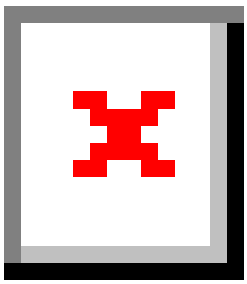
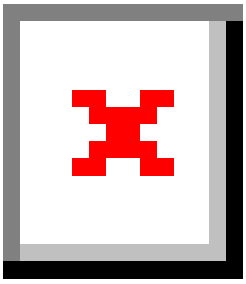
From: ASPI Cyber Policy from Daily Cyber Digest
Sent: Wed, 7 Apr 2021 10:42:55 +1000
To: Julie Igglesden
Subject: Clearview AI used by nearly 2000 US public agencies | Belgian authorities decrypt messages to seize 27 tons of coc…

Clearview AI used by nearly 2000 US public agencies | Belgian authorities decrypt messages to seize 27 tons of cocaine in Europe | Facebook removes 14 networks from 11 countries

ASPI Cyber Policy Apr 7





Follow us on Twitter. The Daily Cyber Digest focuses on the topics we work on, including cyber, critical technologies & strategic issues like foreign interference.

Subscribe now

- **A BuzzFeed News investigation has found that employees at law enforcement agencies across the US ran thousands of Clearview AI facial recognition searches — often without the knowledge of the public or even their own departments. According to reporting and data reviewed by BuzzFeed News, more than 7,000 individuals from nearly 2,000 public agencies nationwide have used Clearview AI to search through millions of Americans' faces, looking for people, including Black Lives Matter protesters, Capitol insurrectionists, petty criminals, and their own friends and family members. *BuzzFeed News***
- **Belgian authorities announced on Monday that they had seized 27.64 tons of cocaine with a street value of 1.4 billion euros ($1.7 billion) in the industrial port of Antwerp over the past two months... Authorities attributed the seizures to the alleged decryption of half a billion messages sent using Sky ECC, a now shut down encrypted phone company and network popular among drug traffickers. *VICE***
- **In March, Facebook removed 14 networks from 11 countries. Five networks — from Albania, Iran, Spain, Argentina, and Egypt — targeted primarily people outside of their countries. Nine others — from Israel,**

Benin, Comoros, Georgia, and Mexico — focused on domestic audiences in their respective countries. *Facebook*

ASPI ICPC

China and Russia's plot to undermine vaccine rollout

Herald Sun

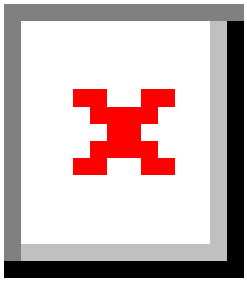
@Sue_Dunlevy

ASPI analyst Ariel Bogle said "it became pretty clear … as various vaccine candidates emerged that they would become a kind of political tool, as well as a health tool, as a way to kind of broadcast scientific achievement for their country."

William Yang

@WilliamYang120

Latest for @dw_chinese (Eng version): @ASPI_org released a study last week detailing the spike of #Xinjiang propaganda efforts by #China. The study shows that Chinese diplomats and state-run media rely on several strategies to try to achieve this goal:



How China uses western social media platforms to amplify its Xinjiang propaganda in 2020?

The Australian Strategic Policy Institute released a new study last week, which shows that Beijing has been trying to reshape the online narrative about the persecution of ethnic minorities in...

williamyang-35700.medium.com

April 5th 2021

60 Retweets**111** Likes

- **Read our report 'Strange bedfellows on Xinjiang: The CCP, fringe media and US social media platforms' here.**

World

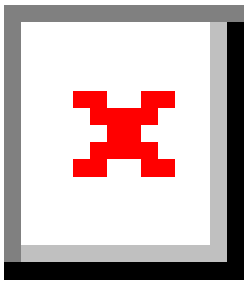
The Cybersecurity 202: A massive Facebook breach underscores limits to current data breach notification laws
The Washington Post
@TonyaJoRiley @aaronjschaffer
Lawmakers and privacy experts are slamming Facebook for its handling of a leak of more than 500 million users' personal information that was posted online for free.

