Attachment C - RF-Enabled Privacy & Security Risks

Documented wireless threats relevant to increasingly RF-dependent environments

ET Docket No. 13-84 | Supplemental material supporting public comment

Scope: This appendix addresses privacy and cybersecurity, not biological RF effects. These issues may be outside the narrow health remand and are presented as technological-development concerns the FCC could address here where appropriate or in a separate proceeding.

Why the distinction matters

Radiofrequency energy does not itself collect personal information. Privacy risk arises when communications systems, protocols, identifiers and RF-enabled devices are abused to identify, track, intercept, impersonate or disrupt communications. Federal cybersecurity guidance documents several such threats.

Documented threat examples

Threat	Documented federal concern	Privacy / safety implication
Rogue cellular base stations / IMSI catchers	NIST describes unauthorized base stations that impersonate legitimate cellular infrastructure and can collect device/subscriber identifiers or exploit legacy-network weaknesses.	Can reveal that a particular device is present in an area; some attack paths may affect confidentiality or availability.
Wi-Fi rogue access points	NIST identifies rogue access points and man-in-the-middle risks on untrusted wireless networks.	Traffic interception, credential exposure or redirection can occur when a device connects to a malicious or impersonated network.
Wireless-device tracking	NIST identifies tracking risks associated with persistent identifiers such as Wi-Fi MAC addresses, while noting modern randomization mitigations.	Identifiers and probe behavior can potentially be used to correlate a device with physical presence.
Bluetooth / short-range threats	NIST catalogs pairing eavesdropping, unauthorized data access, denial-of-service and other Bluetooth threats.	Body-worn and nearby devices expand the number of RF interfaces requiring security controls.
Jamming and spoofing	FCC materials distinguish jamming (interference/blocking) from spoofing (replicating, replacing or modifying signals).	Malicious interference can disrupt authorized communications, positioning or connectivity; unauthorized jamming is generally prohibited.

Questions for future FCC review

- What minimum protections should prevent unauthorized device identification and persistent location tracking?
- How should networks and handsets detect or resist rogue base stations and downgrade attacks involving legacy protocols?
- What transparency should consumers receive about wireless identifiers, location-related metadata and retention?
- How should 5G/6G, direct-to-device satellite, connected-vehicle, wearable and IoT deployments incorporate security-by-design?

- What testing should evaluate resilience to spoofing, jamming and malicious interference while preserving lawful spectrum use?
- Could physical-layer identification techniques create additional privacy implications, and if so, what safeguards or research are warranted?

Careful conclusion

These are established categories of wireless-security risk, but their existence does not establish that a particular person or device is currently being targeted. The policy issue is whether an increasingly RF-dependent environment should be accompanied by stronger detection, authentication, privacy controls, transparency and resilience against misuse.

Sources and record references

1. NIST testimony: Assessment of IMSI Catcher Threats. Explains rogue base stations, IMSI collection, downgrade attacks and privacy implications. Source

2. NIST Mobile Threat Catalogue - Cellular. Catalogues air-interface eavesdropping, rogue-base-station tracking, downgrade attacks and other cellular threats. Source

3. NIST Mobile Threat Catalogue - LANs and PANs. Catalogues rogue Wi-Fi, tracking, eavesdropping and Bluetooth threats. Source

4. NIST Mobile Threat Catalogue - Client MAC Address Tracking. Explains physical tracking risk associated with persistent MAC addresses and mitigations. Source

5. FCC interagency advisory discussing jamming and spoofing. Defines examples of RF jamming and signal spoofing in a federal communications context. Source