Fixing The Internet Of Sh*t

a.k.a. “How to design secure web apps”

A presentation by Greg Slepak

at

Greg Slepak

@taoeffect

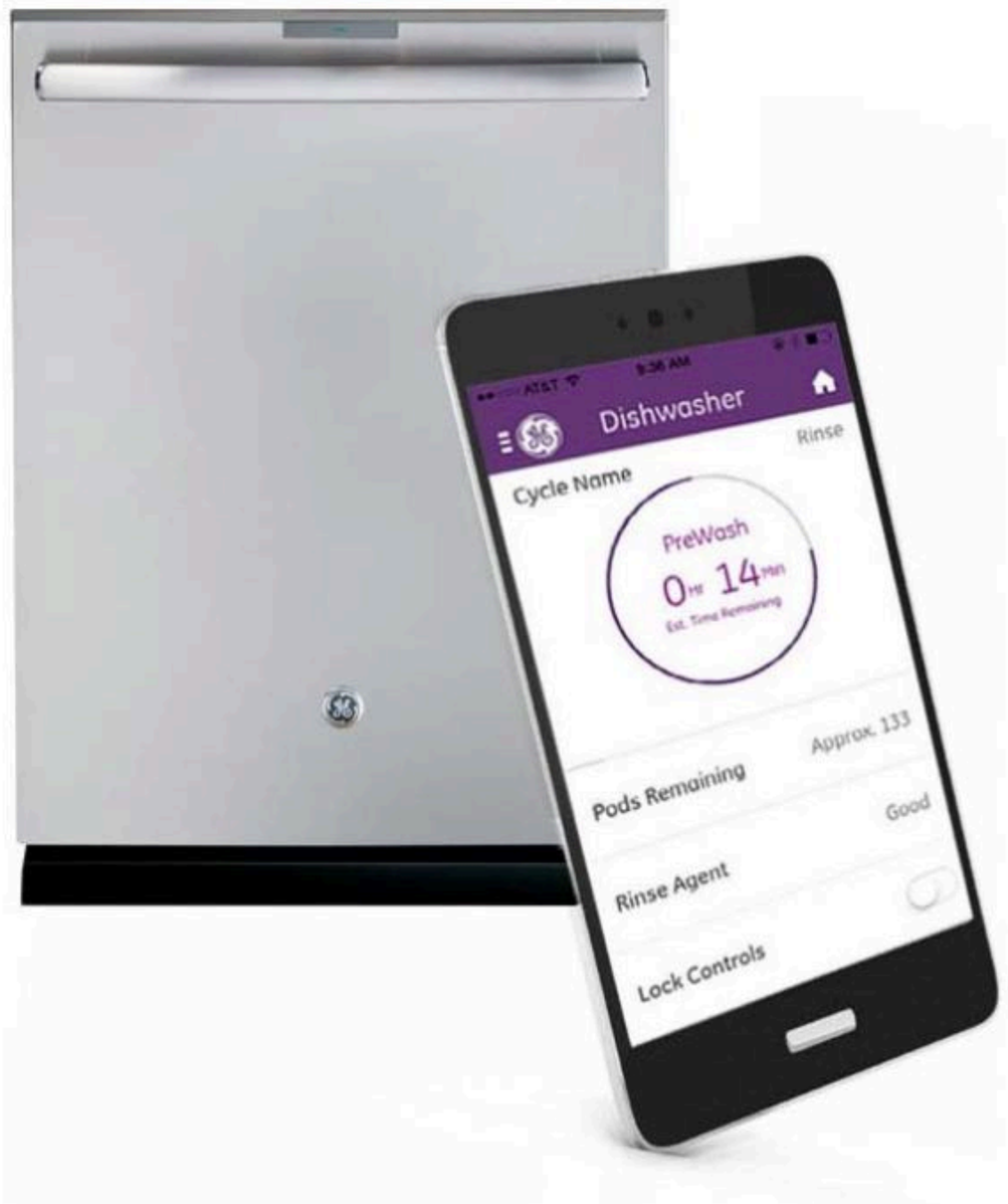
Espionage

okTurtles

GroupIncome

What


SAMSUNG
70°
MOSTLY SUNNY
John-
Congratulations!
Sunday brunch


AT&T
8:36 AM
Dishwasher
Rinse
Cycle Name
PreWash
0 Hr 14 Min
Est. Time Remaining
Pods Remaining
Approx. 133
Good
Rinse Agent
Lock Controls

Is

The Internet of 💩?

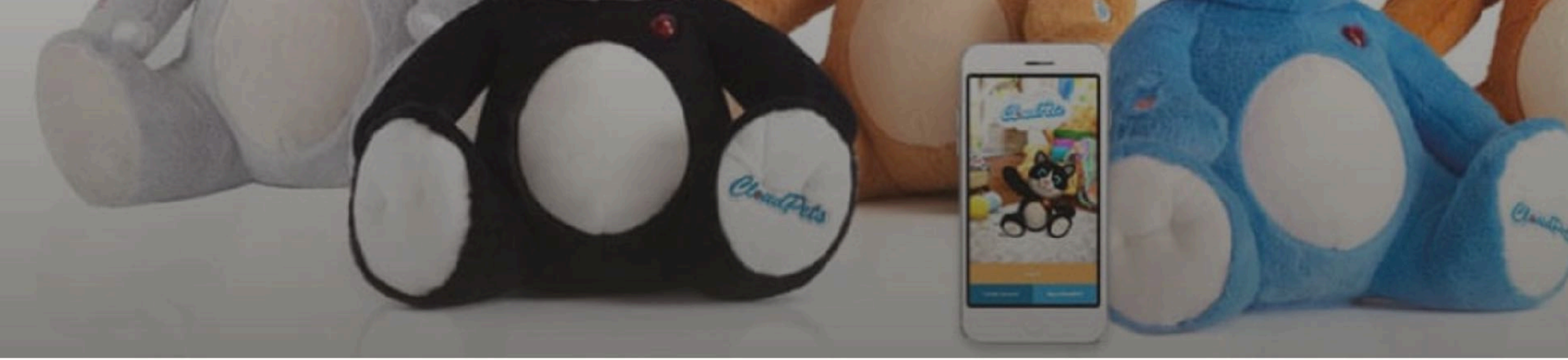
Internet of Shit
@internetofshit

Following

nice idea, but honestly i think this would make me *more* worried about the stove turning it self on

The Internet of 💩?

Inirv React is the first device that lets you control your stove from your smartphone and helps



Data from connected CloudPets teddy bears leaked and ransomed, exposing kids' voice messages

