Cyberwarfare: The New "Colder" War:

Modern cybersecurity threats have evolved into very effective disinformation campaigns and destructive ransomware.

LTC Kevin J Murphy, USAF (Ret)

February 11, 2021

Speaker Description

- Retire USAF Intelligence Officer
- Over 25 years in Cybersecurity

Cyberwarfare: The New “Colder” War:

Agenda:

- Cyberwarfare: What is it?
- Digital Marketing & Consumer Behavior
- Disinformation Operations
- Lessons from the 2019 Canadian Elections
- “So what do we do?”

What is Cyberwarfare?

- Cyberwarfare is an extension of nation state policies
- Another means to achieve political objectives
- Unlike the Cold War:
  - No Détente. There is no international agreement on what limits a cyber-attack would have to exceed in order to trigger a conventional war.
  - No MAD. There is no expectation of "Mutually Assured Destruction" among the attackers. Attack skills and vulnerability will vary among the players.
  - Anonymity. Nation state actors in the cyber world will act far more aggressively and destructively when the attack can't be attributed to any actor.

What are the 4 elements of Cyberwarfare?

- Modern Espionage - Advanced Persistent Threat (APT)
  - Low-cost, low risk, high-return espionage.
  - Examples:
  - APT-28 Fancy Bear – Democrat National Committee Attack of 2016
  - APT 29 Cozy Bear – Phishing expertise
- Data Exfiltration – Steal Information
  - Enterprise Intellectual Property
  - Personal Identifiable Information (PII), Financial Data
  - Government Data
- Data and Infrastructure Destruction (computing and physical)
  - A level playing field for smaller countries; e.g. N Korea
  - Low barriers to entry for any player - Ransomware
- **Disinformation Operations** – Modern propaganda but much more effective

Who Are The Actors?

- **Nation States** –
  - Usually a part of the national intelligence operations
  - Offensive capabilities is generally part of the military
  - Nation state defense is part of a civilian ministry
- **3rd Party Operators** –
  - On contract to the nation state actors
  - Harder to trace to a particular nation state
- **Political Sympathizers** –
  - More loosely affiliated
  - Even harder to trace to a nation state

Modern Espionage

Firewall blocking report

Destination IP	Destination Port (Unique Count)	Source IP (Unique Count)	Source Port (Unique Count)	Event Name (Unique Count)
88.214.193.180	443	Multiple (15)	Multiple (136)	Firewall Drop
136.243.73.56	443	156.74.159.228	Multiple (39)	Firewall Drop
119.28.109.182	80	156.74.90.217	Multiple (28)	Firewall Drop
5.9.7.202	443	156.74.135.245	Multiple (19)	Firewall Drop
85.195.100.210	Multiple (2)	Multiple (9)	Multiple (19)	Firewall Drop
178.62.242.42	Multiple (2)	Multiple (4)	Multiple (12)	Firewall Drop
88.99.5.37	443	Multiple (2)	Multiple (10)	Firewall Drop
85.195.104.157	443	Multiple (2)	Multiple (10)	Firewall Drop
84.22.110.176	443	10.4.162.55	Multiple (10)	Firewall Drop
213.230.210.230	443	Multiple (8)	Multiple (8)	Firewall Drop
88.214.193.110	443	Multiple (3)	Multiple (9)	Firewall Drop
149.202.194.227	Multiple (2)	Multiple (2)	Multiple (5)	Firewall Drop
149.202.212.167	443	Multiple (2)	Multiple (6)	Firewall Drop
92.63.111.166	443	156.74.84.43	Multiple (6)	Firewall Drop
178.63.70.146	443	Multiple (2)	Multiple (5)	Firewall Drop
136.243.74.153	443	156.74.26.203	Multiple (4)	Firewall Drop
51.255.231.130	443	Multiple (2)	Multiple (7)	Firewall Drop
167.114.210.7	443	172.16.102.167	Multiple (4)	Firewall Drop
194.226.130.227	443	172.16.102.232	Multiple (6)	Firewall Drop
144.217.84.97	443	156.74.187.189	Multiple (3)	Firewall Drop
77.246.156.238	443	156.74.84.43	Multiple (3)	Firewall Drop
51.255.232.205	80	156.74.186.237	Multiple (3)	Firewall Drop
148.66.136.190	80	156.74.123.29	22519	Firewall Drop
46.254.20.149	80	156.74.34.93	21817	Firewall Drop
208.91.197.132	443	156.74.20.138	Multiple (3)	Firewall Drop
88.214.193.98	80	Multiple (2)	Multiple (2)	Firewall Drop
88.214.193.9	443	Multiple (2)	Multiple (4)	Firewall Drop
194.226.130.229	443	172.16.102.232	Multiple (4)	Firewall Drop
185.53.178.7	443	156.74.149.252	Multiple (2)	Firewall Drop
31.172.81.172	443	Multiple (2)	Multiple (4)	Firewall Drop
31.172.81.160	443	Multiple (2)	Multiple (4)	Firewall Drop
31.172.81.158	443	Multiple (2)	Multiple (4)	Firewall Drop
88.214.193.33	80	156.74.68.152	23179	Firewall Drop
85.195.107.98	51700	10.5.192.190	51700	Firewall Drop
194.226.130.226	443	172.16.102.232	Multiple (2)	Firewall Drop
194.226.130.228	443	172.16.102.232	Multiple (2)	Firewall Drop
46.36.39.39	443	156.74.20.117	32029	Firewall Drop

- City of Seattle receives 200,000 attacks per month
- Province of British Columbia receives 20 million attacks per month

- Note all the 443 attacks. If you are not doing SSL inspection, then your Threat Hunting team is blind to most attacks

Data Exfiltration

CYBERSECURITY

The g later four susp

PUBLISHED WED, FEB 13 2019 • 3:33 P

U.S. accuses Chinese military hackers in massive Equifax breach over 2 years ago

The 2017 breach affected 145 million Americans, and hundreds of thousands elsewhere in the world

The Associated Press · Posted: Feb 10, 2020 11:17 AM ET | Last Updated: February 10

Kate Fazzini
@KATEFAZZINI

https://www.cnbc.com/2019/02/13/equifax-mystery-where-is-the-data.html

Data Exfiltration

- Solarwinds attack = 3rd Party Software attack.
- This isn't just about Solarwinds; This could be any IT Vendor
  - Ask: "Can this happen here?"
  - What controls do we have in place that would prevent this type of attack?
  - Do we have a secure dev and build environment?
  - Do we have a secure code repository that is monitored and requires 2FA with attribution before code could be checked in?
- Do we require a secure dev and build environment from our vendors? Is it part of our 3rd party agreements?
  - Update your TPRM, and 3rd party agreements
  - Require your IT vendors to code-sign their security patches

Data Exfiltration

- **US Treasury Secretary Janet Yellen has warned of an "explosion of risk" from criminals using digital technologies.**
  - "We're living amidst an explosion of risk related to fraud, money laundering, terrorist financing, and data privacy.
  - "As the pandemic has moved more of life online, crime has moved with it. We're seeing more – and more sophisticated – cyberattacks aimed at institutions that hold up our society: hospitals, schools, banks and even our government," she said.

