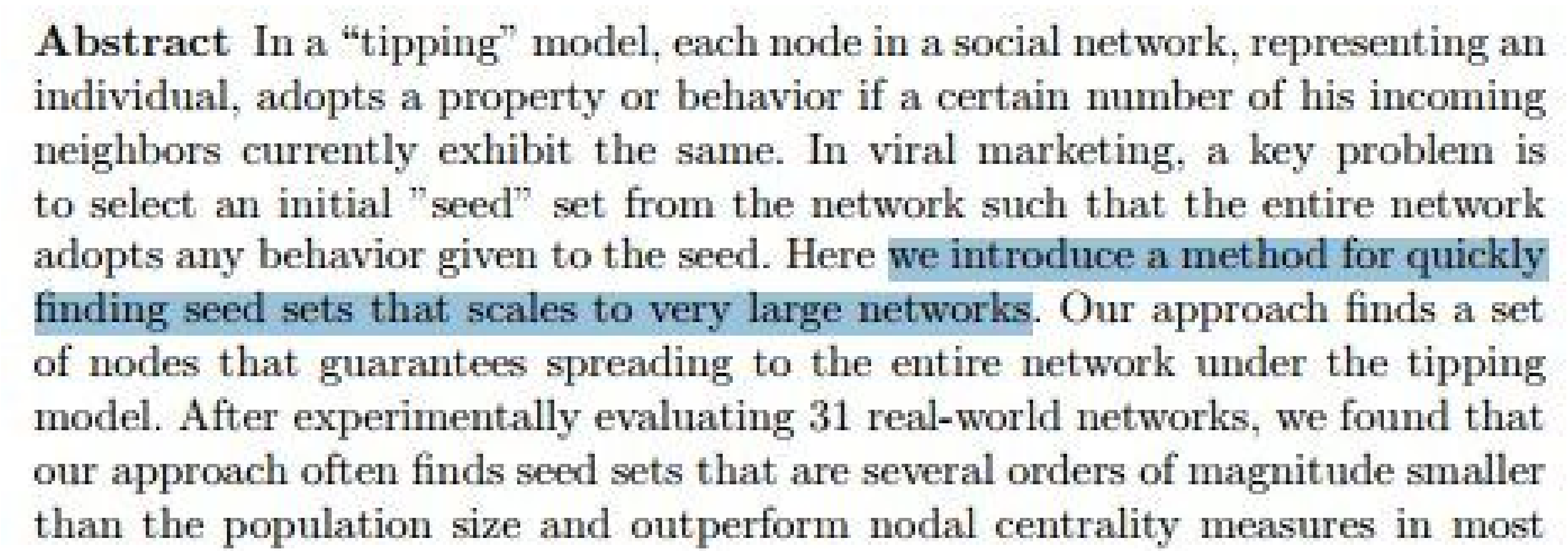
- US Army, Sep 2013

http://www.westpoint.edu/nsc/SiteAssets/SitePages/Publications/shakarianEyrePaulo-heurViralMktTip_main.pdf

2013 US Army:
Seed Sets that Scale to Very Large Network

“...desired output is the smallest possible set of individuals (seed set) such that, if initially activated, the entire population will become activated…”

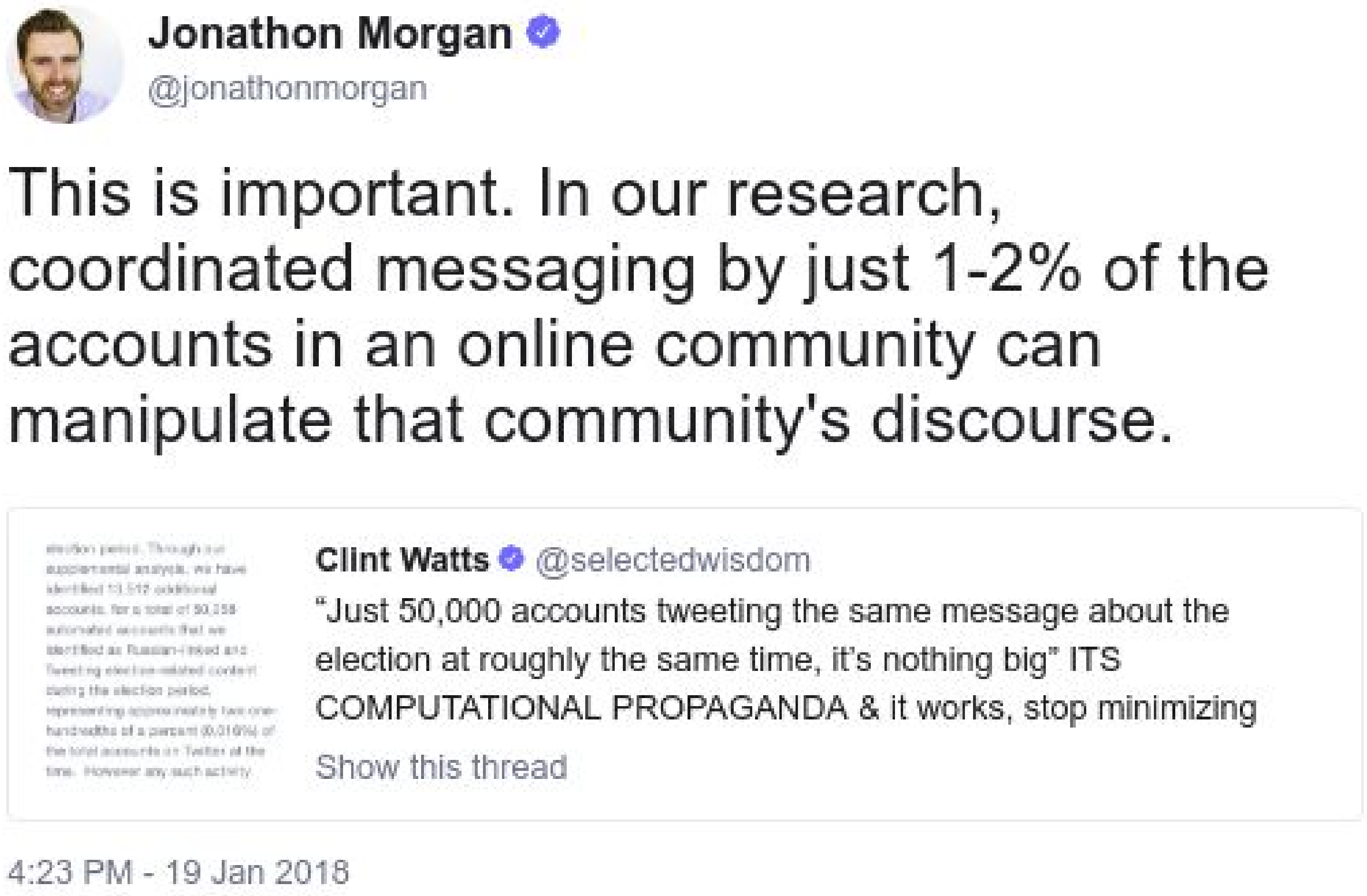
- West Point Military Academy, Network Science Center, Paulo Shakarian et al.



