encryption

workshop & panel session

https://alecmuffett.com/about

Hello,
and welcome to the
encryption workshop and panel session.

2nd May, 2000

So the
2nd of May
in the Year 2000
is a very important date
in the development of
operational security understanding
because

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

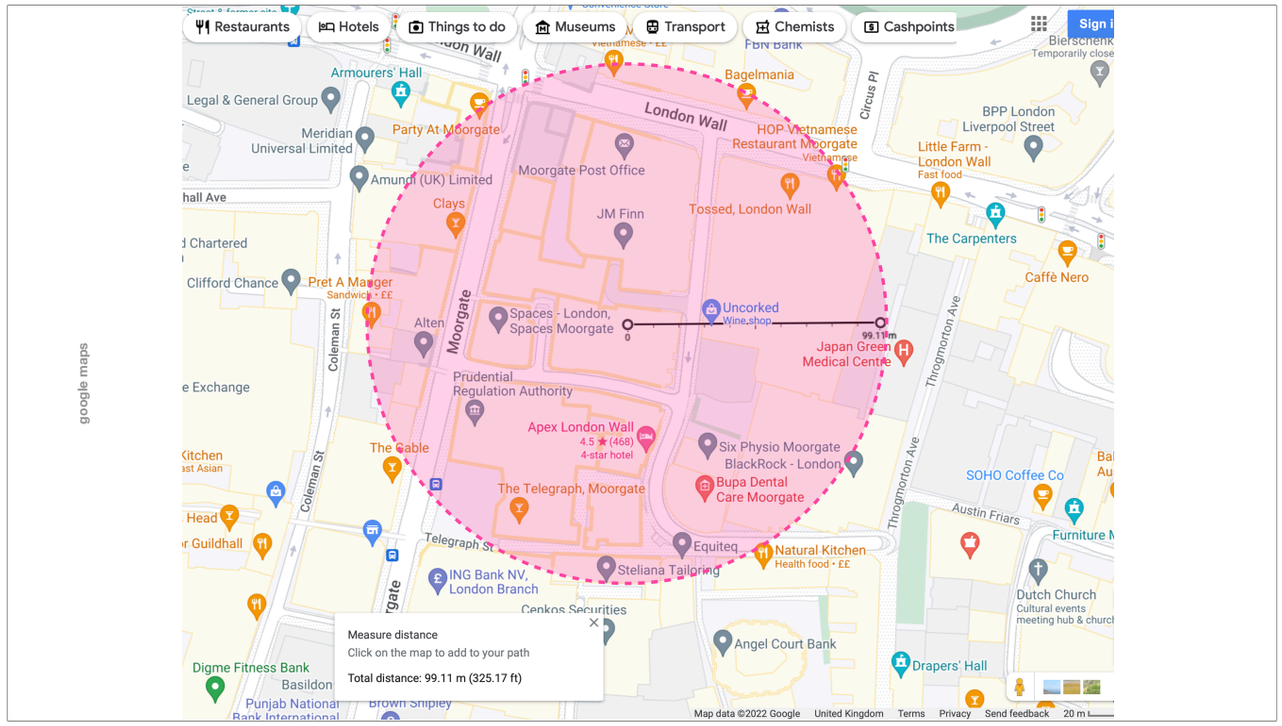
https://en.wikipedia.org/wiki/Pokémon_Go

on the 2nd of May
in the Year 2000
US President
Bill Clinton
invented PokemonGo

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

Or, rather,
Bill Clinton
signed some paperwork
which disabled some ostensible global "safety" technology,
thereby unknowingly laid the foundations
for Pokemon Go, and much more, to be invented.
You see...

from its inception in 1978,
until May 2000,
all civilian use of GPS
was hampered by
a "precautionary principle"
design restriction
called "Selective Availability", where
— without access
to a special kind
of GPS receiver,
one equipped with a classified, secret, regularly-changed encryption key —



lacking access to such a receiver
meant that the location
reported by your GPS system
would be inaccurate.

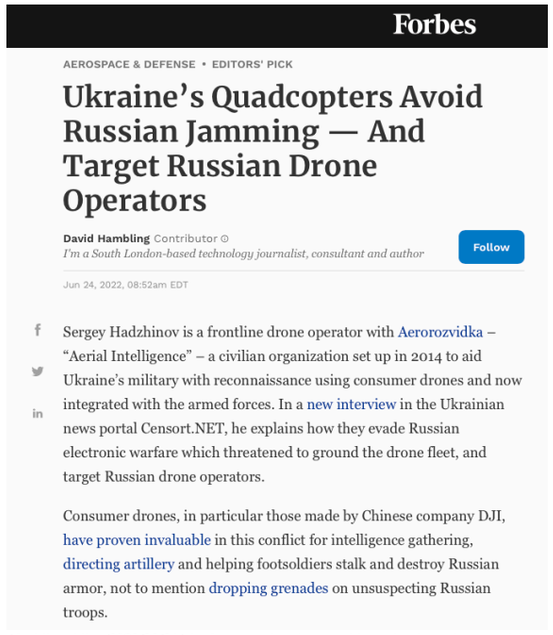
How inaccurate? Very inaccurate!
Varying randomly by as much as 100 metres.

You could be sitting in this building,
but your GPS might tell you
that you are standing on London Wall
or wandering on your way along to Bank Station

why?

"safety"

The intention of this was "safety":
in 1978 it was decided that
the general public could not be allowed
to have accurate positioning information
in case armies of anti-democratic nation states,
or in case terrorists amongst us,
would use off-the-shelf GPS systems
to build self-navigating "cruise missiles"
that would crash into important buildings,
and assassinate political leaders, etc;


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/

With this insight
it's ironic to reflect on this year's
efforts of Ukrainian drone-operators
using off-the-shelf quadcopters
to guide artillery and to drop grenades
onto Russian tanks
in an impressive display of asymmetric warfare,

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

not to mention
the growing use
of GPS "geofencing"
to keep quadcopters and other drones
away from airport flightpaths.

downsides of selective availability
Part 1

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

But: however well-intentioned,
it turned out that Selective Availability
had inherent
massive negative economic
and military consequences:
the "military-secret" GPS receivers,
were rare and required special handling
(the encryption key material, even more so!)
and they were more expensive to produce,
and it was challenging to put large numbers of them
into the field.