US Treasury: Yellen warns of 'explosion' of cybercrime risk - BBC News

Data Destruction

News › UK

North Korea were behi

N

thought to have been carried

ow denies.

FBI warns of "imminent" ransomware attacks on hospital systems

OCTOBER 29, 2020 / 7:41 AM / CBS/AP

On October 24th, P gets Windows

mach

Adobe Flash

The majority of BadRabbit's victims were in Russia

ttack has seen computers go

in Russia, Ukraine, Germany and Turkey.

"The new Cold War with less rules"

Digital Marketing and Consumer Behavior

Today's Marketing Technology

We are not all seeing the same news or even the same facts!

- To determine, predict, and manipulate and behavi...
- ...ns use the same ...s specifically to you.
- Disinform... methods to tailor your fe... ...alytics
- ... (Artificial Intelligence)
  - Face identity recognition
  - Voice identity recognition
  - **News feeds based on previous online activity**
  - **Targeted marketing algorithms**

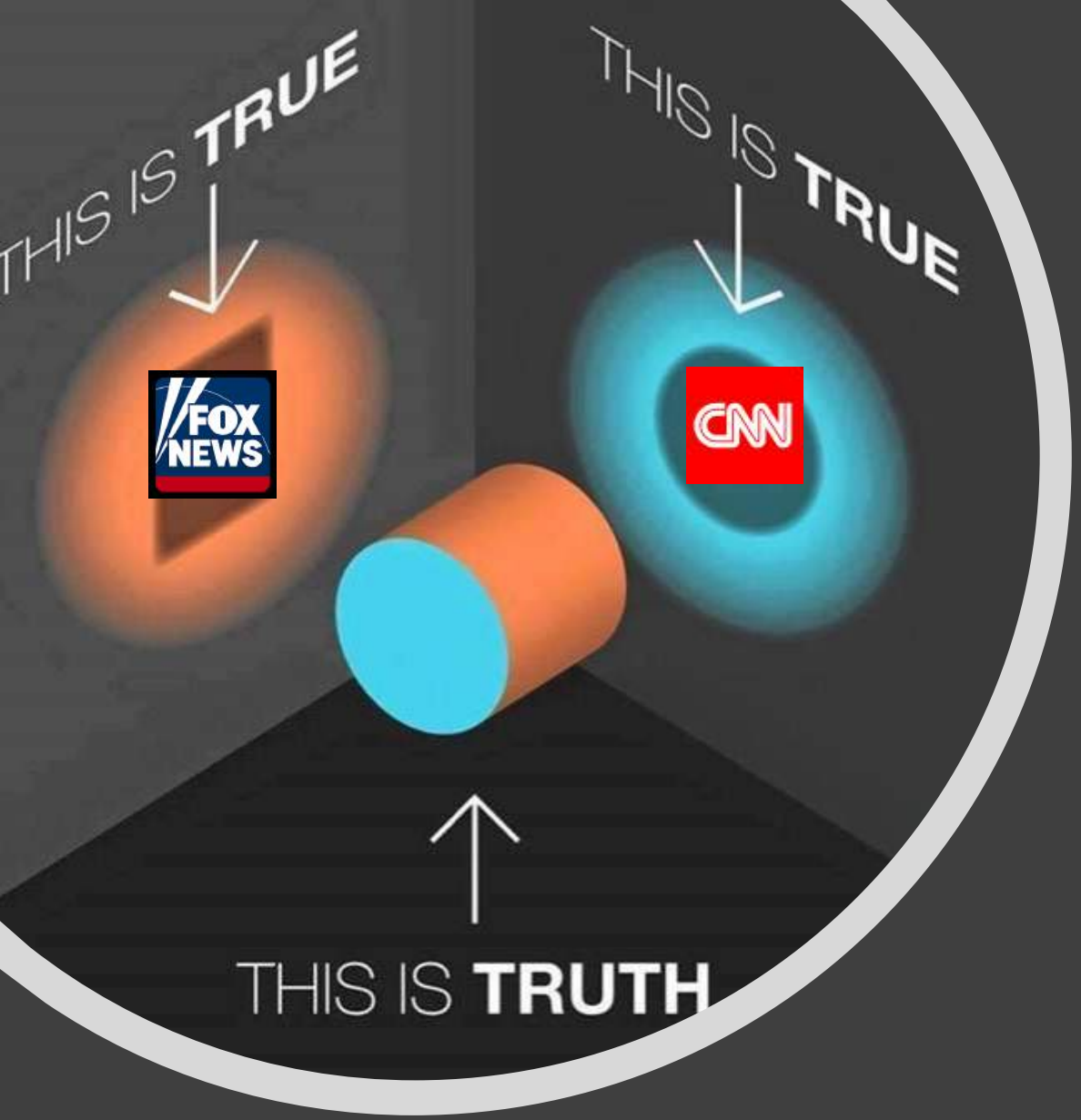
Today's Consumer Digital Behavior

Internet/WIFI

- 24/7 connected devices
  - Instant online news
  - Email, Instant Messaging, forwarding social media articles solely based on headline *("Without ever reading the article")*
  - *Arguing politics with people you don't even know on social media*
  - Netflix
  - Cloud storage
  - Smartphone eCommerce any time of day or night
- Online accounts: banking, health, youth sports, etc.
  - Personal email address as account name?
  - *How many consumers use the same account name and password for banking and social media?* **(Fix this tonight!)**

