encryption

workshop & panel session

https://alecmuffett.com/about

2nd May, 2000

https://en.wikipedia.org/wiki/Bill_Clinton

https://en.wikipedia.org/wiki/Pokémon_Go

https://en.meming.world/wiki/Surprised_Pikachu

GPS.GOV

Official U.S. government information about the Global Positioning System (GPS) and related topics

Search

Home | What's New | Systems | Applications | Governance | Multimedia | Support

Home » Systems » GPS » Modernization » Selective Availability

SYSTEMS:

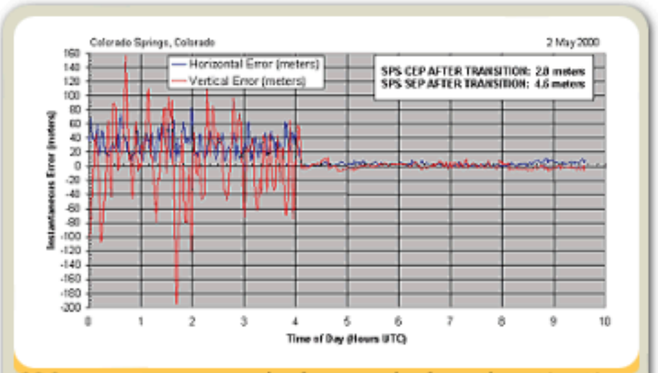
- GPS Overview
- Space Segment
- Control Segment
- Performance
- Modernization
  - Space Segment
  - Control Segment
  - New Civil Signals
  - CNAV Message
  - Selective Availability
- Technical Documentation
- Augmentation Systems
- Other GNSS

Selective Availability

Selective Availability (SA) was an intentional degradation of public GPS signals implemented for national security reasons.

In May 2000, at the direction of President Bill Clinton, the U.S government discontinued its use of Selective Availability in order to make GPS more responsive to civil and commercial users worldwide.

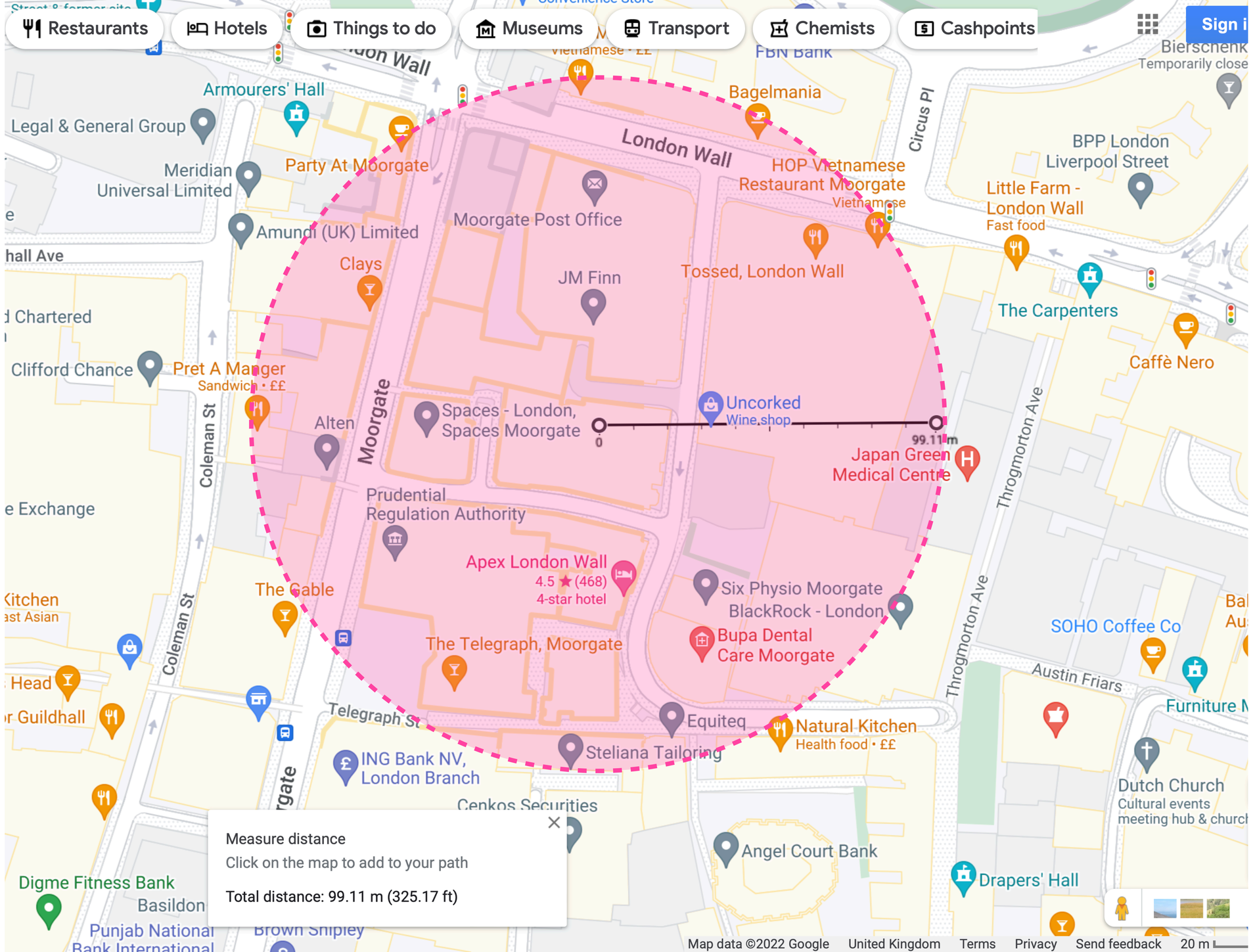
> The United States has no intent to ever use Selective Availability again.



