Reflections on Ten+ Years Past the Snowden Revelations

Background and RFC9446

Stephen Farrell
stephen.farrell@cs.tcd.ie

May 2024

~~Reflections on Ten Years Past the Snowden Revelations~~

~~RFC9446~~

~~Stephen Farrell, Farzaneh Badii,~~
~~Bruce Schneier, Steven M. Bellovin~~

~~IETF 117~~
~~July 2023~~

~~Presenter: stephen.farrell@cs.tcd.ie~~

What happened?

- In 2013, an NSA contractor (Edward Snowden) released a large set of internal, classified documents to reporters who (carefully) published stories based on those
- Overall, those showed that 5-eyes signals intelligence agencies were far more intrusive than had been appreciated
- If you’re not familiar with this stuff or have forgotten, there’s a pretty good timeline at:
  - https://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013%E2%80%93present)

Upstream Collection

- Examine loads of traffic at Internet backbone devices
- Sometimes related to trans-oceanic fibre
- Often with operator co-operation
- Likely involving some filtering and buffering before being sent back to “base”
- Subtle definitions for what “collected” means
  - https://en.wikipedia.org/wiki/Upstream_collection

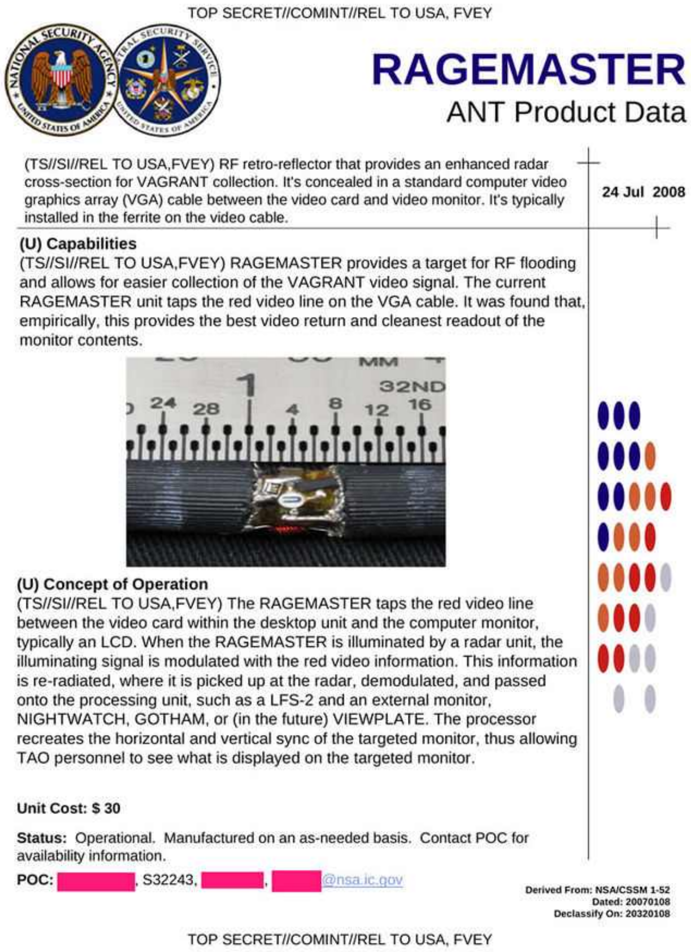
BULLRUN

- One of the programmes disclosed was BULLRUN, an ~US$250m/yr fund to break or work around the kind of security mechanisms we use on the Internet
  - https://en.wikipedia.org/wiki/Bullrun_(decryption_program)
- The DUAL_EC_DRBG fiasco is the kind of thing that may have been a part of that
  - https://projectbullrun.org/dual-ec/documents/dual-ec-20150731.pdf

ROYAL CONCIERGE

- GCHQ (UK signals intelligence agency) monitored ~350 hotels to see who’s booking a room, presumably so they could have fun later
  - https://www.spiegel.de/international/europe/gchq-monitors-hotel-reservations-to-track-diplomats-a-933914.html
- Apparently done by monitoring cleartext emails to see when a reservation confirmation is sent from somewhere interesting to somewhere interesting

ANT Catalog



TOP SECRET//COMINT//REL TO USA, FVEY

RAGEMASTER

ANT Product Data

(TS//SI//REL TO USA,FVEY) RF retro-reflector that provides an enhanced radar cross-section for VAGRANT collection. It's concealed in a standard computer video graphics array (VGA) cable between the video card and video monitor. It's typically installed in the ferrite on the video cable.