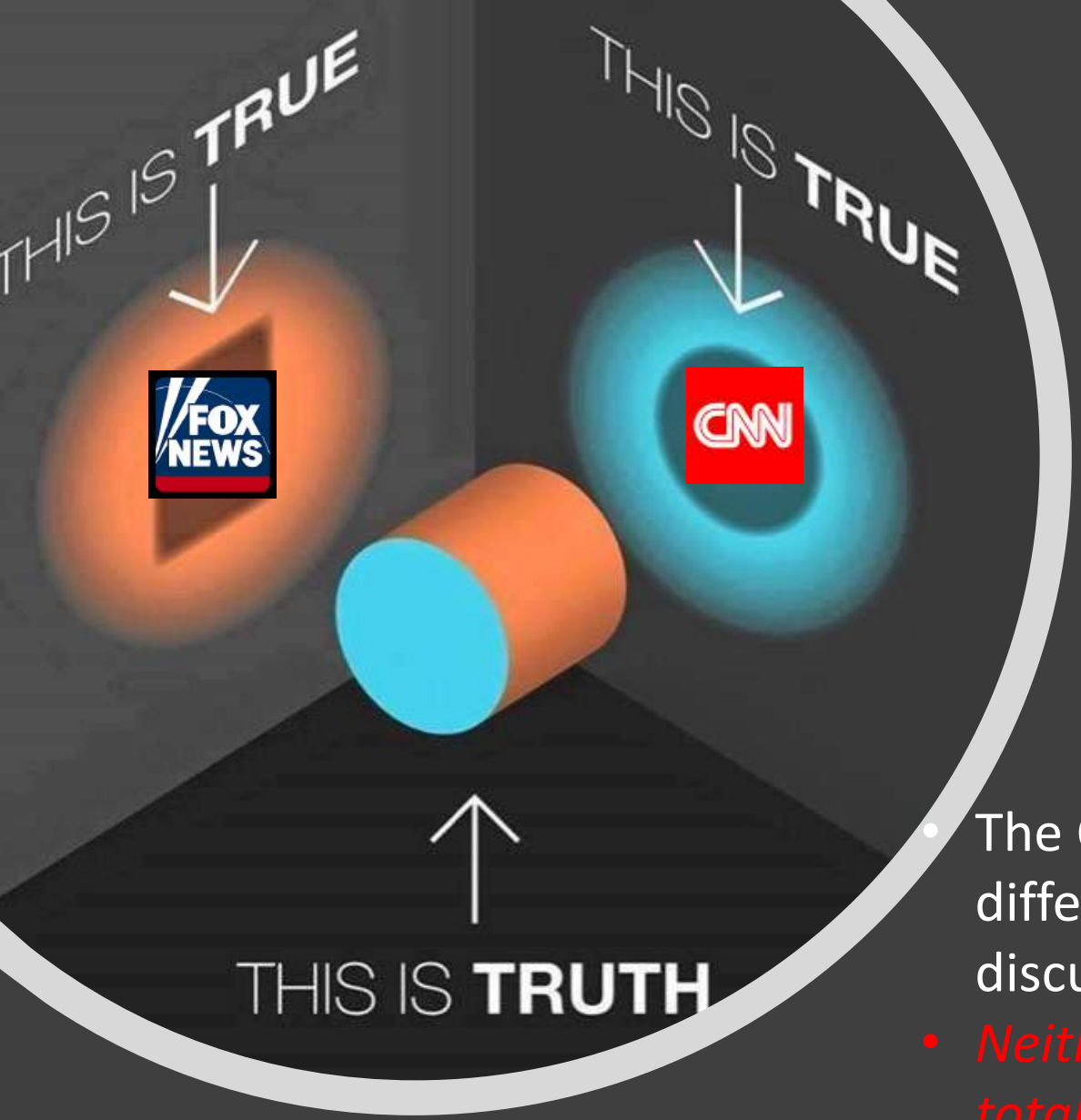
All your activity is tracked for marketing purposes

Disinformation Operations



Disinformation

- **Disinformation** is to confuse not to convince. Could be true but not the full story
  - Cherry Picked Facts
  - Half Truths
  - Political Bias News (CNN vs FOXNews)
- **Misinformation** is Fake News or False information
  - QAnon
  - Facebook, YouTube
  - Conspiracy Theories –e.g. 5G causes COVID-19



Disinformation Example

Had the Titanic sunk today…

- CNN would report that 1500 people perish due to poor maritime standards
- FOX News would report that 700 people are rescued due to the heroics of the crew.

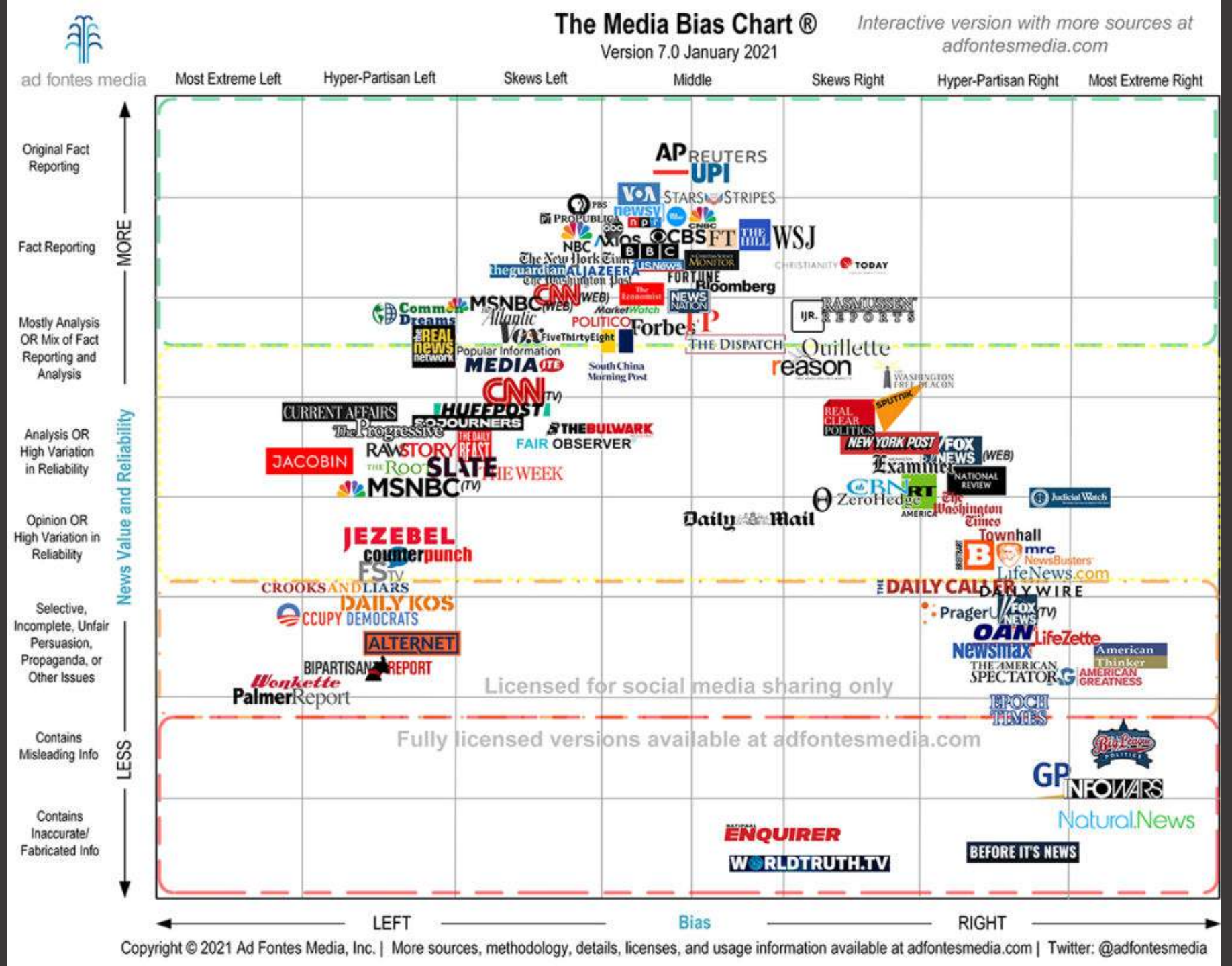
- The CNN and FOX viewers don't realize that they have different facts and therefore cannot have a meaningful discussion.
- *Neither do they realize that they were not told how many total people were on the boat, so they have no context for the fact they were presented*