GPS accuracy errors before and after deactivation of SA (VIEW MORE DATA)

In September 2007, the U.S. government announced its decision to procure the future generation of GPS satellites, known as GPS III, without the SA feature. Doing this will make the policy decision of 2000 permanent and eliminate a source of uncertainty in GPS performance that had been of concern to civil GPS users worldwide.

https://www.gps.gov/systems/gps/modernization/sa/


Restaurants
Hotels
Things to do
Museums
Transport
Chemists
Cashpoints
Sign i
London Wall
Armourers' Hall
Legal & General Group
Meridian Universal Limited
Party At Moorgate
Amundi (UK) Limited
Moorgate Post Office
Clays
JM Finn
Bagelmania
HOP Vietnamese Restaurant Moorgate
Tossed, London Wall
Circus Pl
BPP London Liverpool Street
Little Farm - London Wall
Fast food
The Carpenters
Caffè Nero
Clifford Chance
Pret A Manger
Sandwich · ££
Alten
Moorgate
Spaces - London, Spaces Moorgate
Uncorked
Wine shop
0
99.11 m
Japan Green Medical Centre
Throgmorton Ave
Coleman St
Prudential Regulation Authority
Apex London Wall
4.5 ★ (468)
4-star hotel
The Gable
The Telegraph, Moorgate
Six Physio Moorgate
BlackRock - London
Bupa Dental Care Moorgate
SOHO Coffee Co
Austin Friars
Telegraph St
Equiteq
Natural Kitchen
Health food · ££
Steliana Tailoring
ING Bank NV, London Branch
Cenkos Securities
Angel Court Bank
Drapers' Hall
Dutch Church
Cultural events
meeting hub & church
Digme Fitness Bank
Basildon
Punjab National Bank International
Brown Shipley
Measure distance
Click on the map to add to your path
Total distance: 99.11 m (325.17 ft)
Map data ©2022 Google
United Kingdom
Terms
Privacy
Send feedback
20 m

google maps

why?

"safety"

Forbes

AEROSPACE & DEFENSE • EDITORS' PICK

Ukraine's Quadcopters Avoid Russian Jamming — And Target Russian Drone Operators

David Hambling Contributor ⓘ
I'm a South London-based technology journalist, consultant and author

Follow

Jun 24, 2022, 08:52am EDT

Sergey Hadzhinov is a frontline drone operator with Aerorozvidka – "Aerial Intelligence" – a civilian organization set up in 2014 to aid Ukraine's military with reconnaissance using consumer drones and now integrated with the armed forces. In a new interview in the Ukrainian news portal Censort.NET, he explains how they evade Russian electronic warfare which threatened to ground the drone fleet, and target Russian drone operators.

Consumer drones, in particular those made by Chinese company DJI, have proven invaluable in this conflict for intelligence gathering, directing artillery and helping footsoldiers stalk and destroy Russian armor, not to mention dropping grenades on unsuspecting Russian troops.

https://www.forbes.com/sites/davidhambling/2022/06/24/ukraines-quadcopters-avoid-russian-jamming---and-target-russian-drone-operators/

The long read

The mystery of the Gatwick drone

A drone sighting caused the airport to close for two days in 2018, but despite a lengthy police investigation, no culprit was ever found. So what exactly did people see in the Sussex sky?

by Samira Shackle

"There's no tolerance of people being daft with drones - there'll be laws made and it'll affect everyone who has one."

When Hudson first heard about Gatwick, "I thought this was some absolute idiot and I wanted them caught." But then he realised "the basic facts don't add up". Sussex police had mentioned lights in the corroborated sightings. But if someone had planned the attack, to the extent that they had procured scores of batteries and hacked the drone's in-built geofencing software - which uses GPS to stop drones from flying into restricted zones such as airports or prisons - then why would they leave the lights on? "You'd disable them," said Hudson.

Hudson looked at publicly available information: photographs taken during the incident, and statements by Sussex police. Since then, he has identified

https://www.theguardian.com/uk-news/2020/dec/01/the-mystery-of-the-gatwick-drone

downsides of selective availability

Part 1

- special features for handling classified data to restrict backdoor access
  - → expensive
  - → produced in limited numbers
  - → restricted distribution

Operation Desert Storm

downsides of selective availability

Part 2

- special features for handling classified data to restrict backdoor access
  - → hidebound by government contract & standardisation
  - → limited, stagnant functionality
  - → poor usability

For Immediate Release
Office of the Press Secretary
September 18, 2007

Statement by the Press Secretary

Today, the President accepted the recommendation of the Department of Defense to end procurement of Global Positioning System (GPS) satellites that have the capability to intentionally degrade the accuracy of civil signals. This decision reflects the United States strong commitment to users of GPS that this free global utility can be counted on to support peaceful civil activities around the world.

This degradation capability, known as Selective Availability (SA), will no longer be present in GPS III satellites. Although the United States stopped the intentional degradation of GPS satellite signals in May 2000, this new action will result in the removal of SA capabilities, thereby eliminating a source of uncertainty in GPS performance that has been of concern to civil GPS users worldwide.

GPS benefits users around the world in many different ways, including aviation, road, marine and rail navigation, telecommunications, emergency response, resource exploration, mining and construction, financial transactions, and many more. All users, and their governments, have a stake in the future of GPS. The United States promotes international cooperation in the operation of civil global navigation satellite systems and continues to work to build international support for the protection of these signals from intentional interference and disruption.

###

Return to this article at:
/news/releases/2007/09/20070918-2.html

but what if …?

there would be no…

Pokémon Go

there would be no…

Geocaching

there would be no…

Location-based Games

there would be no…

decent in-car navigation

there would be no…

Uber

there would be no…

Deliveroo

there would be no…

"Gig Economy" (?)

there would be no…

Google Street View

there would be no…

UGC on Street View

there would be no…

"sharing your location"

there would be no…

"finding your family"

there would be no…

child-location tracking & alerts

there would be no…

AirTag, Tile, etc…

there would be no…

decent stolen-car tracking

there would be no…

speed camera alerts

there would be no…

automated recording of walking routes

there would be no…

OpenStreetMap

there would be no…

precision location for hikers, boats, pilots, …

there would be no…

precision crop-spraying

there would be no…

reduction in pollution

there would be no…

location-tagging of photos

there would be no…

searching photo-albums by location

there would be no…

photo-based
open-source intelligence

there would be no…

solution to a bunch of crimes

there would be no…

OSINT evidence re: MH17

this is just a partial list

worse:

we would have no idea that these things should exist

hello!

alecmuffett.com/about

[A…] workshop-style panel will **explain and demonstrate encryption** to the public. It will include a deep dive into:

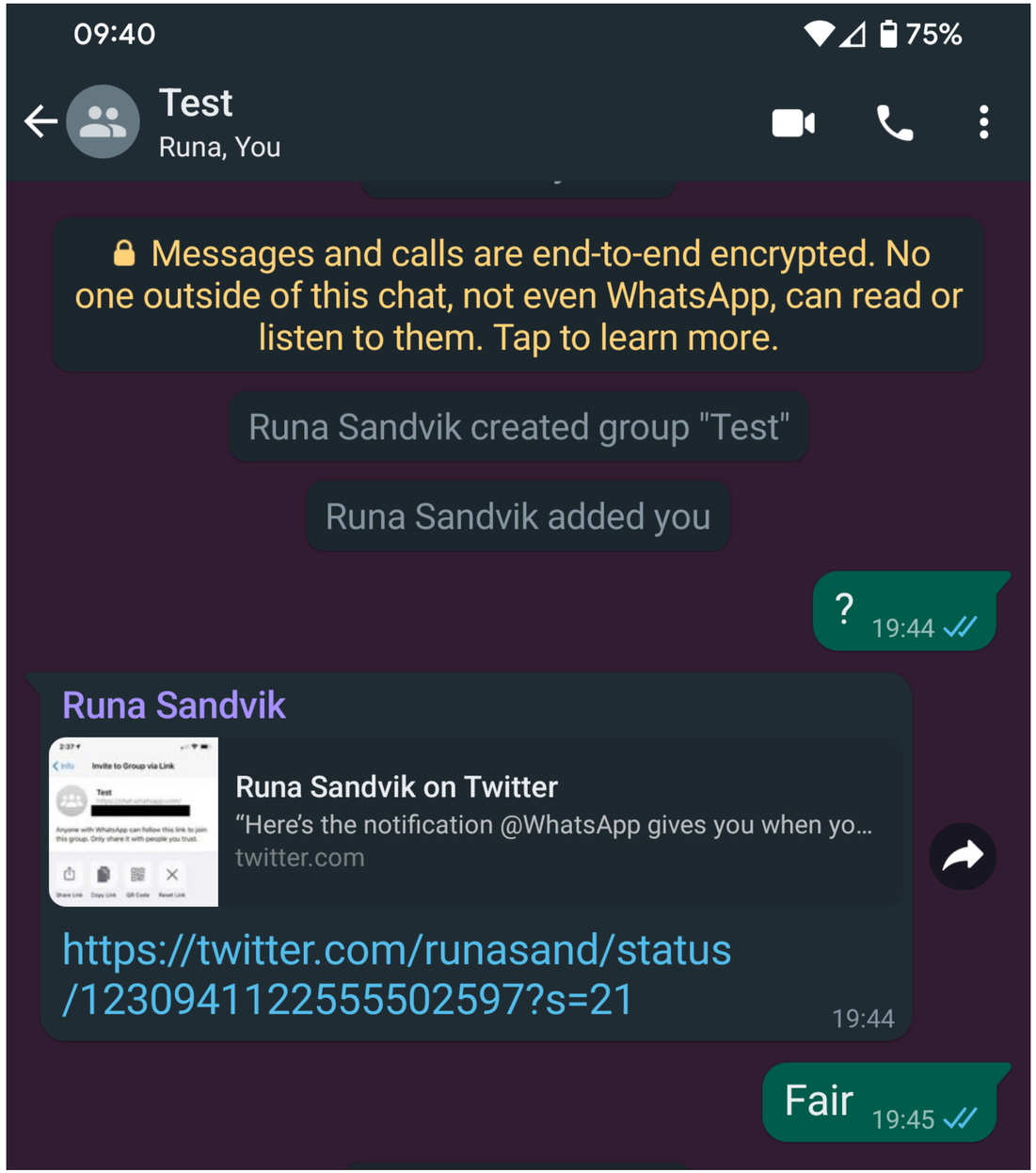
- **how the technologies work**, and participants will be shown…
- **how to secure their digital environment**
- **what to expect** when **submitting information securely to third parties,** and…
- **what strong encryption means.**

This will be followed by a **debate between panellists** on the **merits and risks of encryption.**

Well...

this is so much easier today than it was in 1997

demonstrating encryption



invisible encryption

Apple Card transactions	End-to-end	
Health data	End-to-end	Additional info below
Home data	End-to-end	
Keychain	End-to-end	Includes all of your saved accounts and passwords
Maps Favourites, Collections and search history	End-to-end	
Memoji	End-to-end	
Messages in iCloud	End-to-end	Additional info below
Payment information	End-to-end	
QuickType Keyboard learned vocabulary	End-to-end	
Safari History, Tab Groups and iCloud Tabs	End-to-end	
Screen Time	End-to-end	
Siri information	End-to-end	Includes Siri settings and personalisation, and if you have set up Hey Siri, a small sample of your requests
Wi-Fi passwords	End-to-end	
W1 and H1 Bluetooth keys	End-to-end	

https://support.apple.com/en-gb/HT202303

how encryption works

how to secure your environment

what is your threat model?

what do you need to protect?

Security and Privacy Tips for People Seeking An Abortion

BY DALY BARNETT | JUNE 23, 2022

https://www.eff.org/deeplinks/2022/06/security-and-privacy-tips-people-seeking-abortion

REUTERS®

World Business Legal Markets More

Middle East

2 minute read · September 21, 2022 7:55 PM GMT+1 · Last Updated a month ago

As unrest grows, Iran restricts access to Instagram, WhatsApp

Reuters

[1/2] An Iranian woman living in Turkey points at an old Iranian royal flag during a protest following the death of Mahsa Amini, outside the Iranian consulate in Istanbul, Turkey September 21, 2022. REUTERS/Murad Sezer **Read less**

1 2

https://www.reuters.com/world/middle-east/iran-restricts-access-instagram-netblocks-2022-09-21/

NEWS / POLITICS

Truss phone hacked by Putin spies for top secret information

GLEN OWEN Mail On Sunday Political Editor • **DAN HODGES** Mail On Sunday columnist

OCTOBER 29, 2022

LIZ Truss's personal phone was hacked by agents suspected of working for Russian President Vladimir Putin. They gained access to top-secret details of negotiations with key international allies – as well as private messages she exchanged with her close friend Kwasi Kwarteng, The Mail on Sunday can reveal.

The hack was discovered during the summer Tory leadership campaign, when Ms Truss was Foreign Secretary, but the details were suppressed by the then Prime Minister Boris Johnson and the Cabinet Secretary Simon Case.

One source said the phone was so heavily compromised that it has now been placed in a locked safe inside a secure government location.