24 Jul 2008

(U) Capabilities

(TS//SI//REL TO USA,FVEY) RAGEMASTER provides a target for RF flooding and allows for easier collection of the VAGRANT video signal. The current RAGEMASTER unit taps the red video line on the VGA cable. It was found that, empirically, this provides the best video return and cleanest readout of the monitor contents.

(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The RAGEMASTER taps the red video line between the video card within the desktop unit and the computer monitor, typically an LCD. When the RAGEMASTER is illuminated by a radar unit, the illuminating signal is modulated with the red video information. This information is re-radiated, where it is picked up at the radar, demodulated, and passed onto the processing unit, such as a LFS-2 and an external monitor, NIGHTWATCH, GOTHAM, or (in the future) VIEWPLATE. The processor recreates the horizontal and vertical sync of the targeted monitor, thus allowing TAO personnel to see what is displayed on the targeted monitor.

Unit Cost: $ 30

Status: Operational. Manufactured on an as-needed basis. Contact POC for availability information.

POC: [redacted], S32243, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

- Tap the video signal between computer and monitor
- Retrieve data when illuminated via radar unit (PHOTOANGLO)
- Loads more fun devices and s/w at:
  - https://en.wikipedia.org/wiki/ANT_catalog

IETF

- The Internet Engineering Task Force (IETF) is the main body that defines Internet protocol standards – https://ietf.org/
- Those include specifications for ways to encrypt and otherwise cryptographically protect Internet traffic, e.g. TLS, IPsec, S/MIME, PGP
- IETF participants were not happy about the Snowden revelations

IETF 88 Links

- IETF started to react in 2013, esp. at the November 2013 meeting, a 2014 workshop and subsequently (and it continues today)
- IETF-88 Plenary slides: https://www.ietf.org/proceedings/88/technical-plenary.html
- Video: https://www.youtube.com/watch?v=oV71hhEpQ20&pp=ygUQaWV0ZiA4OCBwbGVuYXJ5IA%3D%3D
- STRINT workshop: https://www.w3.org/2014/strint/

Being Annoyed Helps

- Result was quite a bit of energy directed towards improving deployments, Internet protocols and even IETF processes, including...
  - RFC7258/BCP188
  - The letsencrypt CA, leading to ACME protocol
  - Email transport layer encryption (SMTP/TLS deployment, MTA-STS)
  - Encryption of as much as possible with forward secrecy as a new baseline for transport layer and above (e.g., TLSv1.3, QUIC etc.)
  - DNS privacy (DoT/DoH/ODoH)
  - Caring more about long term identifiers (e.g., randomised MAC addresses, MADINAS WG)
- Other Internet organisations, open-source efforts and related also reacted (some of which gave rise to some of the IETF work above)

Pervasive Monitoring

From RFC7258/BCP188: “Pervasive Monitoring is an Attack”

> Pervasive Monitoring (PM) is widespread (and often covert) surveillance through intrusive gathering of protocol artefacts, including application content, or protocol meta-data such as headers. Active or passive wiretaps and traffic analysis, (e.g., correlation, timing or measuring packet sizes), or subverting the cryptographic keys used to secure protocols can also be used as part of pervasive monitoring. PM is distinguished by being indiscriminate and very large-scale, rather than by introducing new types of technical compromise.