Abstract In a “tipping” model, each node in a social network, representing an individual, adopts a property or behavior if a certain number of his incoming neighbors currently exhibit the same. In viral marketing, a key problem is to select an initial ”seed” set from the network such that the entire network adopts any behavior given to the seed. Here we introduce a method for quickly finding seed sets that scales to very large networks. Our approach finds a set of nodes that guarantees spreading to the entire network under the tipping model. After experimentally evaluating 31 real-world networks, we found that our approach often finds seed sets that are several orders of magnitude smaller than the population size and outperform nodal centrality measures in most

https://www.westpoint.edu/nsc/SiteAssets/SitePages/Publications/shakarianEyrePaulo-heurViralMktTip_main.pdf

2018 Only 1% of Social Accounts Needed to Impact



Jonathon Morgan
@jonathonmorgan

This is important. In our research, coordinated messaging by just 1-2% of the accounts in an online community can manipulate that community's discourse.

election period. Through our supplemental analysis, we have identified 13,512 additional accounts, for a total of 50,258 automated accounts that we identified as Russian-linked and Tweeting election-related content during the election period, representing approximately two one-hundredths of a percent (0.016%) of the total accounts on Twitter at the time. However any such activity

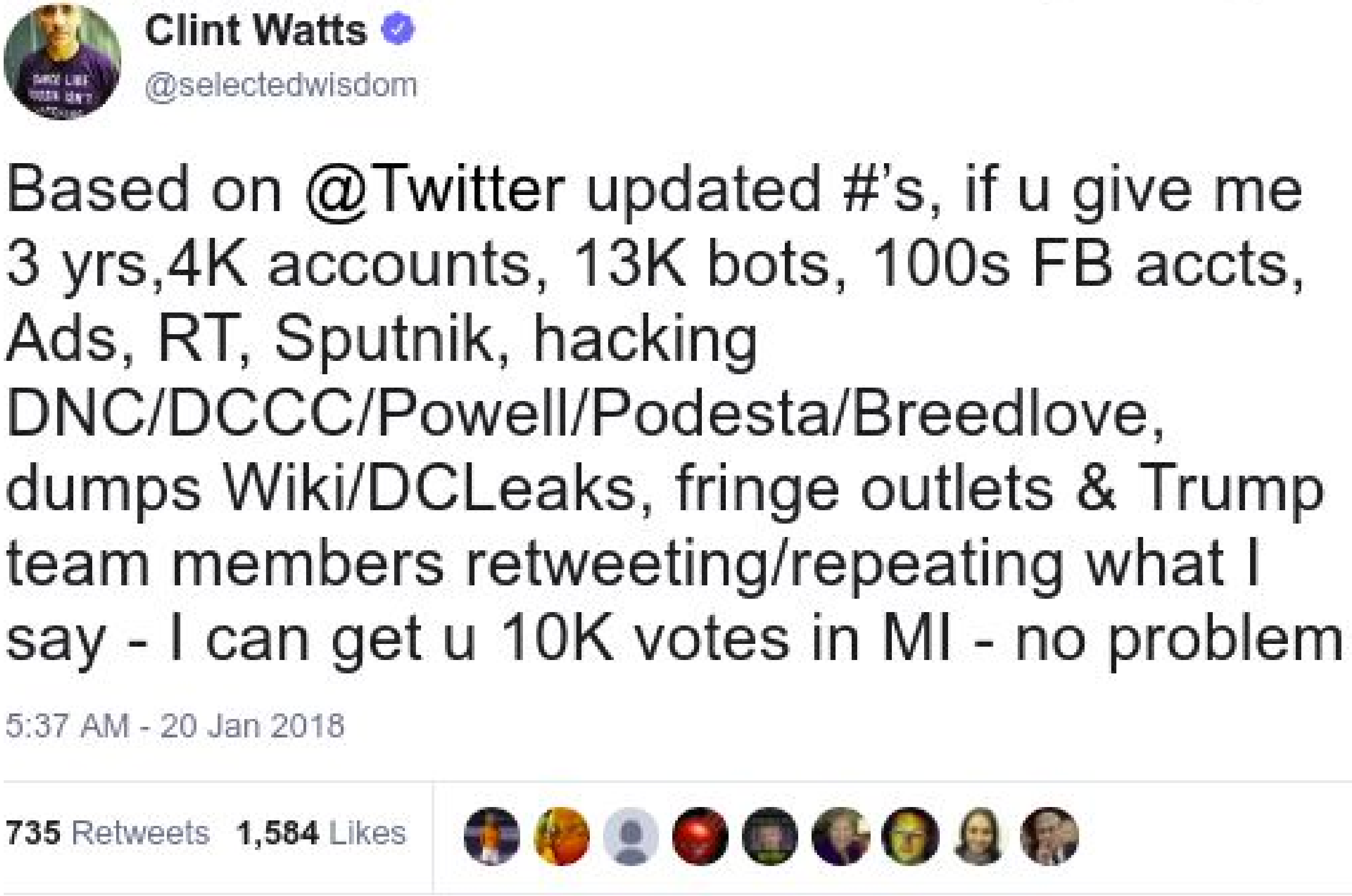
Clint Watts @selectedwisdom
"Just 50,000 accounts tweeting the same message about the election at roughly the same time, it's nothing big" ITS COMPUTATIONAL PROPAGANDA & it works, stop minimizing

