(Geo)Location, Location, Location

Matt Blaze
University of Pennsylvania

“Mobile Devices”

- Computers, but
  - you carry them with you
  - they have lots of sensors (GPS, etc)
  - they transmit (cell, wifi, bluetooth, etc)
  - they rely on services for almost everything
- Dumb phones, smartphones, tablets, “things”

How cellphones work (oversimplified edition)

- Handset is low power 2-way radio with a crappy antenna; you want it to work everywhere
  - max range is a mile or so, depending on terrain
- Cell carrier has overlapping network of towers ("cell sites") across service area so that you're usually in range of at least one
  - handset periodically looks for the cell site with the strongest signal (*usually* nearest) and "registers" with it

But wait...

- Cell company wants to economize on towers, build them as far apart as it can get away with to cover service area
  - should be one or two miles apart, right?
- But radio range isn't the limiting factor
  - high demand
  - limited spectrum
- So cell sites now must be much closer together than radio range would require
  - especially in urban areas
  - some cell sites serve individual floors of buildings

Radios in your phone

- Cellular voice and data (EDGE/3G/4G/LTE)
  - announces self to carrier infrastructure
- WiFi
  - announces self to nearby hotspots
- Bluetooth
  - announces self to other nearby devices
- GPS
  - receiver only, unless carrier asks (E911)

What does your phone know about where it is?

- What cell tower is it registered with
  - accuracy depends on density
- GPS calculation
  - ~3M accuracy
- What WiFi hotspots are nearby?
- Combination of some/all of the above
  - surprisingly accurate

What others learn about where you are

- Cell company learns the cell sites you register with during the day
  - *even when you don't make a call*
- WiFi and BT constantly announce MAC addr to anyone in range
  - address is usually unique & constant for lifetime of handset
- WiFi location reveals loc to platform provider (Google, Apple)
  - often linked to a user account or unique handset ID
- Of course, IP addr is revealed to anyone you talk to on 'net
  - can correlate w/ your location
- Apps leak god-knows-what to app provider, including location

What about the Government?

- Intelligence vs Law Enforcement
- Wholesale vs Targeted
- Realtime vs Prospective vs Retrospective
- Call Metadata vs Geolocation vs Content
- Unilateral vs carrier cooperation
- Curiosity vs Subpoena vs Warrant

Intelligence Agencies (NSA, etc)

Snowden tells us something here

- “215” Program
  - ALL call detail records from US telcos, delivered daily
  - may or may not include location; no content
- Cable tapping program
  - includes content
  - mostly near intl cable landings, but some US traffic
- Handset malware “implants”
  - is your phone really “off”?
- Some leakage from NSA -> domestic law enforcement

Domestic US Law Enforcement

LE more constrained

- Limited budgets, need evidence for court
  - But they do get some data from intel (DEA "Hemispheres")
- Mostly use smaller-scale techniques
  - Call Detail Records
  - Pen Register / Trap & Trace
  - Content Wiretaps
  - E911 "pings"
  - Tower Dumps
  - "StingRay" IMSI intercept devices
  - Compromised target handsets