It is understood that the messages that fell into foreign hands included criticisms of Mr Johnson made by Ms Truss and Ms Kwarteng, leading to a potential risk of blackmail. Sources said that up to a year's worth of messages were downloaded.

https://www.mailplus.co.uk/edition/news/politics/232629/truss-phone-hacked-by-putin-spies-for-top-secret-information

tl;dr

"it depends."

[A…] workshop-style panel will ~~explain and demonstrate encryption~~ to the public. It will include a deep dive into:

- ~~how the technologies work~~, and participants will be shown…
- ~~how to secure their digital environment~~
- what to expect when submitting information securely to third parties, and…
- what strong encryption means.

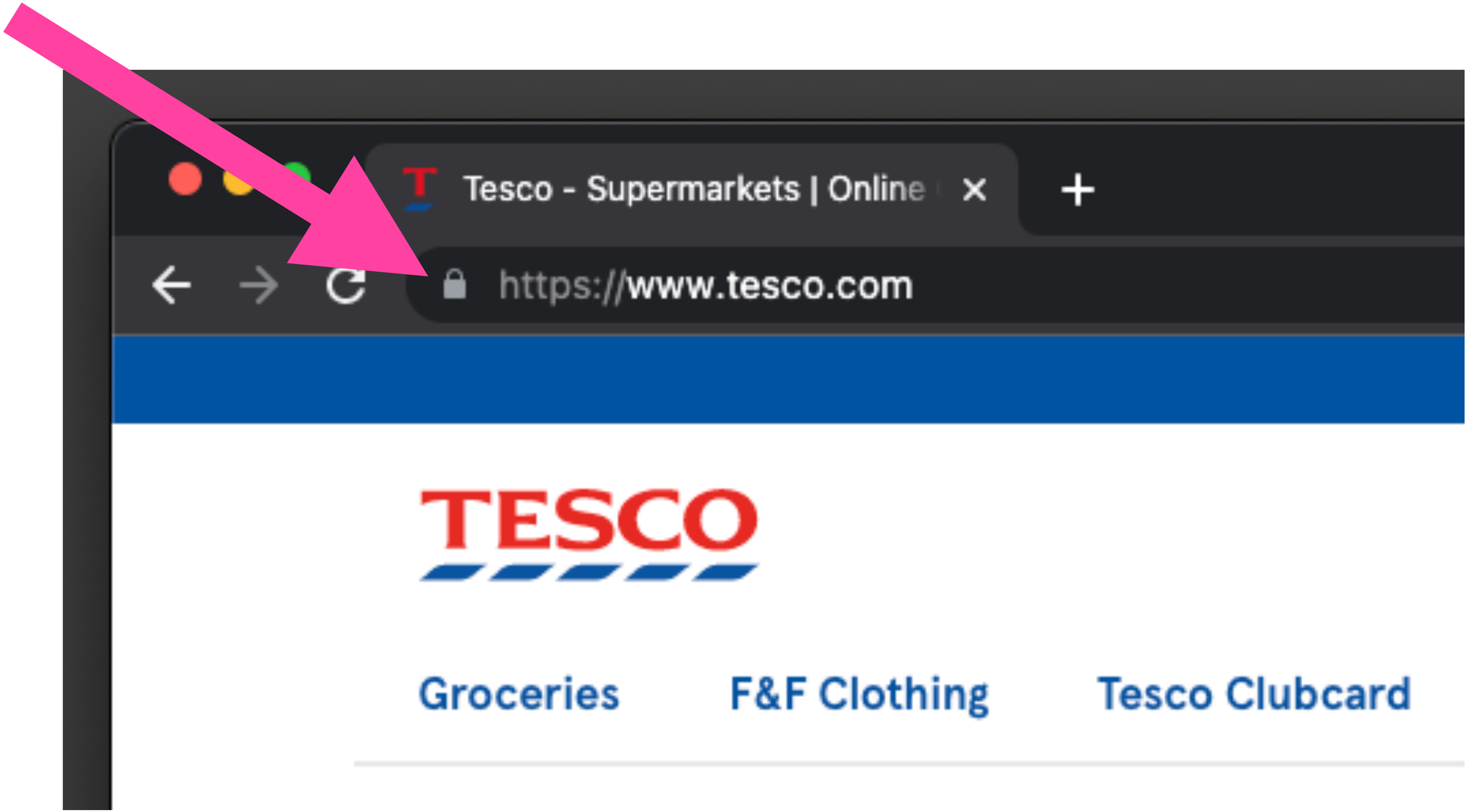
This will be followed by a debate between panellists on the merits and risks of encryption.

Question: what do people expect when submitting information securely to third parties?

Answer: that it will not be seen, nor scanned, nor processed by fourth parties*

*assuming that as phrased, fourth parties are "anybody else"

"Trust"


Tesco - Supermarkets | Online
https://www.tesco.com
TESCO
Groceries
F&F Clothing
Tesco Clubcard

LILY HAY NEWMAN SECURITY JUN 1, 2019 5:00 AM

The Tricky Shenanigans Behind a Stealthy Apple Keychain Attack

An 18-year-old security researcher made headlines earlier this year with KeySteal, a macOS hack. Now he's showing the world how it worked.

IN EARLY FEBRUARY, an 18-year-old German security researcher named Linus Henze demonstrated a macOS attack that would allow a malicious application to grab passwords from Apple's protected keychain. "You know, the ones 'securely' stored so that no one can steal them :)" he wrote. Dubbed KeySteal, the attack called attention to the fact that the macOS keychain makes a very attractive target for hackers. Apple patched the flaw that KeySteal was exploiting at the end of March.

https://www.wired.com/story/keysteal-apple-keychain-attack-shenanigans/

California

This article is more than **2 months old**

Ex-Twitter employee found guilty of spying on Saudi dissidents

Ahmad Abouammo found to have given users' personal information to Mohammed bin Salman's aide

Julian Borger *in Washington*

Wed 10 Aug 2022 01.32 BST

A former Twitter employee has been found guilty of spying on Saudi dissidents using the social media platform and passing their personal information to a close aide of Crown Prince Mohammed bin Salman.

A jury in a federal court in California found Ahmad Abouammo, a dual US-Lebanese national, had acted as an unregistered agent of the Saudi government.