PM is/was not everything

- PM is far from the only security or privacy issue on which we need to work
  - Spam, malware, DDoS, …
  - But mitigations for PM also help a lot with other problems
- Hypothesis: Working to address PM, and prioritising services and mechanisms that mitigate PM and that are also effective against other attacks is doing the “right thing”

Security & Privacy vs. “Management”

- There’s a tension (ack’d in RFC7258) that the better we protect security/privacy, the less well (some) network management tools work
  - There are also elements of mis-trust between some stakeholders that make this harder
- This recurs over and over, and generates angst:
  - Via efforts to break TLS (“Pretty please standardise my MitM technique”)
  - Via efforts to encrypt protocol data units that are relevant for network management causing heartache for network management folks
- Hard to know to what extent this is due to lazy/legacy n/w management techniques and how much it’ll be a lasting problem, but the increasing prevalence of ciphertext and end-to-end encryption will not change
  - In other words: we need to develop new n/w management tools that still work well when networks carry much more ciphertext
- And of course various governments usually have a plan in the drawer for “defeating” encryption that they pull out from time to time as events transpire
  - I think that ship has sailed myself

RFC9446 Overview

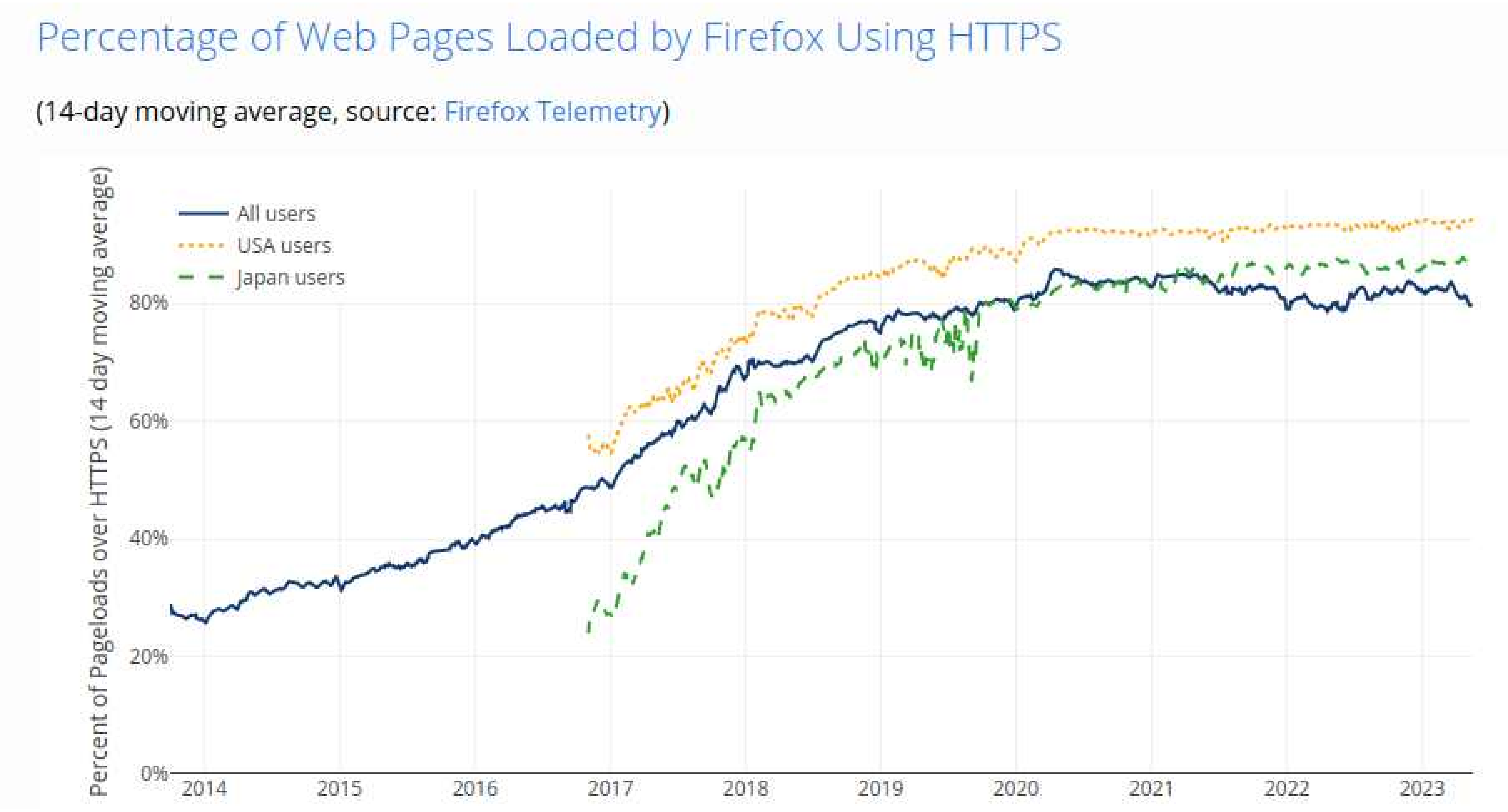
- The Snowden documents were released starting in June 2013 so in 2023 it seemed timely to reflect on what happened and what’s changed?
- RFC9446 is a collection of the authors’ separate reflections and some conclusions
- We hope it spurs others to similarly reflect, reach conclusions, and maybe take action
- Eliot Lear (our esteemed ISE) instigated this, recruited the authors and cat-herded variously