28 FEBRUARY 2017

Source: https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/

Germany bans internet-connected dolls over fears hackers could target children

share

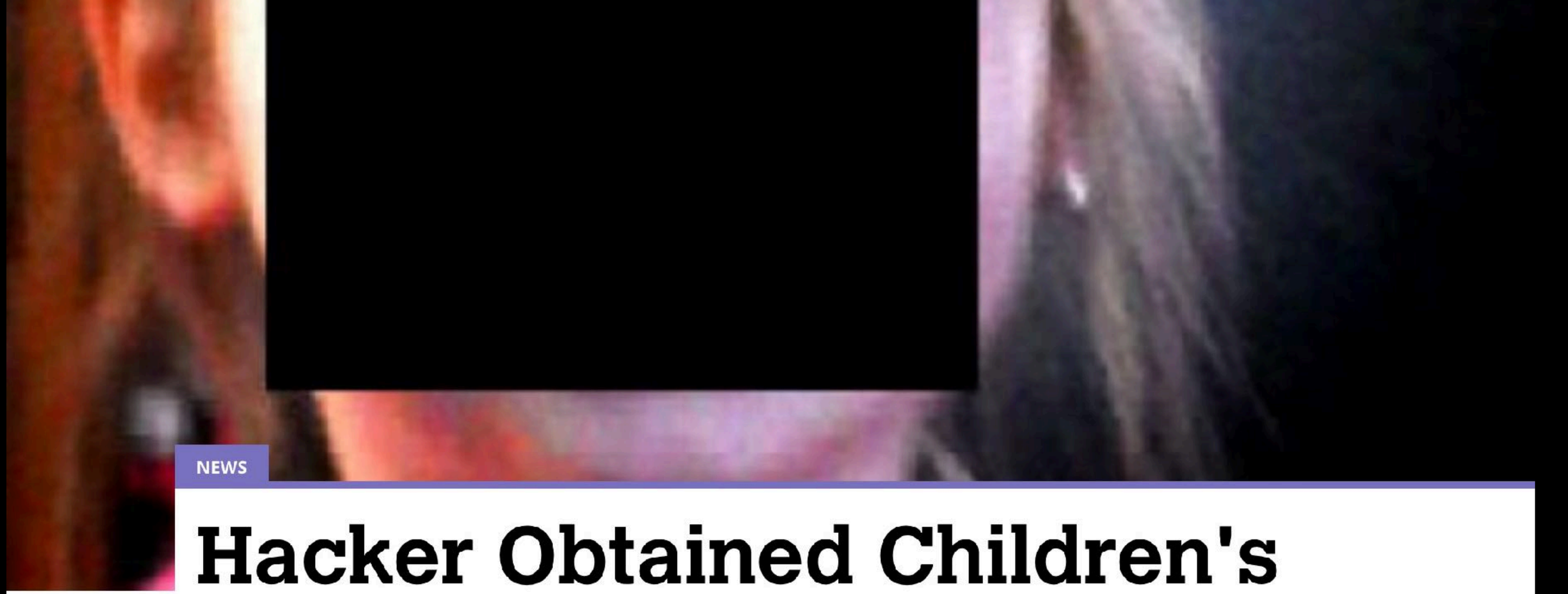
2 Comments

Cayla doll

By **Justin Huggler**, BERLIN

17 FEBRUARY 2017 • 5:02PM

Source: http://www.telegraph.co.uk/news/2017/02/17/germany-bans-internet-connected-dolls-fears-hackers-could-target/



NEWS

Hacker Obtained Children's Headshots and Chatlogs From Toymaker VTech

LORENZO FRANCESCHI-BICCHIERAI

Nov 30 2015, 10:57am

Source: https://motherboard.vice.com/en_us/article/hacker-obtained-childrens-headshots-and-chatlogs-from-toymaker-vtech

Watch Chinese Hackers Control Tesla's Brakes From 12 Miles Away

Thomas Fox-Brewster, FORBES STAFF

I cover crime, privacy and security in digital and physical forms. FULL BIO

SAN FRANCISCO, CA - AUGUST 10: A Tesla Model S is displayed inside of the new Tesla flagship facility on August 10, 2016 in San Francisco, California. (Photo by Justin Sullivan/Getty Images)

Source: https://www.forbes.com/sites/thomasbrewster/2016/09/20/keen-team-remotely-hack-tesla-cars/

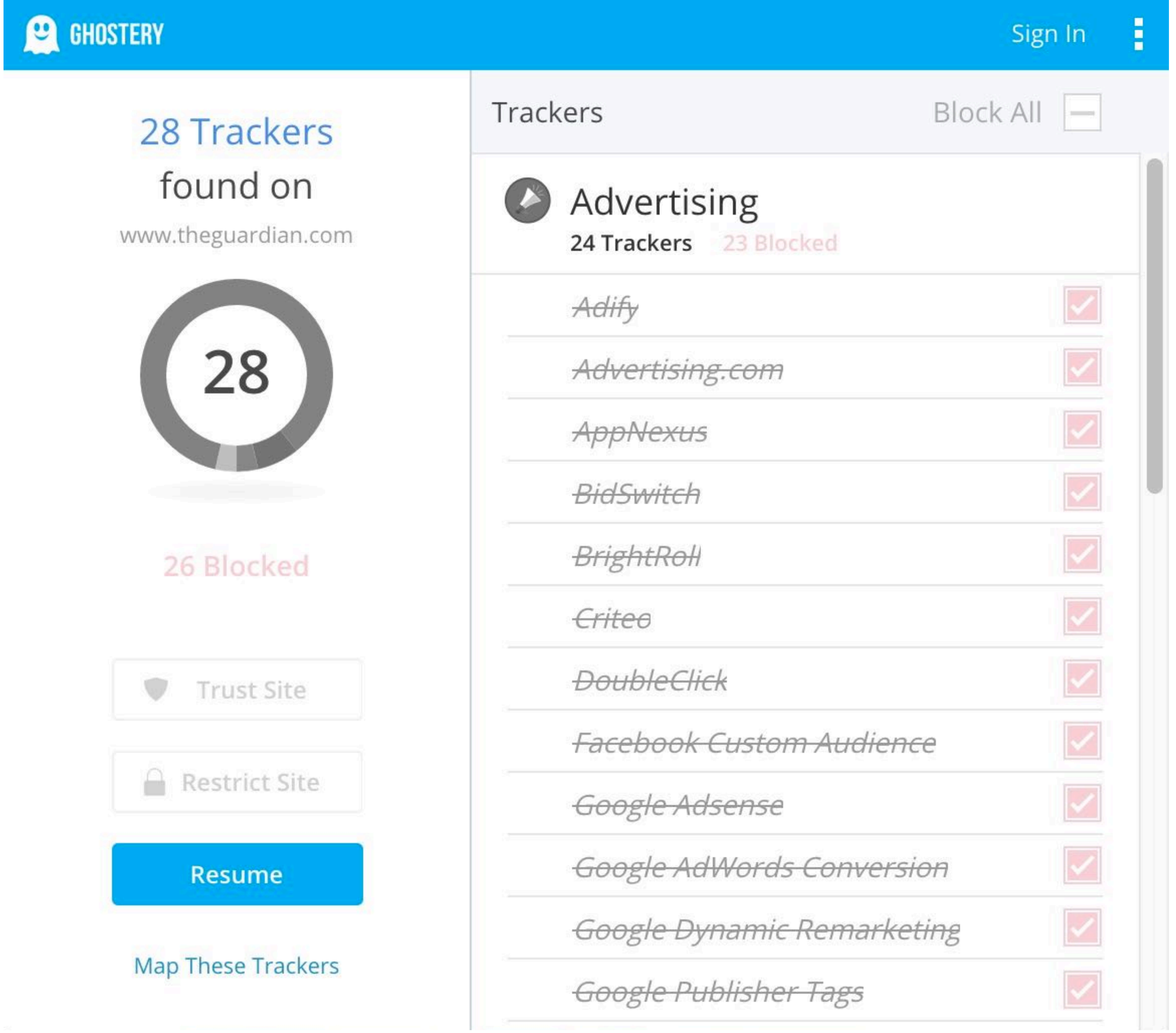
Vibrator Maker To Pay Millions Over Claims It Secretly Tracked Use

March 14, 2017 · 1:52 PM ET

CAMILA DOMONOSKE

Source: http://www.npr.org/sections/thetwo-way/2017/03/14/520123490/vibrator-maker-to-pay-millions-over-claims-it-secretly-tracked-use

It’s more than that.


GHOSTERY
Sign In
28 Trackers
found on
www.theguardian.com
28
26 Blocked
Trust Site
Restrict Site
Resume
Map These Trackers
Trackers
Block All
Advertising
24 Trackers
23 Blocked
Adify
Advertising.com
AppNexus
BidSwitch
BrightRoll
Criteo
DoubleClick
Facebook Custom Audience
Google Adsense
Google AdWords Conversion
Google Dynamic Remarketing
Google Publisher Tags

It’s more than that.

