A few points about cryptography in recent decades

These slides: https://down.dsg.cs.tcd.ie/ripe21/farrell-ripe21.pdf

stephen.farrell@cs.tcd.ie
20210318

TL;DR

Cryptography is so widespread and well-known that the genie is not going back into the bottle, despite causing issues for those who have to adjust to more and more widespread use of the technology. Every time deployment expands, it causes a “sky is falling” reaction from those affected negatively. The sky hasn’t fallen, and won’t.

Let's start in the 19th Century

- A little before the Internet but…wires were tapped
  - http://bugsweeps.com/info/wiretap_short_history.html
  - https://www.counterpunch.org/2013/08/09/a-social-history-of-wiretaps-2/
- Basic law enforcement requirement:
  - Everything needs to be tappable
- Same as current lawful intercept
  - Not clearly a great plan

1999, 2016 – Crypto product survey

- Surveys done in 1999 and 2016 identifying cryptographic products (incl. OSS) available worldwide
  - Fewer in 2016, 546 vs. 805 “foreign,” but crypto is now a mainstream feature more than a product category
- Not clear surveys are commensurate, except for the intended affect on US policy related to cryptography
  - Any such laws are ultimately not a problem as mathematics is not nationalist!
  - They can be a PITA though
- https://cryptome.org/cpi-survey.htm
- https://www.schneier.com/academic/paperfiles/worldwide-survey-of-encryption-products.pdf

2013 - Snowdonia

- Partial timelines:
  - https://en.wikipedia.org/wiki/Global_surveillance_disclosure
  - https://www.theguardian.com/us-news/nsa
- My favourite:
  - https://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo
- My most interesting (politically):
  - https://theintercept.com/2018/02/17/gchq-belgacom-investigation-europe-hack/
- My most interesting (technically):
  - The short-range radar thing
  - https://en.wikipedia.org/wiki/NSA_ANT_catalog

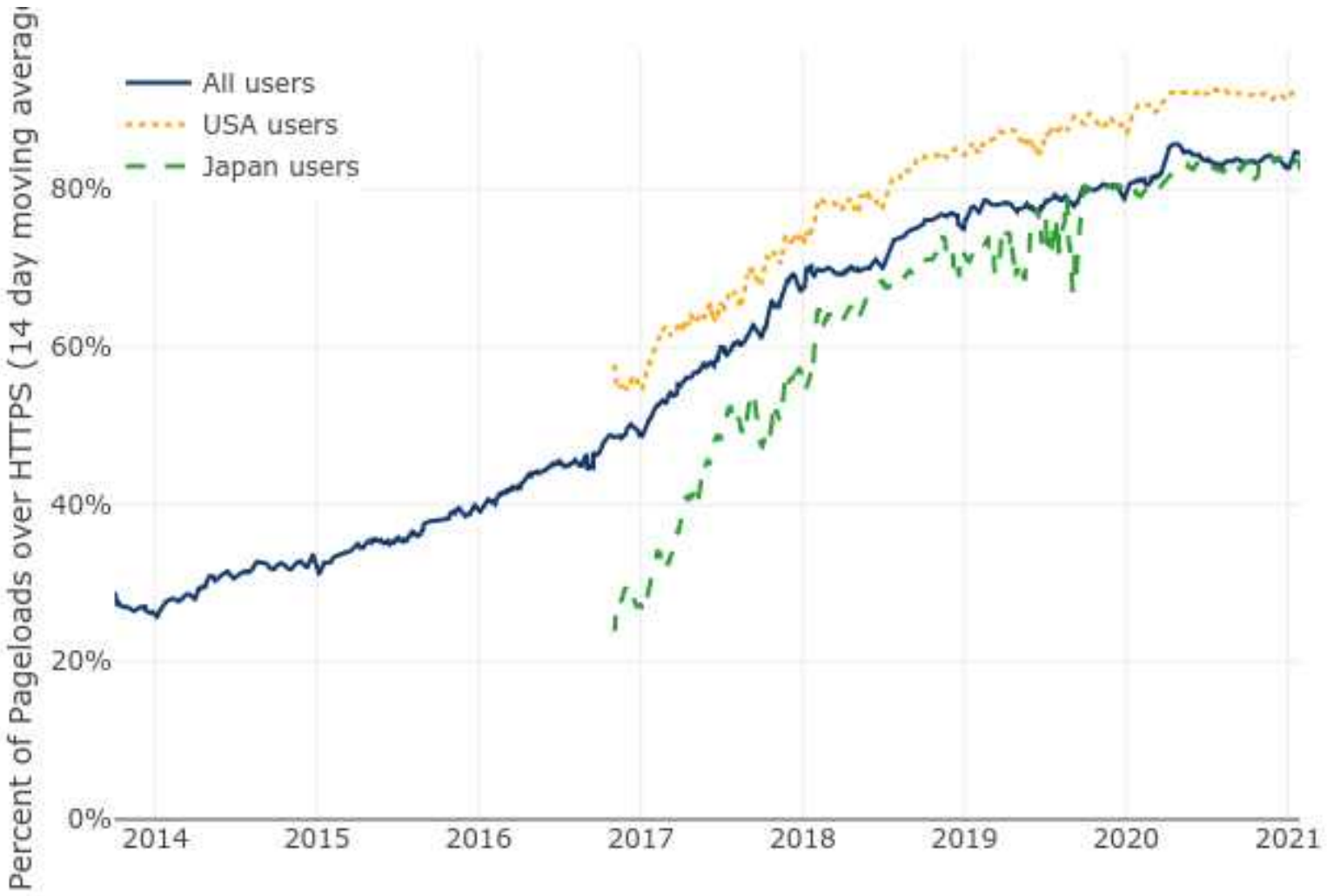
https://en.wikipedia.org/wiki/Edward_Snowden

