TEU00311
What is the Internet doing to me? (witidtm)

Stephen Farrell
stephen.farrell@cs.tcd.ie

https://github.com/sftcd/witidtm
https://down.dsg.cs.tcd.ie/witidtm

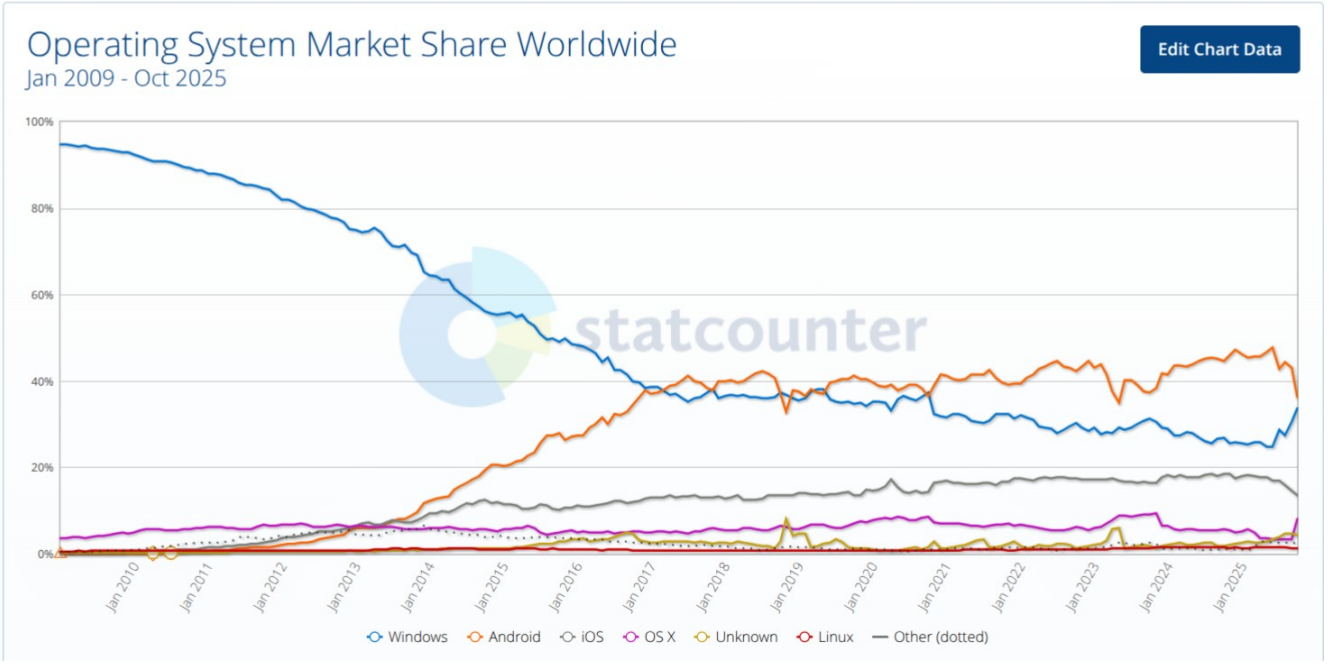
URLs accessed 20251014

Computers, Operating Systems and some example risks

Overall landscape

- Desktops, laptops, tablets, phones, “smart” speakers, home routers, raspberry-Pis, “fitness” devices…are all computers running some operating system
- Differently popular, open, reliable, invasive and general purpose or not
- Your choices should not only be driven by money and ease-of-use, though those factors tend to dominate

Operating Systems Market Shares



Graph: since 2009

Android
Windoze
iOS
OS X
Chrome-OS
...
Desktop Linuxes
e.g Ubuntu

https://gs.statcounter.com/os-market-share#monthly-200901-202510

Linux (laptop/desktop) now approx 3.7%, Chrome-OS 1.5%

Machine/OS issues to consider (1)

- Price, ease of use, updates/support, backup
  - Insurance? Meh;-(
- Security: probability of attack, probability of success, cost (impact) of successful attack
  - Probability of attack relates to market share
- Privacy: hiding in crowds vs. standing out by being more privacy-aware
  - Tension vs. Probability of attack?
- Having backups is your #1 protection – if you do nothing else set that up!
  - But only valuable if you sometimes test restore!
- Automated updates should be considered mandatory, or else you'll eventually suffer
  - Consider how well update system works, some OSes take ages to update
  - Some devices (still!) get no updates – avoid!