MARCH 19, 2017 | BY JEREMY GILLULA

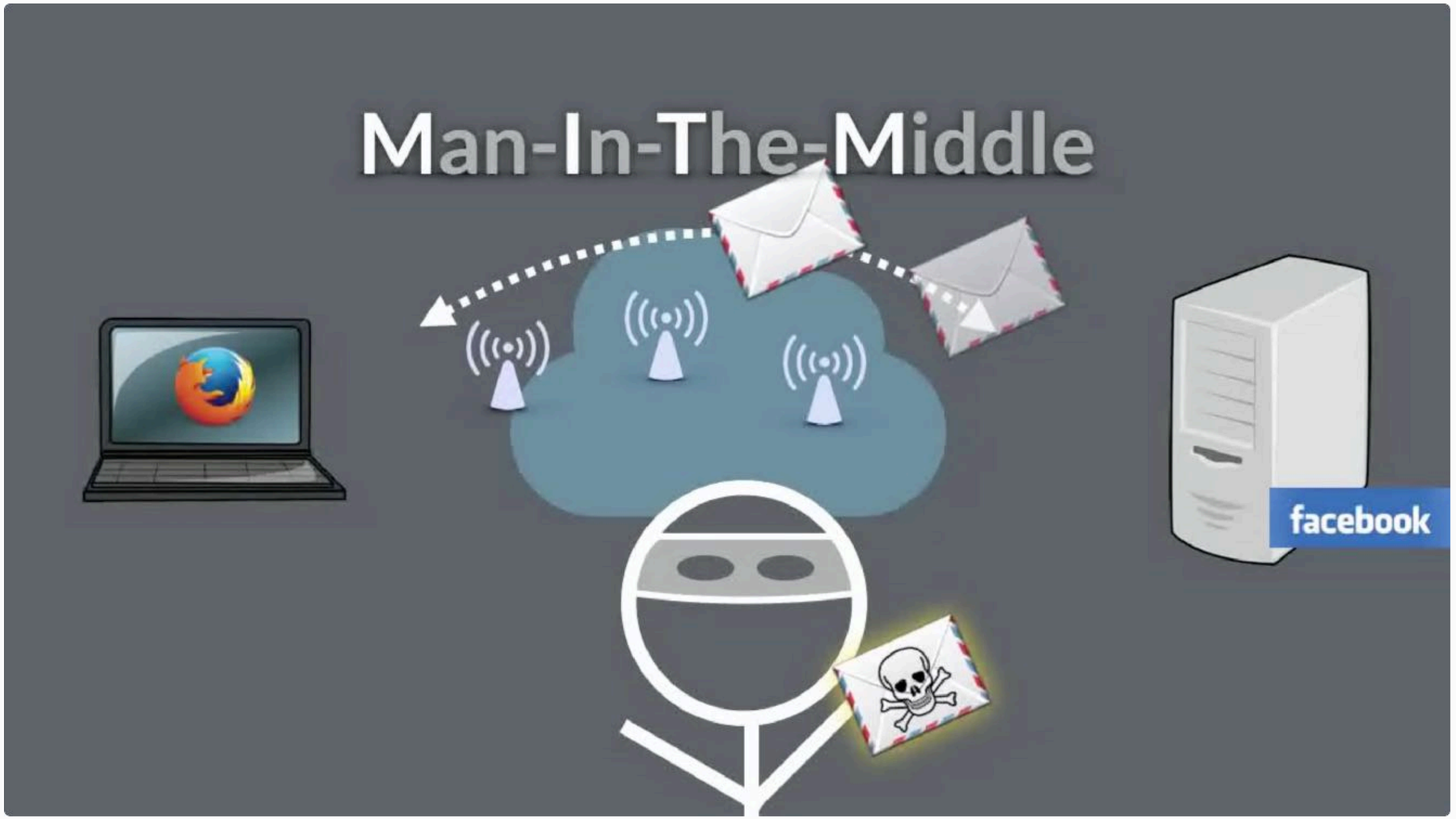
Five Creepy Things Your ISP ~~Could Do~~ if Congress Repeals the FCC's Privacy Protections

Already, *currently*, do!

1. **Injecting undetectable, undeletable tracking cookies in all of your HTTP traffic**
2. **Pre-installing software on your phone and recording every URL you visit**
3. **Snooping through your traffic and inserting ads**
4. **Hijacking your searches**
5. **Selling your data to marketers**

Source: https://www.eff.org/deeplinks/2017/03/five-creepy-things-your-isp-could-do-if-congress-repeals-fccs-privacy-protections

It’s more than that.



Alt video link: https://youtu.be/7QLaKW8ABy4?t=21s

It’s more than that.

Dmitry Chestnykh
@dchest

Follow

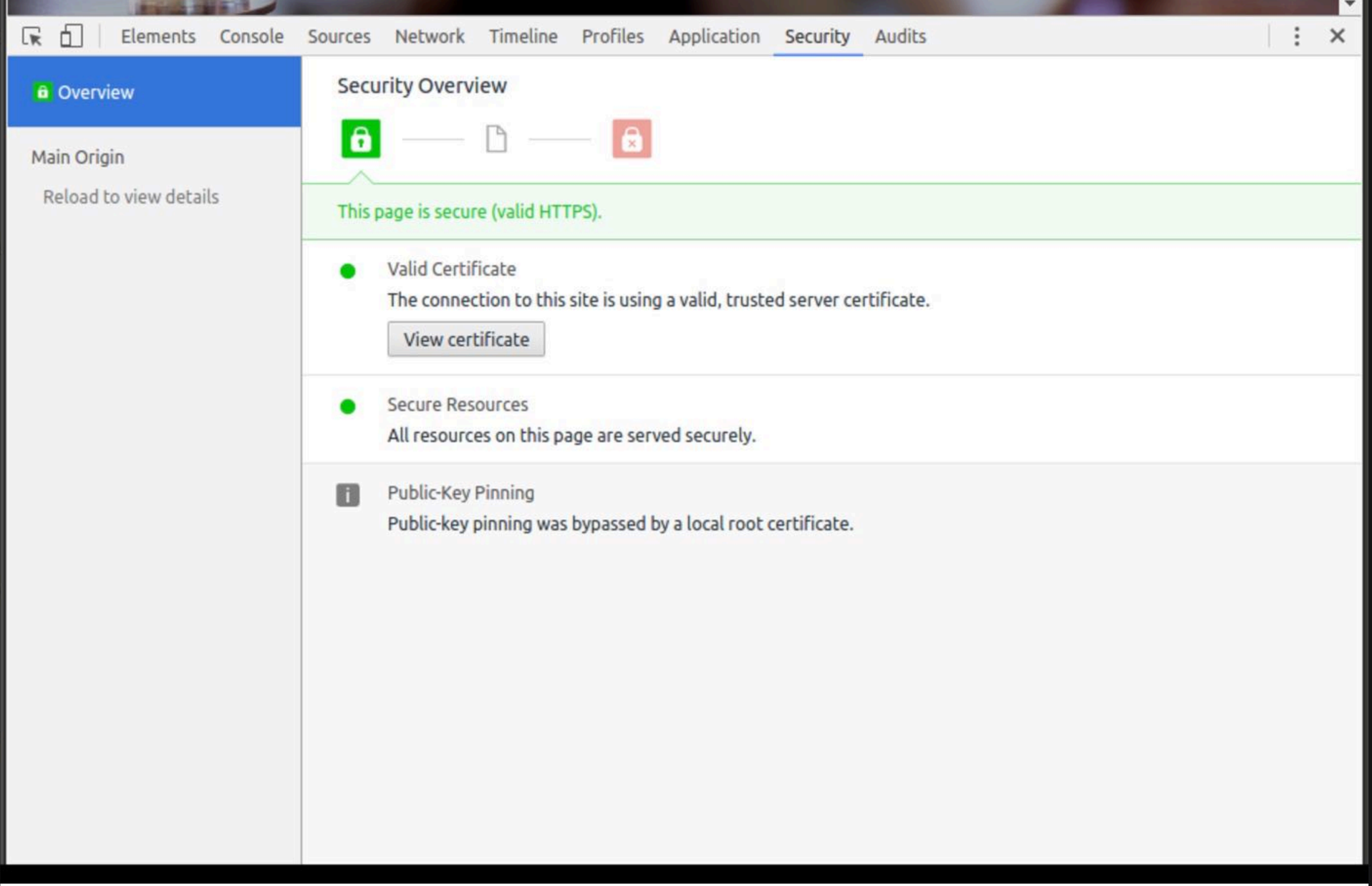
Amazon Drive Platform terms: “Don’t build apps that encrypt customer data” 👆 developer.amazon.com/public/apis/ex …

What Not To Build

We understand that developers spend a lot of time creating apps that customers love to use. We want to give you some guidelines for apps not to build on the Amazon Drive platform to save you time in building something that will not be approved during the App Review process. While this isn't an all-inclusive list, focus your energy on developing apps that solve customer problems, which don't violate our Terms of Use, Brand Guidelines and the App Distribution and Services Agreement.