It’s Four Essays (mostly)

- Bruce provides a contemporaneous account of some of his involvement with the Snowden documents, not previously published
- Stephen recalls what happened within and around the IETF as a result
- Farzaneh considers impacts from a human-rights perspective
- Steve recounts the evolution of crypto-wars from pre-history, via Clipper, through Snowden and up to today
- Each include opinions as to what’s important to consider in all this
  - This talk is mostly about those opinion bits

Some Good News

https://letsencrypt.org/stats/

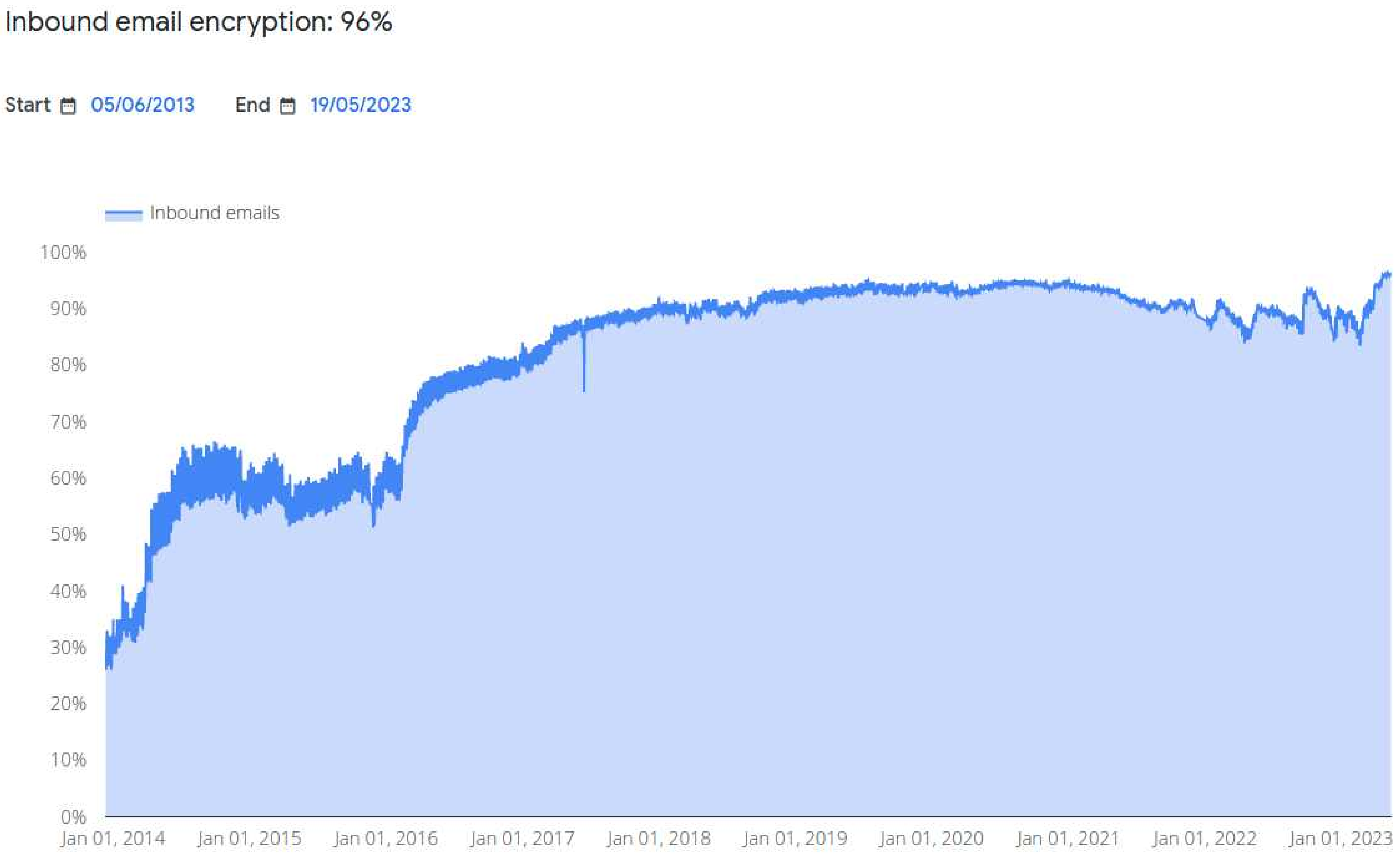


Percentage of Web Pages Loaded by Firefox Using HTTPS

(14-day moving average, source: Firefox Telemetry)