Geopolitical influence on Public Opinion

- Hostile Nation States are using AI to manipulate your personalized news sources. We are not all seeing the same news in our feeds.
- Nation states are using Disinformation Operations against trusted democratic institutions and it is working.
  - This modern propaganda that is so tailored to the individual user that it becomes that persons' reality.
  - Our political leaders are not trained to counter this threat and will struggle to discover truth from fiction.
    - *Note the poorly crafted questions asked at the Zuckerberg hearings.*

Media Bias and Factual News

[Static MBC - Ad Fontes Media]



Geopolitical Threats to our Democracy – Russian Disinformation Operations

- “The mos… …nd the most direct" the Russians ever mou… …ed Putin to "strike at …
  - Jam…
- Russian … actually …
- *"Putin's Reve…* its mastermind's wildest dreams.
  - https://www.cnn.com/2017/10/25/entertainment/putins-revenge-frontline-review/index.html
  - https://www.pbs.org/wgbh/frontline/interview-collection/the-putin-files/

Fake news, even fake fact-checkers, found in run-up to U.S. midterms

Hasty headline-sharing makes us all prone to fall for hoaxes: we're not reading closely enough — if at all

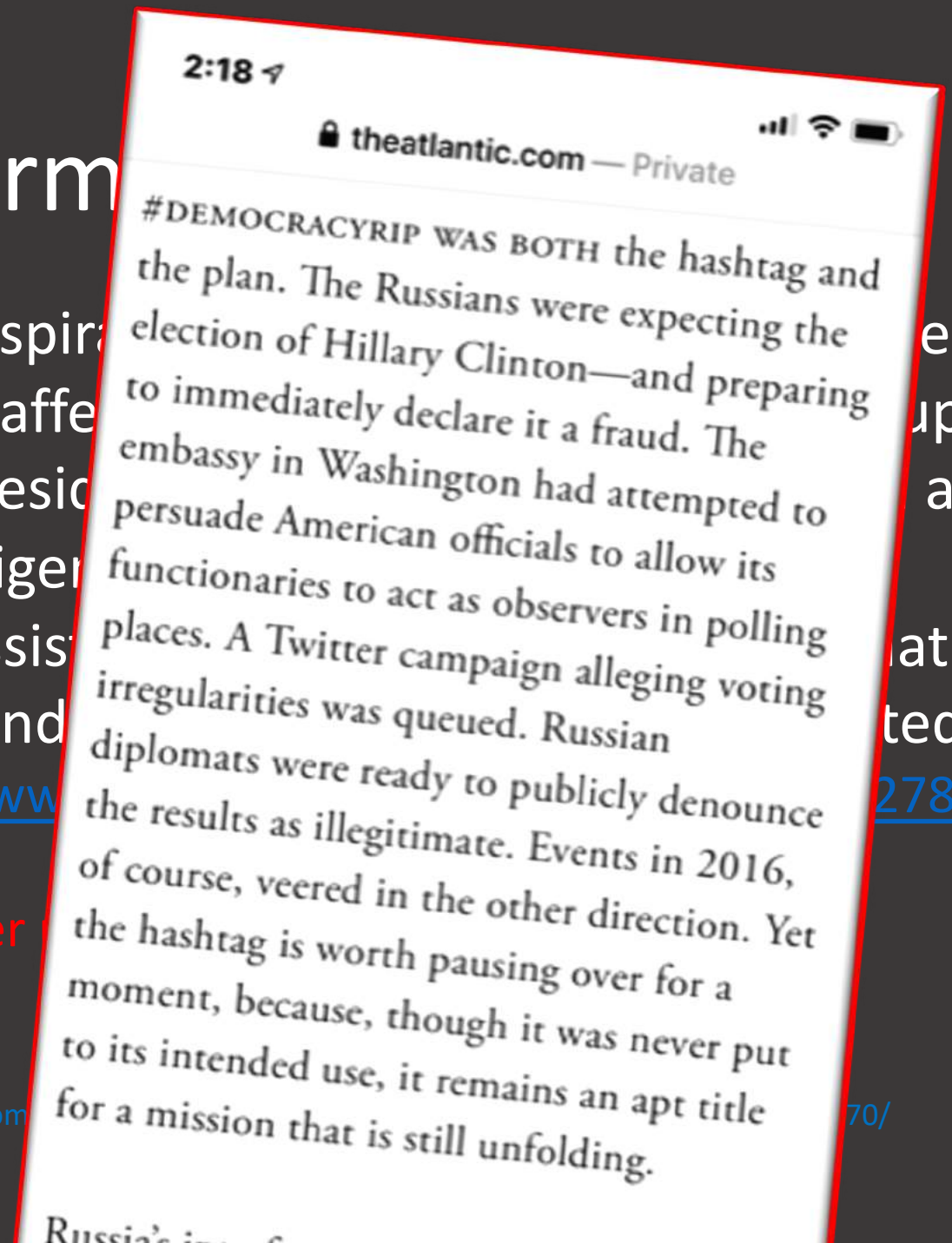
Ramona Pringle · CBC News · Posted: Nov 06, 2018 4:00 AM ET | Last Updated: November 6, 2018