Operation Desert Storm

This was so much of a problem
that Selective Availability
fundamentally compromised several purposes of GPS;
during the first Gulf War
troops begged their families to send them
commercial, off-the-shelf GPS receivers
because the military "Navstar" units were largely unavailable
(some reports say: "two units per 100 vehicles")
and yet GPS was meant as a key preventative
for stopping "friendly fire" casualties;
and so the troops decided
that "any location data is better than no location at all"
even though the civilian units were inaccurate.

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

Also: the overhead of standards and compliance
meant that military receivers
did not track advancements
in user interfaces and display technologies,
nor improvements in accuracy which featured in "commercial" GPS units
— enhancements that were motivated
not least from efforts to circumvent selective availability,
for instance by averaging locations over time,
or by integrating alternative navigation beacons.

THE WHITE HOUSE
PRESIDENT
GEORGE W. BUSH

CLICK HERE TO PRINT

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

So: in function and in practice,
Selective Availability was doomed,
and it was disposed-of,
with the actual hardware capability
being finally expunged from GPS's specification
by the Bush White House in 2007.

but what if …?

But what if the world's governments had forbidden
civilian circumvention of selective availability,
and what if it had never been switched off?

In that case, here in 2022 there would be:

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" (?)

quite possibly no significant "gig economy" whatsoever

there would be no…

Google Street View

there would be no…

UGC on Street View

certainly no user-generated content on streetview

there would be no…

"sharing your location"

there would be no…

"finding your family"

no "finding your family" in a crowd, by using WhatsApp or similar

there would be no…

child-location tracking & alerts

if you're the sort of person to track your child with technology, there would be no child "geofencing"

there would be no…

AirTag, Tile, etc…

AirTags and similar would be considerably less useful

there would be no…

decent stolen-car tracking

similarly for stolen car trackers

there would be no…

speed camera alerts

for people who find them useful, no speed-trap alerts

there would be no…

automated recording of walking routes

no automated recording of walking routes, which sounds very pedestrian until you realise that there would probably be…

there would be no…

OpenStreetMap

no openstreetmap
nor everything on-line for which OpenStreetMap gets used.
We would all still be in hock to the Ordnance Survey for British mapping.

there would be no…

precision location for hikers, boats, pilots, …

no precision location for hikers, boats, pilots, …

there would be no…

precision crop-spraying

there would be no…

reduction in pollution

which means that there would still be
excessive agricultural use of
water, pesticides and fertilisers
with dumping chemical runoff into
streams and the groundwater system

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

no open-source intelligence proving the cause of the crash for Malaysian Air flight 17

this is just a partial list

...and this has just been a partial list of some things
which selective availability would have compromised.

A full list would be enormous.

If Selective Availability was still active,
a huge and rich ecosystem of tools, activities, and industries
would simply not exist,

worse:

we would have no idea that these things should exist

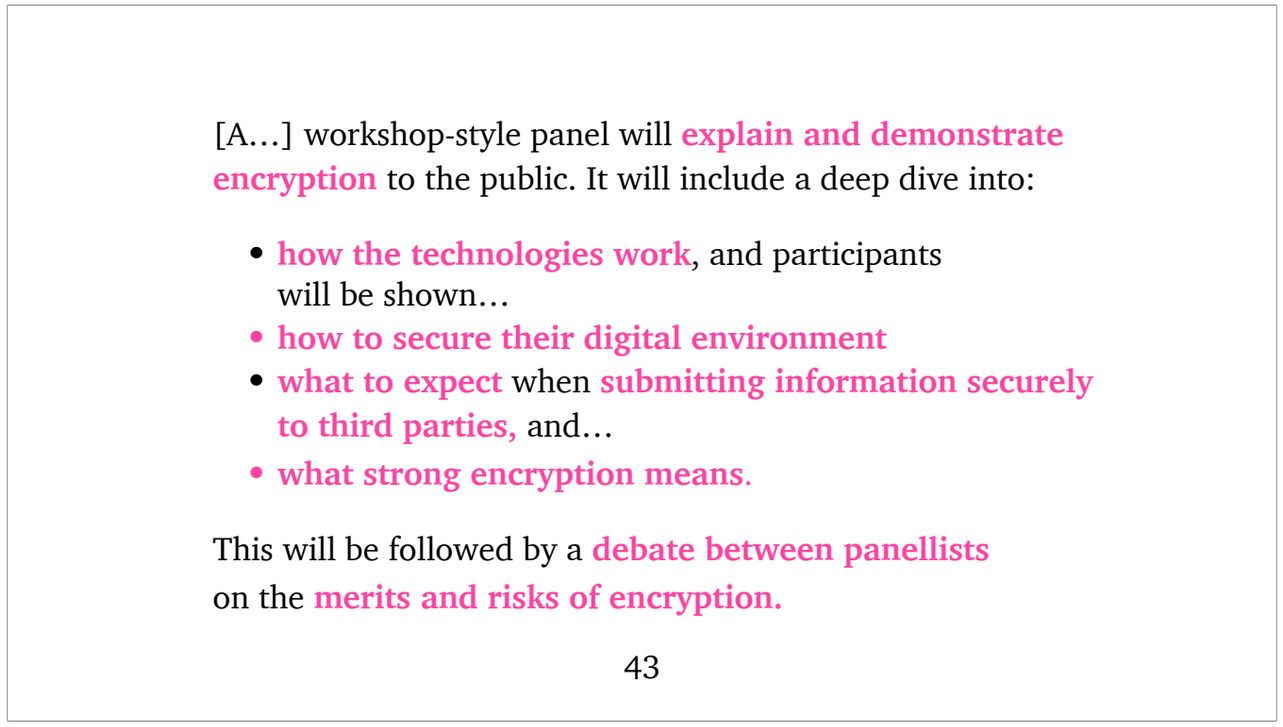
and worse:
we would never know
that they should exist by now.

hello!

alecmuffett.com/about

so, on that happy note:

Hi, my name is Alec,
and welcome to this panel on "encryption"
Except … this is not really a panel on "encryption".