- **DPC statement, re: Dataset appearing online**
  Data Protection Commission
  Facebook assures the DPC it is giving highest priority to providing firm answers to the DPC. A percentage of the records released on the hacker website contain phone numbers and email address of users. Risks arise for users who may be spammed for marketing purposes but equally users need to be vigilant in relation to any services they use that require authentication using a person's phone number or email address in case third parties are attempting to gain access.

Eva

@evacide

Want to know if your personal data is in the Facebook data leak? You can check here:



Have I Been Zucked?

Check if your details are included in the 2019 Facebook data breach.

haveibeenzucked.com

April 6th 2021

573 Retweets **1,060** Likes

March 2021 Coordinated Inauthentic Behavior Report

Facebook

@SGelava@EtoBuziashvili

In March, we removed 14 networks from 11 countries. Five networks — from Albania, Iran, Spain, Argentina, and Egypt — targeted primarily people outside of their countries. Nine others — from Israel, Benin, Comoros, Georgia, and Mexico — focused on domestic audiences in their respective countries.

- **Coordinated Inauthentic Bee-havior**

  Graphika

@SGelava@EtoBuziashvili

On April 6, Facebook announced the removal in March of a network of accounts and pages that it said originated in Egypt and violated its policy against foreign interference. The set consisted of six pages, 17 Facebook accounts, and three Instagram accounts, which posted about news and political events in Amharic, Arabic, and Turkish to target audiences in Ethiopia, Sudan, and Turkey.

- **DFRLab investigation leads to Facebook takedown of assets affiliated with Georgian March party**

  DFRLab

  @jc_stubbs @realShawnEib

  Amid a deepening political crisis in Georgia related to the detention of the leader of the main opposition party, Facebook removed a network connected to the violent far-right and pro-Kremlin party Georgian March.

Nathaniel Gleicher

@ngleicher

1/ Today we shared our March CIB report - it included 14 networks we removed across the world, including in Latin America, the Middle East, Africa and Eastern Europe:

March 2021 Coordinated Inauthentic Behavior Report - About Facebook

We're sharing information about the 14 networks we removed in March as part of our regular CIB reports.

about.fb.com

April 6th 2021

5 Retweets**7** Likes

Australia

Tech industry revolt against Porter's appointment grows

Australian Financial Review

@SaysSmithy

Pressure is rising on Prime Minister Scott Morrison to reverse his decision to appoint Christian Porter as the Minister for Industry, Science and Technology, as more technology industry players spoke out against him taking responsibility for a sector that has sought to increase the participation of women.

ACT government wants to make Canberra the 'cyber capital of Australia'

The Canberra Times

@lucybladen

The ACT government will make a play to position Canberra as the cyber capital of Australia, annoucing plans to establish a new cyber security hub.

Cyber Security NSW needs greater oversight role, parliamentary committee finds

The Mandarin

Shannon Jenkins

The New South Wales government must provide its cyber security agency with a clearer mandate, more independence and increased authority, according to a parliamentary committee report.

Liberal MP Andrew Laming created dozens of Facebook pages to promote LNP and attack opponents

The Guardian

@msmarto

The besieged Liberal National MP Andrew Laming operates more than 30 Facebook pages and profiles under the guise of community groups, including at least three masquerading as news pages, and another posing as an educational institute. The Bowman MP, who is on leave from parliament to undertake empathy counselling following complaints about his behaviour towards women, uses the sites to promote political material and attack his Labor opponents through pages classified with Facebook as “community” and “news” groups. None of the pages include political authorisation disclosures.

China

Chinese Hackers Selling Intimate Stolen Camera Footage

Threat Post

Becky Bracken

Stolen videos captured by tens of thousands of security cameras at private properties throughout China are now for sale across social media, marketed as sex tapes.

China's Huawei Is Winning the 5G Race. Here's What the United States Should Do To Respond

Council on Foreign Relations

@DavidMSacks1

As part of a CFR Independent Task Force on BRI, we analyzed every country’s official policy toward Huawei 5G and the extent to which this pressure campaign has succeeded. We found that in addition to the United States, eight countries have

issued outright bans of the company. Almost all of these are close U.S. allies such as Australia, Japan, and the United Kingdom. More countries have taken a quieter approach, attempting to simultaneously allay U.S. concerns and not provoke a Chinese response. Some have taken measures that amount to a de facto ban without actually barring Huawei.