Some Good News

https://transparencyreport.google.com/safer-email/overview



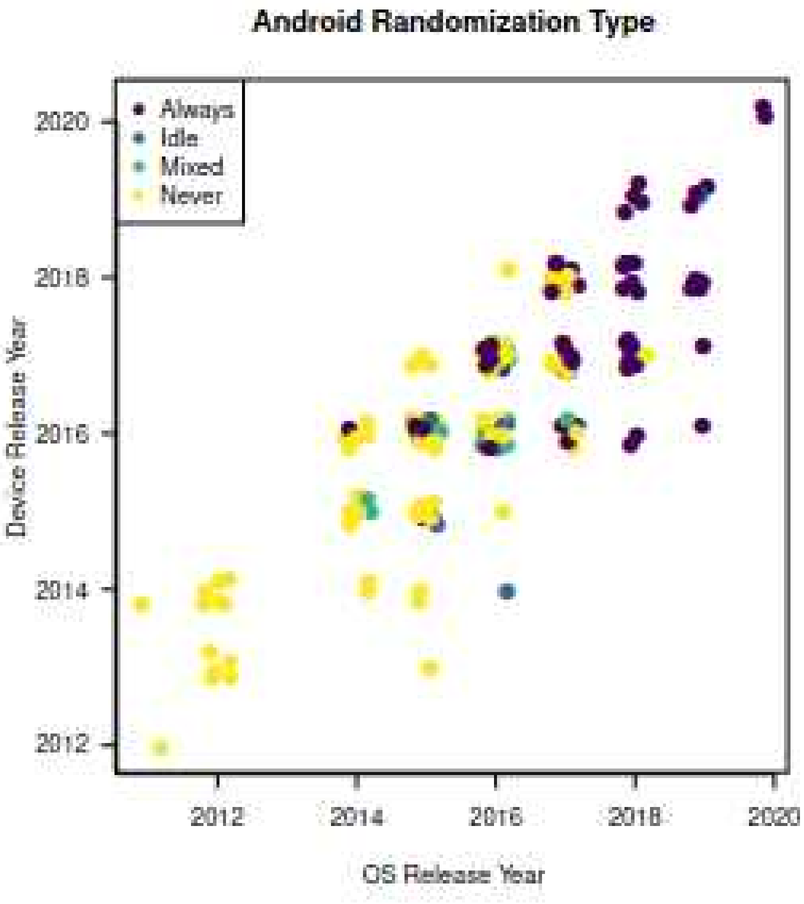
Inbound email encryption: 96%

Start 05/06/2013 End 19/05/2023

Some Good News