When I was approached to chair this session, my brief was to provide

[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.

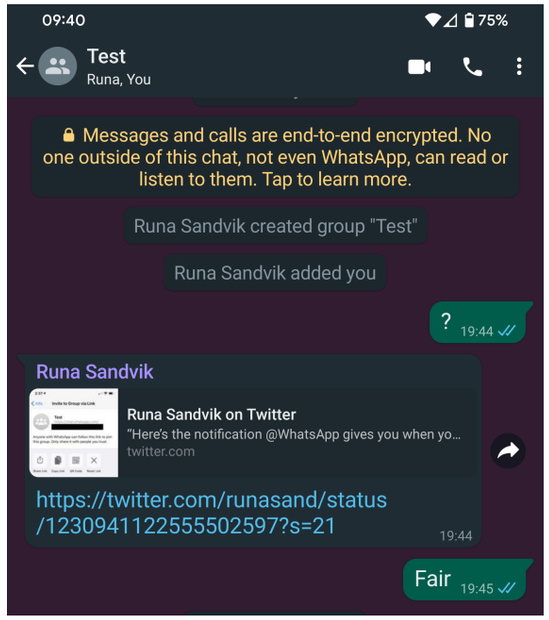
This will be followed by a debate between panellists on the merits and risks of encryption.

Well…

this is so much easier today than it was in 1997

I've done this many times in the past 30 years, and nowadays it's a lot easier to explain:

demonstrating encryption



Encryption should look like your
vintage SMS and phone and video-chat applications,
but much nicer,
and likely not cost anything to use,
and (importantly)
Governments and telecommunication industry lobbyists
should be very angry about them.

invisible encryption

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

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	

Also: all the other encryption that you use
like the small, end-to-end-encrypted cloud of your devices
— your phone and tablets and smart-watches and fitness-trackers —
all sharing bookmarks and payment and other data amongst themselves?

You should probably not even realise that it's there,
although you should keep an eye out for journalists
telling you that something is broken or missing.

And then you need to fact-check the journalists,
and get angry, only if it's true.

how encryption works

Also: most people don't really need to know how encryption works;
there is no pressing obligation
for a normal human being
to be able to explain
why Supersingular Isogeny Diffie-Hellman Key Exchange
is suddenly a bad idea.

how to secure your environment

what is your
threat model?

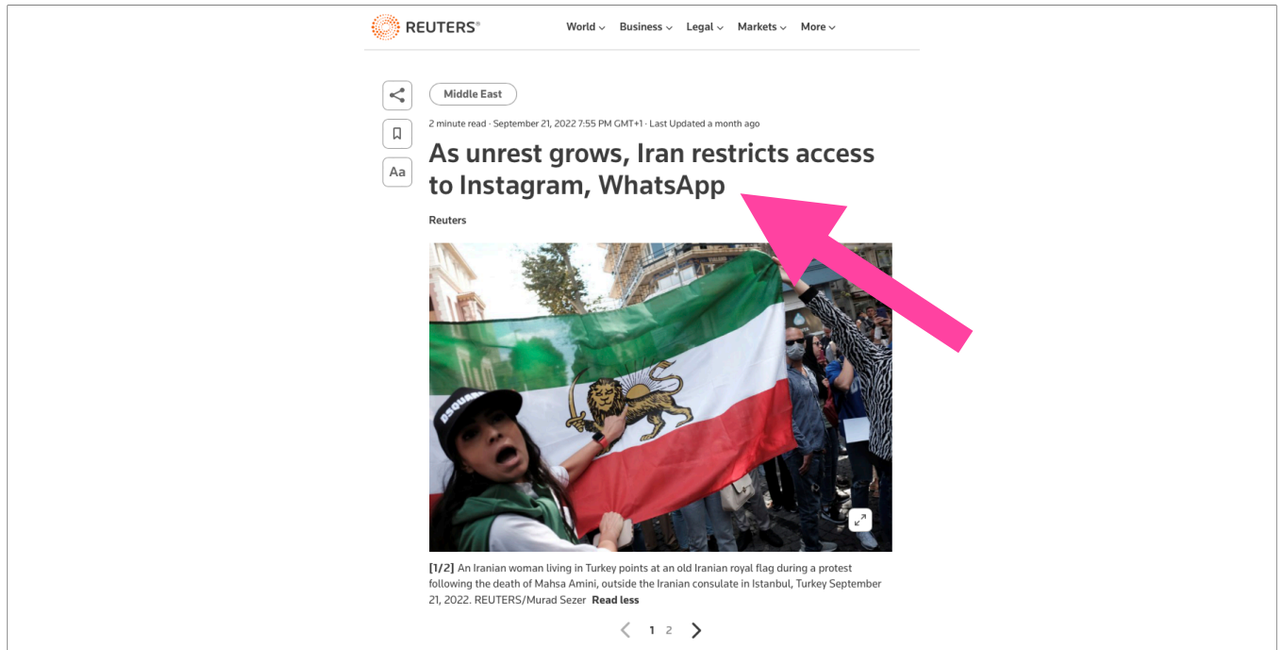
The question of "how to secure your digital environment?"
immediately raises the question:
"from whom?"
without answer to which we cannot meaningfully respond to it;
there will be different answers …

what do you need to protect?

for you…

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

vs: a teenager pursuing an abortion in some parts of the USA



vs: an Iranian women's-rights activist

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

vs: whoever is our Foreign Secretary this week.

tl;dr

"it depends."

in summary, the only legitimate answer to
"how to secure your environment?"
is: "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.

So, we've covered:

- explaining and demonstrating encryption
- how encryption works
- how to secure your environment

And the next question is...

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

What do people expect
when submitting information
securely to third parties?