Show this thread

4:23 PM - 19 Jan 2018

https://twitter.com/jonathonmorgan/status/954509759281094656

2018 “I can get you 10K votes in MI no problem”



Clint Watts
@selectedwisdom

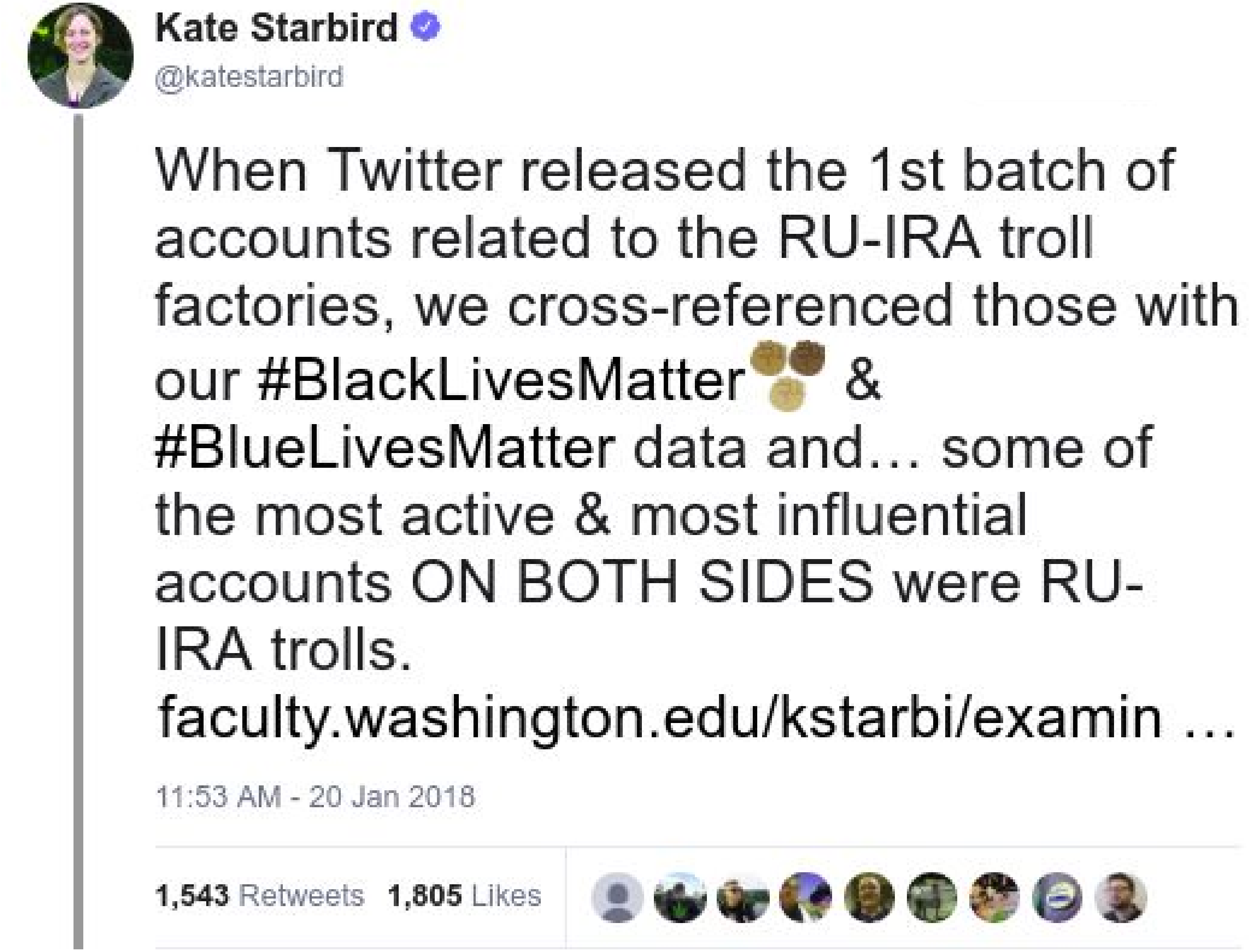
Based on @Twitter updated #'s, if u give me 3 yrs,4K accounts, 13K bots, 100s FB accts, Ads, RT, Sputnik, hacking DNC/DCCC/Powell/Podesta/Breedlove, dumps Wiki/DCLeaks, fringe outlets & Trump team members retweeting/repeating what I say - I can get u 10K votes in MI - no problem

5:37 AM - 20 Jan 2018

735 Retweets 1,584 Likes

https://twitter.com/daviottenheimer/status/929778397328355334

2018 RU Engaged in Grey Battles



Kate Starbird

@katestarbird

When Twitter released the 1st batch of accounts related to the RU-IRA troll factories, we cross-referenced those with our #BlackLivesMatter ✊✊✊ & #BlueLivesMatter data and… some of the most active & most influential accounts ON BOTH SIDES were RU-IRA trolls. faculty.washington.edu/kstarbi/examin …