Target-based LE Techniques

Call Detail Records

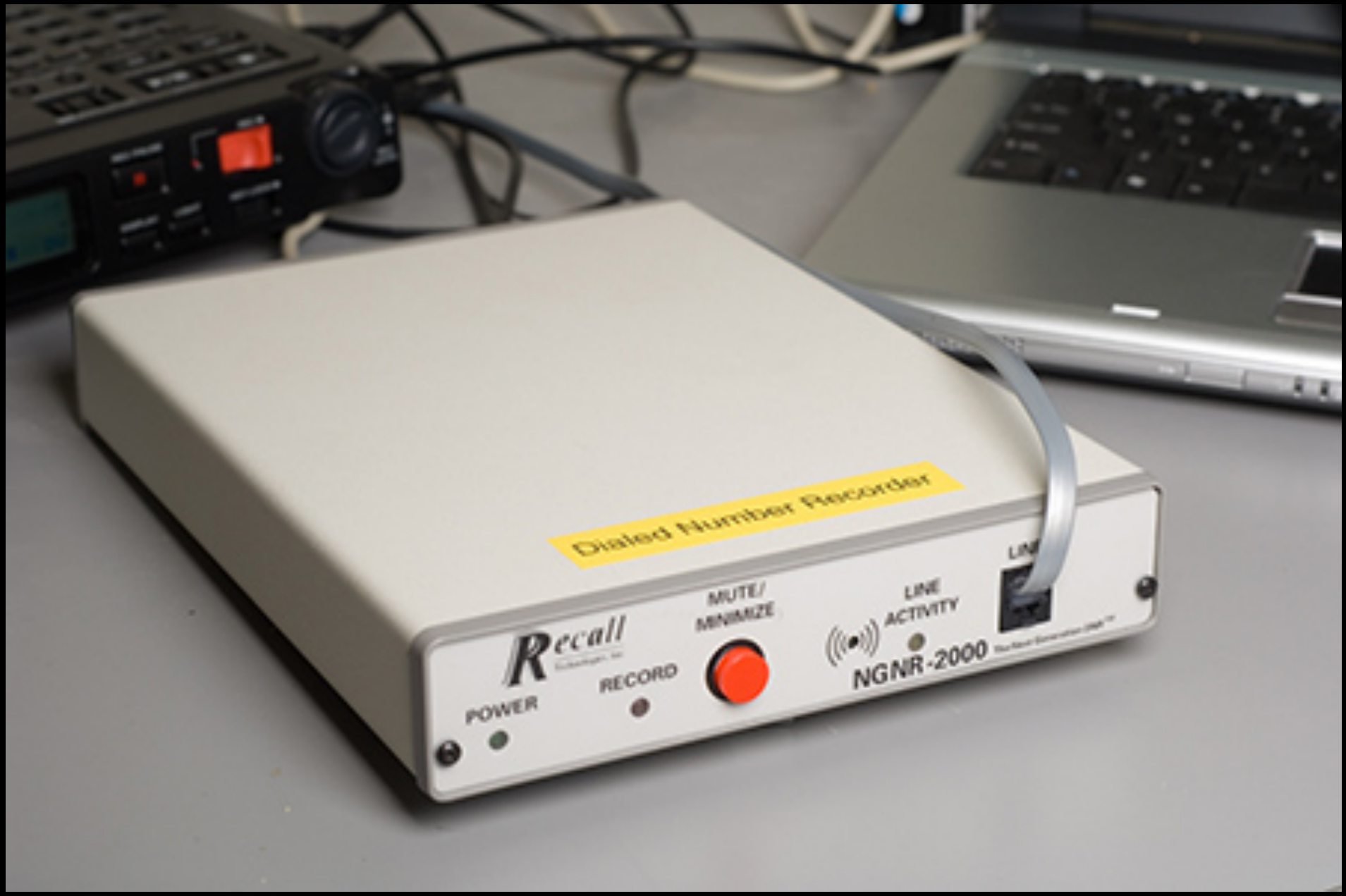
- Every time you make/receive a voice call or initiate a data connection, the carrier creates a "call detail record" (CDR)
  - "billing record", even if not itemized on bill
- Time, number called, duration, cell site ID
  - location accuracy depends on cell density
  - records at start & sometimes end of call
- CDRs maintainted for a while (18 month min)

LE use of CDRs

- LE agency can request a target's CDRs over some period
  - Requires "relevance" to investigation
- May or may not include cell site location
  - unsettled law, different practices by different agencies, courts and carriers
- Location accuracy depends on cell density
  - can be large or small radius (microcells)
- Generally limited to call records, not everything telco has
- Retrospective (you can be targeted after the fact)

Pen Register / Trap & Trace

- Like a CDR request, but prospective
- Real time delivery of target's call metadata going forward
- Similar (low) legal standard as CDR request
  - may or may not include location (unsettled)
- Uses standard CALEA interfaces
  - more expensive than CDR request


Dialed Number Recorder
Recall
POWER
RECORD
MUTE/
MINIMIZE
LINE
ACTIVITY
NGNR-2000

Content Wiretaps ("Title III")

- What we think of when we think of wiretap
- Standard CALEA interface can deliver call content (& SMSs) in real time to law enforcement
  - provisioned by carrier
- Includes cell site location
- High legal standard to get ("Title III")
  - probable cause + other techniques would fail
- Expensive, requires real time monitoring

E911 “pings”

- FCC E911 mandate for high-accuracy phone location capability for 911 callers
- Uses handset GPS, tower triangulation, etc
- Can be triggered by carrier, too
  - no 911 call actually required
  - sometimes at law enforcement request

