Privacy and Surveillance Technology in Pocahontas County

Materials for the Pocahontas County Commission

Regular meeting, Tuesday, October 20, 2026 · Marlinton

Submitted by: Andrew McAfee, Board President, Safe Home LTD · PO Box 64, Green Bank, WV 24944 · 304-456-4011 · safehomenow@yahoo.com

What I am asking the Commission to do

Adopt the attached one-page resolution, or refer it to the Prosecuting Attorney for review and set a date to consider it.

What the resolution does, in brief

- No county funds, property, poles or contracts for license plate readers or similar surveillance networks without public notice, a hearing and a recorded vote.
- Safeguards for any system approved: a warrant for data access except in emergencies, no sale of data, deletion within 7 days, search logs and a yearly public report.
- A request that county offices, including the Sheriff's Office, report within 60 days what surveillance technology they use.
- Prescribed medical devices and residents' own closed home security systems are not affected.
- A request to our legislators to support a 2027 state law, with copies to the Governor and the House Committee on Government Organization.
- A simple way for residents to report wireless equipment installed in their homes without their consent. Any RF meter, or none, is enough to file, and residents may add free screening by a volunteer technician. The Clerk logs each complaint as a public record; the Commission forwards it to the Prosecuting Attorney and the Attorney General's Consumer Protection Division, and may arrange independent confirmation of the device's radio emissions and the data it collects, including at the Prosecuting Attorney's request. No spending is required.

In this packet

- Draft resolution (1 page)
- "How We Are Tracked Wirelessly": a cited inventory of the documented ways wireless devices collect personal data, with its own source list (5 pages)
- Sources for the facts cited on this cover page and in the resolution (1 page)
- "The Internet of Bodies Is Already Here": a cited handout on body-worn devices and how personal data is used and sold (5 pages)
- Wireless Device Complaint Form, the form a resident would file under item 7 of the resolution (2 pages)
- "What I bought: a doorbell." A one-page illustration of what a common home device can collect (1 page)

Every fact in these materials is linked to a government record, court decision, standards body or news report on the sources pages, so it can be checked independently. This is a citizen's proposal for the Commission's consideration, not legal advice.

POCAHONTAS COUNTY COMMISSION

RESOLUTION NO. 2026-____

A Resolution on Surveillance Technology and the Privacy of Pocahontas County Residents

WHEREAS, the County Commission has "superintendence and administration of the internal police and fiscal affairs" of the county under W. Va. Code §7-1-3, including the county's funds, property and contracts;

WHEREAS, automated license plate reader (ALPR) systems, such as those sold by Flock Safety, photograph every passing vehicle and record its plate, description, time and location in cloud databases that other agencies across the country can search;

WHEREAS, West Virginia has no statute regulating license plate readers or the data they collect, and the Legislature is examining the issue, with a House committee hearing set for November 9, 2026 and legislation expected in the 2027 regular session;

WHEREAS, in Monongalia County, a review of the Sheriff's Office's own audit records found that the county's camera data was included in more than 3 million searches by nearly 4,000 organizations, many outside West Virginia, in the first nine months of 2026;

WHEREAS, Pocahontas County is home to the Green Bank Observatory and lies within the National Radio Quiet Zone, and its residents have long valued a quiet, private way of life;

WHEREAS, residents may find wireless transmitting equipment installed in or on their homes without their informed consent, or equipment that transmits data about them without their knowledge, and the county has no procedure for receiving and referring such reports; and

WHEREAS, the Commission wishes to protect residents' privacy without interfering with prescribed medical devices or with residents' own security systems on their own property;

NOW, THEREFORE, BE IT RESOLVED by the Pocahontas County Commission that:

1. **County funds, property and contracts.** No county funds, county property, county-owned poles or county contracts shall be used for license plate readers or similar networked surveillance systems unless the Commission first gives public notice, holds a public hearing and approves the system by recorded vote.

2. **Required safeguards.** Any system the Commission approves must require a warrant for access to its data except in a documented emergency; prohibit the sale of the data; delete data within 7 days unless it is evidence in an active case; keep audit logs of every search; and be reported publicly once a year.

3. **Inventory.** The Commission requests that every county office, including the Sheriff's Office, report within 60 days any surveillance technology, vendor network access or data-sharing agreement it uses or has agreed to.

4. **What this does not cover.** This resolution does not apply to prescribed or implanted medical devices, or to closed security systems that residents own, operate and control on their own property.

5. **Request to the Legislature.** The Commission asks the members of the Legislature representing Pocahontas County to support 2027 legislation requiring a warrant to access license plate reader data, prohibiting the sale of that data, limiting retention, requiring audits and penalizing misuse.

6. **Copies.** The County Clerk shall send copies of this resolution to the Governor, the members of the Legislature representing Pocahontas County, and the House Committee on Government Organization.

7. **Complaints about wireless devices.** Residents may file written complaints with the County Clerk about wireless transmitting equipment installed in or on their property without their informed consent, or that transmits data about them. A resident may identify such equipment with any radio-frequency meter or detector, of any make or quality, or may file without any measurement, and no complaint shall be refused or delayed because of the type or quality of the instrument used. A resident may have the equipment screened by a person of the resident's choosing, including a volunteer technician, at no cost to the county, and may add the results to the complaint. The Clerk shall log each complaint as a public record. The Commission shall forward each complaint and its documentation to the Prosecuting Attorney and to the Attorney General's Consumer Protection Division. Where confirmation is needed, the Commission may, on its own motion or at the request of the Prosecuting Attorney, arrange: (a) independent testing of the equipment's radio emissions by a licensed professional engineer, an accredited test laboratory, or the FCC Enforcement Bureau; (b) independent examination of what data the equipment collects and where it transmits that data, by a certified digital forensic examiner or a state university laboratory; and (c) a request that the Attorney General use its investigative authority to obtain the operator's records of what data the equipment collects, retains and shares. Nothing in this item requires the county to spend funds; the Commission may arrange confirmation within available funds or through public agencies.