Abouammo was found to have used his position at Twitter to find personal details identifying critics of the Saudi monarchy who had been posting under anonymous Twitter handles, and then supplying the information to Prince Mohammed's aide Bader al-Asaker.

https://www.theguardian.com/us-news/2022/aug/09/twitter-saudi-arabia-dissident-spying

A Civil Society Glossary and Primer for End-to-End Encryption Policy in 2022

Metadata

"strong" encryption

Foreword

Three fundamental questions have driven the *Crypto Wars* [11] for the past 30+ years, and they are approximately as follows:

1. should individuals remain free to keep a secret, even from the state?
2. should consenting parties remain free to communicate in a manner that is private, even from the state?
3. should third parties ever be obliged to *not enable* – or even *actively prevent* – access to the above freedoms?

Readers are encouraged to consider the entirety of this report in the light of these three questions. They are key to everything which follows, and I shall return to them in the afterword.

https://alecmuffett.com/alecm/e2e-primer/

sidebar

Who am I?

I am a full-time SAHD, so…

"Consultant?"

Stephen Bonner, Executive Director of Regulatory Futures at the Information Commissioner's Office

Alec Muffett, Led the team that added end-to-end encyption to Facebook Messenger

Dan Sexton, Chief Technology Officer at the Internet Watch Foundation

we are more than our labels

giving people everywhere, greater privacy, assurance and confidence, and enabling them to keep secrets, even from the state

important

that doesn't mean that it's not a scary proposition

if people can keep & communicate secrets

it can assist their ability to…

- disrupt order
- conspire
- perpetrate abuse & fraud
- propagate harmful information or data
- undermine accountability for their actions

Blog

We continued to remove violative content as it was posted on the platform in the days that followed. By 14th July, 1,961 Tweets had been removed proactively following the Final, with a total of 126 removed from reports.

99% of the accounts suspended were not anonymous

Following the Tournament, we undertook ou analysis of the Tweets removed and account suspended. This is to ensure we have a comprehensive understanding of the behaviour we encountered and the users involved, and that the steps we take going forwards can be as effective as possible. While that work is continuing, we wanted to share some initial findings.

ars TECHNICA SUBSCRIBE SIGN IN

SO MUCH FOR OPSEC —

Paris police find phone with unencrypted SMS saying "Let's go, we're starting"

Phone likely led authorities to Saint-Denis, where clash left suspected dead.

CYRUS FARIVAR - 11/18/2015, 6:55 PM

French police found an unencrypted, unlocked phone in a trash bin outside the Bataclan concert hall in Paris that contained a text sent in the clear: "On est parti on commence." ("Let's go, we're starting").

This lead may have led French authorities to an apartment in Saint-Denis, where a Tuesday night shootout left two suspects dead, including the believed mastermind, Abdelhamid Abaaoud. The assault comes just days after last Friday's Paris terrorist attack perpetrated by members of the Islamic State (also known as Daesh, ISIS, or ISIL) resulted in the murder of 129 people.

According to the French newspaper *Libération*, the police also located a map of the Bataclan on the same phone. However, authorities were unable to identify the recipient of the phone message.

Despite that setback, French investigators were seemingly able to get a tower history of the phone and then locate a hotel in Alfortville, just outside the French capital. At that hotel, the bank card of Salah Abdeslam, one of the suspected terrorists still at large, reserved two rooms the night before the attack.

https://blog.twitter.com/en_gb/topics/company/2020/combatting-online-racist-abuse-an-update-following-the-euros

https://arstechnica.com/tech-policy/2015/11/paris-police-find-phone-with-unencrypted-sms-saying-lets-go-were-starting/

some people are bad people…

…but at what point is it
"worse than the disease"
to impinge upon good people?

"Selective Privacy?"

there would be no…

<insert innovation here>

"safety"

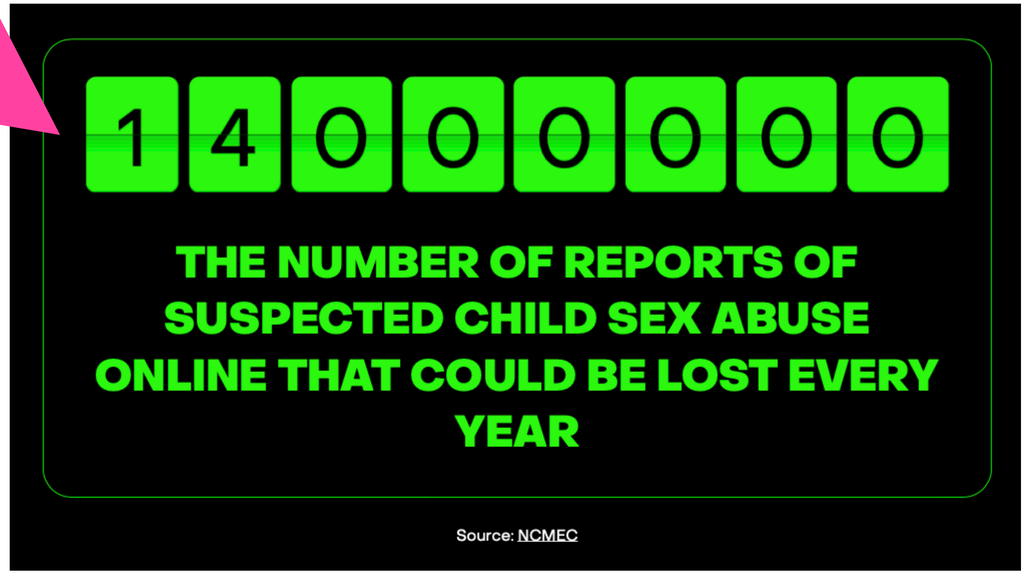
"a vast multitude of things* which can be achieved and harms which can be avoided by giving people everywhere, greater privacy, assurance and confidence, and enabling them to keep secrets, even from the state"

*including many forms of safety

which would you choose?

"precautionary principle?"

Let's work together to ensure we keep children safe online without compromising user privacy



DEAR MARK...

Rhiannon is a survivor and subject matter specialist from the Marie Collins Foundation. She recently wrote a letter to Mark Zuckerberg outlining why it's time to work together on making sure social media platforms protect privacy, without making it easier for child sex abusers to groom and exploit children.