Pervasive Monitoring

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

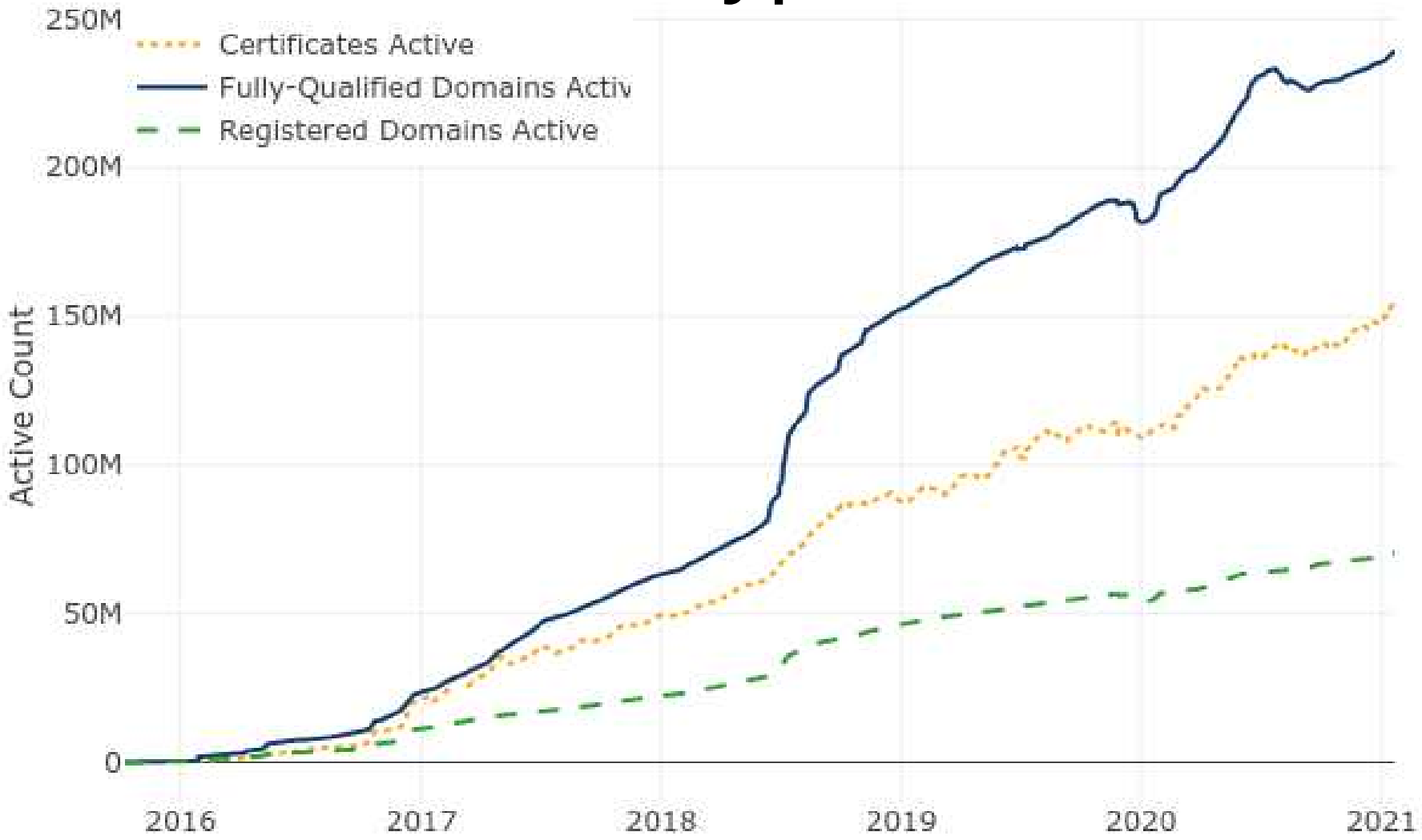
> Pervasive Monitoring (PM) is widespread (and often covert) surveillance through intrusive gathering of protocol artefacts, including application content, or protocol meta-data such as headers. Active or passive wiretaps and traffic analysis, (e.g., correlation, timing or measuring packet sizes), or 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.

