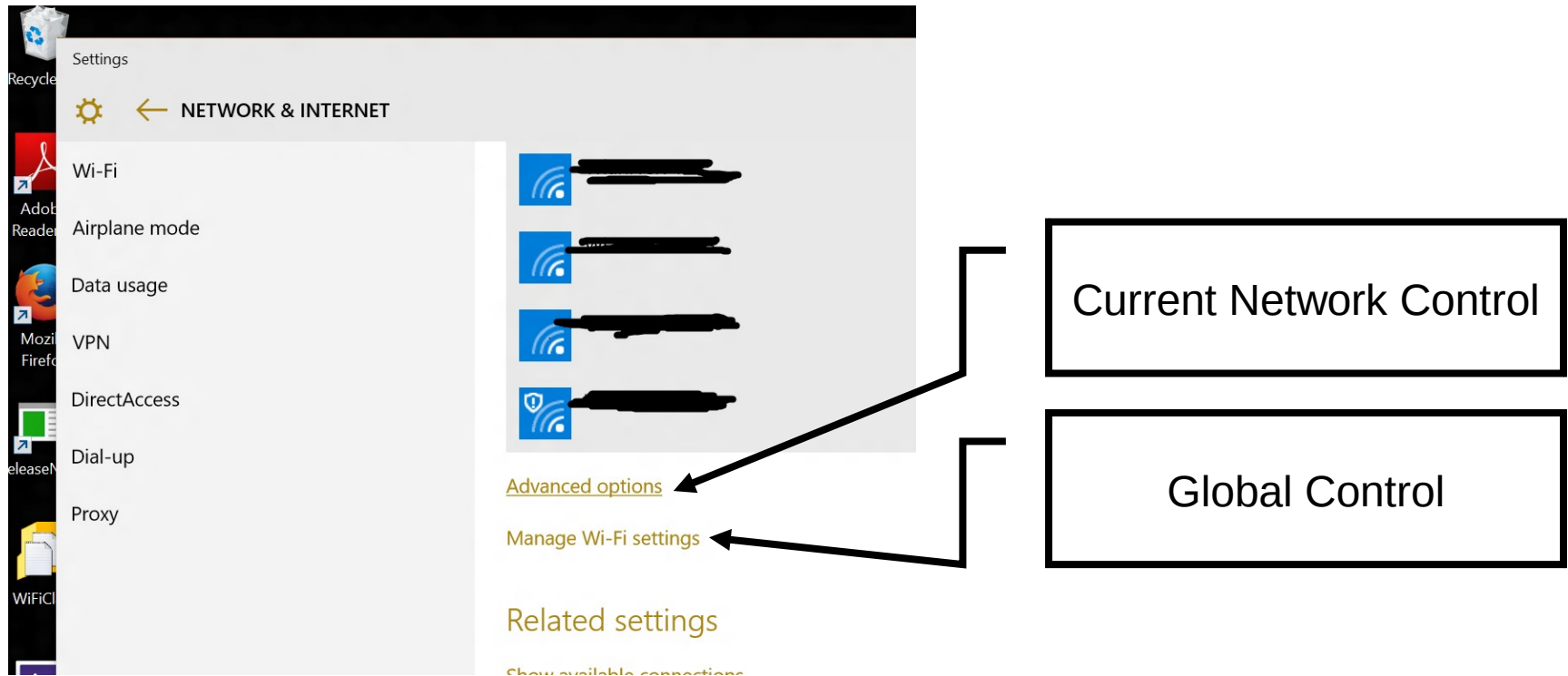# Experience with MAC Address Randomization in Windows 10

Christian Huitema
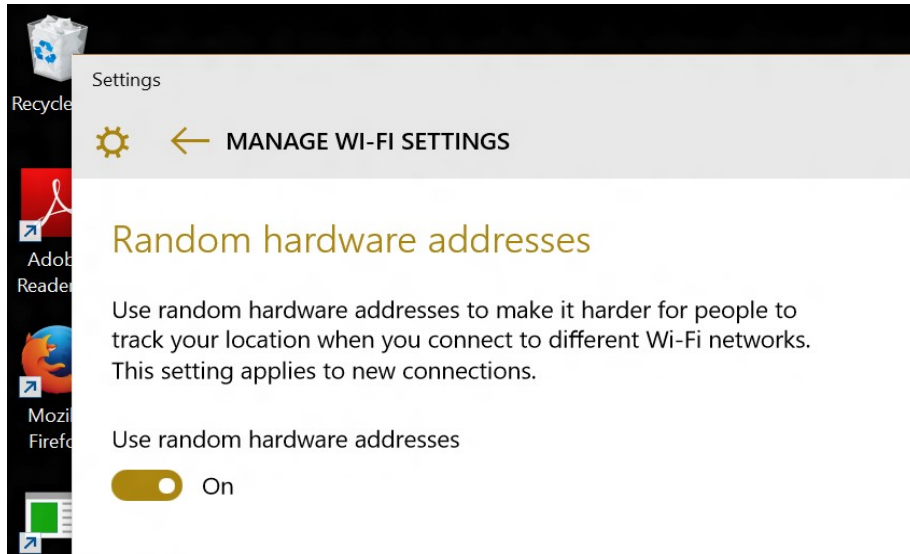
Huitema@microsoft.com

IETF 93, Prague, July 2015

# MAC Address Randomization controlled from Windows 10 Wi-Fi UI

Current Network Control

Global Control

MAC Randomization in WIndows 10 - IETF 93

Global Control for MAC Address Randomization in Windows 10

Settings

⚙ ← **MANAGE WI-FI SETTINGS**

Random hardware addresses

Use random hardware addresses to make it harder for people to track your location when you connect to different Wi-Fi networks. This setting applies to new connections.