11:53 AM - 20 Jan 2018

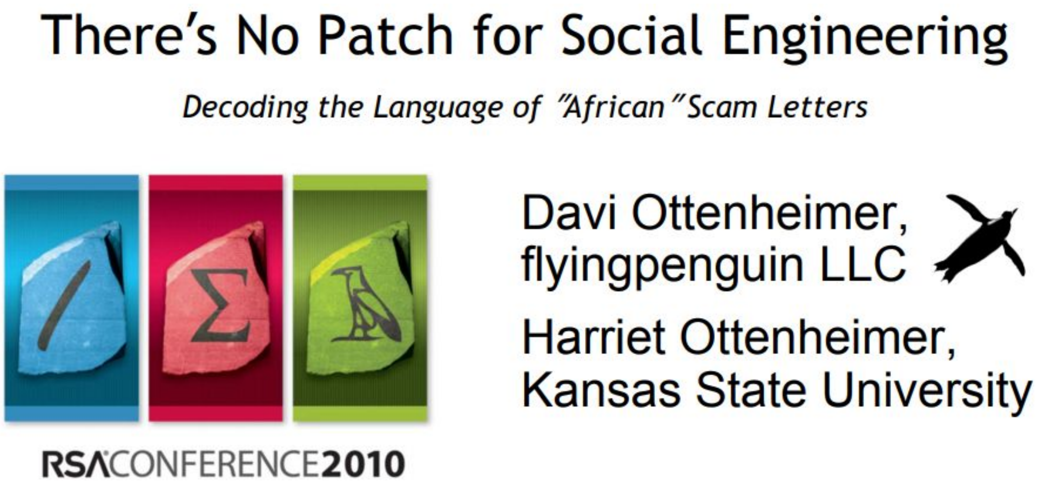
1,543 Retweets 1,805 Likes

https://twitter.com/katestarbird/status/954804195269361664

Objective Fact: Advertising is Misinformation

“A ‘game’ that has victims rather than players, hardly can be called a game at all. Instead, it is an example of carefully crafted social engineering that allows attackers to transfer value (from victims to themselves) without proper authorization.”

"Any system or network that has been optimized for advertisements has been implicitly optimized for spreading misinformation."



There’s No Patch for Social Engineering

Decoding the Language of "African" Scam Letters

Davi Ottenheimer, flyingpenguin LLC

Harriet Ottenheimer, Kansas State University

RSACONFERENCE2010

http://smerity.com/articles/2018/turing_test_isnt_won_its_lost.html
http://www.flyingpenguin.com/?p=85

GOP Deregulated Misinformation to Children

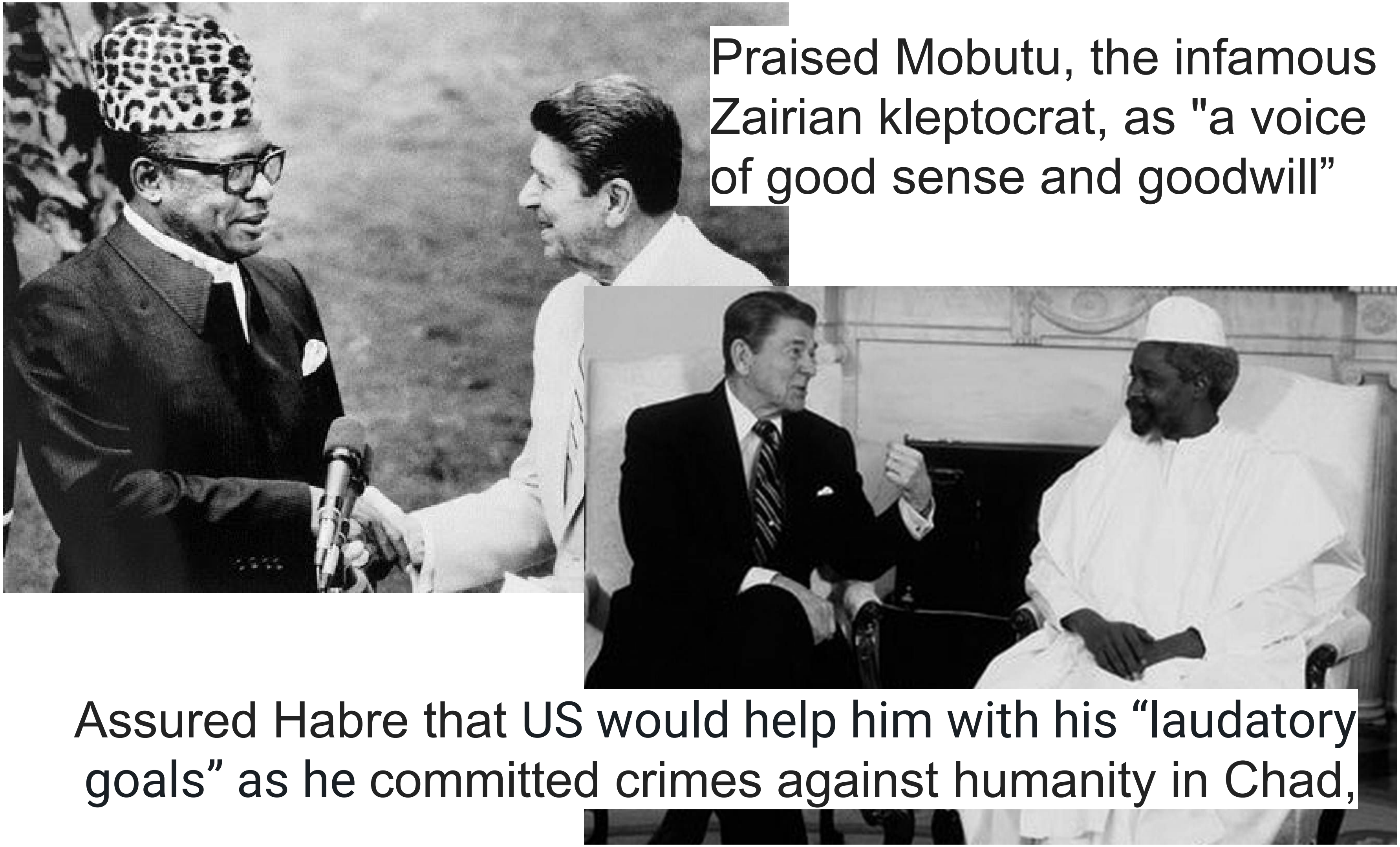
1984: removed limits to harmful children advertising, said adversaries must not be judged for content that targets receive

1988: vetoed overwhelming support for limits to harmful advertising, said any protection of children from harm would oppress rights of advertisers

- Congress: must address “ideological child abuse” risk
- Broadcasters: “we expected the President to sign it”
- POTUS: attackers must not be subject to “tastes of agency officials”

http://www.nytimes.com/1988/11/07/us/reagan-vetoes-bill-putting-limits-on-tv-programming-for-children.html