https://www.petsymposium.org/2021/files/papers/issue3/popets-2021-0042.pdf

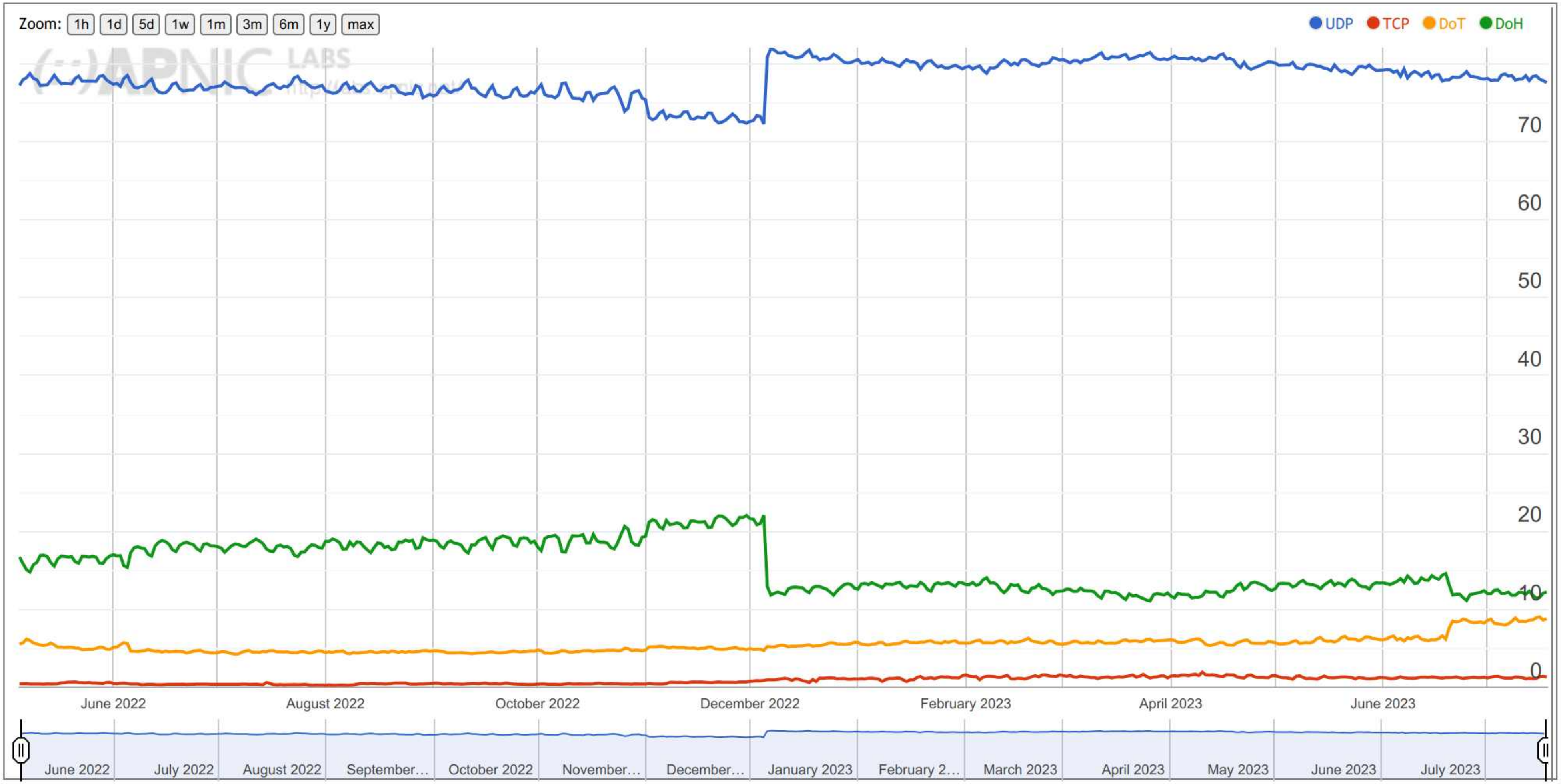
MAC address randomisation being deployed and getting (slowly?) better