Adopted this ____ day of _____, 2026.

_____	_____	_____
President	Commissioner	Commissioner

Attest: _____, County Clerk

How We Are Tracked Wirelessly: A Cited Inventory

Safe Home LTD · Research summary · October 2026

How to read the tags. Court = a judge or jury decided it. Agency = a government agency's finding, order or report. Company = the company's own documents. Research = a published technical study. Allegation = claimed in a lawsuit, not decided. Report = credible news reporting. Law = statute or bill text. For the Commission or a skeptical audience, lead with Court and Agency items. Numbers in brackets point to the sources list at the end.

1. Inside the home

- **[Agency]** Amazon kept children's Alexa voice recordings indefinitely by default, and kept some data even after parents asked for deletion. Amazon paid a $25 million civil penalty (FTC and Justice Department, 2023). [1]
- **[Company]** On March 28, 2025, Amazon ended the Echo setting "Do Not Send Voice Recordings." Alexa requests on those devices now go to Amazon's cloud instead of being processed in the home. [2]
- **[Report]** Google contractors listen to Google Assistant and Google Home recordings to improve speech recognition. A contractor leaked more than 1,000 clips to Belgian broadcaster VRT, some recorded without anyone saying "OK Google"; Google confirmed the leak (2019). [3,4]
- **[Court]** Apple paid $95 million to settle claims that Siri was activated unintentionally and recorded private conversations from 2014 to 2024. Apple denied wrongdoing. [5]
- **[Agency]** Ring (owned by Amazon) let employees and contractors view customers' private videos. One employee watched thousands of videos of 81 women, including in bedrooms. Ring paid $5.8 million (FTC, 2023). [6,7]
- **[Company]** Company policies change; laws hold. Ring ended police video requests in its Neighbors app in January 2024, then brought them back in 2025 as "Community Requests" through police-technology company Axon. A planned Flock version was canceled in February 2026 before launch, but the Axon partnership remains active. [8,9,10]
- **[Company]** Where the law requires consent, Ring turns the feature off. Its face-recognition feature, Familiar Faces, "is not available for customers in Illinois, Texas, and Portland, Oregon due to specific legislation." Elsewhere, Ring leaves visitor consent to the camera owner, and a visitor who wants their face deleted must ask that owner. [11,12]
- **[Company]** Amazon Sidewalk turns Echo speakers and Ring cameras into a neighborhood wireless mesh that shares a slice of your internet with nearby devices. It was switched on by default in 2021; owners must opt out. [13]
- **[Company]** Smart thermostats sense more than temperature. Google says the Nest thermostat's sensors record humidity, motion and ambient light and "can also sense presence in the room." Phone geolocation tells the thermostat whether you are home. [14,15]
- **[Company]** Your Wi-Fi router can become a motion sensor. Comcast's Xfinity "WiFi Motion" detects people moving by how their bodies disturb the Wi-Fi signal, and Wi-Fi sensing works through walls. [16,17]
- **[Allegation]** Texas sued Sony, Samsung, LG, Hisense and TCL in December 2025. It alleges their smart TVs use automated content recognition (ACR) to capture what is on screen and sell viewing data without consent. [18]

- **[Agency]** Some apps listened through the phone microphone for ultrasonic "audio beacons" hidden in TV ads, which people can't hear, to log what households watch. The FTC warned 12 app developers using SilverPush code (2016). [19]

2. Lighting, utilities and public infrastructure

- **[Company]** LED lights can broadcast location. Philips (now Signify) supermarket LED fixtures send an invisible coded flicker that a store app reads through the phone camera, pinpointing the shopper's position in the aisle. Signify says the light itself doesn't read the phone; the app does the locating. [20]
- **[Agency]** Smart streetlights can carry cameras and license plate readers. San Diego's streetlights record high-definition video 24 hours a day, and police use them in investigations under a city surveillance policy. [21]
- **[Court]** A federal appeals court held that collecting smart-meter readings at 15-minute intervals is a Fourth Amendment search, because the data reveals what goes on inside the home (Naperville, 7th Cir. 2018). [22]
- **[Court]** Sacramento's public utility (SMUD) searched customers' smart-meter data for "high usage" homes and sent police more than 33,000 tips without warrants for over a decade. A California judge ordered the program ended in November 2025. [23,24]
- **[Agency]** Smart-meter data can flow to outside companies through "Green Button Connect," a federal standard that automatically transfers a customer's usage data to a third party once the customer authorizes it. [25]
- **[Report]** License plate reader networks pool data across agencies. In Monongalia County, WV, the Sheriff's Office's own audit records showed its Flock camera data was searched more than 3 million times by nearly 4,000 organizations in nine months. [26]

3. Your phone

- **[Company]** "Off" isn't fully off. Since iOS 15 (2021), a powered-off iPhone keeps sending a Bluetooth signal so the Find My network can locate it, like an AirTag. Apple tells users to keep this on so devices can be found "even if they're powered off." [27,28]
- **[Research]** On recent iPhones, the Bluetooth, NFC and ultra-wideband chips keep running for up to 24 hours after power-off. Researchers at TU Darmstadt showed malware could be loaded onto the Bluetooth chip and run while the phone is "off" (2022). [29]
- **[Court]** In 2006 federal judges approved the FBI's "roving bug" in a New York organized-crime case: suspects' cell phone microphones were used to record nearby conversations. News reports said this worked "even when the devices are switched off," but the case record did not establish that. [30]
- **[Research]** From about September 2024 to June 2025, Meta's Facebook and Instagram apps on Android silently linked people's web browsing to their identities through a hidden channel on the phone ("localhost"). Meta stopped the day researchers published. [31,32]
- **[Court]** A federal jury found Meta violated California's wiretap law by collecting menstrual and pregnancy data that women entered in the Flo app (August 2025). [33]
- **[Agency]** Location data brokers sell phone location trails. In May 2026 the FTC barred Kochava from selling location data tied to clinics, places of worship, shelters and similar sensitive places without consent. [34]