Context: Reagan Big Proponent of Tyranny



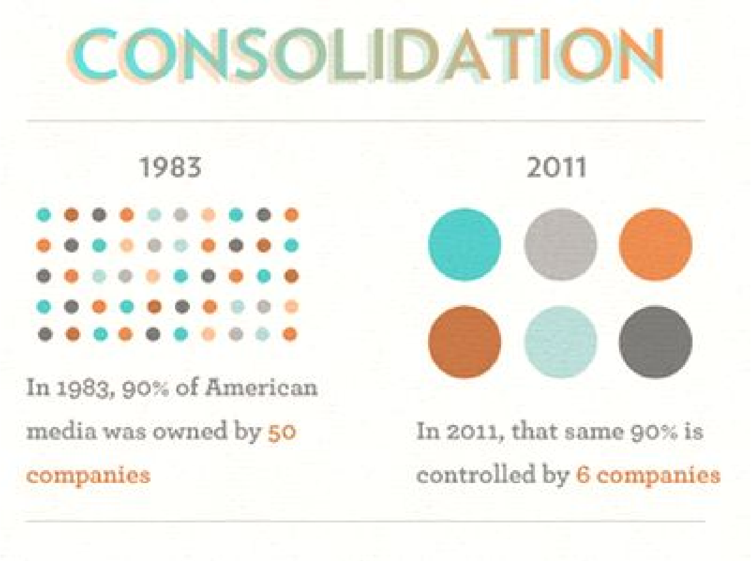
Praised Mobutu, the infamous Zairian kleptocrat, as "a voice of good sense and goodwill”

Assured Habre that US would help him with his “laudatory goals” as he committed crimes against humanity in Chad,

http://www.metroactive.com/papers/metro/05.22.97/cover/mobutu-9721.htm
http://www.presidency.ucsb.edu/ws/?pid=34455l

10y Later Deregulation of Misinformation = Polarized

- 1996 Telecommunications Act
  - Near-total rollback of 1934 US gov effort to stop Nazi (America First) propaganda
  - Politicians claimed “innovation” would come from deregulation
  - Introduction of FOX News



In 1983, 90% of American media was owned by 50 companies

In 2011, that same 90% is controlled by 6 companies

- 2015 Assessment of Act
  - Harmful monopolies created, massive and historic consolidation of US media
  - Large (FOX and NBC) replaced small, independent TV stations and cable news channels
  - “Structural media changes caused US attitude polarization”

“..news use contributes to increasing levels of affective polarization in US”

https://news.wsu.edu/2015/09/24/study-links-u-s-polarization-to-tv-news-deregulation/
http://businessinsider.com.au/these-6-corporations-control-90-of-the-media-in-america-2012-6

“Grey Zone” (Subtle) Methods for Strategic Objective

Threat Definition:

Adversaries unable/unwilling to expend resources on conventional means, who still want to achieve a strategic objective, develop ways to erode stability/order and paralyze responses through ambiguous/deceptively aggressive actions (tactical operations that avoid alarm).

Hidden Hot Battle Lessons of Cold War

All Learning Models Have Flaws, Some Have Casualties

Davi Ottenheimer

- Wants post-Vietnam conflict with USSR
- Seeks inexpensive “No-Win War” in “South”
    - $100m cost of stable “win” deemed too visible, requiring oversight
    - $14m budgeted for Angola subversion, hidden from US public