HTTPS Growth



https://letsencrypt.org/stats/ based on FF telemetry https://docs.telemetry.mozilla.org/datasets/other/ssl/reference.html

Letsencrypt Growth



https://letsencrypt.org/stats/

DNS Privacy

- DNSSEC provides integrity and origin authentication but confidentiality/privacy was never considered a requirement
- Since 2013 that has changed
- QNAME minimisation RFC 7816
- DNS padding RFC 7830
- DNS-over-TLS (DoT) on port 853 RFC 7858
- DNS-over-HTTPS (DoH) often on port 443 RFC8484
  - Highly controversial, mostly IMO not because of confidentiality but because it moves the point of control
- Work on TLS for recursive to authoritative (slowly) ongoing

QUIC

- QUIC is a new transport protocol that runs over UDP and that encrypts a lot
  - https://datatracker.ietf.org/doc/charter-ietf-quic/
  - Goal is the same security properties as TLS1.3/TCP
- QUIC is already deployed to some extent
- Privacy is not the only reason things like QUIC use encryption
  - Cleartext allows middleboxes to see and mess with traffic, which has good and bad aspects
- Will likely provide examples of the tension between privacy and the ability to manage a network mentioned in RFC 7258
- And yes, there's a DNS-over-QUIC (DoQ) proposal too:-)

New(-ish) Crypto Things

- Dual-ec fiasco is a reminder we need a large/diverse set of academic cryptographers http://dualec.org/
- PQ algorithms will likely be combined with “classic” ciphers giving us possibly substantially bigger keys and/or signatures and/or ciphertexts
- Some new crypto primitives (e.g. OPRFs) might get traction if they offer benefits (e.g. for privacy-friendly telemetry), or… they might just get ignored – too early to tell
- Fully Homomorphic Encryption (FHE) would still be great but still doesn’t exist (in usable form)

Two More Prosaic Challenges

- Devices generate data & send to some host often secured via (D)TLS
- Today, there's no great way to get a server cert to use for that host unless the host has a DNS name
  - Leads to device → cloudy-server lock-in
- Challenge: find ways to authenticate and securely exchange keys between (small) devices and hosts that the device-owner chooses
- Challenge: sometimes emitting a packet (encrypted or not) leaks privacy sensitive information
  - E.g. query sent to NTP server => person arrived home and stuff woke from suspend

Thanks!