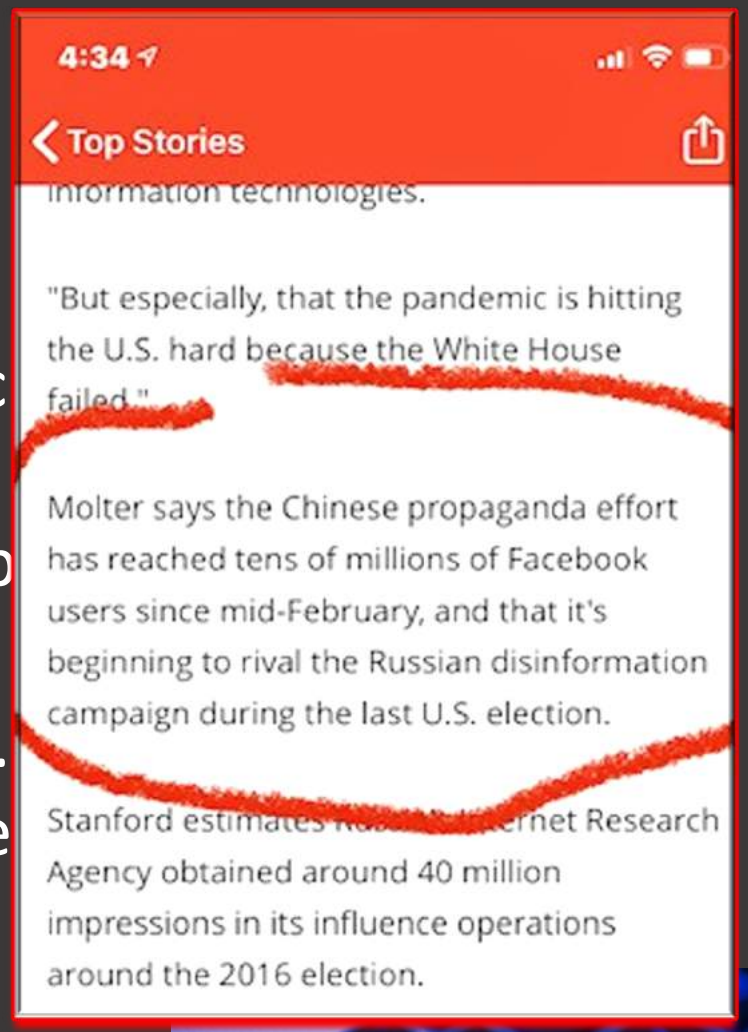
Disinform

In 2016 a conspir… emoc
Committee staffe… up on
by allies of Presid… and p
Russian intelliger…
- A former assis… at U.S.
officials found… ted the
https://ww… 27826

"Lock her …
"Killary"

https://www.theatlantic.com… 70/





Lessons Learned from the 2019 Canadian Elections

Learning from the Canadian National Elections in October 2019

- F… oreign
  - C…
    - …tes,

Sprint Wi-Fi VPN 10:33 PM 94%

Top Stories news

Researchers found evidence of Twitter troll activity in the last week of the federal election

Some of … #Trudeau … accounts … linking ther… and the Am…

Posted: October 25, 2019 1:00 AM PDT

Last Updated: 11 hours ago

Roberto Rocha, CBC News

Did Twitter trolls try to …

…nstalled on their …et visitors for …dian Press)

Most of Canada's top websites won't post federal election ads this year

Many of the most popular sites decided it was too late to set up a registry

Elizabeth Thompson · CBC News · Posted: May 01, 2019 4:00 AM ET | Last Updated: May 1

…during the … those videos violate the site's … standards.