Middling News

https://stats.labs.apnic.net/edns/XA

Cloudflare Open Recursive Resolver DNS Query Profile for World (XZ)



4 points from Bruce’s essay

- Maybe the implant catalog wasn’t a Snowden document?
- All we learned then is well out of date, we don’t know what’s been done since
- IETF 88 participants were indignant
- Despite the outcry, not much changed (visibly) in terms of US govt approach

4 points from Stephen’s essay

- Pushback against more encryption comes from those affected (but who get over it) and from those who just don't want it
- We didn't try tackle commercial surveillance near as much (RFC7258 does apply!)
- Regulators may stymie permissionless innovation
- We should think more about the ethics of what we do

4 points from Farzaneh’s essay

- Hard to empirically measure Snowden's effect
- We've never considered human rights that much, not clear that's changed
- Maybe not Snowden, but WHOIS -> RDAP took a long time
- Impact assessment may reveal how protocols have an impact on which and whose human rights

4 points from Steve’s essay

- Governments have long used encryption—and tried to break other folks’ encryption
- “Spies gonna spy”—if encryption is in the way, they’ll (somehow) try to work around it
- Even if our protocols are great, implementations, overall systems & s/w are not (c.f. ransomware)
- We should worry more about metadata

Current Work

- IETF work to improve comsec continues, e.g.:
  - TLS Encrypted Client Hello (ECH)
  - Hybrid post-quantum crypto schemes
  - Oblivious HTTP/DoH and similar
  - Privacy preserving metrics
  - Eventually, we’ll get a lot more interested in countering traffic analysis
- But… annoyance also dissipates...

Surveillance Capitalism

- Internet engineers found it quite possible to act based on their annoyance with signals intelligence agencies
- It seems harder to get them to do something about the legal but hugely privacy-invasive systems their employers deploy
- Advertising business model is basically pervasive monitoring
  - Pretty similar to the effect of breaches and data leaks (other than seemingly legal)
- Result: IMO the Internet is “worse” now than it was in 2013
  - Government regulators seem keen to step in, maybe correctly
  - That risks the permissionless innovation that lead to success for the earlier Internet
- Maybe: we should stop considering that we somehow “own” data we collect just because we control a copy