Use random hardware addresses

⬤ On

- Only present if the hardware is recent and supports randomization.

- Applies to "roaming" between network:
  - If on, Wi-Fi probes will be sent from a random MAC Address.
- Applies to new connections:
  - MAC address: Hash(Secret, SSID, connection ID)
  - By default, same address for all connections to same SSID.
  - Different connection ID if the network is "forgotten", then re-connected.
- Does not change the state of existing connections
  - Office, Home

Per Network MAC Randomization Setting in Windows 10
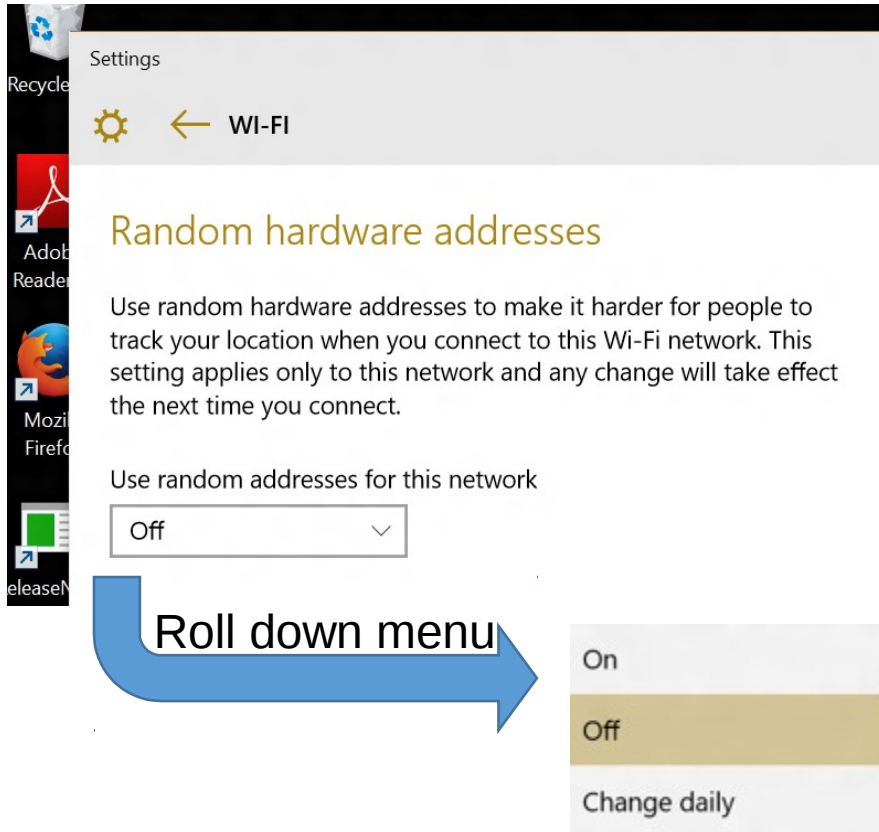
- Applies to currently connected network

- Three Options:
  - Off : use HW MAC
  - On : use fixed Random MAC
  - Change Daily: pick a new Random MAC every day

MAC Address Randomization FAQ

Why not ON by default?	There are known cases where it breaks (see next slide). We want to get more telemetry first, to know how bad it really is out there.
What about enterprises?	Can use scripts to install Wi-Fi profile with randomization OFF.
What about MAC Address filtering?	Turn randomization OFF, connect, then turn randomization ON again. System will remember your network.
What kind of MAC address?	U=1, G=0, plus 46 random bits. Using Crypto API to make sure the bits are "really" random.
Will I pay twice for Wi-Fi at the hotel?	No. We pick a random MAC "per SSID" by default, so the hotel sees just one device.
What about the Windows Phone?	Supported on the phone as well, same algorithms. The UI is a bit different, to fit on the phone.
Is that enough to be anonymous?	Of course not. DHCP, DNS, web Cookies… But it prevents the "obvious" wireless tracking, and it enables progress.

Personal Experience

- Self Hosting for the past 6 months (including IETF 92, Dallas)
- Only observed a single case of Hot Spot refusing connection
    - Mall in Bellevue, WA. Not clear why.
- Observed two funny interactions in "Change Daily" mode
    - Got asked every day to "Accept the terms and conditions" by captive portal
    - Filled up the internal table of a Home Wi-Fi router
        - DHCP leases were larger than one day, several MAC/IP for the same name,
        - router's DNS server got very confused.
- Overall, works great