USA

Surveillance Nation

BuzzFeed News

@RMac18 @caro1inehaskins @bri_sacks @_loganmcdonald

A BuzzFeed News investigation has found that employees at law enforcement agencies across the US ran thousands of Clearview AI facial recognition searches — often without the knowledge of the public or even their own departments.. According to reporting and data reviewed by BuzzFeed News, more than 7,000 individuals from nearly 2,000 public agencies nationwide have used Clearview AI to search through millions of Americans' faces, looking for people, including Black Lives Matter protesters, Capitol insurrectionists, petty criminals, and their own friends and family members.

- **Your Local Police Department Might Have Used This Facial Recognition Tool To Surveil You. Find Out Here.**

  BuzzFeed News

  @RMac18 @caro1inehaskins @bri_sacks @_loganmcdonald

  Search through BuzzFeed News' database to find out if the police department in your community is among the hundreds of taxpayer-funded entities that used Clearview AI's facial recognition.

After A Major Hack, U.S. Looks To Fix A Cyber 'Blind Spot'

NPR

@gregmyre1

The National Security Agency considers itself the world's most formidable cyber power, with an army of computer warriors who constantly scan the wired world. Yet by law, the NSA only collects intelligence abroad, and not inside the U.S.

How Google's Big Supreme Court Victory Could Change Software Forever

TIME

@maddiecarlisle2

The Court's ruling in Google LLC v. Oracle America, Inc. upheld long standing industry practices that have furthered development of software that's compatible with other programs, legal experts tell TIME. The ruling means copyright holders for software "can't maintain a monopoly over critical interface aspects," argues Jeanne Fromer, a professor of copyright law at New York University School of Law—and those aspects can be used by both users and programmers to more easily switch between products.

- **Supreme Court sides with Google in copyright fight against Oracle**
  The Hill
  @johnkruzel @chrisismills
  The Supreme Court on Monday sided with Google in the company's high-stakes intellectual property fight with Oracle, finding that the search giant's copying of certain Java lines to develop its Android platform constituted fair use.

How the far-right group 'Oath Enforcers' plans to harass political enemies

The Guardian

@jason_a_w

Revealed: online chats indicate some members are threatening to unleash harassment tactics on officials and government workers

Google AI Research Manager Quits After Two Ousted From Group

Bloomberg

@nicoagrant @josheidelson @dinabass

Google research manager Samy Bengio, who oversaw the company's AI ethics group until a controversy led to the ouster of two female leaders, resigned on Tuesday to pursue other opportunities.

How online harassment led to a historic court case

Chicago Booth Review

@jprollert

As a law student, Brittan Heller was the target of a campaign of online harassment that created enormous stress for her personal and professional lives, led her to fear for her safety, and ultimately prompted her to file a landmark lawsuit.

House panel investigating YouTube for advertising practices on kids' platform

The Hill

@JordanNichelleW

A House panel launched an investigation Tuesday into YouTube's advertising practices on its platform for children.

Congress Says Foreign Intel Services Could Abuse Ad Networks for Spying

VICE

@josephfcox

A group of bipartisan lawmakers, including the chairman of the intelligence committee, have asked ad networks such as Google and Twitter what foreign companies they provide user data to, over concerns that foreign intelligence agencies could be leveraging them to harvest sensitive information on U.S. users, including their location.

North Asia

Delta Electronics completes first smart factory

DigiTimes

Max Wang

Power supply maker and energy management solution provider Delta Electronics has upgraded a plant in Taiwan to a smart factory based on 5G private network through cooperation with Far EasTone Telecommunications (FET), Microsoft and PTC, according to Delta.

Europe

Decrypted Messages Lead to Seizure of 27 Tons of Cocaine in Europe

VICE

@gabriels_geiger

Belgian authorities announced on Monday that they had seized 27.64 tons of cocaine with a street value of 1.4 billion euros ($1.7 billion) in the industrial port of Antwerp over the past two months... Authorities attributed the seizures to the alleged decryption of half a billion messages sent using Sky ECC, a now shut down encrypted phone company and network popular among drug traffickers.