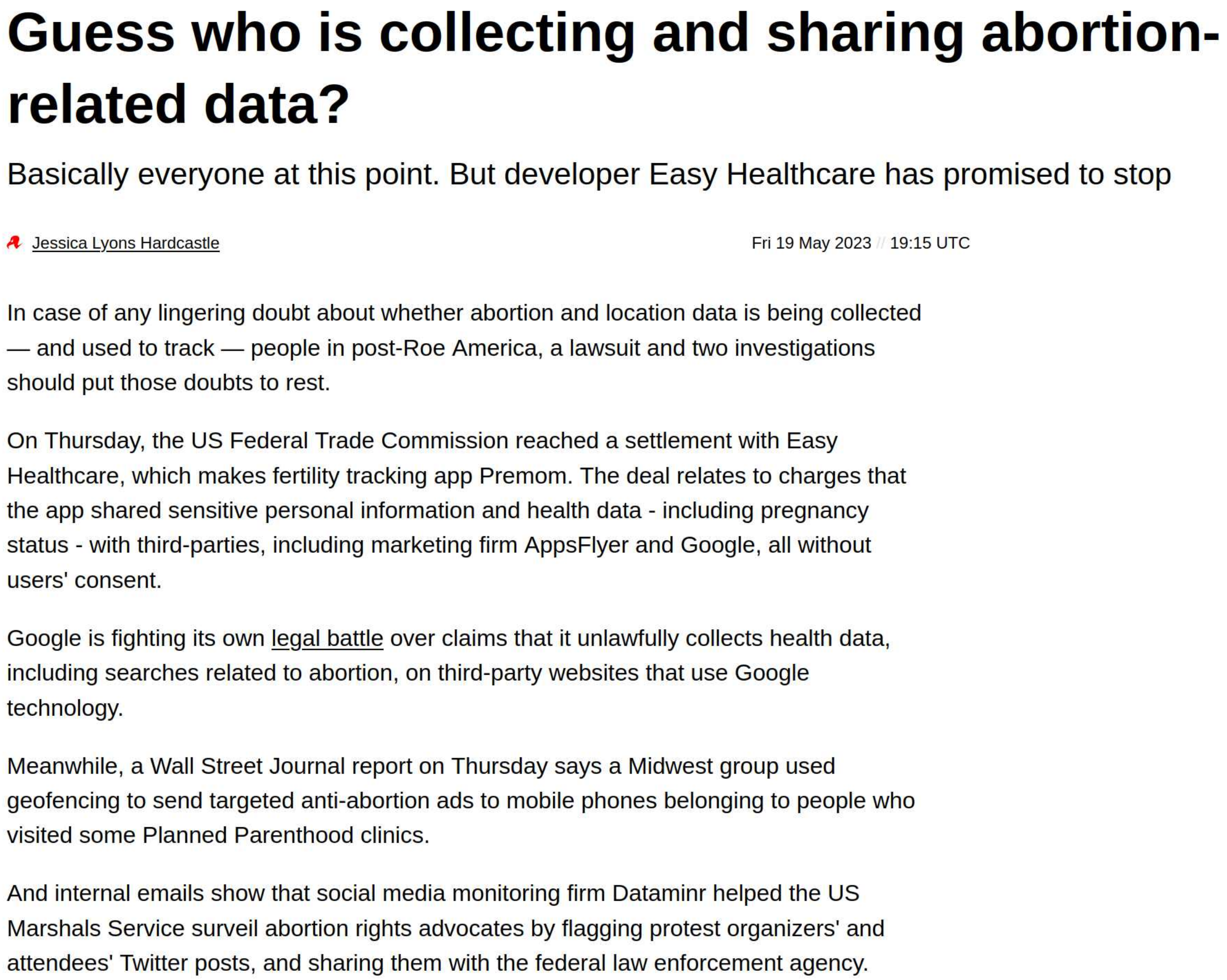
How bad does this get?

https://www.theregister.com/2023/05/19/abortion_data_tracking_cases/

- Regardless of what one thinks about abortion, we can probably all agree that it’s related data needs to be handled cautiously, ethically and with care for people in difficult situations.

- The web and mobile app ecosystem clearly leads developers and deployers to utterly lose sight of that.

- The answer here isn’t better network protocols, but ethical behaviour (that then requires good network protocols).



Guess who is collecting and sharing abortion-related data?

Basically everyone at this point. But developer Easy Healthcare has promised to stop

Jessica Lyons Hardcastle Fri 19 May 2023 // 19:15 UTC

In case of any lingering doubt about whether abortion and location data is being collected — and used to track — people in post-Roe America, a lawsuit and two investigations should put those doubts to rest.

On Thursday, the US Federal Trade Commission reached a settlement with Easy Healthcare, which makes fertility tracking app Premom. The deal relates to charges that the app shared sensitive personal information and health data - including pregnancy status - with third-parties, including marketing firm AppsFlyer and Google, all without users' consent.

Google is fighting its own legal battle over claims that it unlawfully collects health data, including searches related to abortion, on third-party websites that use Google technology.

Meanwhile, a Wall Street Journal report on Thursday says a Midwest group used geofencing to send targeted anti-abortion ads to mobile phones belonging to people who visited some Planned Parenthood clinics.

And internal emails show that social media monitoring firm Dataminr helped the US Marshals Service surveil abortion rights advocates by flagging protest organizers' and attendees' Twitter posts, and sharing them with the federal law enforcement agency.

Conclusions

- Snowden’s revelations were a big deal and did lead to significant change in Internet protocols and deployments
  - We’re not done with that work
- We know that things in many ways are worse now for people using the Internet
- Probably good if we reflect on all that and see what else needs doing and what needs changing
- My main take away: we should apply RFC7258 to protocols usable by commercial snoops just as much as we did government snoops

Thanks

Offline questions welcome too
stephen.farrell@cs.tcd.ie

These slides also at:
https://down.dsg.cs.tcd.ie/rfc9446-pressie-tcd.pdf