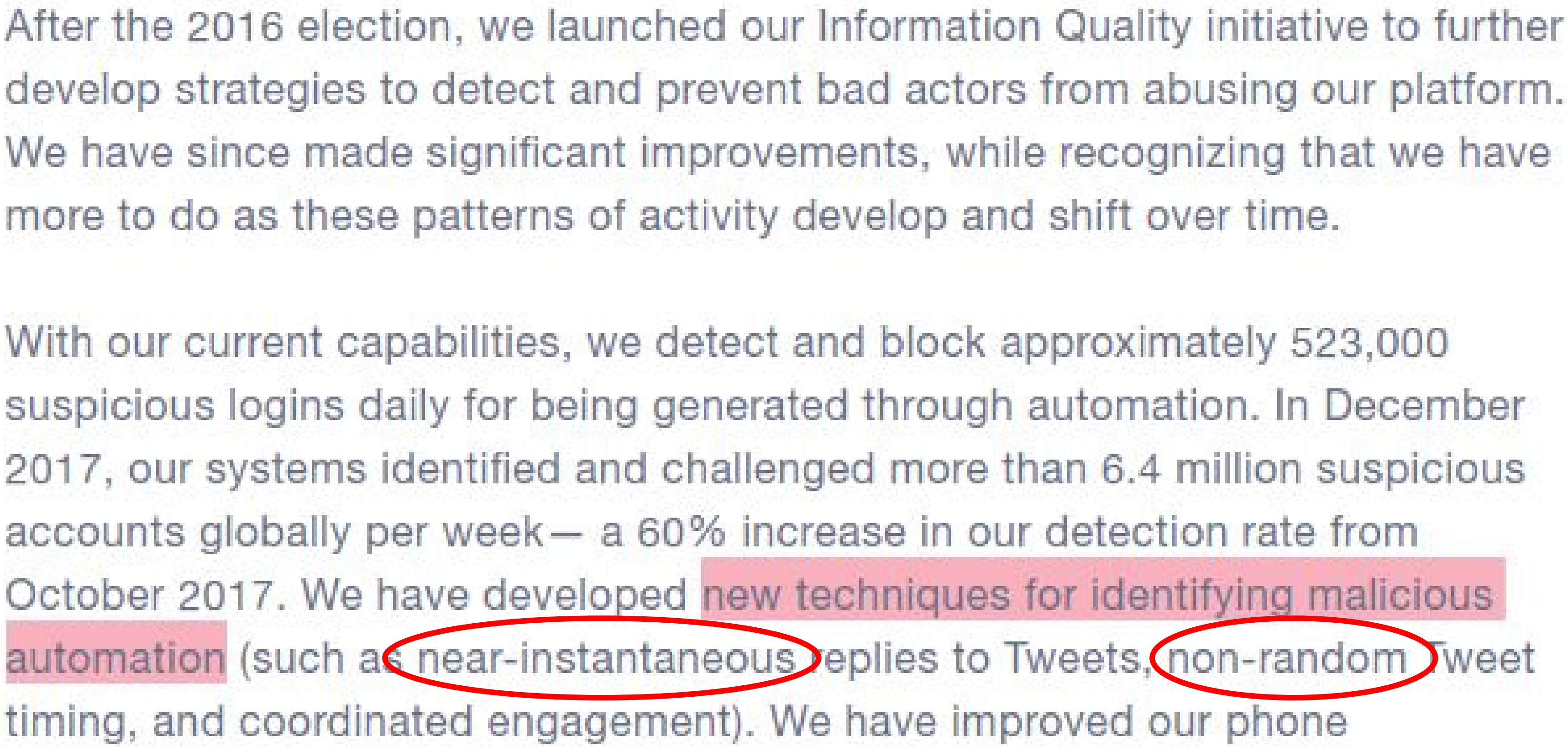
http://www.flyingpenguin.com/?p=22640

Twitter Attempting Ad “Transparency Center” to Expose Grey Zone Attacks:

- all ads currently on site including "promoted-only"
- how long have run
- targeted at specific users
- all political ads and their buyer using clear label

https://www.cnet.com/news/twitter-to-share-identity-of-political-ad-buyers-new-ad-transparency/

Caveat: “New” Methods May Be Easily Bypassed (Timing Attacks)



After the 2016 election, we launched our Information Quality initiative to further develop strategies to detect and prevent bad actors from abusing our platform. We have since made significant improvements, while recognizing that we have more to do as these patterns of activity develop and shift over time.

With our current capabilities, we detect and block approximately 523,000 suspicious logins daily for being generated through automation. In December 2017, our systems identified and challenged more than 6.4 million suspicious accounts globally per week— a 60% increase in our detection rate from October 2017. We have developed new techniques for identifying malicious automation (such as near-instantaneous replies to Tweets, non-random Tweet timing, and coordinated engagement). We have improved our phone

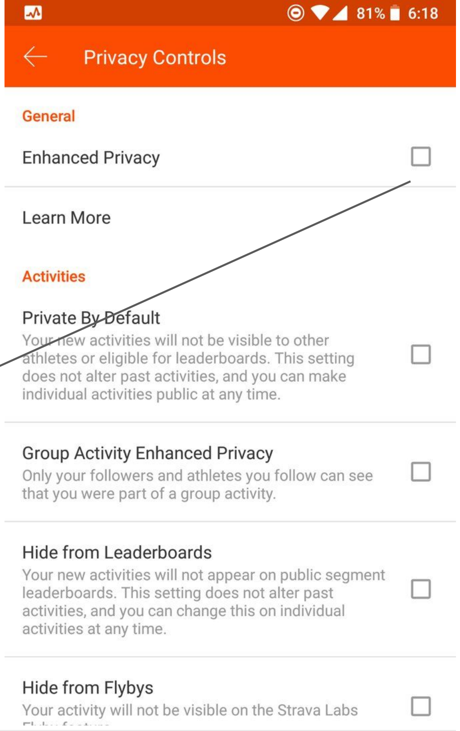
https://blog.twitter.com/official/en_us/topics/company/2018/2016-election-update.html

So What Happens After Transparency?

(Regulation: Authorization of Data Judgement)

Choose wisely:

1) Minority rule via technology-savvy secret police?
2) Opening back doors (anon) for (flash) mob entry?
3) Democratic law-based open governance model?



Privacy Controls

General

Enhanced Privacy ☐

Learn More

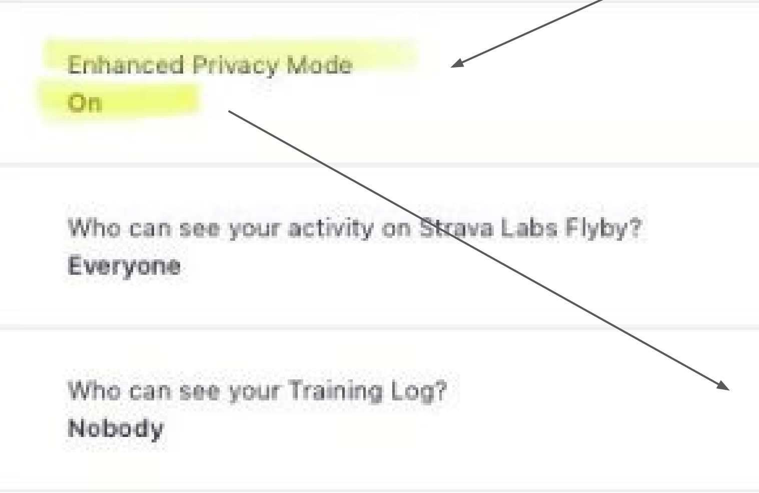
Activities

Private By Default ☐
Your new activities will not be visible to other athletes or eligible for leaderboards. This setting does not alter past activities, and you can make individual activities public at any time.

Group Activity Enhanced Privacy ☐
Only your followers and athletes you follow can see that you were part of a group activity.

Hide from Leaderboards ☐
Your new activities will not appear on public segment leaderboards. This setting does not alter past activities, and you can change this on individual activities at any time.

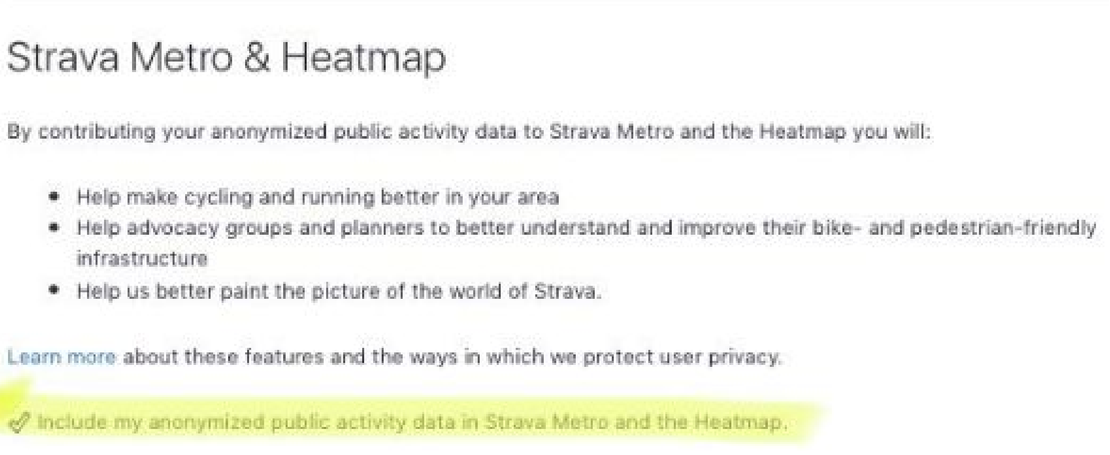
Hide from Flybys ☐
Your activity will not be visible on the Strava Labs