- Don’t build apps that support commercial use
- Don’t build apps that encrypt customer data
- Don’t build apps that harm customers or their data
- Don’t build apps that make excessive requests to the API
- Don't build apps that infringe trademark, copyright or intellectual property
- Don't build apps that scrape content or allow customers to copy content from websites
- Don't build apps that promote illegal peer-to-peer file sharing
- Don’t build apps that use business names and/or logos in a manner that can mislead, confuse or deceive customers (e.g., do not copy the look and feel of Amazo Drive branded apps)
- Don't build apps that confuse or mislead customers
- Don't build apps that impersonate or facilitate impersonation of others in a manner that can mislead, confuse or deceive customers

Source: https://twitter.com/dchest/status/846786101020909568



Greg Slepak @taoeffect · 4 Jul 2016

This is @ChromiumDev's idea of "showing people they're being MITM'd":
bugs.chromium.org/p/chromium/iss… pic.twitter.com/NKdAbUbNjP

Source: https://twitter.com/taoeffect/status/750200660272885764

Filippo Valsorda 
@FiloSottile

Follow

Sigh. TLS 1.3 temporarily turned off in Chrome Stable because of intercepting proxies. bugs.chromium.org/p/chromium/iss…

BlueCoat and other proxies hang up during TLS 1.3

Project Member Reported by jayhlee@google.com, Feb 21

```
Chrome Version: 56
OS: Chrome and Windows

What steps will reproduce the problem?
(1) BlueCoat 6.5 proxy.
(2) Chrome OS 56 or Chrome browser 56
(3) Attempt to connect to a Google service (youtube, accounts.google.com, etc.

What is the expected result?
Successful connection. Client and proxy may negotiate down to TLS 1.2 instead of TLS 1.3.

What happens instead?
When Chrome attempts to connect via TLS 1.3, BlueCoat hangs up connection.
```

Source: https://twitter.com/FiloSottile/status/835269932929667072

Source: https://bugs.chromium.org/p/chromium/issues/detail?id=694593

Blue Coat

American Company Blue Coat, specialized in online security, is best known for its Internet censorship equipment. This equipment also allows for the supervision of journalists, netizens and their sources. Its censorship devices use Deep Packet Inspection, a technology employed by many western Internet Service Providers to manage network traffic and suppress unwanted connections.

The Company

Country of origin: USA
Website:www.bluecoat.com

Blue Coat is a large IT company based in Sunnyvale, California, that is best known for providing filtering and censorship devices for countries such as Syria and Burma. The company also provides network analysis systems called "Intelligence Centres," which are used by companies and governments to monitor online traffic and identify performance problems. They allow for the monitoring of individual online behaviour.

*They're listening to **this** company. Not you.*
*Compromising your **home** Internet connection to secretly spy on employees.*

Source: https://surveillance.rsf.org/en/blue-coat-2/

Catalin Cimpanu
@campuscodi

Follow

Sounds about right: "Google has officially vertically integrated the Internet."

aduffy 19 hours ago [-]

You can now have a website secured by a certificate issued by a Google CA, hosted on Google web infrastructure, with a domain registered using Google Domains, resolved using Google Public DNS, going over Google Fiber, in Google Chrome on a Google Chromebook. Google has officially vertically integrated the Internet.

reply

Study shows Google may influence how you vote

Cynthia McKelvey—Aug 4, 2015 at 11:46AM | Last updated Dec 11, 2015 at 6:20AM

The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections

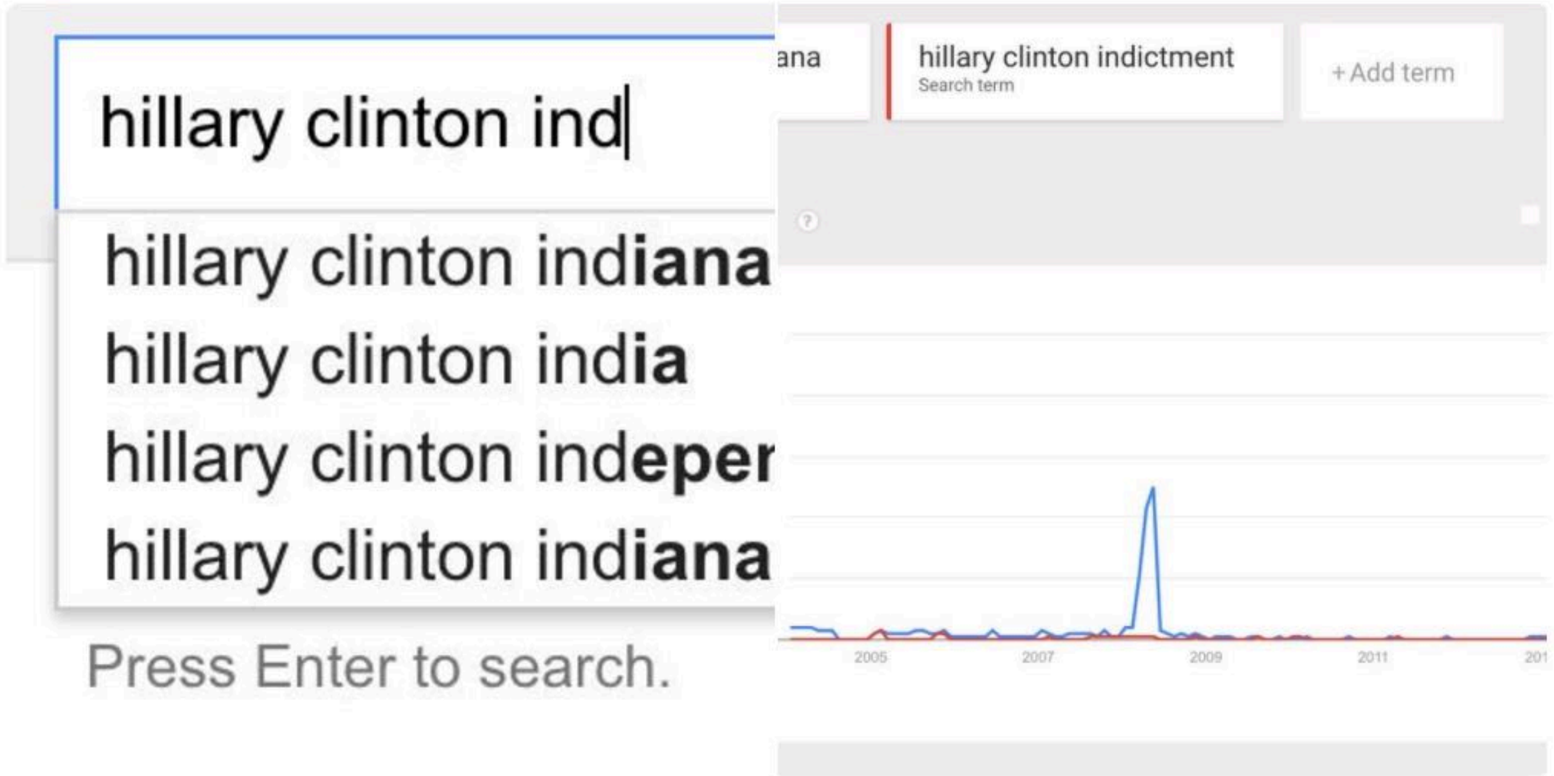
Robert Epstein[1] and Ronald E. Robertson

Source: https://www.dailydot.com/layer8/search-engine-manipulation-effect-election/

Source: http://www.pnas.org/content/112/33/E4512.abstract

Greg Slepak
@taoeffect

.@google appears to be manipulating the election: youtube.com/watch?v=PFxFRq… HT @SourceFed



Source: https://twitter.com/taoeffect/status/741330301943615490

Source: https://twitter.com/taoeffect/status/741355355448303616

Source: https://lobste.rs/s/5har3y/google_appears_be_manipulating_election/comments/agd297#c_agd297