…ews · Posted: May 29, 2019

Fal

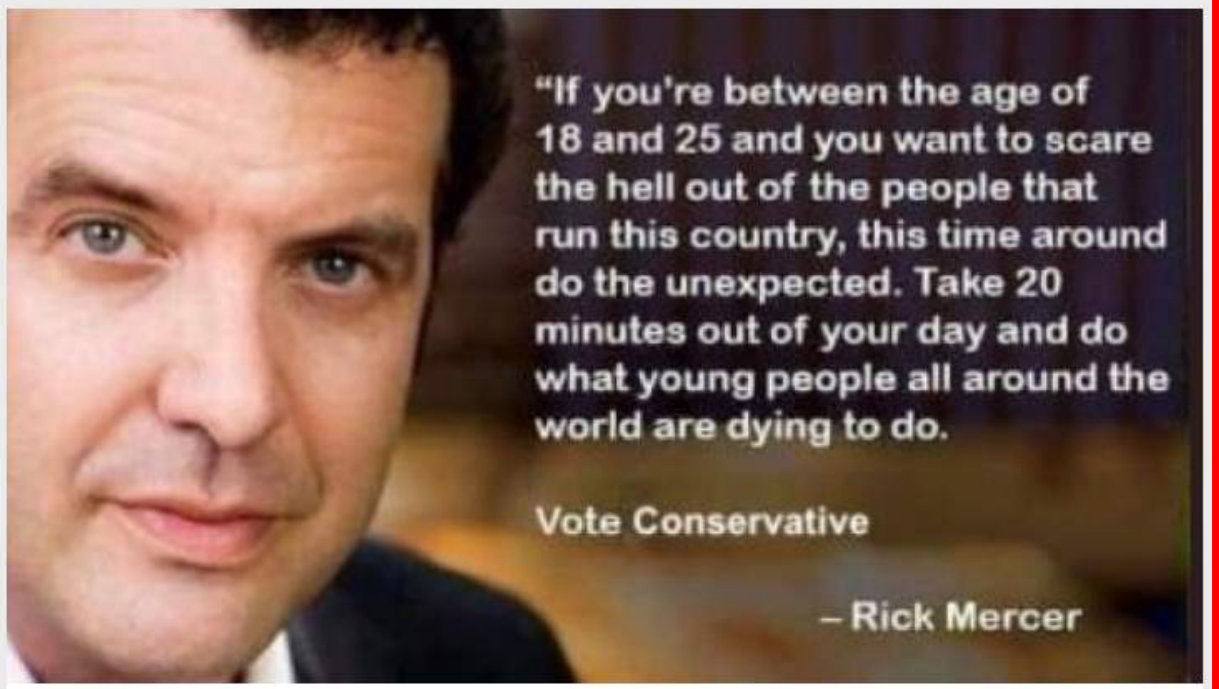
An c
to g
anal
c

Top Stories news

**False onl
claims R
married
Morneau**

The rumou
shows hov
false repor
during an election

Posted: September 18, 2019



Conservative riding association posts fake meme of Rick Mercer endorsing party

September 18

CBC | MENU

Sections

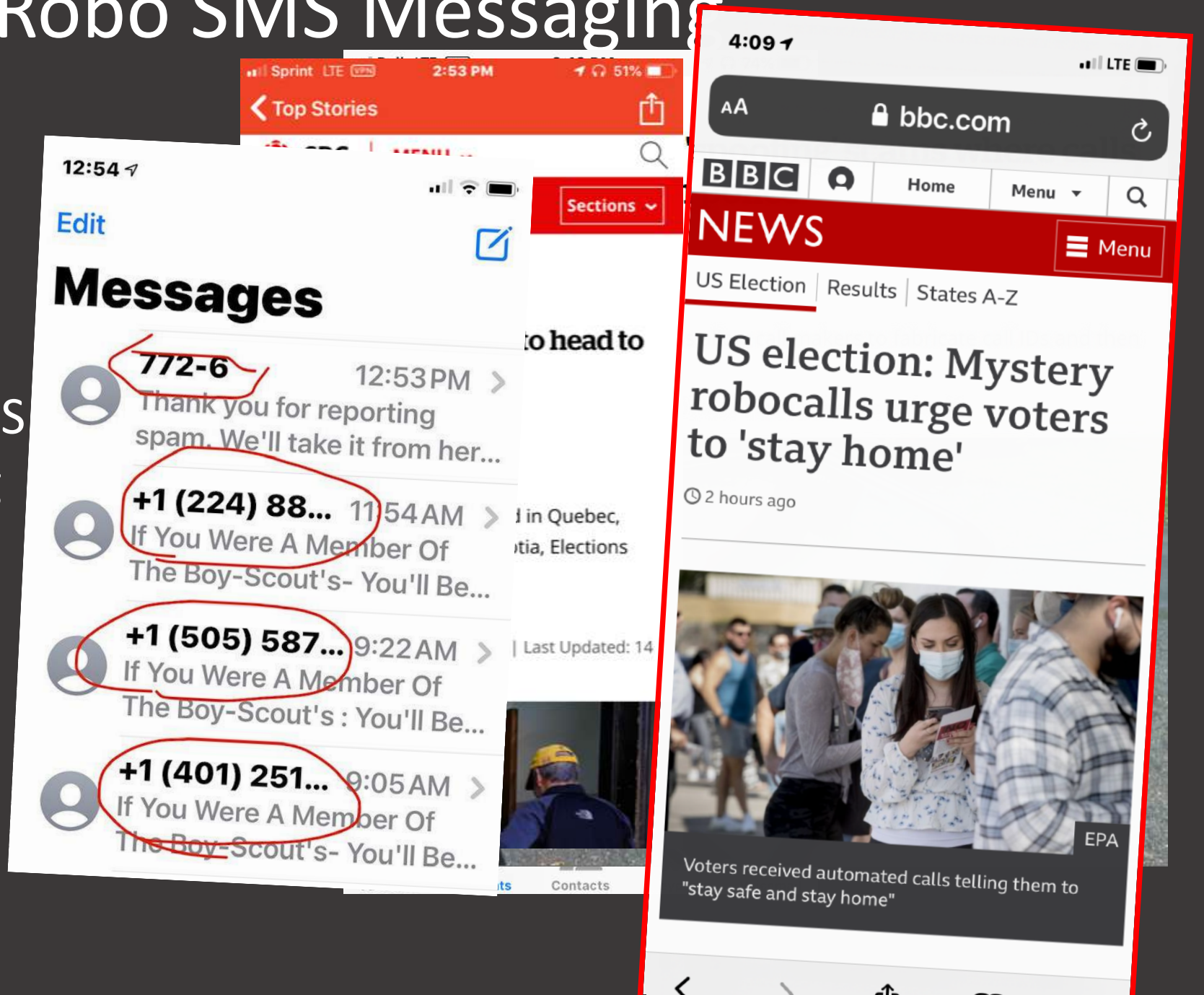
**ves forced to delete
ng Trudeau under
stigation**

demands Tories remove
omedian wants young
people to 'vote Conservative'

Peter Zimonjic · CBC News ·
Posted: Sep 17, 2019 8:10 PM ET | Last Updated:

Robo Calling, Robo SMS Messaging

- Robo call number sequencing last year in Canada
- Expect to see Robo SMS messaging for phishing in the US



Geopolitical Threats: Predictable Citizen Online Behavior

- "Research has shown that 6 out of 10 of [illegible] article just based on [illegible] prone [illegible]
  - "[illegible]
  - *read[illegible]*
- Click ba[illegible] model
  - https:/[illegible] readin[illegible] redirect=on

Social Media Threats to Democracy

Governments are calling for regulation becau
can no longer distinguish truth from dis

Citing U.S. social media failings

- https://www.bloomberg

- Ame to live-stream the worst mass
- Americ what is truth or even have the same facts

Geopolitical Threats to Democracy – Predictions

There were so many domestic disinformation posts that it didn't really matter.

- Russia's interference in 2016 was a [illegible] attacks for the 2020 US
- [illegible] poised and ready [illegible] night stating voting irregularities in swing states
- Iran and N Korea's involvement is less certain
- What will be the reaction from radical US voters?

Russia's Social Media Influence Operations – Multi-platform, Full Spectrum

Objective	Platforms	Purpose & Advantages
Placement	Primary: *4Chan, Reddit* Secondary: *8Chan, YouTube, Facebook*	• Insert forgeries into social media discussions • Seed conspiracies into target audiences • Spread kompromat on targeted adversaries, both true & false information • Hides Kremlin attribution, provides plausible deniability
Propagation	*Twitter*	• Spread narratives through overt Kremlin accounts & covert troll farm personas • Amplify select target audience stories & preferable narratives supporting Kremlin goals *(Computational propaganda make falsehoods appear more believable through repetition & volume)* • Inject stories into mainstream media worldwide • Attack political opponents, foreign policy experts & adversarial media personalities
Saturation	Primary: *Facebook* Secondary: *Google, LinkedIn, Instagram, Pinterest*	• Amplify political & social divisions, erode faith in democracy through discussions & ads • Pull content from other platforms into trusted friends & family discussions • Recruit target audience for organic propaganda creation/distribution or physical provocations (protests, rallies or even violence)
Hosting	*YouTube*	• Overt propaganda posts obscuring Kremlin hand (RT) • Sharing of video content to target audience via producers & reporters rather than standard television channels

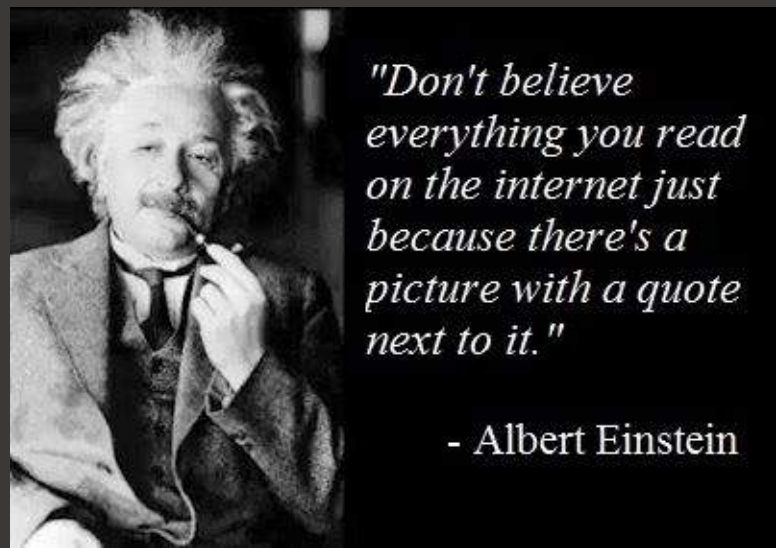
Source: C. Watts (Foreign Policy Research Institute, Alliance For Securing Democracy, Center For Cyber & Homeland Security)

So what can you do?