Machine/OS issues to consider (2)

- Openness – to what extent can someone find out what's going on under the hood?
- Even if you can't/don't do that, whether or not others can makes a difference
- It's a big world and many of the tech issues you face will have been overcome by someone else sometime
  - And likely being nerdy, they won't have been able to resist telling the world how they fixed stuff:-)
- But: "open" tends to be correlated with "hard to use" or "for nerds"

Machine/OS issues to consider (3)

- To be fair, there are also some benefits in a more complete but closed ecosystem, like Apple's
  - https://help.apple.com/pdf/security/en_GB/apple-platform-security-guide-b.pdf
  - Note: the above document is written for someone like me, it may be a tough read;-) But it is very thorough – Dec 2024 version is 250 pages
- Apple's "Personal Safety User Guide" (2025) may be more relevant for you:
  - https://help.apple.com/pdf/personal-safety/en_GB/personal-safety-user-guide-en_GB.pdf
  - That's only 142 pages:-)
- Interesting to compare/contrast today's "major" OSes – Windows, Android, Apple with what the FOSS movement would like
  - FOSS: https://en.wikipedia.org/wiki/Free_and_open-source_software

End of Life

- Devices do not last forever – batteries have a limited number of charge cycles
- When (when, not if!) a device fails or is lost/stolen, what will you lose?
  - See “backup” point earlier
- When (when, not if!) a vendor turns off support, or a service (e.g. OS updates, some photo-sharing feature), what will happen to your stuff?
- When you’re done with the hardware, what do you do?
  - “Two-thirds of used disc drives on Craigslist and eBay contain sensitive data” is a 2016 article, no reason to expect that’ll change v. soon

    https://www.itpro.co.uk/security/26814/two-thirds-of-used-disc-drives-on-craigslist-and-ebay-contain-sensitive-data

Device-based tracking/surveillance

- Anything with “location services” can be unexpectedly dodgy
  - **Image metadata inside the image file can include location**
  - “Fitness” trackers
- Cell-tower history within mobile operators
- List of Wi-Fi networks to which you’ve attached sometime
- **Bluetooth Tracking**
- “Smart” speakers
- “Security” cameras
- Telemetry from applications or OS
- Software update!
  - But didn’t we want that? Yes. But can’t it help tracking? Yes. Hmm...

MAC Addresses

- Device-tracking often (ab)uses **long-term hard-coded identifiers** such as MAC addresses (or IMEI/IMSI in mobile n/w)
- MAC address: link layer address (mostly) hardcoded to radio or other network chip
  - Same form of address used in WiFi and most other network protocols at link layer, e.g. Bluetooth
  - Roughly: how two devices on the same local area network (LAN) identify one another
- Looks like “6C:9C:ED:87:27:60” (48 bits) - 1st half is manufacturer ID (Cisco), 2nd half device-ID (a WiFi router that is/was in TCD SCSS)
  - You can look up manuf IDs from the registry, e.g. https://www.macvendorlookup.com/ accessed 20250916
- MAC address is often fixed for the lifetime of the device; There is now a 64-bit version, not sure how widely used yet
  - You can probably see these in your “about device” tab or similar

Randomised MACs

- MAC address randomisation is a good idea and now fairly well deployed
  - Often, the MAC address only really needs to be stable for a session, so can be randomised
  - But – if you paid for the hotel WiFi that might be based on your MAC address, or an enterprise network might use MAC addresses to decide which machines are allowed on the local network, or the machine may be a switch/router/server where changing MAC address would break stuff or be inefficient
- So you can’t always randomise, and doing so well needs higher-layer controls
- HOWTO turn on varies by OS and version
- On an android 10 phone I used have:
  - Developer options/Enhanced Wi-Fi MAC randomisation
  - You may need to turn on developer options first (search for HOWTO)

Bluetooth

- Early BT devices regularly broadcast their MAC addresses
- Later BT specs try to fix this, allowing support for randomised MAC addresses
- All good so? Nope!
  - Even if MAC addresses and payload identifiers change randomly, doing so out of sync enables tracking, sometimes indefinitely (read paper, and see next slide)
  - Becker, J., Li, D., & Starobinski, D. (2019). “Tracking Anonymized Bluetooth Devices,” Proceedings on Privacy Enhancing Technologies, 2019(3), 50-65. doi: https://doi.org/10.2478/popets-2019-0036
- Generalising: identifier correlation over time, devices and networks, is a very hard problem to mitigate – similar issues with DHCP leases, IP and email addresses, account names and web artefacts (cookies etc.)