- **[Report]** "Stingrays" (cell-site simulators) imitate a cell tower. Every phone in range, not just a suspect's, gives up its identifying number and location, including inside homes. Federal agencies and many police departments use them. [35]
- **[Agency]** Google paid Texas $1.375 billion (2025) to settle claims that it tracked people's movements, private searches, voiceprints and facial geometry without proper consent. Google admitted no wrongdoing. [36]

4. Your car

- **[Agency]** GM and OnStar collected drivers' precise location and driving behavior and sold it, including to consumer reporting agencies that affect insurance rates, without informed consent. The FTC's final order (January 2026) bans that sharing for five years. [37]

5. Government collection and data brokers

- **[Court]** The NSA's bulk collection of Americans' phone records under Section 215 of the Patriot Act was never authorized by the statute (2nd Cir. 2015). The Ninth Circuit later held it violated FISA and "may well have been unconstitutional" (2020). [38,39]
- **[Report]** Section 702 of FISA, which collects communications of foreign targets and sweeps in Americans' messages, lapsed June 12, 2026. Providers are still cooperating under the existing court certification, which runs until March 17, 2027. No reauthorization has passed. [40,41]
- **[Agency]** Intelligence agencies buy Americans' data instead of getting warrants. A declassified government report confirmed purchases of smartphone location data, web browsing data and connected-vehicle data. The NSA acknowledged buying internet browsing records (2024). [42,43]
- **[Court]** Oracle paid $115 million to settle a class action alleging it built profiles of people's online and offline activity and sold them without consent. Oracle denied wrongdoing; payments began in 2026. [44,45]

6. Voting equipment

- **[Agency]** The federal voting system standard says wireless "can provide an entry point to the voting system for attackers" and requires that voting systems "must not be capable of establishing wireless connections." [46,47]
- **[Agency]** Virginia's WinVote touchscreens tallied votes over Wi-Fi protected by the key "abcde," which could not be changed, and votes could be edited undetected. Virginia decertified them the day its IT agency reported (April 14, 2015). [48]
- **[Law]** West Virginia law requires voting systems to be nonnetworked and never connect to the internet, but does not expressly ban wireless hardware inside them. A 2025 bill would; it says disabling wireless in software is not enough. [49,50]

What the record does not support, or only partly supports

Leaving these out keeps the strong items credible. A skeptic who catches one overstatement will dismiss the whole list.

- **Oracle as "the NSA's data platform since 9/11."** I found no public record of this. Documented: Oracle's first customer was the CIA, and the company took its name from a 1977 CIA database project. Oracle's data-broker practices led to the $115 million settlement above. [51]

- **Siri uploading conversations to your Facebook feed.** No evidence. The Siri settlement involved accidental recordings. Meta says it doesn't use the microphone for ads or the feed. A 2018 Northeastern University study of more than 17,000 Android apps found none secretly turning on the microphone, though some sent screen recordings to third parties. Cox Media Group advertised an "Active Listening" ad service; in 2026 the FTC found the service was fabricated and fined the company. [52,53,54]
- **Phones listened to while powered off.** Not demonstrated on modern phones. What is documented: radios keep transmitting after power-off (Find My), a research demonstration of malware on the Bluetooth chip, and a court-approved microphone bug whose "switched off" claim was never established in court.
- **A smart thermostat that hacked a voting machine.** This traces to a December 2020 Justice Department email claiming a Dominion machine reached the internet "through a smart thermostat" with a trail to China. No evidence was given, and the Deputy Attorney General refused to act on it. [55]
- **Smart-meter data "sold to corporations."** I found no documented case of a utility selling identified customer data. Documented: warrantless sharing with police (Sacramento), and automatic third-party transfers once a customer authorizes them.
- **"The Patriot Act is unconstitutional."** Courts held the bulk phone program illegal under the statute, and one appeals court said it "may well have been" unconstitutional. No court has issued a final constitutional ruling. Section 215 itself expired on March 15, 2020. [56]

Why this matters in Pocahontas County

- Almost every item above depends on a radio transmitter: a speaker, thermostat, router, meter, light, camera, car or phone. The common thread is a device transmitting data its owner never knowingly agreed to send.
- That is the problem item 7 of the privacy resolution addresses: a place to report a transmitter you didn't consent to, logged and referred without cost to the county.
- Federal and state law covers only pieces of this list. That is why the resolution also asks the Legislature for a 2027 state law.

Sources

1. FTC, Amazon Alexa (2023): https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever
2. AP, Amazon ends Echo privacy option (2025): https://apnews.com/article/amazon-privacy-echo-7fb3c19fa7f664bde5c5be259f8b23ee
3. VRT NWS (2019): https://www.vrt.be/vrtnws/en/2019/07/10/google-employees-are-eavesdropping-even-in-flemish-living-rooms/
4. CNBC (2019): https://www.cnbc.com/2019/07/11/google-admits-leaked-private-voice-conversations.html
5. Reuters, Siri settlement (2025): https://www.reuters.com/legal/apple-pay-95-million-settle-siri-privacy-lawsuit-2025-01-02/
6. FTC, Ring (2023): https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users
7. CBS News (2023): https://www.cbsnews.com/news/amazon-ring-ftc-lawsuit-customer-videos/
8. CNN (2024): https://www.cnn.com/2024/01/24/tech/amazons-ring-video-sharing-with-police
9. Consumer Reports: https://www.consumerreports.org/electronics/personal-information/can-federal-law-enforcement-access-your-ring-doorbell-videos-a4894322123/
10. NBC News (2026): https://www.nbcnews.com/news/us-news/amazon-no-longer-working-police-tech-flock-safety-super-bowl-ad-rcna258855
11. Ring, Intelligent features: https://ring.com/support/articles/de7qi/intelligent-features
12. Amazon letter to Sen. Markey (Nov. 2025): https://www.markey.senate.gov/imo/media/doc/amazon_markey_response_ring_frt_november_2025.pdf
13. ABC News (2021): https://abcnews.com/GMA/Living/amazon-activates-internet-sharing-service-sidewalk-turn-off/story?id=78170286
14. Google Nest Help: https://support.google.com/googlenest/answer/14748002?co=GENIE.Platform=Android&hl=en
15. Wirecutter, smart thermostats: https://www.nytimes.com/wirecutter/reviews/the-best-thermostat/?eafs_enabled=false