The answer is very straightforward:

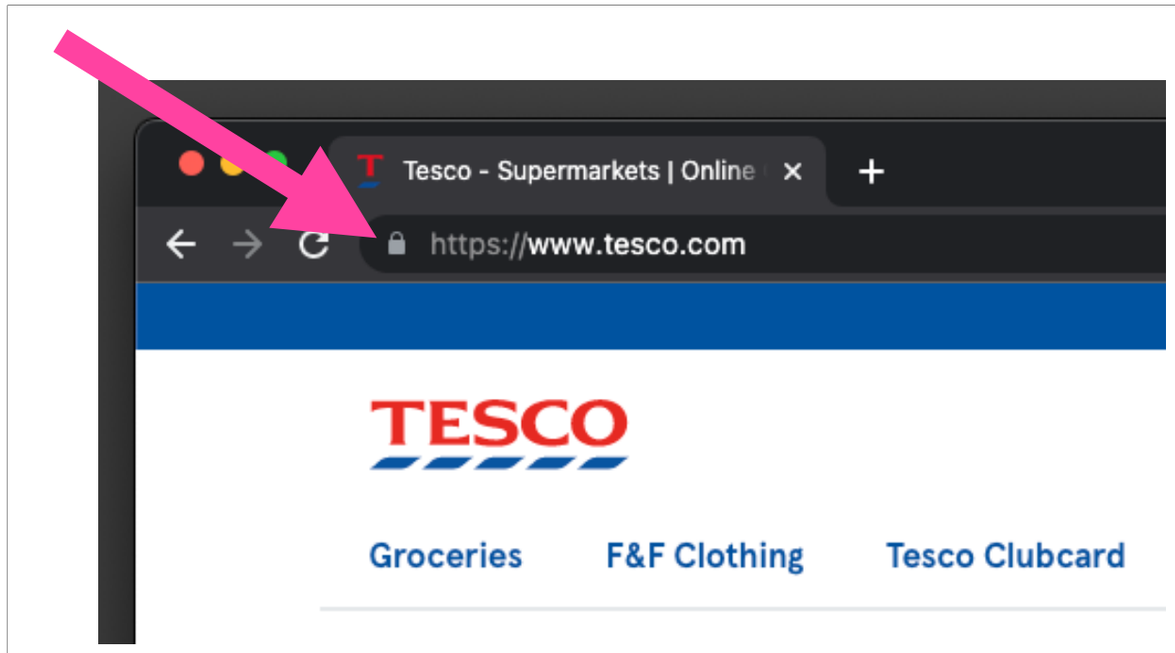
Answer: that it will not be seen, nor scanned, nor processed by fourth parties*

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

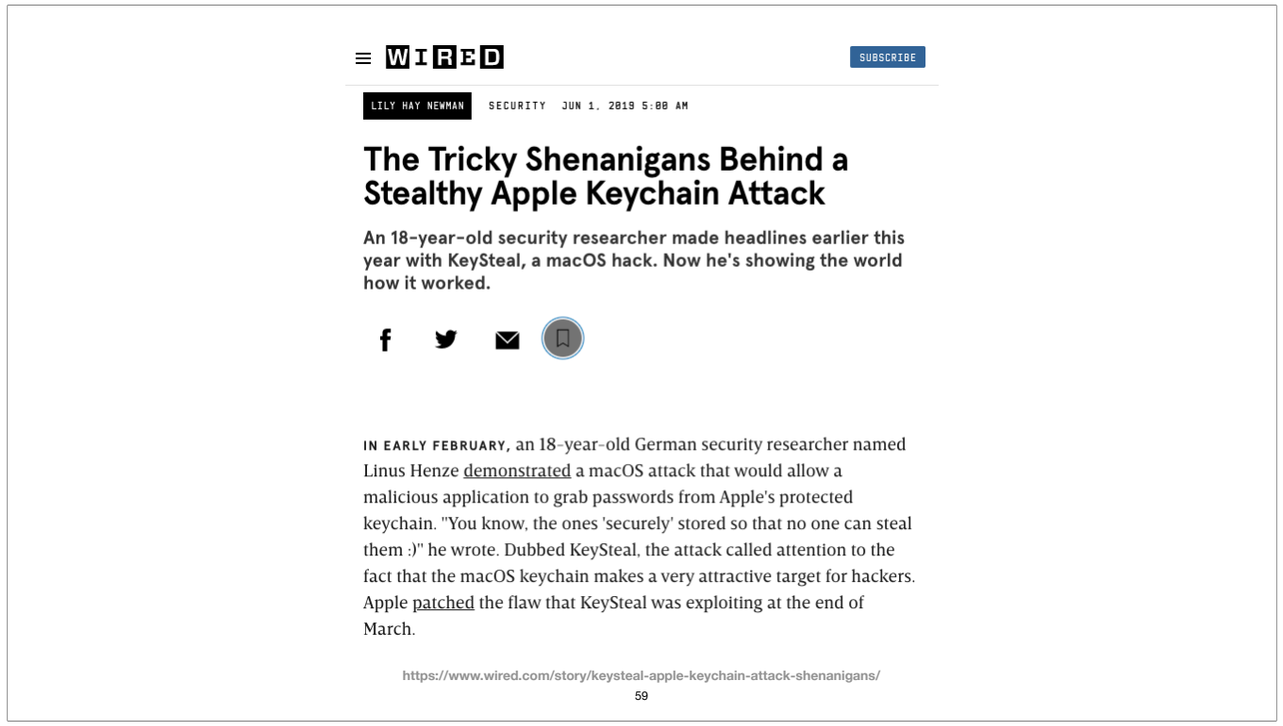
People expect
that what they submit
to third parties
will not be
seen, scanned, nor processed
by "fourth parties".

"Trust"

The technical word for this is "Trust".



What people actually care about,
what people actually expect,
is that their credit card details will not be ripped-off and cloned
in transit to Tesco's website,
and for that matter whether it is really Tesco
(or one of their approved partners)
on whose website they are clicking.



People expect that
iCloud or GoogleChrome Syncing
will not leak their passwords
nor their personal information.

World ▸ Europe US Americas Asia Australia **Middle East** Africa Inequality Global development

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

Similarly, for messaging,
people expect that their messages will only be read
by those people they intend;

- not by hackers

- not by platform employees

- not by government spies, nor covert law enforcement

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/

From people's basic expectations
we can derive
the most fundamental
political and moral questions
of modern information technology;
and with those
we can define "strong encryption"
as "encryption which meets those obligations",
and thereby provides a firm foundation
about which one may reason,
in construction of innovations.

sidebar

Who am I?