The campaign is funded by the UK Government and has been developed by a steering group of child safety organisations with support from M&C Saatchi. The steering group has not been paid to take part.

https://noplacetohide.org.uk/

Focusing on Prevention

To understand how and why people share child exploitative content on Facebook and Instagram, we conducted an in-depth analysis of the illegal child exploitative content we reported to the National Center for Missing and Exploited Children (NCMEC) in October and November of 2020. We found that more than 90% of this content was the same as or visually similar to previously reported content. And copies of just six videos were responsible for more than half of the child exploitative content we reported in that time period. While this data indicates that the number of pieces of content does not equal the number of victims, and that the same content, potentially slightly altered, is being shared repeatedly, one victim of this horrible crime is one too many.

https://research.facebook.com/blog/2021/02/understanding-the-intentions-of-child-sexual-abuse-material-csam-sharers/

https://about.fb.com/news/2021/02/preventing-child-exploitation-on-our-apps/

The fact that only a few pieces of content were responsible for many reports suggests that a greater understanding of intent could help us prevent this revictimization. We worked with leading experts on child exploitation, including NCMEC, to develop a research-backed taxonomy to categorize a person's apparent intent in sharing this content. Based on this taxonomy, we evaluated 150 accounts that we reported to NCMEC for uploading child exploitative content in July and August of 2020 and January 2021, and we estimate that more than 75% of these people did not exhibit malicious intent (i.e. did not intend to harm a child). Instead, they appeared to share for other reasons, such as outrage or in poor humor (i.e. a child's genitals being bitten by an animal). While this study represents our best understanding, these findings should not be considered a precise measure of the child safety ecosystem. Our work to understand intent is ongoing.

Based on our findings, we are developing targeted solutions, including new tools and policies to reduce the sharing of this type of content. We've started by testing two new tools — one aimed at the potentially malicious searching for this content and another aimed at the non-malicious sharing of this content. The first is a pop-up that is shown to people who search for terms on our apps associated with child exploitation. The pop-up offers ways to get help from offender diversion organizations and shares information about the consequences of viewing illegal content.

https://research.facebook.com/blog/2021/02/understanding-the-intentions-of-child-sexual-abuse-material-csam-sharers/

https://about.fb.com/news/2021/02/preventing-child-exploitation-on-our-apps/

Centre for Missing and Exploited Children (NCMEC) via their 'CyberTipline'. NCMEC reviews the content and, if appropriate, reports it to the relevant authority. In the UK this is the National Crime Agency (NCA). In order to understand what mitigations are appropriate, it is important to understand the scale of online child sexual abuse. The statistic most often used to illustrate this is the number of reports received by NCMEC which amounted to 29.4 million in 2021. However, without context this number provides little useful information and can be easily misinterpreted. In the same year the NCA received 102,842 reports from NCMEC, but some of these were incomplete or, once investigated, not found to be child abuse. Of the 102,842 reports, 20,038 were referred to local police forces and started (or contributed to) investigations. In the same year, over 6,500 individuals were arrested or made voluntary attendances due to offences related to child abuse and over 8,700 children were safeguarded. These numbers more accurately illustrate the scale of the societal problem of child sexual abuse in the UK, of which the online component is significant. We would like to be able to show the causal link between individual CyberTips and convictions. However, this is not currently possible; industry notifications may lead to a completely new investigation, provide new evidence to allow investigations into an existing suspect or provide further evidence of scale of offending to an existing prosecution and

Child protection plans

A child becomes the subject of a **child protection plan** if they are assessed as being at risk of harm at an initial child protection conference.

The number and rate (per 10,000 children) of children on protection plans peaked in 2018 (figures as at 31 March) and has since fallen for the third consecutive year in 2021.

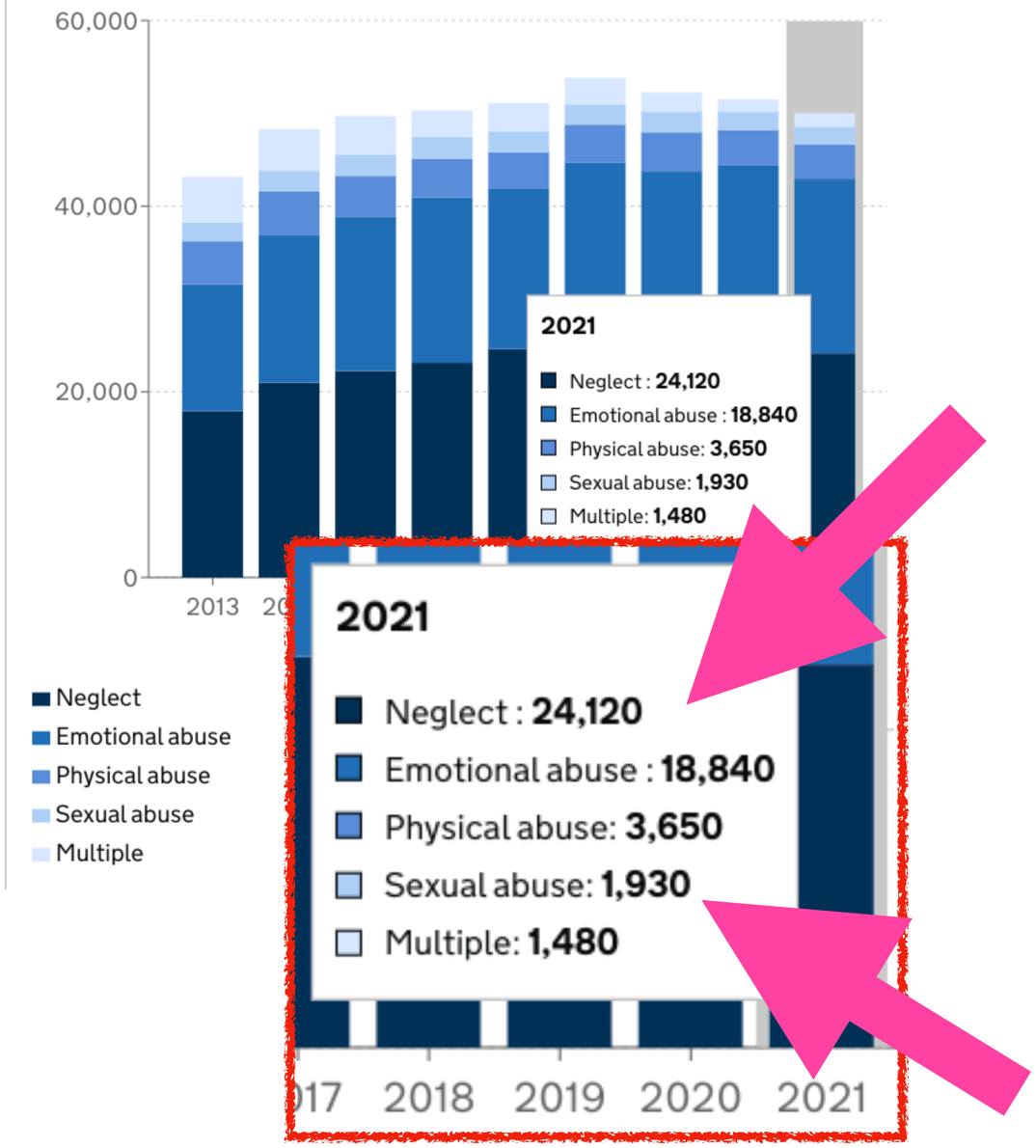
The number of children on protection plans is at its lowest point since 2015, and the associated rate is at its lowest point since 2013.