16. Xfinity, WiFi Motion: https://www.xfinity.com/support/articles/wifi-motion
17. The Verge (2026): https://www.theverge.com/tech/982689/comcast-xfinity-wifi-motion-privacy-concerns-response
18. Texas Attorney General (2025): https://www.texasattorneygeneral.gov/news/releases/attorney-general-paxton-sues-five-major-tv-companies-including-some-ties-ccp-spying-texans
19. FTC, SilverPush (2016): https://www.ftc.gov/news-events/news/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-silverpush-code
20. Signify, Carrefour (2015): https://www.signify.com/global/our-company/news/press-release-archive/2015/20150521-where-are-the-discounts-carrefours-led-supermarket-lighting-from-philips-will-guide-you
21. City of San Diego, Smart Streetlights impact report: https://www.sandiego.gov/sites/default/files/2024-05/sip-smart-streetlights-impact-report.pdf
22. Naperville Smart Meter Awareness v. Naperville (7th Cir. 2018): https://law.justia.com/cases/federal/appellate-courts/ca7/16-3766/16-3766-2018-08-16.html
23. EFF (2025): https://www.eff.org/deeplinks/2025/11/victory-court-end-dragnet-electricity-surveillance-program-sacramento
24. Privacy Guides (2025): https://www.privacyguides.org/news/2025/11/22/california-court-ends-smart-meter-dragnet-surveillance-program/
25. U.S. Department of Energy, Green Button: https://www.energy.gov/data/green-button
26. WV News (2026): https://www.wvnews.com/news/wvnews/monongalia-county-flock-camera-data-searched-3-million-times-group-says/article_7dbbf05e-bb5b-46ff-a291-470c94fff948.html
27. Apple Support, Find My: https://support.apple.com/en-us/102648
28. 9to5Mac (2021): https://9to5mac.com/2021/06/07/ios-15-find-my-network-can-find-your-iphone-when-it-is-powered-off/
29. Ars Technica (2022): https://arstechnica.com/information-technology/2022/05/researchers-devise-iphone-malware-that-runs-even-when-device-is-turned-off/
30. Ars Technica (2006): https://arstechnica.com/tech-policy/2006/12/8343/
31. Radboud University (2025): https://www.ru.nl/en/research/research-news/new-research-highlights-privacy-abuse-involving-meta-and-yandex
32. The Register (2025): https://www.theregister.com/security/2025/06/04/meta-pixel-halts-android-localhost-tracking-after-disclosure/1189660
33. CNBC (2025): https://www.cnbc.com/2025/08/07/jury-rules-meta-violated-law-in-period-tracking-app-data-case.html
34. FTC, Kochava (2026): https://www.ftc.gov/news-events/news/press-releases/2026/05/ftc-ban-kochava-subsidiary-selling-sensitive-location-data-settle-charges-they-sold-location-data
35. ACLU, Stingray tracking devices: https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices
36. Texas Attorney General (2025): https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-finalizes-historic-settlement-google-and-secures-1375-billion-big-tech
37. FTC, GM/OnStar (2026): https://www.ftc.gov/news-events/news/press-releases/2026/01/ftc-finalizes-order-settling-allegations-gm-onstar-collected-sold-geolocation-data-without-consumers
38. ACLU v. Clapper (2nd Cir. 2015): https://law.justia.com/cases/federal/appellate-courts/ca2/14-42/14-42-2015-05-07.html
39. Reuters, U.S. v. Moalin (2020): https://www.reuters.com/business/media-telecom/us-court-mass-surveillance-program-exposed-by-snowden-was-illegal-2020-09-03/
40. Washington Times (Oct. 13, 2026): https://www.washingtontimes.com/news/2026/oct/13/world-not-end-doomsday-warnings-fisa-lapse-proven-wrong/
41. Congressional Research Service: https://www.congress.gov/crs-product/R48592
42. ODNI declassified report (2022, released 2023): https://archive.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf
43. TechCrunch (2024): https://techcrunch.com/2024/01/26/national-security-agency-americans-internet-browsing-records-warrantless/
44. Reuters (2024): https://www.reuters.com/legal/oracle-reaches-115-mln-consumer-privacy-settlement-2024-07-19/
45. The Hill (2026): https://thehill.com/business/6101988-payment-size-revealed-in-massive-oracle-settlement-heres-how-much-youll-get/
46. EAC, VVSG 2.0: https://www.eac.gov/sites/default/files/TestingCertification/Voluntary_Voting_System_Guidelines_Version_2_0.pdf
47. NIST, VVSG 2.0 guidance: https://nvlpubs.nist.gov/nistpubs/vts/NIST.VTS.200-2.ipd.pdf
48. Princeton CITP (2015): https://blog.citp.princeton.edu/2015/04/15/decertifying-the-worst-voting-machine-in-the-us/
49. W. Va. Code §3-4A-9: https://code.wvlegislature.gov/3-4A-9/
50. HB 2489 (2025): https://www.wvlegislature.gov/Bill_Status/bills_text.cfm?billdoc=hb2489%20intr.htm&yr=2025&sesstype=RS&i=2489
51. BBC, Oracle's origin: https://www.bbc.com/news/technology-54148474
52. Meta Newsroom: https://about.fb.com/news/h/facebook-does-not-use-your-phones-microphone-for-ads-or-news-feed-stories/
53. Engadget, Northeastern study (2018): https://www.engadget.com/2018-07-03-research-facebook-probably-isnt-listening-phone.html
54. Malwarebytes, FTC on Cox (2026): https://www.malwarebytes.com/blog/news/2026/05/company-bragged-phone-mics-could-listen-to-conversations-they-couldnt
55. Business Insider (2021): https://www.businessinsider.com/trump-appointed-doj-official-claimed-chinese-thermostats-changed-votes-2021-8
56. EFF, Section 215 expired (2020): https://www.eff.org/deeplinks/2020/12/section-215-expired-year-review-2020