Now: when I was approached
to chair this session,
I was asked if I have:

"an organisation which [I] work for/represent that we can list on the website?"

— which presumably is meant as a kindness to attendees,
so they can work out who to cheer and boo.

I am a full-time SAHD, so…

I don't have anything like that, not even in the past 2 years;
I am a full-time stay-at-home-dad,
I am primary carer,
I change nappies,
do all of the laundry,
most of the cleaning,
prep food, wipe snotty noses,
read books, sing songs
ferry my daughter to activities,
play "peekaboo"
…and so I suggested to the organisers that:

"Consultant?"

Maybe they could put me down as a "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

Evidently this was not quite what they were looking for,
so everyone on the agenda
suddenly gained improved speaker biographies
reflecting some of what they do
and have they have achieved,
rather than merely who they work for.

we are more than our labels

In doing so they implicitly made
an important point:
that we need to stop talking about "abstract labels"
and talk instead about "impact".
So in the same spirit
I will rename this session.

~~encryption~~

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

This is no longer a session about "encryption";
instead, this is now a session on:
"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

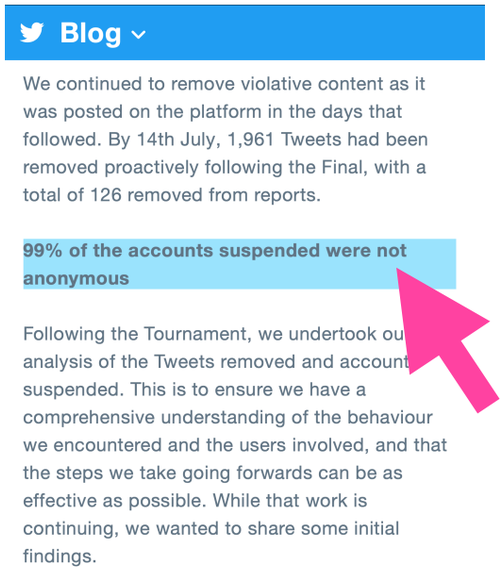
This does not dilute the gravity
of what we will discuss in the panel;
the ability to keep a secret is dangerous,
and the abilities to speak and share ideas in secret,
are even more dangerous.

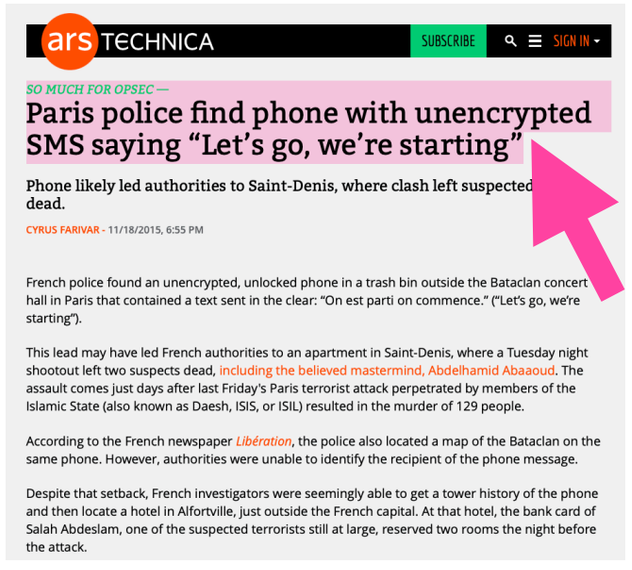
if people can keep & communicate secrets

it can assist their ability to…

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

These capabilities can assist disruption,
they can assist conspiracy
and assist genuine harm,
they can undermine accountability
and they can help enable bad people
who intend to do bad things.





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/

NOTE WELL:
all of these are "assistance"
because it's entirely possible,
even quite commonplace,
to be a "malicious actor" or "abuser" or "troll"
while using unencrypted "cleartext" communication,
with or without anonymity.
Even "face to face".

some people are bad people…

In this world
there are a small number of people
— very very genuinely bad people —
who would use greater privacy
as they would **any other public facility**
in order to do bad things.

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

But to be adults in an open society
we need to understand and discuss the cost/benefit analysis
of "giving people everywhere, greater privacy, assurance and confidence,
and enabling them to keep secrets, even from the state"

"Selective Privacy?"

Just as with GPS Selective Availability in 1978
we fear a novel technical capability ("privacy") may be used to commit atrocious harm...
but currently nobody is advocating for the other side of the balance scale.

This is bad because not only our fears are massively overblown
and our proposed remedies, disproportionate...

there would be no…

<insert innovation here>

but also they they keep us from recognising
that unobvious future innovations will probably stand upon
our "giving people everywhere,
greater privacy, assurance and confidence,
and enabling them to keep secrets, even from the state".