YouTube

Search

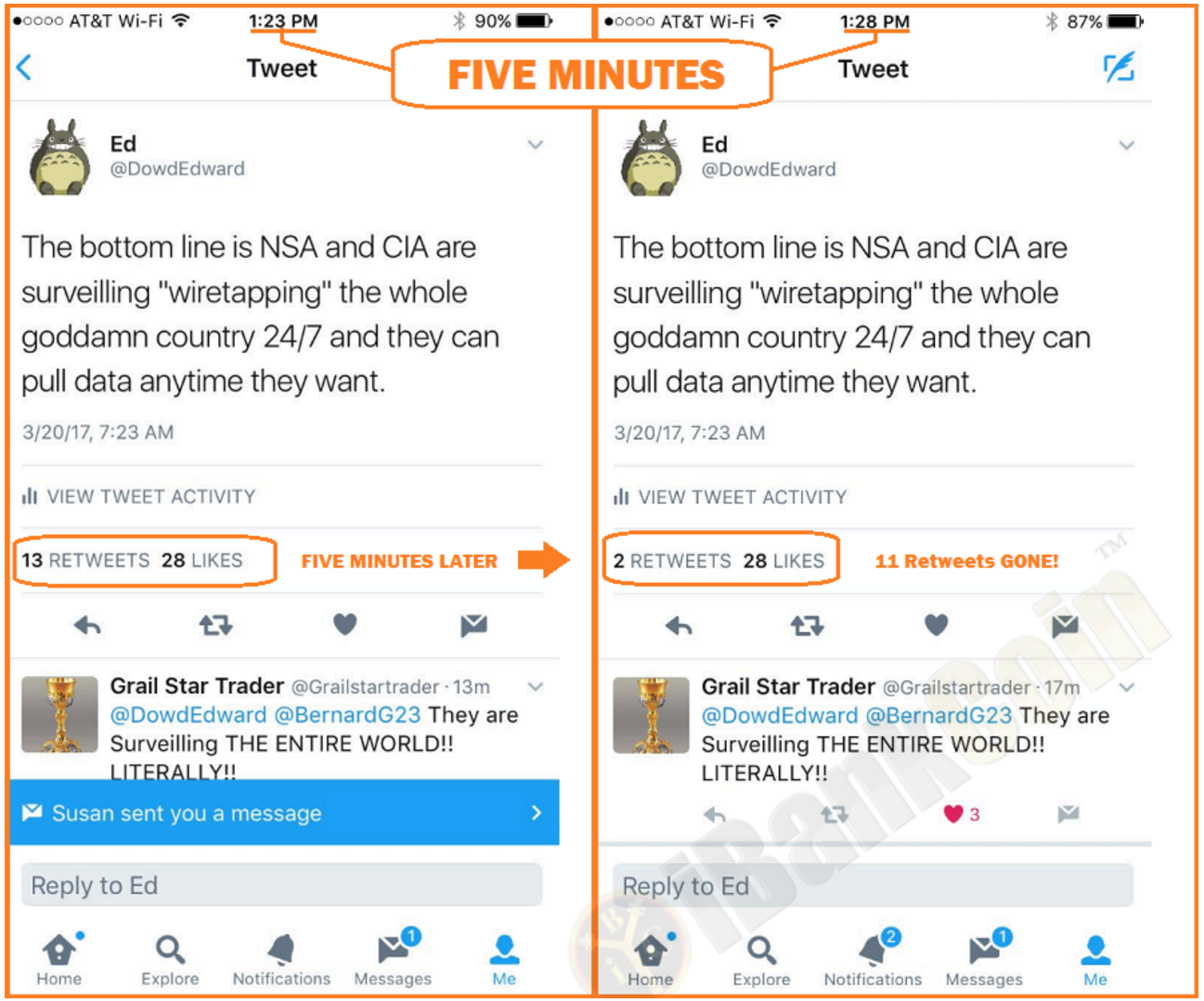
This video is unavailable.

Sorry about that.

“Sorry about that.”

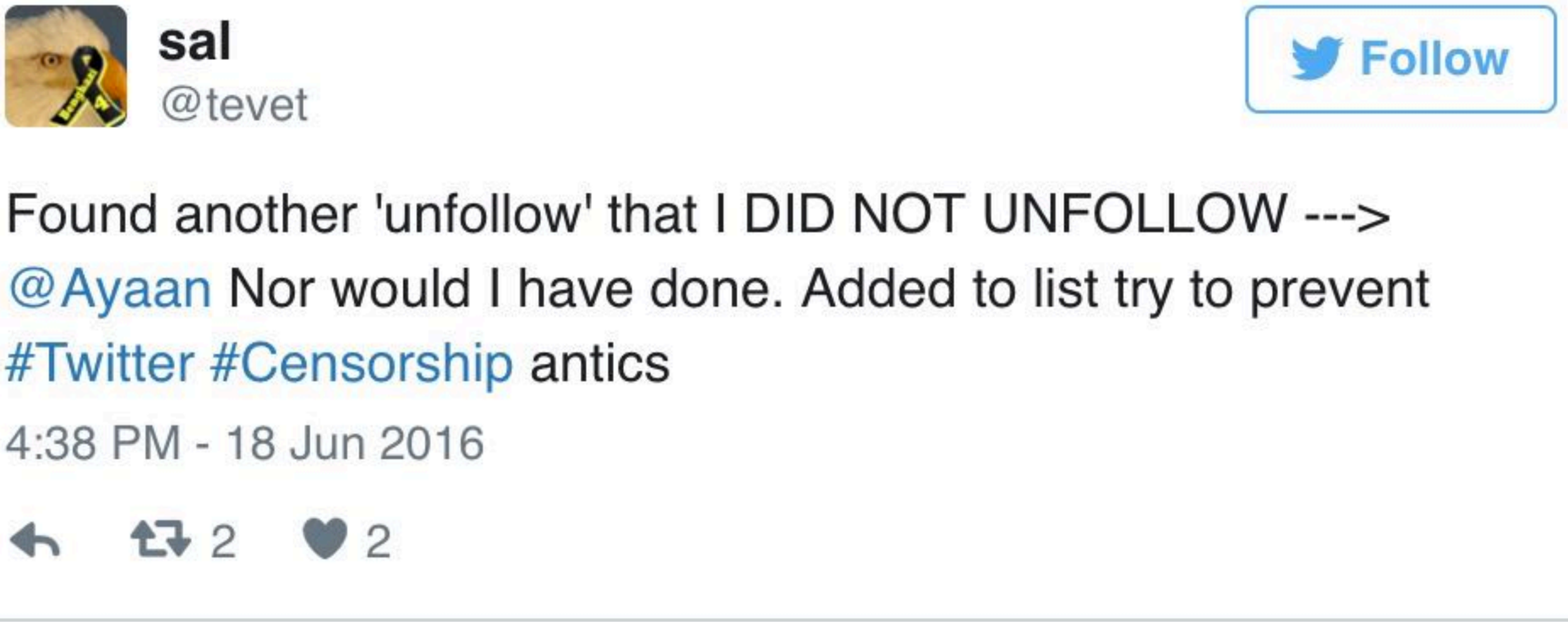
Speaking of censorship…

BUSTED! Twitter Caught Manipulating Tweets Of Former BlackRock Fund Manager Critical Of CIA and NSA