Sources for the Facts Cited

Privacy and surveillance technology · Pocahontas County Commission · October 20, 2026

1. Commission authority over county fiscal affairs, W. Va. Code §7-1-3
https://code.wvlegislature.gov/7-1-3/

2. Radio Astronomy Zoning Act, enforcement by the Prosecuting Attorney, §37A-1-5
https://code.wvlegislature.gov/37A-1-5/

3. Radio Astronomy Zoning Act, injunctions, §37A-1-6
https://code.wvlegislature.gov/37A-1-6/

4. How Flock license plate readers work (Flock Safety)
https://resources.flocksafety.com/meetflock/

5. West Virginia has no license plate reader statute (RecordingLaw)
https://www.recordinglaw.com/us-laws/automated-license-plate-readers/west-virginia-alpr-laws/

6. Monongalia County camera data in 3 million searches (WV News, Oct. 15, 2026)
https://www.wvnews.com/news/wvnews/monongalia-county-flock-camera-data-searched-3-million-times-group-says/article_7dbbf05e-bb5b-46ff-a291-470c94fff948.html

7. Reported license plate reader near Marlinton (DeFlock)
https://deflocktheusa.com/flock-cameras/west-virginia/marlinton/

8. House committee asks Flock to testify Nov. 9, 2026 (West Virginia Watch)
https://westvirginiawatch.com/2026/10/13/west-virginia-lawmakers-ask-flock-representative-to-testify-at-november-meeting/

9. Sen. Oliverio proposes warrant, no data sale, 7-day deletion (WV News)
https://www.wvnews.com/news/wvnews/wv-sen-mike-oliverio-calls-for-warrant-requirement-other-restrictions-on-flock-cameras-in-west/article_0943053e-907c-41e1-a1cd-79293b59365e.html

10. Gov. Morrisey supports guardrails (WV News)
https://www.wvnews.com/news/wvnews/morrisey-says-he-supports-potential-legislation-to-put-guardrails-on-flock-cameras/article_60de3bcb-3281-4709-9a00-2e49e88a53a5.amp.html

11. Huntington guardrails ordinance (WOWK)
https://www.wowktv.com/news/west-virginia/cabell-county-wv/huntington-council-passes-new-guardrails-for-flock-cameras/

12. Dane County, Wis., removes Flock funding from sheriff's budget (Wisconsin Watch)
https://wisconsinwatch.org/2026/05/wisconsin-flock-camera-ai-surveillance-backlash-police-privacy-dane-county-milwaukee/

13. Knox County, Tenn., bans fixed plate readers (Knox News)
https://www.knoxnews.com/story/news/politics/2026/08/31/knox-county-bans-flock-cameras-amid-surveillance-backlash/91545538007/

14. Monroe County, Mich., stops sheriff's Flock use (Detroit News)
https://www.detroitnews.com/story/news/local/michigan/2026/09/02/flock-cameras-off-limits-to-monroe-county-sheriff-after-board-vote/91588133007/

15. West Virginia counties have only powers granted by the state (T. Weston, Inc. v. Mineral County)
https://www.courtswv.gov/sites/default/pubfilesmnt/2023-11/32890.pdf

16. FTC final order: GM/OnStar sold drivers' location data (Jan. 2026)
https://www.ftc.gov/news-events/news/press-releases/2026/01/ftc-finalizes-order-settling-allegations-gm-onstar-collected-sold-geolocation-data-without-consumers

17. FTC: GoodRx shared health data, $1.5 million penalty (2023)
https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising

18. FTC: many health apps and devices are not covered by HIPAA
https://www.ftc.gov/business-guidance/resources/complying-ftcs-health-breach-notification-rule-0

19. Smart-meter data is a Fourth Amendment search (7th Cir. 2018)
https://law.justia.com/cases/federal/appellate-courts/ca7/16-3766/16-3766-2018-08-16.html

20. Observatory staff: "We don't have that type of authority" (Popular Mechanics)
https://www.popularmechanics.com/space/telescopes/a29589714/town-wifi-illegal/

Sources for the body-device handout are listed on its last page.

Wireless body devices are real. So is the data they send.

Licensed by the FCC. Built to an IEEE standard. Approved by the FDA. Often not protected by HIPAA.