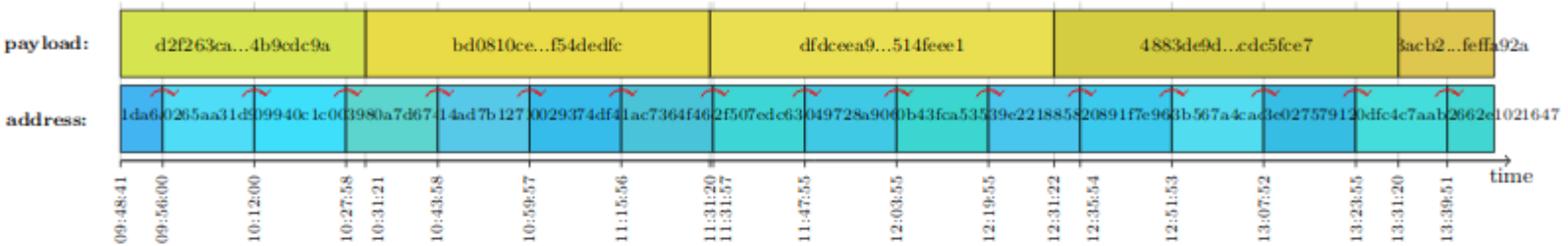


Fig. 9. An experiment illustrating the carry-over effect on Windows 10 devices. Asynchronous value changes allow updating the device identity whenever it changes.

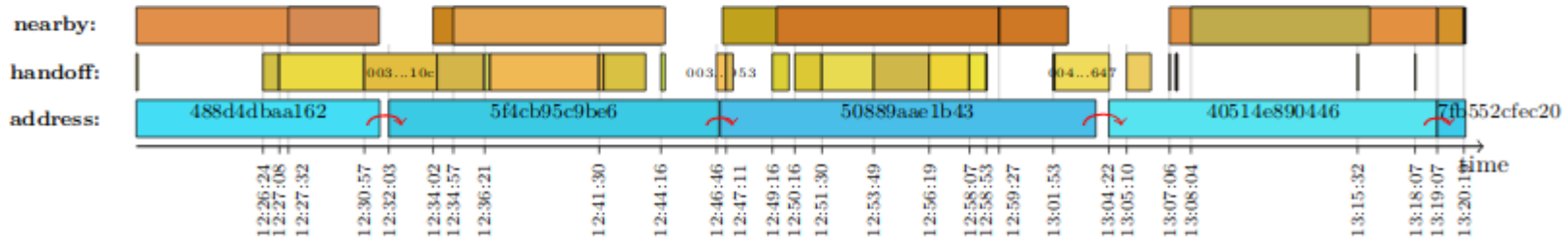
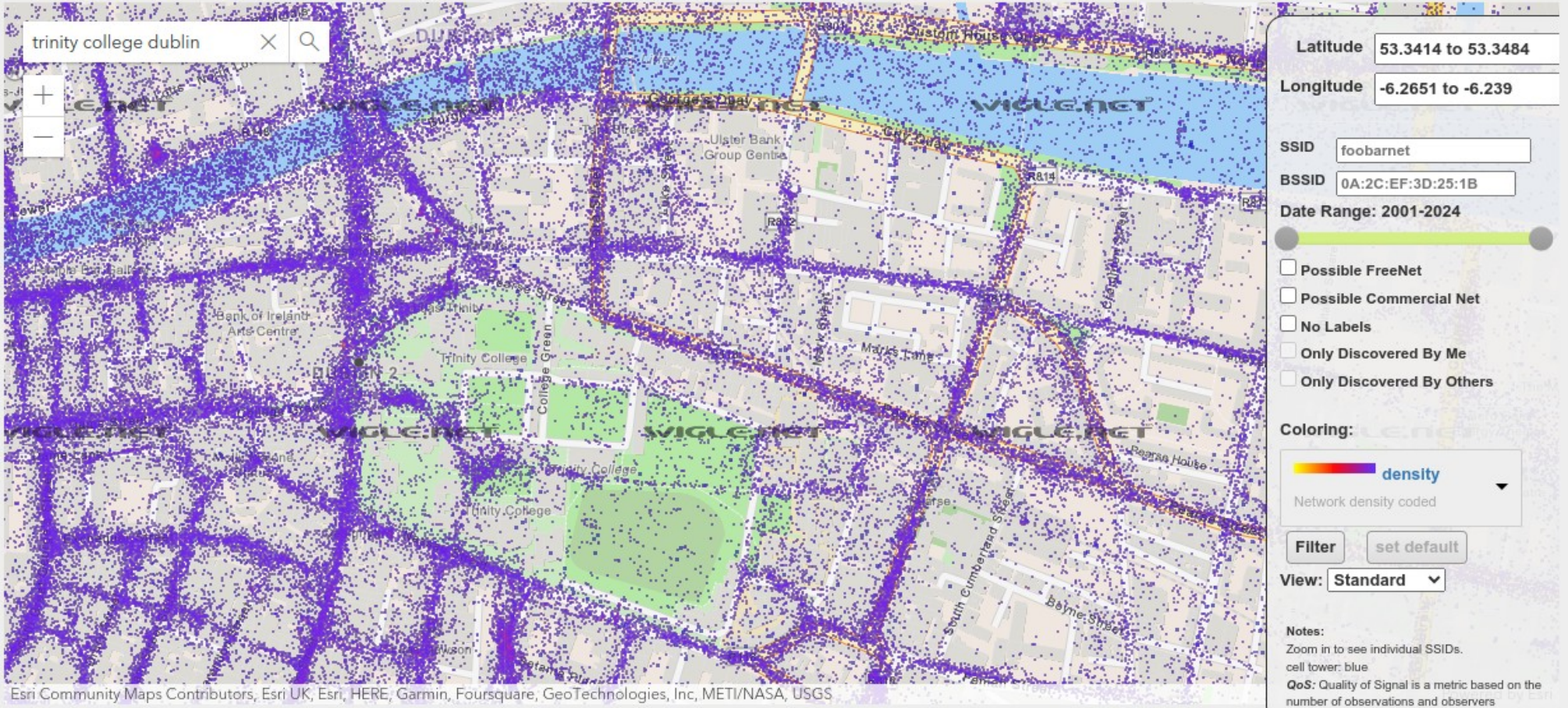