Get Your News from Reputable Sources

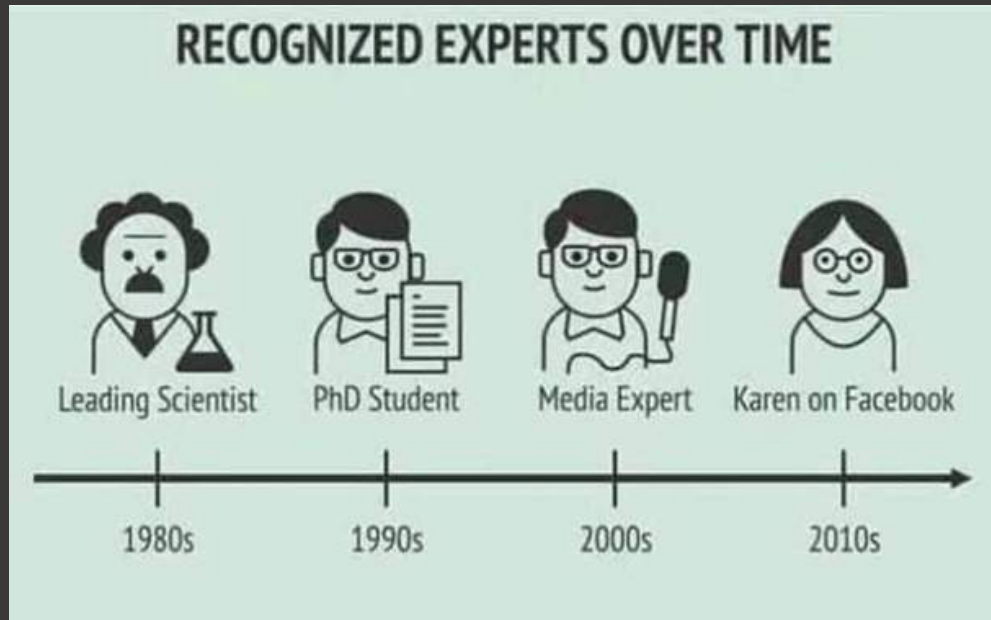
- Not Social Media!
  - Not Facebook, Instagram, Twitter or YouTube
  - Not from Memes! *Who do you think has the time to build all of those clever memes? Hint: Organizations that want to influence your thinking and behaviour.* Don't forward social media posts unless you created it.
- Get news from beyond your normal tailored news feeds! Not just Apple News, Google News, Putin News.
  - Tailored news plays to your implicate bias based on your previous online behavour.
  - You will only see what the algorithm thinks you want to see
  - You will be missing the opposing viewpoint
- Vary your news sources
- News shows are not news; their entertainment

Just No!