Enhanced Privacy Mode
On

Who can see your activity on Strava Labs Flyby?
Everyone

Who can see your Training Log?
Nobody



Strava Metro & Heatmap

By contributing your anonymized public activity data to Strava Metro and the Heatmap you will:

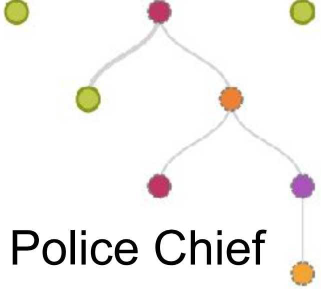
- Help make cycling and running better in your area
- Help advocacy groups and planners to better understand and improve their bike- and pedestrian-friendly infrastructure
- Help us better paint the picture of the world of Strava.

Learn more about these features and the ways in which we protect user privacy.

✓ Include my anonymized public activity data in Strava Metro and the Heatmap.

https://twitter.com/Matt_Cagle/status/957748059651231744
https://twitter.com/xntrik/status/957800013731545088

“If black shoot them”



-- Facebook messages leaked from US Police Chief

Regulated transparency

“...instructed a police recruit to shoot black teenagers on sight if caught smoking marijuana, according to court documents.

‘Fuck the right thing. If black shoot them’ ...part of what the Jefferson County attorney’s office described as a pattern of ‘**highly disturbing racist and threatening Facebook messages**’ from Shaw.

“...responsibility lends itself to a higher level of **public scrutiny**. While the court understands how embarrassing the documents may be to Shaw personally, **they are not of the private nature intended to be shielded from public disclosure**. The documents **reveal opinions and prejudices that bring into question Shaw’s integrity** as a law enforcement officer who has been entrusted to serve and protect all members of society.”

-- Kentucky Judge

https://www.theguardian.com/global/2018/jan/22/if-black-shoot-them-former-kentucky-acting-police-chief-instructed-a-recruit

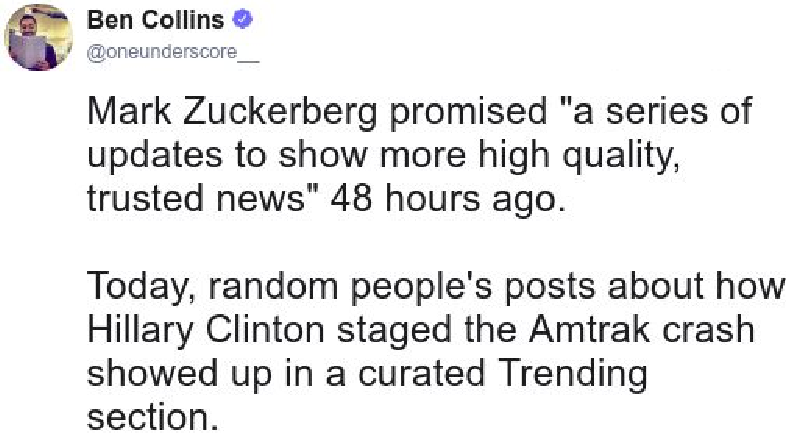
Google (Prematurely?) Claims Massive Security Win

“99% of apps with abusive contents were identified and rejected ***before anyone could install***”

“significant improvements in our ability to detect abuse - such as impersonation, inappropriate content, or malware - through new machine learning models and techniques”

https://android-developers.googleblog.com/2018/01/how-we-fought-bad-apps-and-malicious.html

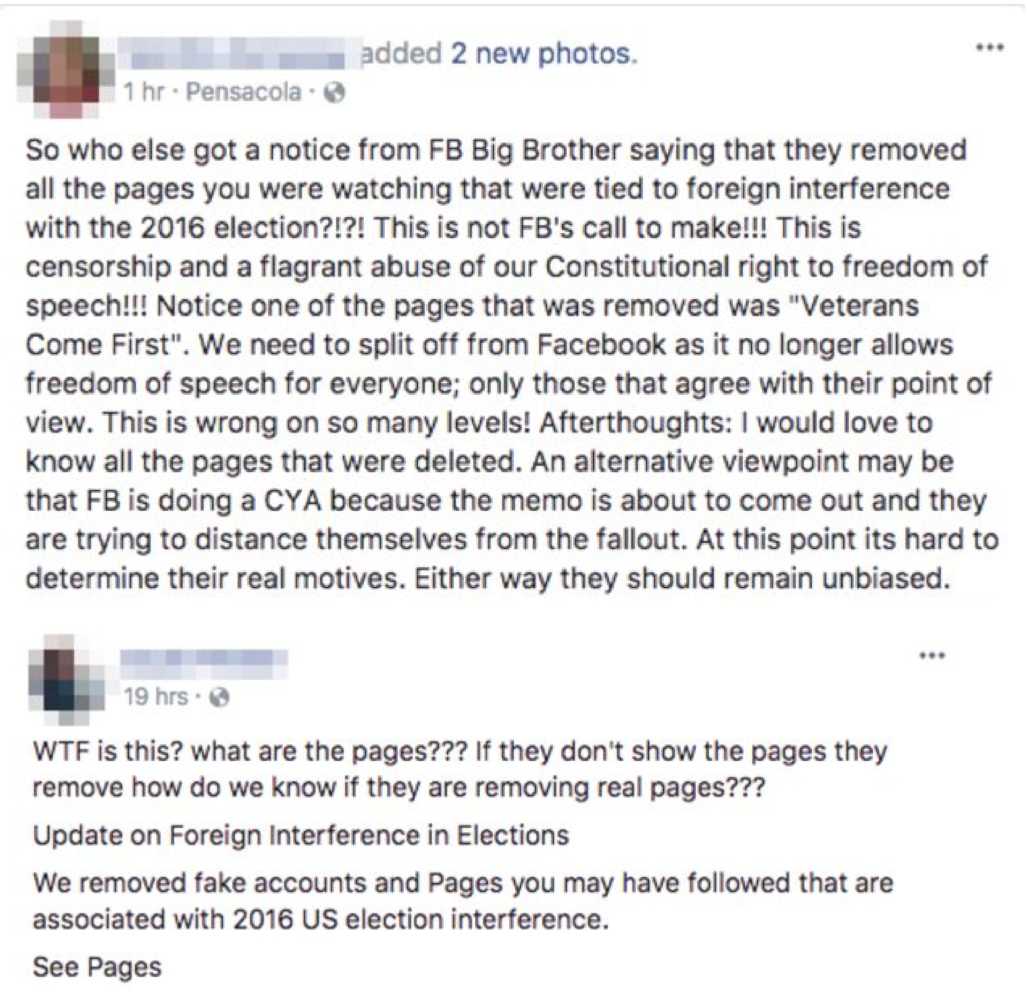
While Facebook Gets Breached Again and Again Because...