Fig. 10. This timeline shows address-carryover across 5 random addresses on iOS. The first three hops occur via the handoff identifying token, the last one occurs via the nearby token. Different colors denote different values.

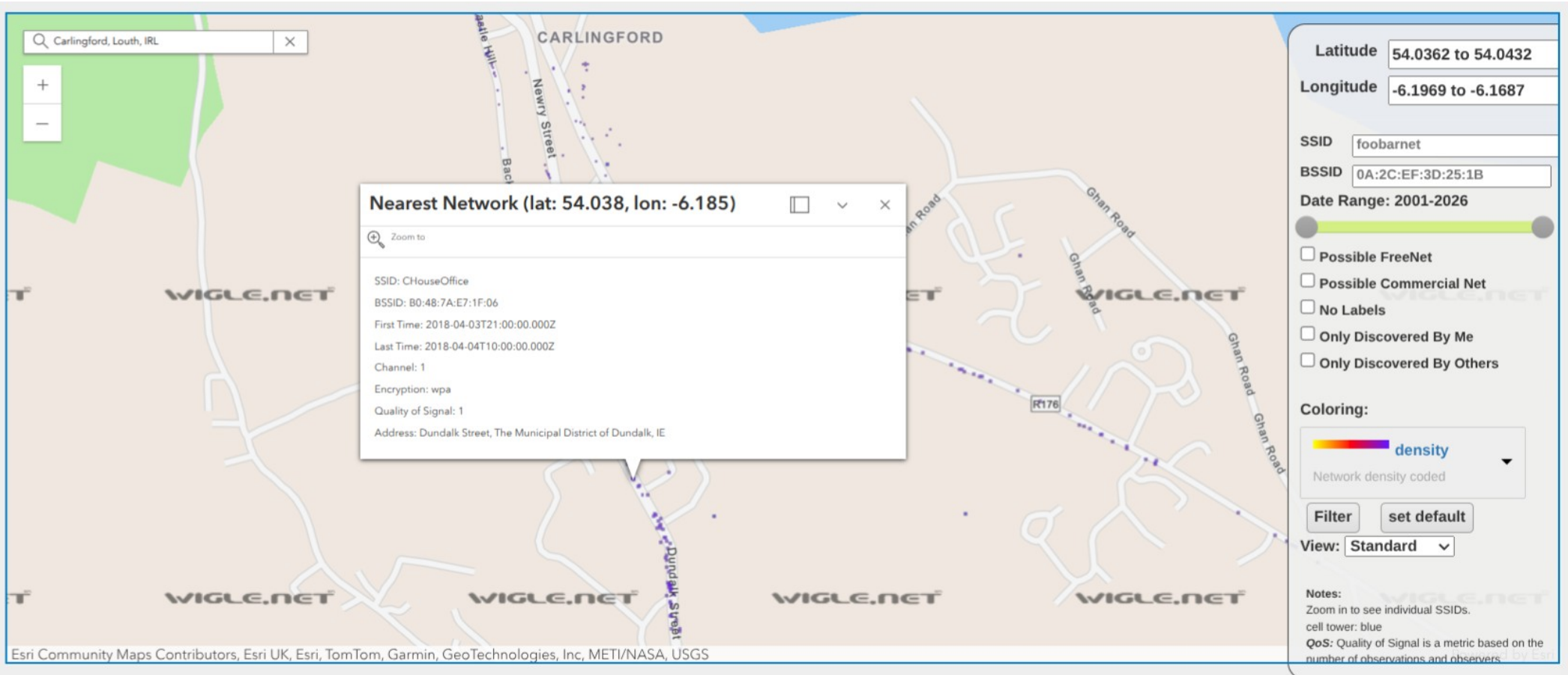
Interesting MAC Address Leak

- Sep 2023 DefCon talk:
  - https://www.youtube.com/watch?v=cO1JSzAdPM8
- Top half of Bluetooth Low Energy (BLE) MAC address in beacons is often the manufacturer ID (OUI)
- Not many manufacturers make e.g. tasers, stun guns or holsters for police guns
- Manufacturers do Bluetooth-enable those, e.g. to log extraction of gun from holster, to trigger body-cam recording if taser fired
- If you see BLE beacons for those OUIs, then chances are someone using those devices is nearby
- Wardriving databases (e.g. https://wigle.net/) contain historic geo-located scans
- The same issues may arise for other BLE enabled things you carry!

wigle.net


trinity college dublin
Latitude 53.3414 to 53.3484
Longitude -6.2651 to -6.239
SSID foobarnet
BSSID 0A:2C:EF:3D:25:1B
Date Range: 2001-2024
Possible FreeNet
Possible Commercial Net
No Labels
Only Discovered By Me
Only Discovered By Others
Coloring:
density
Network density coded
Filter
set default
View: Standard
Notes:
Zoom in to see individual SSIDs.
cell tower: blue
QoS: Quality of Signal is a metric based on the number of observations and observers
Esri Community Maps Contributors, Esri UK, Esri, HERE, Garmin, Foursquare, GeoTechnologies, Inc, METI/NASA, USGS

Wiggle.net/Carlingford Co. Louth



Unwanted Trackers

- Apple AirTags and similar BLE-based systems have been abused to track e.g. intimate partners
- How they work (briefly):
  - Tag emits BLE beacon with encrypted ID