These slides: https://down.dsg.cs.tcd.ie/ripe21/farrell-ripe21.pdf

stephen.farrell@cs.tcd.ie
20210318

The Encryption Debate

Patrik Fältström
Technical Director and Head of Security
Netnod

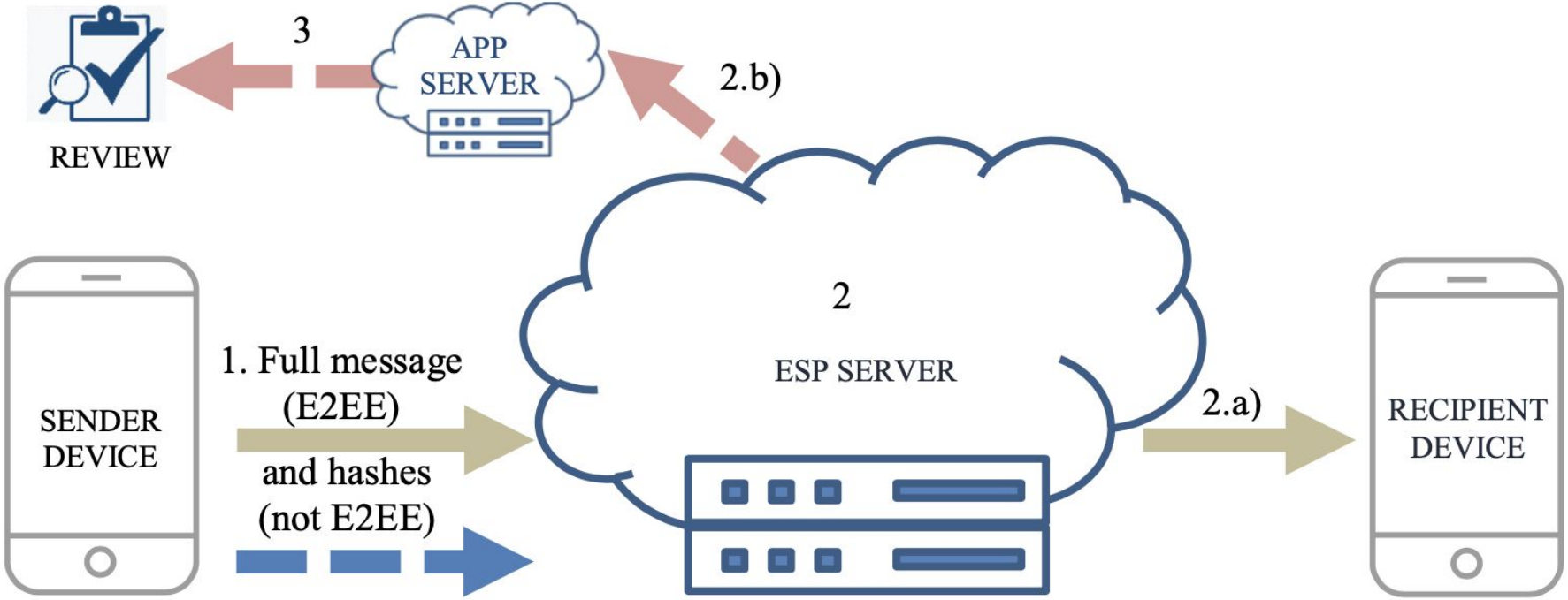
Encryption is bad

- Clipper chip 1993-1996
  - Encrypt stuff, but with backdoor
- UK 2017
  - Forbid E2E encryption
- EU 2020
  - Backdoor in chats
- The interest has never really died