The number of children on protection plans at 31 March 2021 shows a fall of 3% compared with a year earlier, and this is supported by findings during the same week from the Vulnerable Children and Young people survey. However, the survey also shows that for large parts of the year (June 2020 to January 2021), the number of children on protection plans was higher than the same period a year earlier, thereby showing that the overall pattern was not consistent throughout the year.

"The number and rate…
of children on protection plans…
has since fallen for the third
consecutive year in 2021."

Chart | Table

Number of children with protection plans by initial category of abuse as at 31 March, 2013 to 2021, England

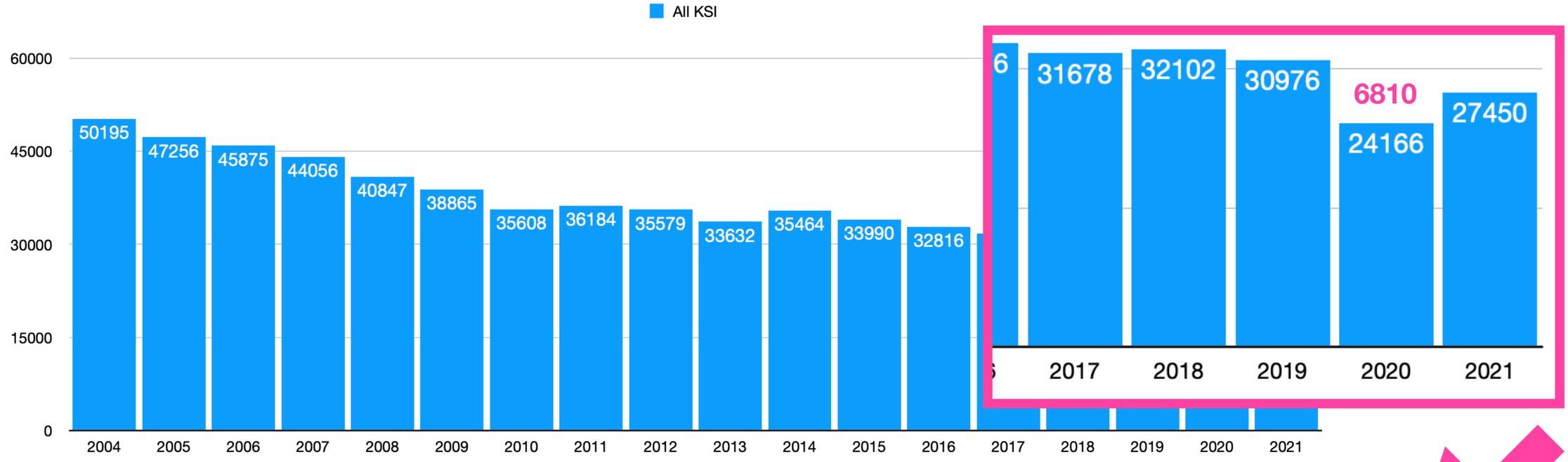


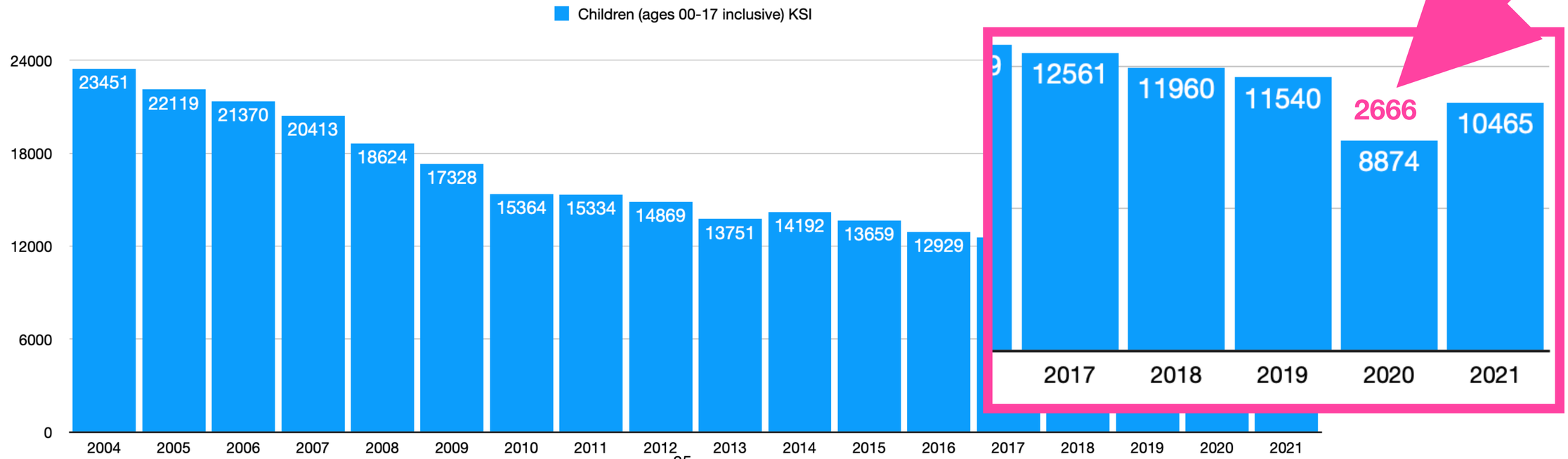
https://explore-education-statistics.service.gov.uk/find-statistics/characteristics-of-children-in-need/2021

we have a big societal problem with child care, and it's not "tech"

"*...but if one child can be saved!*"

https://github.com/alecmuffett/uk-roads-ksi-2004-thru-2021





therefore: lockdown!