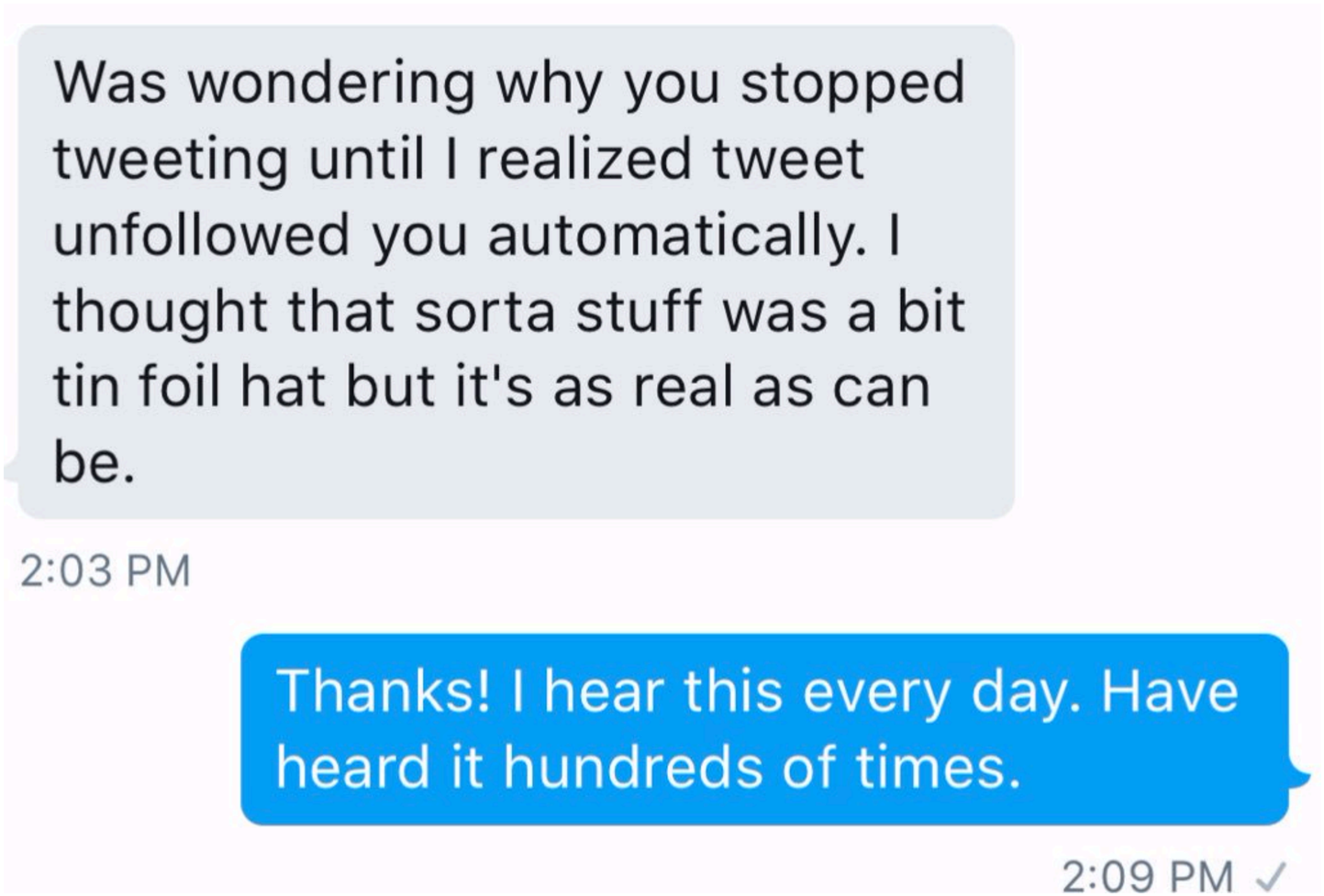
Source: http://www.zerohedge.com/news/2017-03-23/busted-twitter-caught-manipulating-tweets-former-blackrock-fund-manager-critical-cia

BUSTED! Twitter Caught Manipulating Tweets Of Former BlackRock Fund Manager Critical Of CIA and NSA



Source: http://www.zerohedge.com/news/2017-03-23/busted-twitter-caught-manipulating-tweets-former-blackrock-fund-manager-critical-cia

BUSTED! Twitter Caught Manipulating Tweets Of Former BlackRock Fund Manager Critical Of CIA and NSA



Source: https://twitter.com/Cernovich/status/829814703656357889

Greg Slepak
@taoeffect

How often does this happen to your tweets?
fixingtao.com/other/images/t …

0% 1/week or more

0% 1/month or more

17% all the time

83% never?

6 votes • Final results

Tweet Activity

Greg Slepak @taoeffect
Which is better and why?

No one has engaged with your Tweet… yet.
Please check back later!

Source: https://twitter.com/taoeffect/status/844312296981639168

Greg Slepak
@taoeffect

Have you noticed tweet notifications automagically disappear / get cleared on your device's lock screen by themselves?

19% I've paid attention, & Y

25% I've paid attention, & N

56% I haven't paid attention

16 votes • Final results

Source: https://twitter.com/taoeffect/status/841410104125620225

Greg Slepak
@taoeffect

Twitter apparently deleting people's tweets now.

> **AJ Joshi** @AJ
> @taoeffect I didn't delete that (from memory) it was disconnected

Source: https://twitter.com/taoeffect/status/834537993985679360

“Bugs”?

The “Internet of Sh*t”
is
“The Internet”

…ok.

… what happened to
“fixing it”?

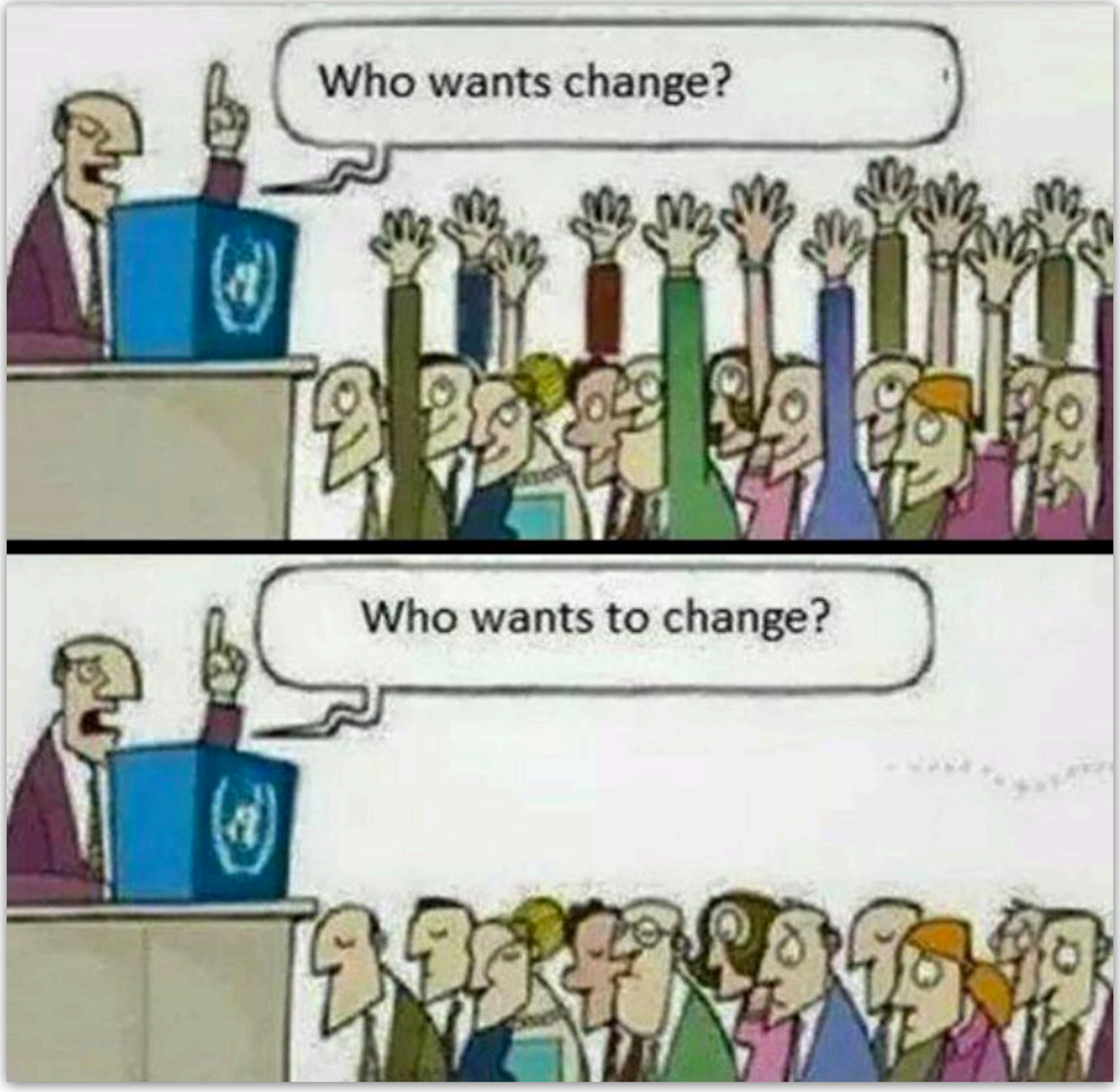
A better question is:

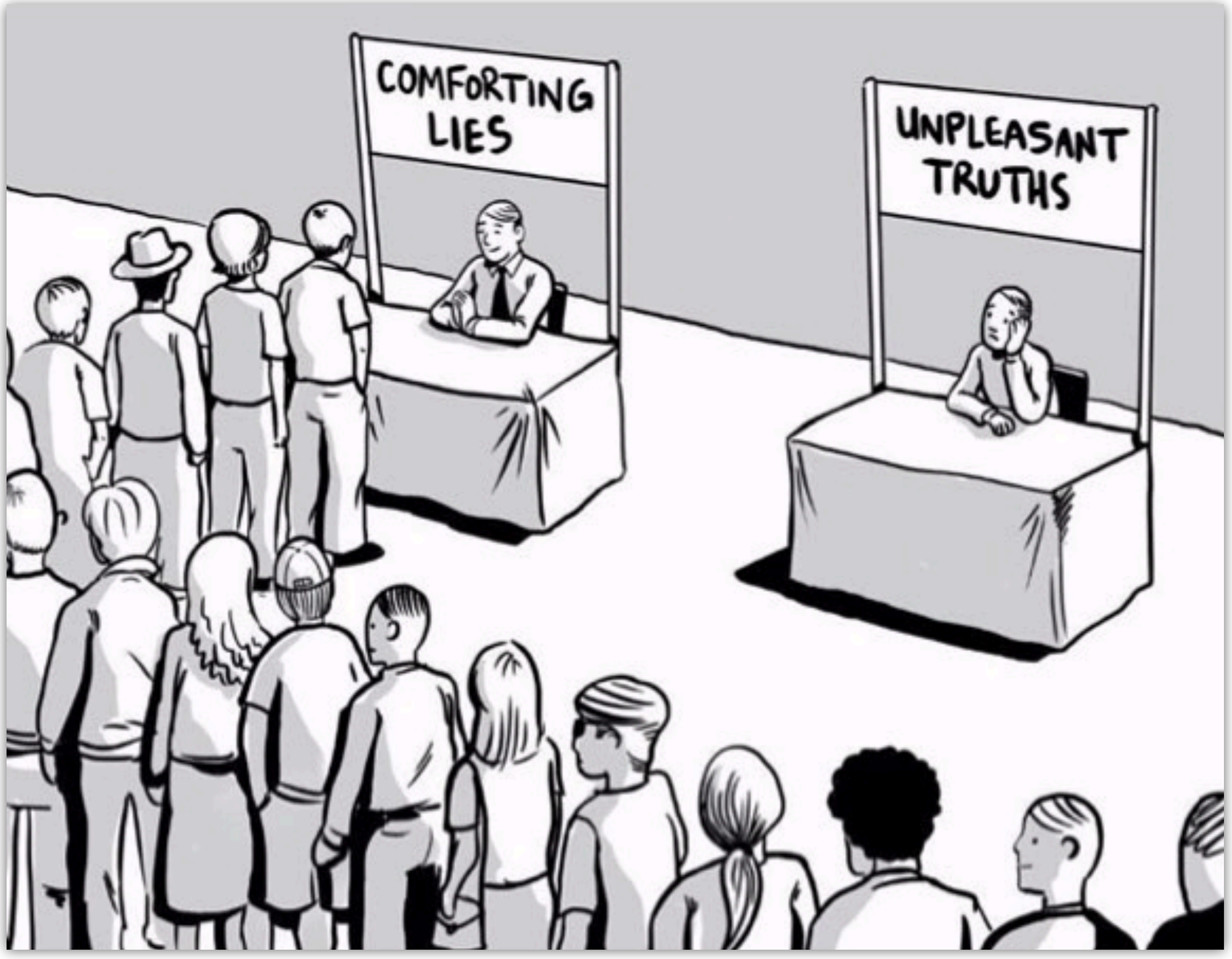
Do you *want* to fix it?

Raise your hand
if you want this fixed

Raise your hand
if *you* would **help** fix this

(if you could)


Who wants change?
Who wants to change?


COMFORTING LIES
UNPLEASANT TRUTHS

Before we start,
a few inspirational quotes

:-)

“Be the change you want to see in the world.”

“Insanity is doing the same thing over and over and expecting a different result.”

“80% of solving a problem is understanding it.”

so… you’re 80% there already???

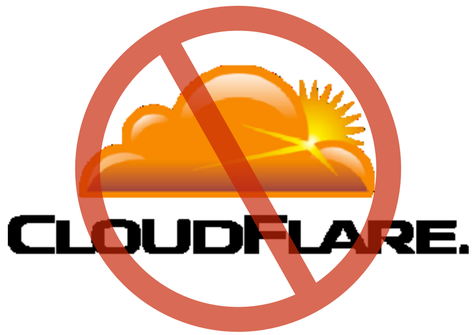
Break Down The Problem Into Manageable Pieces

1. Economic

2. Technological

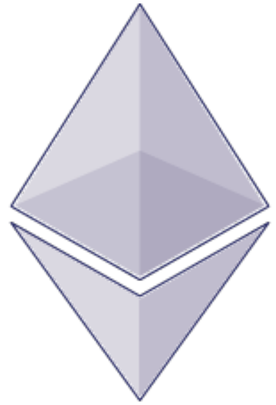
Economic

Invest in *solutions* instead of *problems*



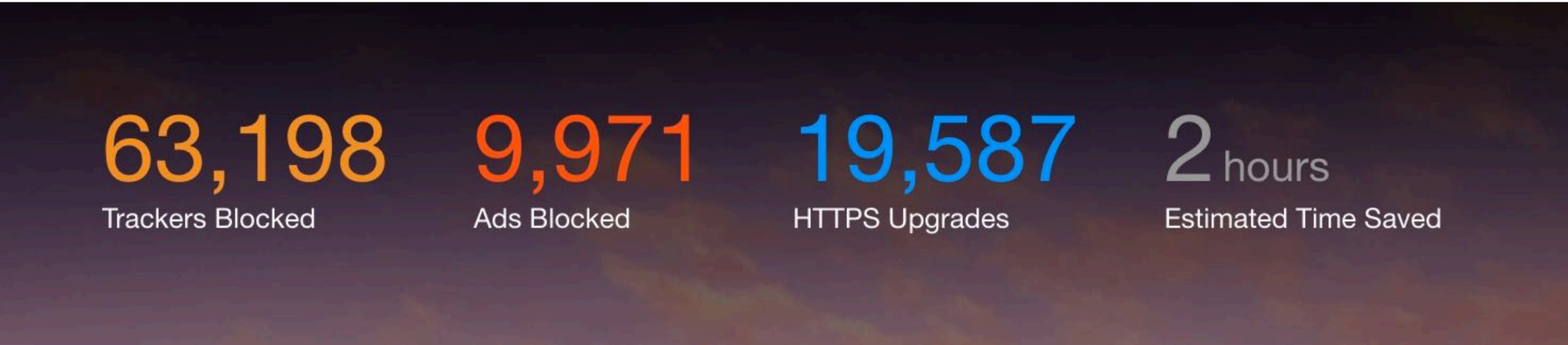
Invest in decentralization






And use small(er) VPS providers

Brave


63,198
Trackers Blocked
9,971
Ads Blocked
19,587
HTTPS Upgrades
2 hours
Estimated Time Saved