1 ON THE BODY
Implants, sensors, watches, pumps send readings

→

2 NEARBY HUB
Phone, monitor or home gateway collects them

→

3 INTERNET + SERVERS
Data goes to company and medical servers

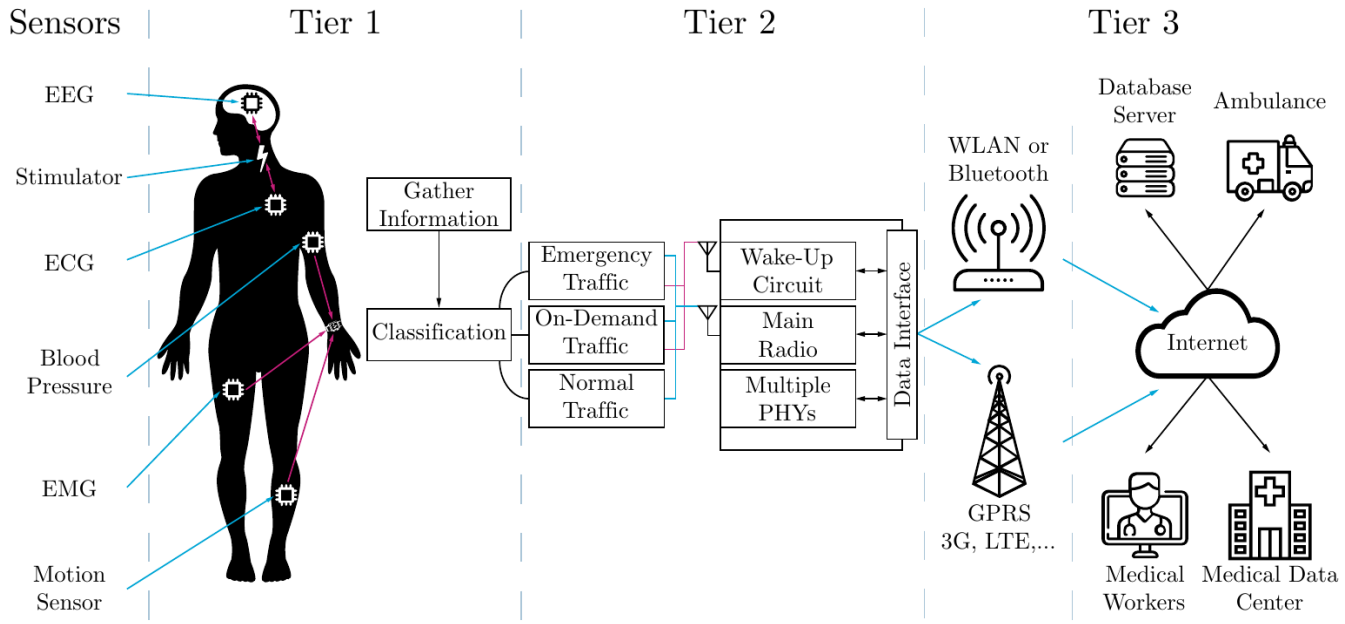


Figure 1. How a body area network moves data, from a published security study of the IEEE 802.15.6 standard: G. Hahn et al., Fig. 2 (arXiv:2201.06354, 2022).

1	**The FCC licensed radio bands for body networks in 2012.** 401–406 MHz for implants, 2360–2400 MHz for body sensors. Source: FCC
2	**The IEEE wrote the standard for networks "inside a human body."** IEEE 802.15.6, the same body that writes Wi-Fi standards. Source: IEEE
3	**RAND calls it the "Internet of Bodies."** Its 2020 report covers devices that send body data over the internet. Source: RAND RR-3226
4	**The FDA recalled insulin pumps that could be hacked wirelessly.** Medtronic MiniMed pumps. Source: FDA recall
5	**Most fitness and health apps aren't covered by HIPAA.** Fitness trackers, diet apps, connected BP cuffs. Source: FTC

It isn't a theory. The question is who controls the data.

The proof: five facts you can check yourself

Every fact and graphic comes from the federal government, a standards body, or a major research institution. None of it depends on trusting a commentator.

1. The FCC set aside radio frequencies for wireless networks on the human body

- In 2012 the FCC allocated spectrum for **Medical Body Area Networks (MBANs)**, making the U.S. "the first country in the world to make spectrum available for this specific usage." MBANs are "networks of wireless sensors, often no bigger than a Band-Aid" (FCC).
- The MBAN band is **2360–2400 MHz**. The FCC's **MedRadio** service at **401–406 MHz** serves "implanted cardiac pacemakers and defibrillators as well as neuromuscular stimulators" (FCC MedRadio). MBANs at 2390–2400 MHz "can be used at any location, including in-home" (NPSTC).

The skeptic test: Look up "MedRadio" and "MBAN" on fcc.gov.

2. There is an international engineering standard for wireless networks "inside a human body"

- **IEEE 802.15.6-2012, Wireless Body Area Networks**, covers "short-range, wireless communication in the vicinity of, or inside, a human body" (IEEE via Standards.ie). It defines protocols "for both on-body and in-body communication" (IEEE Technology Navigator). NIST, a federal agency, published the propagation models used to write it (NIST).

The skeptic test: Search "IEEE 802.15.6" at standards.ieee.org. It's the same organization that writes the Wi-Fi standards.

3. RAND, a major nonpartisan research organization, named it the "Internet of Bodies"

- RAND's 2020 report *The Internet of Bodies: Opportunities, Risks, and Governance* describes "a growing industry of devices that monitor the human body and transmit the data collected via the internet" (RAND RR-3226).
- RAND says these devices "can track, record, and store users' whereabouts, bodily functions, and what they see, hear, and even think." Lead author Mary Lee: "There's not a lot of clarity about who owns the data, how it's being used, and even who it can be sold to" (RAND).
- The benefits are real too. Artificial pancreases and smart stents "will surely keep more people alive" (RAND).
- The World Economic Forum sorts these devices by implanted vs. worn and medical vs. non-medical (Figure 2). RAND's own art shows implanted devices and how their data has been used in court (Figures 3 and 4).

The skeptic test: Download report RR-3226 free at rand.org.

4. The FDA has recalled wireless medical devices because they could be hacked

- In 2019, Medtronic MiniMed insulin pumps sold in the U.S. were recalled because "an unauthorized person could potentially connect wirelessly to a nearby insulin pump to change settings and control insulin delivery" (FDA recall database).
- Since March 29, 2023, Section 524B of the Food, Drug, and Cosmetic Act requires makers of internet-connected "cyber devices" to submit cybersecurity plans, security updates, and a software bill of materials (FDA).

The skeptic test: Search "MiniMed cybersecurity" in the FDA recall database.