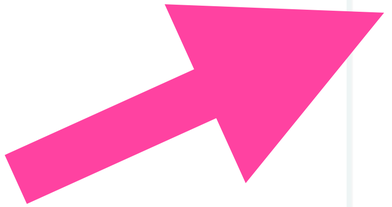
"abstract safety"

"living"

"allowed?"

"people should not be allowed to keep secrets from the state!"

"secrets"



WORLD

Video Shows Russian Police Allegedly Stopping People to Screen Phones

BY SHIRA LI BARTOV ON 3/7/22 AT 12:57 PM EST

SHARE

WORLD | RUSSIA | UKRAINE | POLICE | CELL PHONES

Listen to this article now

Powered by Trinity Audio

00:00 02:48

Russian police were allegedly stopping civilians on the street in Moscow and demanding to search their cell phones on Sunday, according to a video posted on Telegram by reporter Anna Vasilyeva with the Russian newspaper *Kommersant*.

The video was reposted on Twitter by Kevin Rothrock—an editor for the Russian- and English-language news outlet Meduza—where it has reached 5.9 million views. The clip appeared to show two armored police officers stopping at least five people on the street in Lubyanka Square in Moscow and scrolling through their cell phones as the civilians looked on.

Rothrock said in his post that the officers were "reading their messages" and "refusing to release them if they refuse."

https://www.newsweek.com/video-shows-russian-police-allegedly-stopping-people-screen-phones-1685502

surveillance compliance?

who will be the arbiter of which states may spy upon which users?

Things which cannot be "a little bit…"

- "you" / "pregnant"
- "data" / "analysable-surveillable"

Revealed: anti-terror snooping law used for fly-tippers and parking

Campaigners say councils are using Ripa powers to catch 'low-level' offenders and disregarding the public's right to privacy

Yohannes Lowe

Sun 8 Aug 2021 11.00 BST

Councils have used controversial surveillance legislation to combat "low-level" offences, such as the misuse of blue badge parking permits, fly-tipping and benefit fraud, an *Observer* investigation has found.

The Regulation of Investigatory Powers Act (Ripa) 2000 gives certain public bodies the right - under limited circumstances - to conduct surveillance activities, including for crime prevention and national security purposes.

At least 70 councils in England and Wales were authorised to use Ripa powers between January 2018 and March 2021 to gather evidence via cameras, street surveillance and informants or undercover officers.

The law restricts local authorities in England and Wales to use the surveillance powers only to investigate crimes that carry a prison term of at least six months, unless they relate to the sale of alcohol or tobacco products to underage buyers.

https://www.theguardian.com/world/2021/aug/08/revealed-anti-terror-snooping-law-used-for-fly-tippers-and-parking

IMPORTANT: Please ensure that the Notes Page is read in conjunction with the data in this report to ensure that it is interpreted correctly.

Count of Offences of Disclose private sexual photographs and films with intent to cause distress Recorded between 2015 and 2021

Outcome	2015	2016	2017	2018	2019	2020	2021	Grand Total
Outcome Pending	0	0	0	1	9	29	553	592
Charged/Summonsed	23	27	49	32	32	33	14	210
Charge/Summons Alternate offence	0	0	0	0	8	3	4	15
Caution - youth	3	1	0	1	3	3	0	11
Caution - adult	21	27	15	8	16	12	11	110
Adult offender cautioned alternate offence	0	0	0	1	1	2	1	5
Community Resolution	9	0	0	3	2	2	1	17
Not in public interest (CPS)	4	0	0	0	0	0	0	4
Not in public interest (Pol)	32	2	0	0	0	0	0	34
Prosecution prevented. - Suspect Age	0	0	0	1	0	0	0	1
Prosecution prevented - Victim/informant/witness ill/dead	0	0	1	0	0	0	0	1
Evidential difficulties victim based	28	35	32	52	33	52	37	269
Suspect identified; Victim supports; evidential difficulties	60	98	138	221	233	263	144	1157
Suspect identified; Victim not support; evidential difficulties.	59	98	133	164	201	272	215	1142
Investigation. complete: no suspect identified	44	40	67	74	105	135	110	575
Transferred to External Agency	1	0	1	2	0	0	2	6
Further Investigation NIPI (Police)	0	0	1	3	1	1	1	7
Grand Total	**284**	**328**	**437**	**563**	**644**	**807**	**1093**	**4156**

Count of victims of Disclose private sexual photographs and films with intent to cause distress Recorded between 2015 and 2021

Age	Female	Male	Unknown	Grand Total
Age Unknown	6	2	0	8
Under 18	512	90	2	604
18-25	1477	248	3	1728
26-29	490	118	3	611
30-39	712	233	5	950
40-49	240	79	0	319
50+	71	44	0	115
Grand Total	**3508**	**814**	**13**	**4335**

Notes

Source System
Data taken from CRIS on the 02/03/2022
Date Range
The Recorded date is between 01/01/2015 and 31/12/2021
Definition
Data is a count of offences by outcome and victims of the below home office code

008/71 - Disclose private sexual photographs and films with intent to cause distress

1093 image-based sexual abuse logged by the Met Police, in 2021

is the solution to "nerd harder?"

Josh Denzel: ‘We Need To Teach Young Men That Sexist Football Banter Is A Catalyst For Violent Behaviour Towards Women’

Ahead of the FIFA World Cup next month, when instances of domestic violence are set to spike, sports presenter Josh Denzel talks to Grazia about his new Women's Aid campaign with the Home Office.

BY GEORGIA ASPINALL | POSTED ON 26 10 2022

In less than one month the 2022 FIFA World Cup begins, with England men’s football team taking on Iran on the 21st November. After a summer of incredible wins for the women’s team, the nation is set to go feral for football once more. But while we’re celebrating the best of sport, there’s also a sinister issue that lies beneath the surface: domestic violence.

‘They key messaging for me, and I’m definitely not a leading voice in this but just one of them, is just to teach your friends by educating rather than embarrassing them,’ Josh explains. ‘You don’t have to make it a big scene at the time of the event happening, speak to them privately and try and educate them in softer way explaining why that behaviour might be perceived as sexist or why it’s unacceptable.

https://graziadaily.co.uk/life/in-the-news/world-cup-domestic-violence-womens-aid-campaign-josh-denzel/

?

"nothing to hide" → "nothing to fear"

do you have something to protect?

giving everyone everywhere, greater privacy, assurance and confidence, and enabling them to keep secrets, even from the state

panel