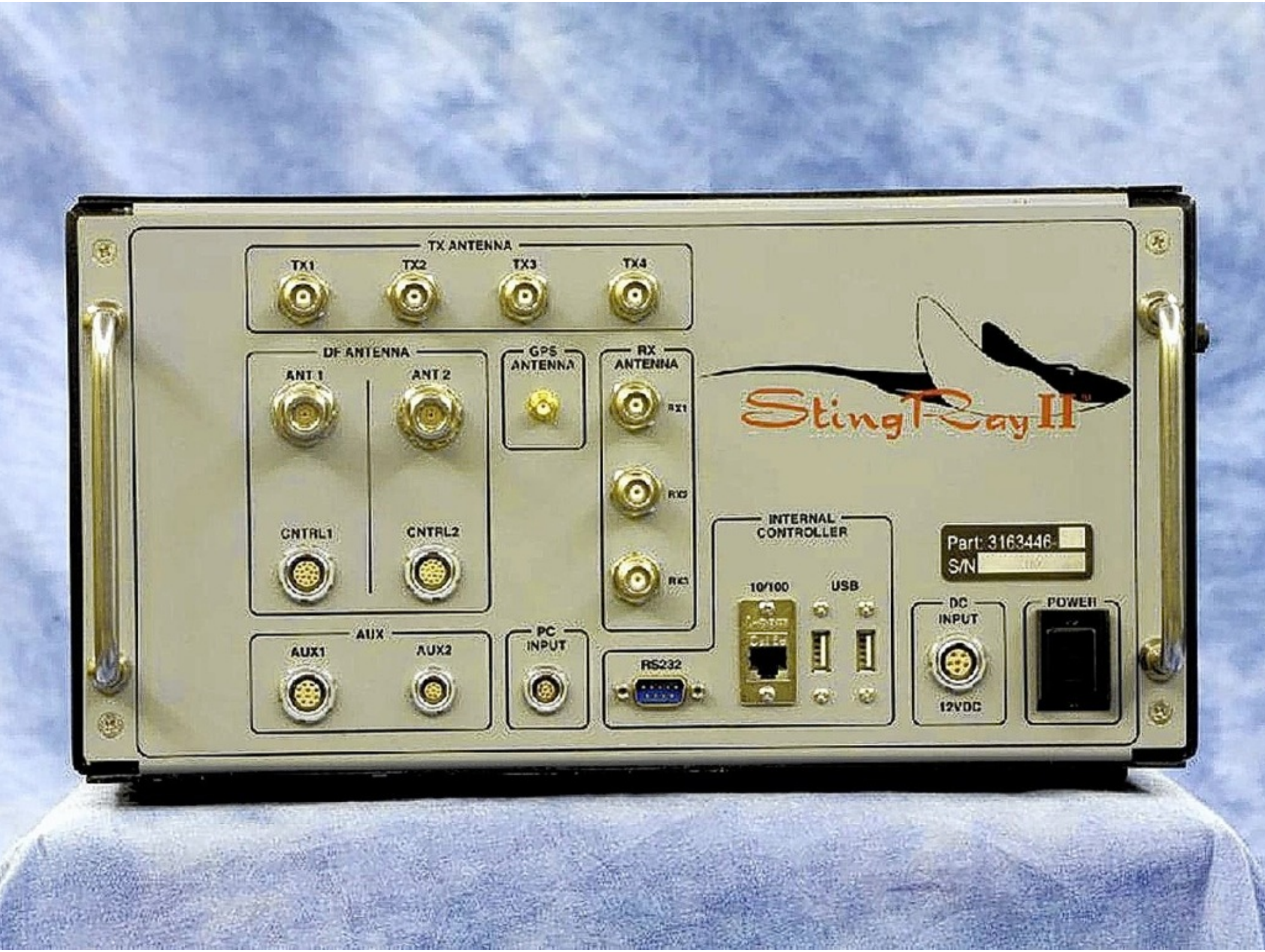
Location-based LE techniques

“Tower Dumps”

- Standard carrier service to LE that we know about thanks to 2011 ACLU public records request
  - not widely known, even by some LE agencies
- LE can request list of all handsets/subscriber accounts that registered with a particular cell site during a particular interval
  - inherently un-targeted, except by location
- Unsettled legal standard, varies by jurisdiction

“StingRays” / “IMSI catchers”

- Portable device that pretends to be a cell site
  - registers all phones in an area, then drops out
  - used early in investigation to ID target phone
- Usually no backhaul (so no content collection)
- Marketed to LE by Harris (older version is “TriggerFish”)
  - mostly federal, but also state & local
- Can be handheld with directional antenna
  - but typically used in a car (bulky & obvious)
- Unclear what the legal standard is


TX ANTENNA
TX1
TX2
TX3
TX4
DF ANTENNA
ANT 1
ANT 2
CNTRL1
CNTRL2
GPS ANTENNA
RX ANTENNA
RX1
RX2
RX3
AUX
AUX1
AUX2
PC INPUT
RS232
INTERNAL CONTROLLER
10/100
USB
Part: 3163446
S/N
DC INPUT
12VDC
POWER
StingRay II

Intel -> LE
"trickle down spying"

- Moore's law applies to spying
  - what NSA uses today, the Tucson PD will have tomorrow
  - StingRays will get smaller and cheaper
  - Data collection and analysis gets cheaper
  - Handset malware implants will spread
- DEA *Hemispheres*
  - AT&T gave DEA unfettered access to CDRs
  - new phrase: "parallel construction"

Countermeasures

The Metadata is the Message

- We have great technology for protecting *content* (crypto)
- We have less great technology for protecting metadata
  - This is a great area to be doing research and building tools

What about Tor?

- Tor is great
  - prevents observer from learning who you're communicating with
- But:
  - Doesn't work for regular voice calls
  - Doesn't prevent your carrier from learning & logging your access point

Learning from *The Wire*

- Burner phones!
  - anonymous account (cash?)
  - changed frequently
  - avoid linking to your old network (hard!)
- Changing phone changes your ID
  - but change MAC address, too