Explore new economic systems

GroupIncome

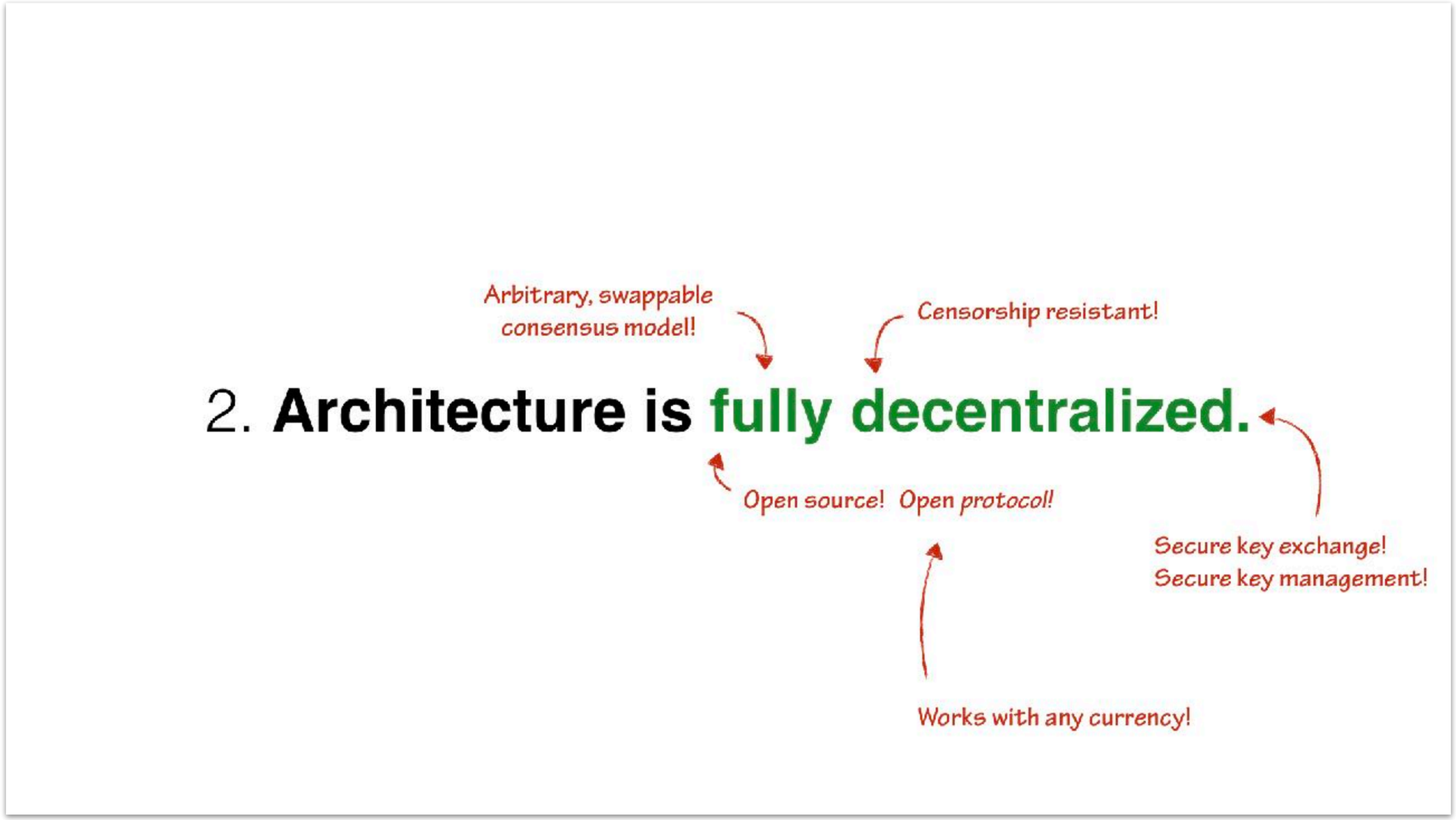
Patreon

Technological

The decentralization of a system can be measured.

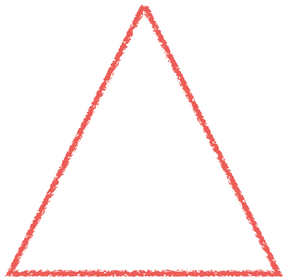
Alt video link: https://www.youtube.com/watch?v=7S1IqaSLrq8

Centralized systems are <u>incapable</u> of censorship-resistance.



Screenshot of the 3rd “Short” here: https://groupincome.org/shorts/

Last time…



Zooko’s Triangle

?

“Decentralized Consensus-based Namespaces”

Answer: DPKI

A “decentralized consensus-based namespace”
provides **censorship-resistance** and **user-owned and controlled identities**

Answer: DPKI

That means **security.**

Decentralized Public Key Infrastructure

A White Paper from Rebooting the Web of Trust

by (alphabetical by last name) Christopher Allen, Arthur Brock, Vitalik Buterin, Jon Callas, Duke Dorje, Christian Lundkvist, Pavel Kravchenko, Jude Nelson, Drummond Reed, Markus Sabadello, Greg Slepak, Noah Thorp, and Harlan T Wood

Abstract

Today's Internet places control of online identities into the hands of third-parties. Email addresses, usernames, and website domains are borrowed or "rented" through DNS, X.509, and social networks. This results in severe usability and security challenges Internet-wide. This paper describes a possible alternate approach called *decentralized public key infrastructure (DPKI)*, which returns control of online identities to the entities they belong to. By doing so, DPKI addresses many usability and security challenges that plague traditional public key infrastructure (PKI). DPKI has advantages at each stage of the PKI life cycle. It makes permissionless bootstrapping of online identities possible and provides for the simple creation of stronger SSL certificates. In usage, it can help "Johnny" to finally encrypt thanks to its relegation of public key management to secure decentralized datastores. Finally, it includes mechanisms to recover lost or compromised identifiers.

Source: https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust/blob/master/final-documents/dpki.pdf

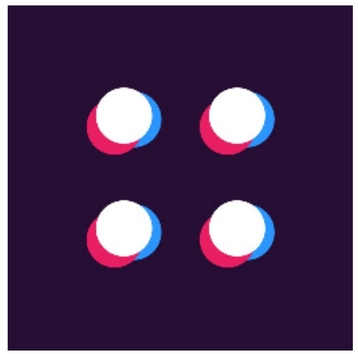
Source: https://blog.okturtles.com/2016/02/turtle-status-letter-1-browser-extension-dnschain-dpki-more/#DPKI

Comparison

	Google's CT	Google's KT	CONIKS	DPKI
MITM-detection	🤔	🤔	✅	✅
MITM-prevention	❌	❌	✅ (*)	✅
Internet scalable	✅	✅	✅	🤔
Economically backed security	❌	❌	❌	✅
Censorship resistant	🤔	❌	❌	✅
DoS resistant	✅	🤔	🤔	✅

https://blog.okturtles.com/2017/02/coniks-vs-key-transparency-vs-certificate-transparency-vs-blockchains/

Potential Partial Implementations



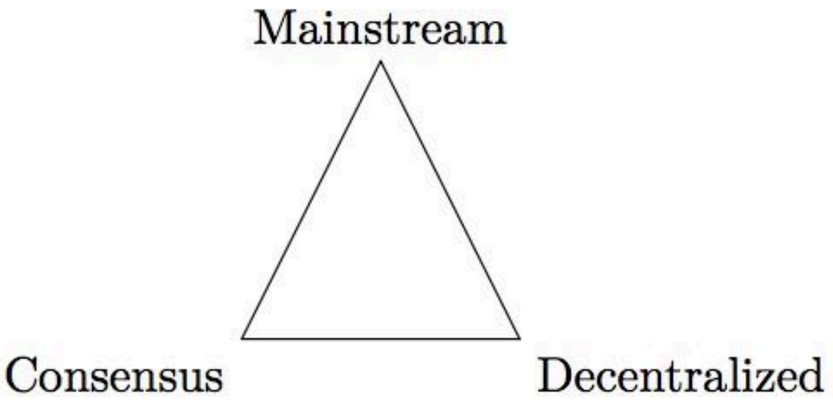
Blockstack

DCS / Slepak's Triangle

Source: https://blog.bigchaindb.com/the-dcs-triangle-5ce0e9e0f1dc

Source: https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2016/blob/master/topics-and-advance-readings/Slepaks-Triangle.pdf

We observe that any single system may possess, at most, two of three properties:



- **Consensus** means the system has participants who regularly come to agreement about changes to the system's shared state (shared resource). The interval at which the system comes to agreement is its *period*, π.
- **Mainstream** (or **Scalable**) means the system is, *by itself*, capable of competing with the transactional demands placed on a leading centralized competitor.[1]
- **Decentralized** means the system meets two related notions of *decentralization*:

[1] For example, we could compare Bitcoin's transaction rate to VISA's, or BitTorrent's ability to stream movies to Netflix.

Source: https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2016/blob/master/topics-and-advance-readings/Slepaks-Triangle.pdf

Recap

***Avoid* centralized systems**

(when possible, but **especially** for key management)

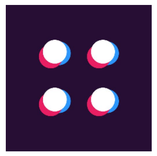
Use + support + design decentralized systems

Questions?

Decentralize All The Things!


GroupIncome


okTurtles


Blockstack

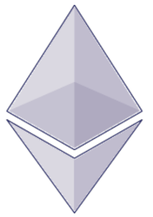

Patreon

blog.okturtles.com <- DPKI


Brave

IPFS


Bitcoin


Ethereum


ZeroNet