Ben Collins
@oneunderscore__

Mark Zuckerberg promised "a series of updates to show more high quality, trusted news" 48 hours ago.

Today, random people's posts about how Hillary Clinton staged the Amtrak crash showed up in a curated Trending section.



[redacted] added 2 new photos.
1 hr · Pensacola ·

So who else got a notice from FB Big Brother saying that they removed all the pages you were watching that were tied to foreign interference with the 2016 election?!?! This is not FB's call to make!!! This is censorship and a flagrant abuse of our Constitutional right to freedom of speech!!! Notice one of the pages that was removed was "Veterans Come First". We need to split off from Facebook as it no longer allows freedom of speech for everyone; only those that agree with their point of view. This is wrong on so many levels! Afterthoughts: I would love to know all the pages that were deleted. An alternative viewpoint may be that FB is doing a CYA because the memo is about to come out and they are trying to distance themselves from the fallout. At this point its hard to determine their real motives. Either way they should remain unbiased.

[redacted]
19 hrs ·

WTF is this? what are the pages??? If they don't show the pages they remove how do we know if they are removing real pages???

Update on Foreign Interference in Elections

We removed fake accounts and Pages you may have followed that are associated with 2016 US election interference.

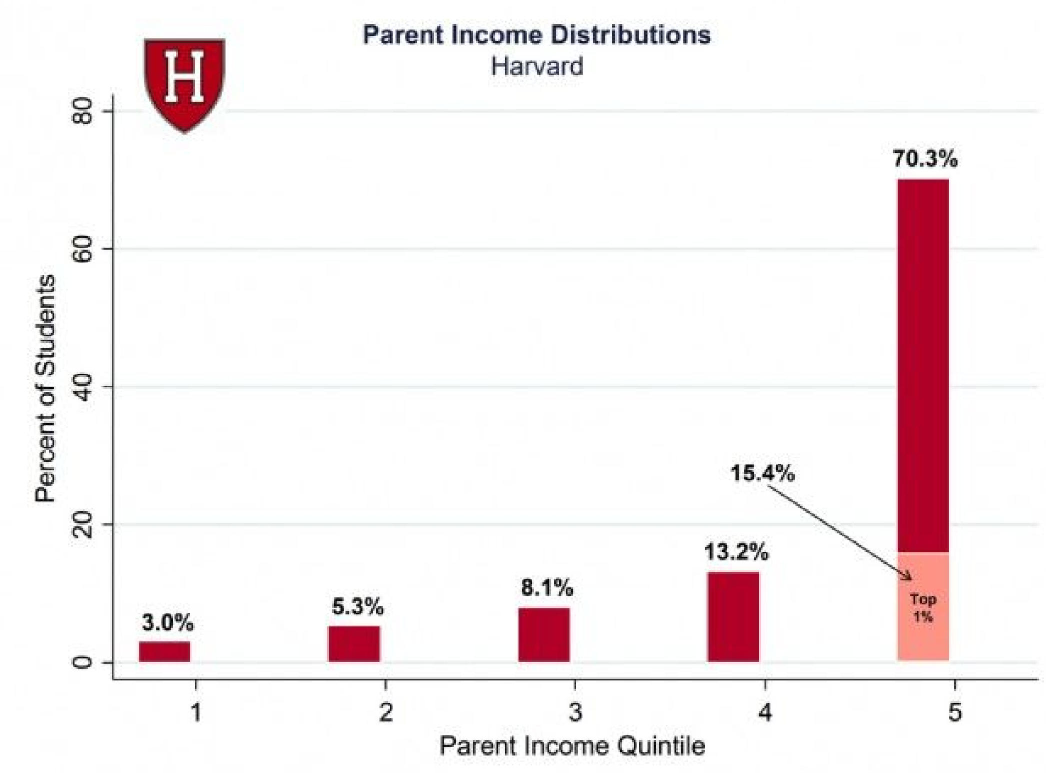
See Pages

https://gizmodo.com/facebook-users-cry-censorship-after-being-told-which-ru-1822552451
https://twitter.com/oneunderscore__/status/958810972604518400

REMEMBER

Cyber Doesn’t Kill People, Harvard-Trained People Kill People

> "*Wouldn’t it be cool if you could shoot somebody in the face at 200 kilometers and they don’t even know you’re there?*"



-- Harvard graduate who used to work at Pentagon, planning to enable driverless cars for killing the poor

https://www.defensenews.com/congress/budget/2018/01/30/selva-fy19-budget-sees-increasing-investments-in-ai-machine-teaming/

APPSEC - CALIFORNIA

2018

OWASP

Unpoisoned Fruit:

Seeding Trust into a Growing World of Algorithmic Warfare

Davi Ottenheimer

mongoDB