5. Much body data has no HIPAA protection, and it can be used in court

- The FTC: "many companies that collect people's health information – whether it's a fitness tracker, a diet app, a connected blood pressure cuff, or something else – aren't covered by HIPAA" (FTC).
- RAND found "a patchwork of regulations" because "the rules are different in every state" (RAND). In Ohio v. Compton (2016), police obtained a man's pacemaker records by warrant, and a judge ruled the data admissible (Figure 4).

The skeptic test: Read the FTC page above. It's the government's own wording.

Figure 2. What counts as the Internet of Bodies

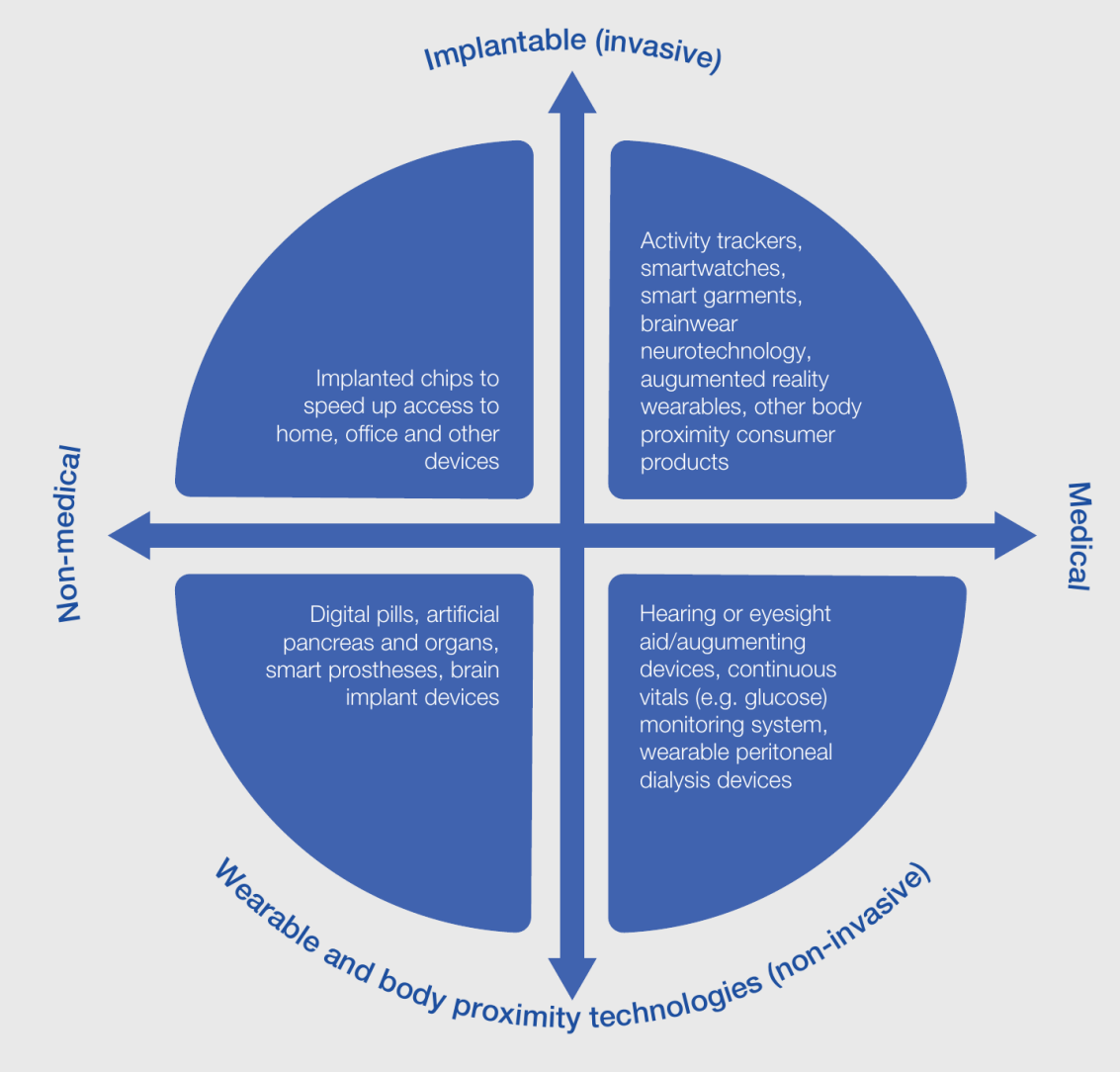


Figure 2. Examples of Internet of Bodies technologies. Source: World Economic Forum, *Shaping the Future of the Internet of Bodies*, Figure 1, p. 7 (WEF, 2020).

Why it matters here in the Quiet Zone

- **These devices are radio transmitters.** MBAN, MedRadio, and Bluetooth devices all transmit. Inside the 10-mile Radio Astronomy Zone, they're part of the same radio environment as Wi-Fi.
- **Any county policy must protect patients first.** A rule on "wireless devices that collect private data" must expressly exempt prescribed medical devices: pacemakers, defibrillators, insulin pumps, glucose monitors, hearing aids, and hospital monitoring. Without that exemption, it endangers lives.
- **The real issue is the data, not the device.** Target **who collects body data, where it goes, and who can sell or share it**, not patients.