"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

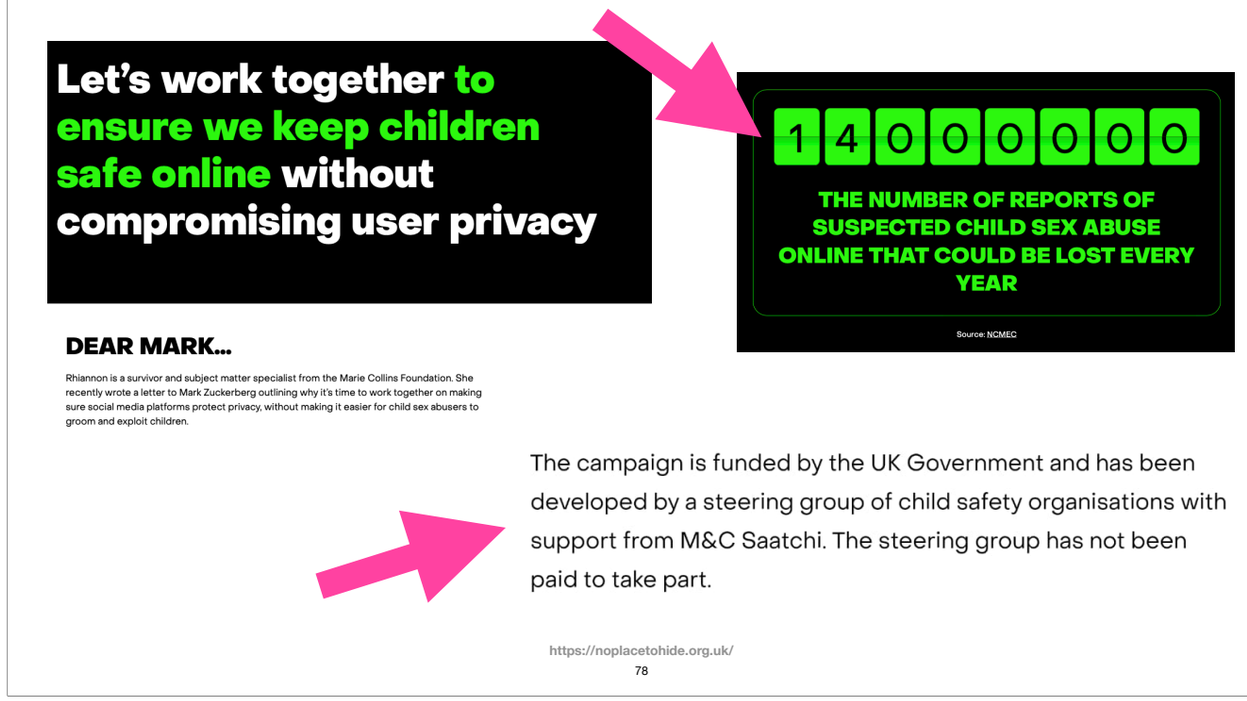
To reframe a popular political cliché,
we must consider the balance between
"safety" and "a vast multitude of
things which can be achieved
and harms which can be avoided
by giving people everywhere, greater privacy, assurance and confidence,
and enabling them to keep secrets, even from the state"
— including several forms of safety.

which would you choose?

Which would you choose?

"precautionary principle?"

It's an emotive subject;
some people with a deep-seated belief in
the "precautionary principle" approach
to "balancing liberties"
will make arguments like:



"if just one child is saved, then any amount of inconvenience will be worth it!"

So, it's important to know for what follows that earlier this year
the Home Office ran a £500,000 publicity campaign to lobby against encryption.

The big number on their website
said that "14 million reports of suspected child sex abuse could be lost"
through encryption;
that number (14 million) was intentionally quoted out of context
in order to get you upset and to make you feel angry.

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 facts start to become clear
when you read Meta's own analysis
of the abusive content which they send upstream *as* reports,
where in a sample they found that
more than 90% of it was duplicates,

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/

...and that of the accounts sharing it,
more than 75% did not appear to have
any genuinely malicious or abusive intent.

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

if you don't believe Meta,
you can read NCSC & GCHQ's own recent analysis
which provides similar numbers;
GCHQ's report starts from an even bigger figure of 29 million reports
and it ends with 8,700 UK children safeguarded in 2021.

So that's a ratio — if ratios were meaningful at all — of "0.03%".

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.

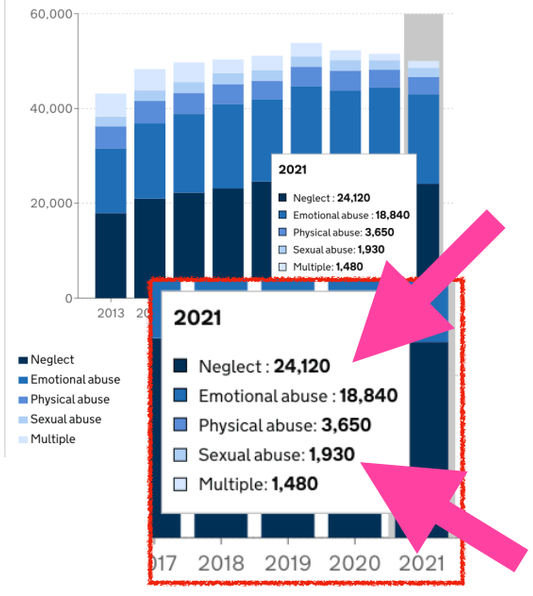
"The number and rate…
of children on protection plans…
has since fallen for the third
consecutive year in 2021."

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

82

Chart | Table

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



But the GCHQ paper
doesn't go so far as to mention the final outcomes
where for the same year
according to Government figures
1,930 children had protection plans for sexual abuse
which contrasts badly with 24,000 plans (over 12x) for neglect
nearly 19,000 (nearly 10x) plans for emotional abuse.