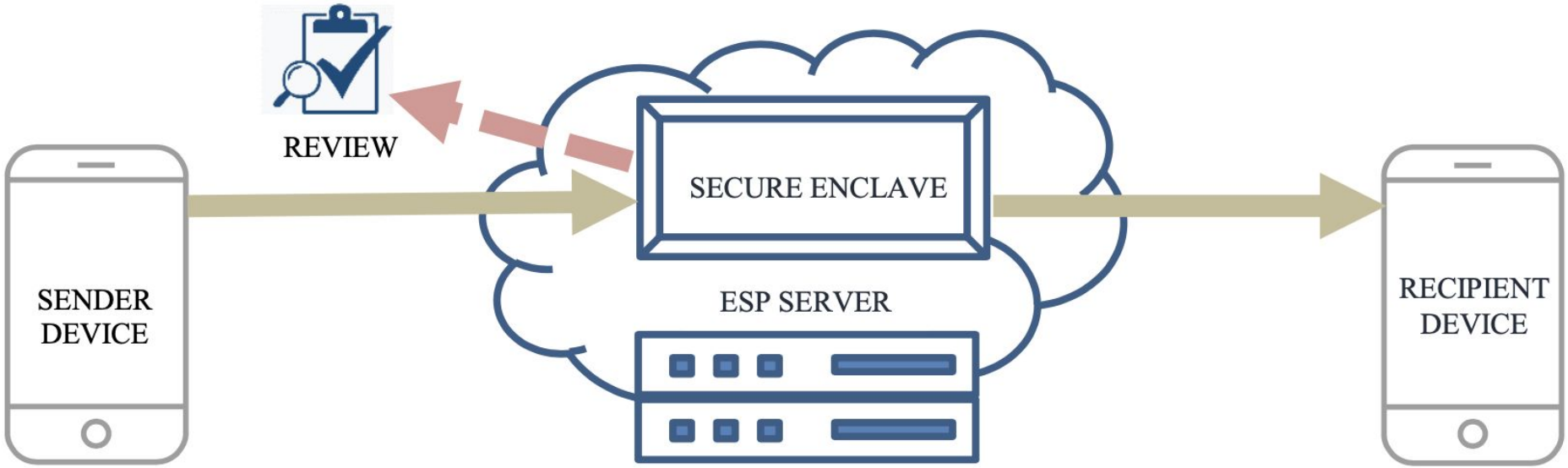
What do people believe?

- One can have encrypted connections
  - While allowing law enforcement access unencrypted data
- We can limit who can access unencrypted information
  - As if we do not see breaches every week
- We can allow law enforcement access unencrypted information
  - Without having a backdoor
- By sending encrypted messages and hashes we keep secrets
  - Without understanding what hashes discloses
- Criminals do follow legislation
  - All clients will do whatever legislation require clients to do

Example


3
APP SERVER
2.b)
REVIEW
2
ESP SERVER
SENDER DEVICE
1. Full message (E2EE)
and hashes (not E2EE)
2.a)
RECIPIENT DEVICE

Example


REVIEW
SECURE ENCLAVE
ESP SERVER
SENDER DEVICE
RECIPIENT DEVICE

European Commission Guiding principles

An **optimal solution** to the problem is one that would **allow users to enjoy the benefits of encryption** with regards to privacy and data protection **while allowing law enforcement agencies to preserve their capability to lawfully intercept** communications or **gain lawful access to encrypted devices and encrypted data** when this is warranted by a judge, prosecutor, or similar empowered official.

On the stage: Encrochat

- EncroChat handsets emerged in 2016
- EncroChat, an OTR-based messaging app which routed conversations through a central server based in France (and other apps)
- The NCA, the National Gendarmerie and Dutch police collaboration
- National Gendarmerie injected a malware that allowed them to read messages before they were sent and record lock screen passwords
- Data was distributed to other European partners, including the UK, Sweden and Norway
- Technology could "identify and locate offenders by analysing millions of messages and hundreds of thousands of images"

Are we stuck?

- Law enforcement can not have discussions in public
- Civil society and technical community must have discussions in public
- Many arguments are round square in a square hole
- The best way out, but have yet to see in the real world, might be if law enforcement accept that they can't snoop while technical community and civil society come with constructive suggestions on *what to do*
- And if you think internet communication is what we talk about, think about on **all** kinds of traffic, including person-carried medical device readings.