Pandemic brought surge in French cyber attacks, warns Thales CEO

Financial Times

@DavidKeo @peggyhollinger

The number of cyber attacks hitting critical French businesses jumped fourfold last year as hackers and states took advantage of the Covid-19 pandemic to make money and sow chaos, said the boss of French security and technology group Thales.. France's cyber security agency, the ANSSI, clocked 200 large-scale cyber attacks on so-called Operators of Vital Importance in 2020 compared to just 50 the year before, according to the company. The ANSSI keeps a list of around 250 such companies across 12 areas of critical infrastructure such as banking, health and defence.

European Institutions Were Targeted in a Cyber-Attack Last Week

Bloomberg

@albertonardelli @nat_droz

A spokesperson for the commission said that a number of EU bodies "experienced an IT security incident in their IT infrastructure." The spokesperson said forensic analysis of the incident is still in its initial phase and that it's too early to provide any conclusive information about the nature of the attack.

Middle East

Israeli Snoop-for-Hire Posed as a Fox News Journalist for a Spy Operation

The Daily Beast

@arawnsley

Operatives from an Israeli private investigations company posed as a Fox News journalist and an Italian reporter in an attempt to dig up dirt on lawsuits against the emirate of Ras Al Khaimah in the UAE, The Daily Beast can reveal.

Gender and Women in Cyber

The Opportunities—and Obstacles—for Women at NSA and Cyber Command

WIRED

@lilyhnewman

WIRED spoke with three women working in cybersecurity in the US intelligence committee about the progress of recent years and the work that remains.

Misc

Apple's C.E.O. is making very different choices from Mark Zuckerberg

The New York Times

Tim Cook views privacy as ‘one of the top issues of the 21st century.’ Other tech leaders don’t seem to agree.

YouTube says it’s getting better at taking down videos that break its rules. They still number in the millions.

The Washington Post

@GerritD

The Google-owned site is blocking millions of videos that contain hate speech and disinformation, but researchers say there’s more it could do.

I Called Off My Wedding. The Internet Will Never Forget

WIRED

@LaurenGoode

In 2019, I made a painful decision. But to the algorithms that drive Facebook, Pinterest, and a million other apps, I'm forever getting married.

Follow the money: to rein in Big Tech, lawmakers are right to focus on business models

Tech Policy Press

@ellerybiddle

Facebook and Google have made broad-based commitments to protect human rights and the public interest, but only to the extent that this won’t interfere with their ad-based profit models. Lawmakers are right to follow the money.

Research

China as a ‘cyber great power’: Beijing’s two voices in telecommunications

Brookings

@RushDoshi @edelabruyere

External Chinese government and commercial messaging on information technology (IT) speaks in one voice. Domestically, one hears a different, second voice. The former stresses free markets, openness, collaboration, and interdependence, themes that suggest Huawei and other Chinese companies ought to be treated like other global private sector actors and welcomed into foreign

networks. Meanwhile, domestic Chinese government, commercial, and academic discourse emphasizes the limits of free markets and the dangers of reliance on foreign technologies — and, accordingly, the need for industrial policy and government control to protect technologies, companies, and networks.

Events

Kirstine Stewart

@kirstinestewart

Can't wait for this deep dive and hear Simon Milner @Facebook, Australia's @tweetinjules @eSafetyOffice and Lene Wendland UNHRC, moderated by @AlOraibi. Lessons learned, impact on content and how to move forward?
Part of @wef #GTGS21

Countering Harmful Content

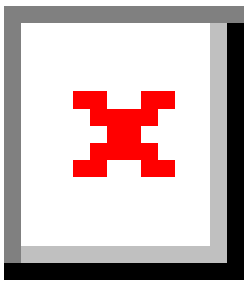
The use and abuse of technology platforms as "arbiters of truth" pose a significant challenge in an era when civic life is becoming increasingly digitized. How can businesses and governments design and enforce more effective policies for content accountability and transparency? Simultaneous interpr...

weforum.org

April 6th 2021

3 Retweets**5** Likes

Share



If you liked this post from Daily Cyber Digest, why not share it?

Share