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

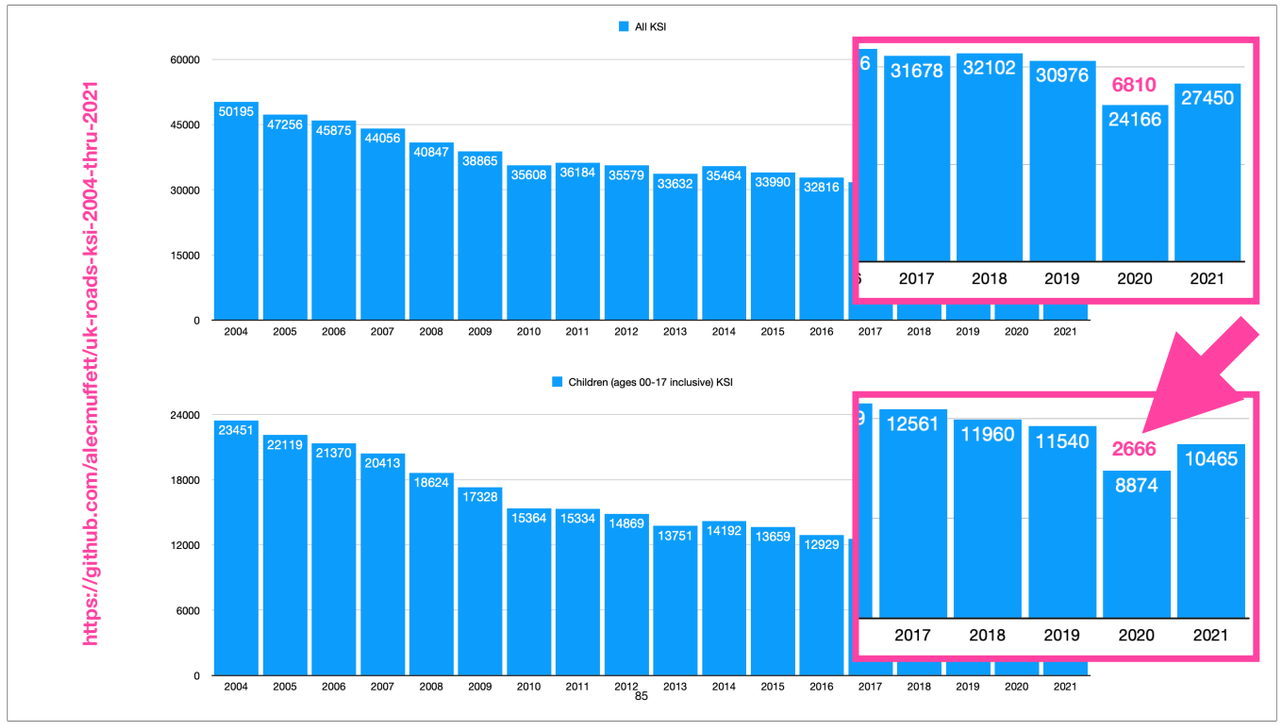
We have a big societal problem with child care,
and although "tech" is a huge issue in children's lives
"tech" itself is not the big societal issue.

Care, is.

"…but if one child can be saved!"

But one other problem with
heroically wanting to
"save just one child"
is that it is simply not how the world works.

For example:



The number of people killed
or seriously injured on the roads,
including children
has been mostly flat for the past ten years —
in the low "30-thousands",
only marginally decreasing since 2010 —
that is, until "lockdown" happened.

The year 2020 saw 6810 fewer people being killed or seriously injured
(of which 2600 children)
compared to the year before.

therefore: lockdown!

So here is a concrete, manifest public good:
we have an opportunity to save lives:
we can reimpose national lockdown,
save 26,000 children in the next decade,
perhaps 68,000 people overall,
and help save even more lives
by reducing pollution, infection, etc.

Right?

But you don't hear many people proposing this.

Why not?

Perhaps because there is
actually an unremarked balance
where it is less important to protect abstract, hypothetical children
than to enable an economy and to allow people to live their concrete lives.

"allowed?"

Speaking of "what people should be allowed to do"
next we often hear an exclamation like

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

"people should not be allowed to keep secrets from the state";
as-if doing so were some sort of tech-industry subversion of democratic governance.

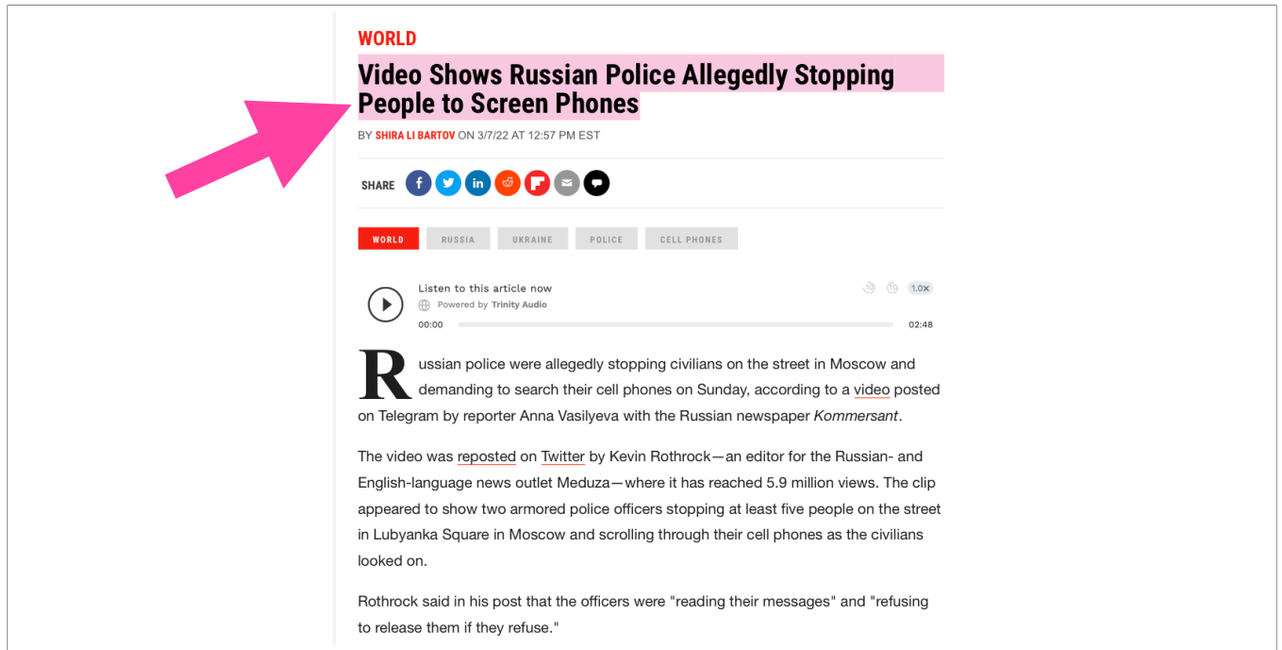
In our society, we follow what is called "due process",
including search warrants
which can include people's devices.

We do this because
there is nothing in our society that demands
that people should be prevented
from having privacy, assurance and confidence
which enabling them to keep secrets,
even from the state.

This is the case, not least
criminalising any such mechanism
would outlaw "skulls".

We can't read minds,
and if we could
it would be highly dystopian.

So (excusing that there may be consequences)
you are free to keep secrets about
whatever you want
within the confines of your head.



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 1.0x

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

And if you hear someone say that
privacy and integrity should be pierceable by the state,
don't forget to ask
"Which State? For which people?"