  - Nearby participating devices encrypt their location “with” BLE beacon and send to service provider
  - When device “lost” query service provider for records encrypted for your device to get location(s)
  - A good crypto scheme for this can be derived so service provider doesn’t learn too much
- Unwanted tracker detection: When device is “lost” and seen frequently by one other device (the one possibly being tracked), device may be “uncloaked” e.g. by causing it to emit sound
- The companies involved are currently trying to standarise ways in which such unwanted tracking could be detected
  - https://datatracker.ietf.org/wg/dult/about/
  - https://github.com/bdetwiler/draft-detecting-unwanted-location-trackers/
  - A proposal that group considered: https://eprint.iacr.org/2023/1332.pdf - has a nice description of the problem and proposal for those used to ready crypographic specifications
- What do we think about that?

Malicious Software (Malware)

- Malware on your devices could:
  - Exfiltrate your data (keyboard sniffers, ID theft, “wallet” attacks, mobile app “SDKs”)
  - Work for someone else (cryptominers, clickfraud/adware)
  - Be part of a botnet (DDoS)
  - Encrypt your files (ransomware)
  - (Sometimes) survive factory-reset (though less commonly)
- Technical types: viruses, worms, trojans, ...
  - We’re less concerned here with how malware works or details of how to detect/prevent malware doing bad things
  - More interesting is: How can you avoid or recover?
- Note that anti-malware tools (e.g. anti-virus) can look similar to malware - they both want access the “innards” of the OS/network-interactions – that can make such tools attractive as a target

How malware may arrive...