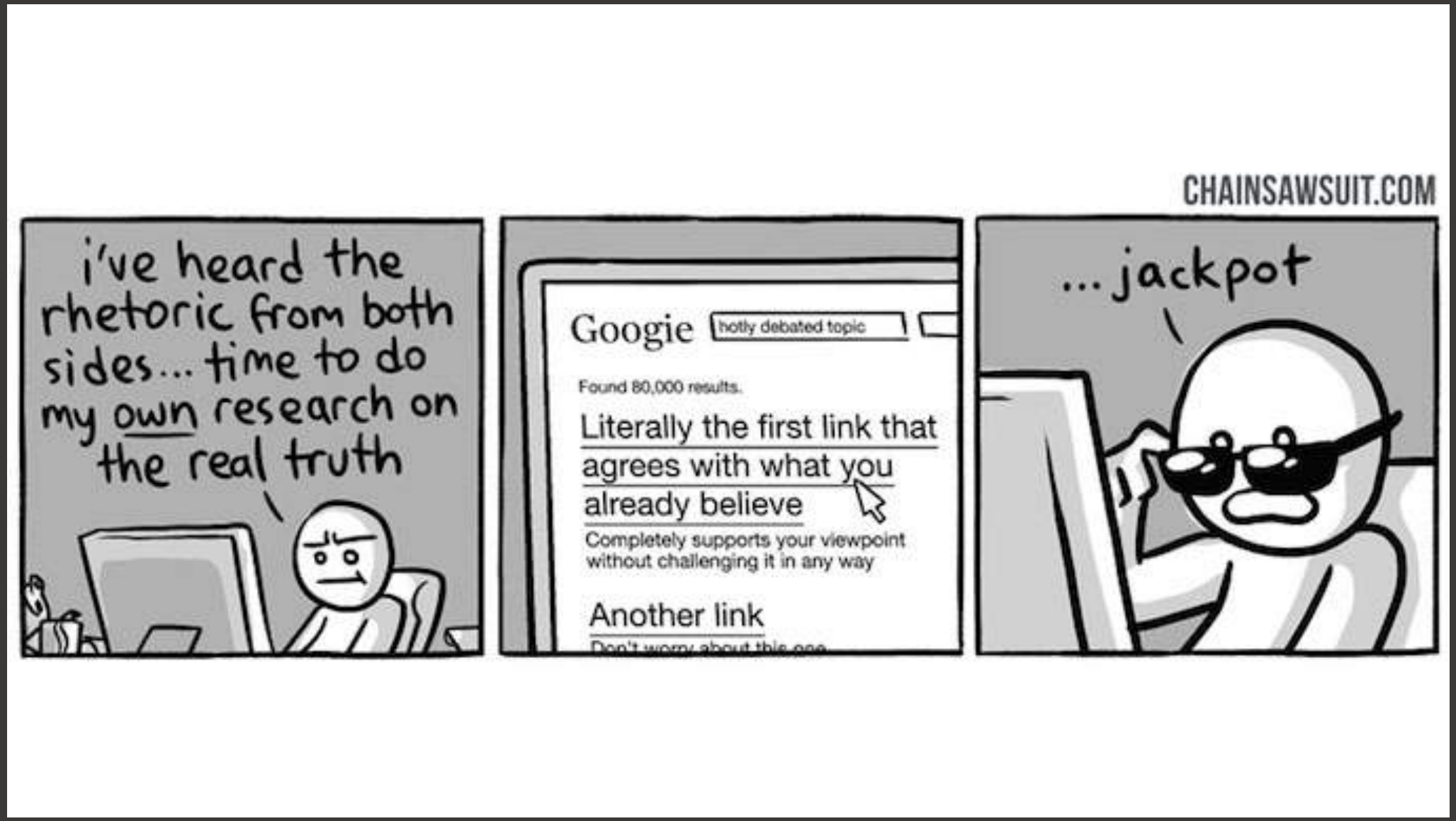


Critical Thinking beats Disinformation

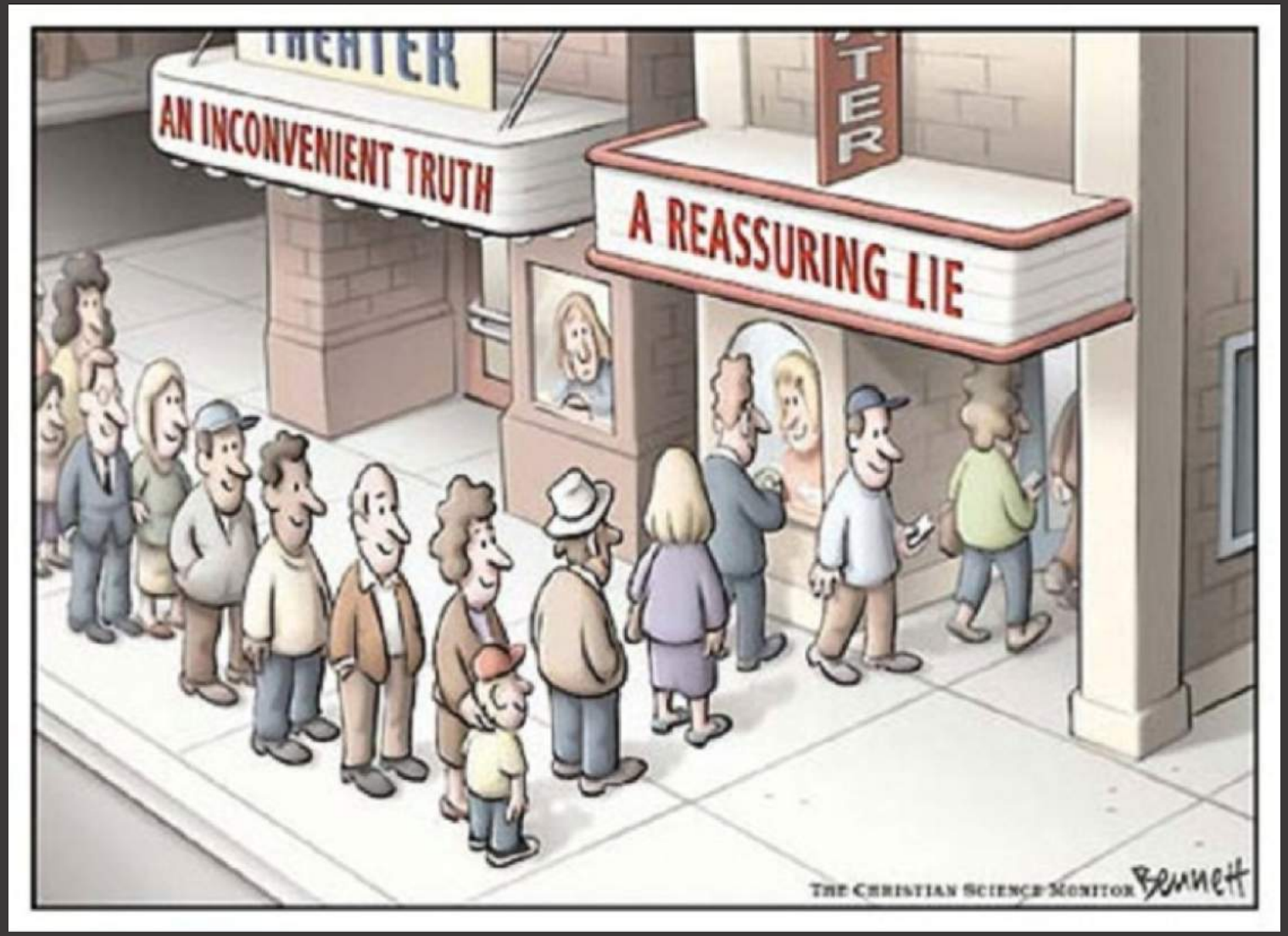
- Seek out the logical opposing view that wont show up in your news feeds.
  - Critical thinking always looks for multiple views of an issue.
  - When our personalized news feeds show the opposition as “idiots” you are being manipulated.
    - The opposition are logical people, and they will present well thought out views.
    - Always look for views that are presented as logical arguments. (Not sound bytes)
- Most of life is not sensational.
  - Daily life is generally mundane.
  - But the sensational gets us to click on the link.
  - Clicking on the link is what sells ads.
  - That’s how the eCommerce model works.



Confirmation Bias



Confirmation Bias



How to Spot Misinformation

https://crankyuncle.com/how-to-spot-and-tag-misinformation/

Tips to protect yourself from disinformation

- Is your Social Media being used against you?
- Is your news being manipulated to your current political beliefs?
- Are you receiving “fake” news? Where are the footnotes or references from the news article that you are being presented?
- Talking heads is not news; its commentary
- What are the credentials for the “Expert?”
- Don’t use a news source that you would not have used as a reference in a college research paper.
- Don’t get your news from Social Media or YouTube
- Always look for the opposing viewpoint.
- Are you being presented with bias news or cherry picked facts?
- What information is being omitted?
- Memes are not news: Ever wonder who has time to build all those Facebook memes?
- Dont forward social media posts that are not yours.
- Not all doctors are experts in epidemiology
- Not all scientist are climate scientist
- Recognize that a person that does not agree with your view may have different facts than you. Agree on all the relevant facts first. Not just the ones you may have.
- Always look for opposing views that are presented as logical arguments.
- Be open to new data that my change your viewpoint.
- **Show respect for the other person**

References

- https://www.fpri.org/article/2017/10/extremist-content-russian-disinformation-online-working-tech-find-solutions/
- https://www.rand.org/pubs/research_reports/RR2713.html
- https://www.scientificamerican.com/article/cognitive-ability-and-vulnerability-to-fake-news/
- https://www.cbsnews.com/news/trump-facebook-twitter-covid-19-flu/
- https://www.usatoday.com/story/tech/2020/09/22/fake-facebook-pages-accounts-from-china-targeted-election-trump-biden/3497641001/
- https://www.dw.com/en/zhenhua-data-leak-exposes-chinas-new-hybrid-warfare/a-55083540
- Balding warns that institutions and individuals in the West are underestimating the scale of the Chinese surveillance state and resources Beijing is pouring in to influence operations.
- "When democratic countries are faced with authoritarian threats that are seeking to influence individuals, politicians or universities, they should probably rethink the standards of data privacy and data security for citizens," he said.
- https://crankyuncle.com/how-to-spot-and-tag-misinformation/
- https://iopscience.iop.org/article/10.1088/1748-9326/aaa49f
- An effective rebuttal requires three elements. Fact. Myth. Fallacy. This video to explain how to tie these together into a cohesive debunking.
- https://eutoday.net/news/security-defence/2020/eeas-reports-fake-news
- *we urged the European Commission to counter aggressive Russian and Chinese propaganda efforts that are exploiting the COVID-19 pandemic to undermine the EU and sow mistrust in the local population towards the European Union.*
- https://www.adfontesmedia.com/