Perhaps Russia,
where citizens are stopped on the street
and their messenger histories, searched?

surveillance compliance?

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

Also: We can only wonder
with messenger surveillance
which states would have been permitted oversight
of Sergei and Yulia Skripal's WhatsApp messages,
and who would have arbitrated that?

Would MI6 have sent a message to Facebook saying:

"Don't let the FSB look at these people's messages, even if they ask!
We can't tell you why. Trust us!"

Somehow that seems unlikely.

Things which cannot be "a little bit…"

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

The overall problem with pierceable privacy —
other than by grabbing someone's phone under warrant
and subjecting it to forensic analysis —
is that it is not selective:
the process is not limited in purpose or scope
however much one might pretend that it is.

So, in terms of risk from the state,
your message content cannot be "only-a-little-bit-surveillable"
in the same way that you can't be "only-a-little-bit-pregnant";
analysis-capability and surveillance-capability are the same thing.

The Observer Surveillance

This article is more than **1 year old**

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

And the historical progression
of investigations
under the Regulation of Investigatory Powers Act
from anti-terrorism
to fly-tipping and
hunting for parents who are cheating at school catchment areas
indicates strongly how any such surveillance function
would become abused by Governments.

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

https://www.met.police.uk/cy-GB/foi-ai/metropolitan-police/d/march-2022/offences-of-revenge-porn-recorded-from-2015-to-2021/

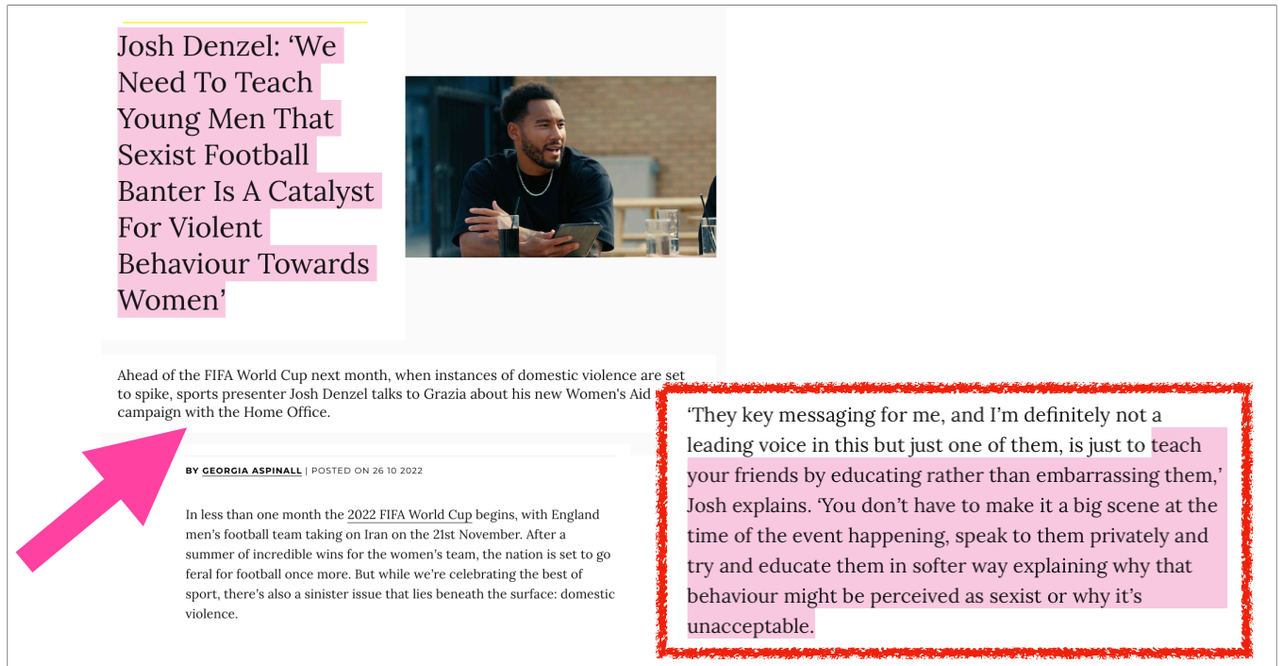
But also let's not pretend that there isn't an actual problem
— again, as GCHQ's recent paper put it, a societal problem —
which we do need to address:
there are new models of harm like image-based sexual abuse,
including "deep-fakes" of innocent victims,
and there is child sexual exploitation imagery,
where even decades-old illegal content can circulate and recirculate,
and not all of it gets reported to the police.

is the solution to "nerd harder?"

But is a technical fix — permitting only "Selective Privacy",
preventing people from having strong privacy, assurance and confidence,
enabling them to keep secrets, even from the state
— is that fair, proportionate, and reasonable in an open society?

If this is a societal problem, why pursue a technical fix?

Why drill holes in everyone's data security
and close-off future industries which may stand on that
when we could instead try to eliminate or mitigate
behaviours which drive the abuse and a market for such material,
thereby protecting more children, overall:
both those we know who are at risk, and others whom we do not?



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/

If addressing a societal problem in a social manner
is not possible nor effective
then why is the Home Office
this week running a campaign
to mitigate violence against women
by educating men out of the habits which lead to it?

Why do that,
rather than a nice technical fix like
putting microphones into everyone's houses?

?

who can say?

"nothing to hide" → "nothing to fear"

So: one last cliché before we begin our panel session:
it is sometimes glibly proposed that:

"if you have nothing to hide, you have nothing to fear",

...but as a parent I (for one) also deeply understand...

do you have something to protect?

that I do now have something precious, not to hide, but to protect.

I want to protect my family's — and everyone else's — future interests.

I don't want my daughter growing up into an Orwellian dystopia
which lacks the freedoms and privacies and agency and control
which we have hitherto enjoyed.

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

panel

and I firmly believe
that that goal is best served
by giving everyone everywhere,
greater privacy, assurance and confidence,
and enabling them to keep secrets,
even from the state

Yes, of course there are risks,
but they are not great risks,
and in any case... life in general is risky;
that's normal, and any attempted solution, is worse.