- Pre-installed (accidentally or deliberately, bloatware/crapware)
- Supply chain attacks (e.g., buy a popular npm library, infect that, or generate a new library with a typosquatted name)
- Appear to be an application or browser extension that someone may want (e.g., phone torch app)
- Mail attachment (pdf, zip, tar, ...) in spam or spear-phish – be careful of how email addresses and file names are displayed in your mail user agent!
- Drive-by exploitation via web-site/browser vulnerability
- Fake QR code leading to site encouraging download/install
- USB stick (watering hole attack)
- USB charger (how much do you trust Dublin Bus? :-)

Actors in the “AppStore” model

- The interested parties include the OS vendors, device manufacturers, mobile network operators, app developers and the services those apps use/enable
  - Your interests likely come last in that list, despite what most of the others may say, and even if they really mean what they say!
  - Their interests won’t always be aligned either (e.g. mobile network operator vs. over-the-top service provider)
  - And there are non-stupid bad actors in the game, esp. in the app developer and services-those-use/enable cohorts
- So what do you think are their interests?
  - OS makers: Google (android), Apple (IOS), Canonical (Ubuntu)
  - Device manufacturers: Samsung, Apple, Huawei, Sony, …
  - Mobile network operators: China Mobile, … Vodafone, … Telefonica, … Eir, Three
  - App developers: Google, Apple, device makers plus many others I’ve never heard of
  - Service providers: Google, Facebook, Twitter, … Netflix, Sky, ...

“AppStore” Permissions model

- Both iOS and android “app” install processes use a “permissions” model, windoze, chromebooks and MAC OS are heading that way more
  - As is Ubuntu, but only sort-of, it being a much more open OS
- Android used (before 2015) present “permissions needed” only at install time, now both it and iOS pop up permission requests when the app first tries to make use of something “sensitive”
  - But are those permission classes really meaningful? And do they protect you? TBH: I find it hard to tell
- Research in this space also seems less concentrated on how well all this protects users and more on how “well accepted” it is by users, e.g.:
  - Reinfelder, Lena, et al. "An Inquiry into Perception and Usage of Smartphone Permission Models." International Conference on Trust and Privacy in Digital Business. Springer, Cham, 2018.
    - zzhttps://www.researchgate.net/profile/Lena_Reinfelder/publication/326630389_An_Inquiry_into_Perception_and_Usage_of_Smartphone_Permission_Models_15th_International_Conference_TrustBus_2018_Regensburg_Germany_September_5-6_2018_Proceedings/links/5c0e58564585157ac1b73e03/An-Inquiry-into-Perception-and-Usage-of-Smartphone-Permission-Models-15th-International-Conference-TrustBus-2018-Regensburg-Germany-September-5-6-2018-Proceedings.pdf
  - Rajivan, Prashanth, and Jean Camp. "Influence of privacy attitude and privacy cue framing on android app choices." Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016). 2016.
    - https://www.usenix.org/system/files/conference/soups2016/wpi16_paper-rajivan.pdf
  - Could be I didn’t spend enough time looking though (I did look around in 2019 but didn’t repeat since:-)

Some ISPs also track

- US Federal Trade Commission Oct 2021 report
  - https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf
- Major US ISPs sneakily “sharing” info about their customers
- Not that surprising

What do I use?

- Main devices:
  - Home router: OpenWRT (Turris Omnia)
  - Laptop: Ubuntu (Framework 13)
  - Phone: Murena teracube 2e de-Googled Android
  - A cardboard box: with a pile of old phones and laptop hard-drives:-)
- The above is not a recommendation for you, just what I use
- Various others @ home and for work, mostly Ubuntu servers on hosted virtual machines (VMs), some real (“bare-metal”) servers and some old laptops
- Other people on my home network use android, iphone, mac, (currently no windoze)
- Main living room laptop also runs Ubuntu and is entirely usable for non-nerds

If you wanna try Ubuntu...

- Ideally try with old laptop
  - Drivers for newer models can take a while to catch up with proprietary versions, esp for WiFi
- You can try before installing to hard drive by running from a “live” USB stick
- You can make system dual-boot if you wanna try some more but still keep your earlier OS

What do you use?

What would you like to use?

What do you dislike that you use?