Figures 3 and 4. Implanted devices, and their data in court

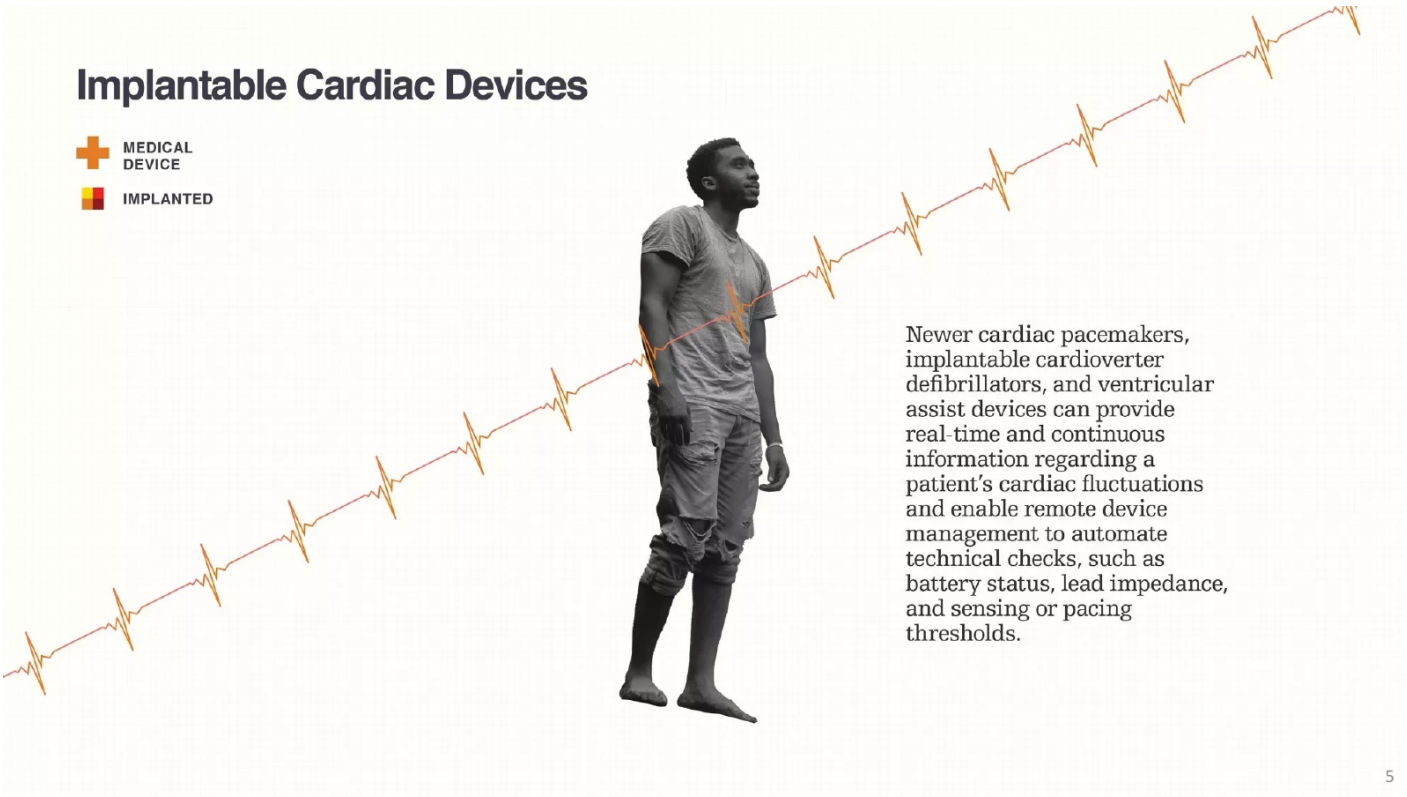


Figure 3. Implanted cardiac devices report continuously. Art by Giorgia Lupi for the RAND Corporation, © 2022 RAND; slide 5 of Mary Lee, "Internet of Bodies: Our Connected Future" (RAND presentation).



Figure 4. Ohio v. Compton: pacemaker data used as evidence. © 2022 RAND Corporation; image credit Getty Images/DKosig; slide 13 of the same presentation (RAND presentation).

Where the data goes: documented cases

Body data is only part of it. Apps, cars and utility meters collect personal data too, and companies have shared or sold it without people knowing.

Source of data	What happened
Health app GoodRx (2023)	Shared users' prescriptions and health conditions with Facebook, Google and others for years, despite promising not to, and used them to target ads. $1.5 million penalty (FTC).
Data brokers Duke University (2023)	11 of 37 brokers contacted were willing to sell data on Americans with depression, anxiety, bipolar disorder and more, some with names and addresses, for as little as $275 for 5,000 records (Duke Sanford).
Connected car GM / OnStar (2025–26)	Collected drivers' precise location and driving behavior, including hard braking, late-night driving and speeding, and sold it to consumer reporting agencies. Insurers used it to deny coverage and set rates (FTC complaint; final order).
Smart electric meter Naperville, IL (2018)	The meters record home energy use every 15 minutes, and the city stores it for up to 3 years. A federal appeals court ruled this is a Fourth Amendment "search" because the data reveals what goes on inside the home: when people are home, sleep, cook or use appliances. It upheld the program only because the data stays with the utility and isn't given to police without a warrant (7th Cir. opinion; EFF).

Ask before you sign up: Who gets my data? Is it sold or shared? Can I opt out or get it deleted?

What to say in 30 seconds

> "*The FCC gave out radio frequencies for body sensor networks in 2012. The IEEE wrote the engineering standard for networks 'inside a human body' the same year. RAND calls it the Internet of Bodies. The FDA has recalled insulin pumps that could be hacked wirelessly. The FTC says most fitness and health apps aren't covered by HIPAA. An Ohio court let police use a man's pacemaker data. None of this is a theory. Health apps, cars and smart meters already share or sell data. The question is who controls it.*"

Sources

- FCC, Connect2HealthFCC: https://www.fcc.gov/general/connect2healthfcc-wireless-health-and-medical-devices-background
- FCC, MedRadio: https://www.fcc.gov/medical-device-radiocommunications-service-medradio
- NPSTC, FCC MBAN summary (2012): https://www.npstc.org/download.jsp?tableId=37&column=217&id=2378&file=2012_May_Communicator_120531.pdf
- IEEE 802.15.6-2012 (Standards.ie): https://shop.standards.ie/en-ie/standards/ieee-802-15-6-2012-572140_saig_ieee_ieee_1309511/
- IEEE Technology Navigator, Body Area Networks: https://technav.ieee.org/topic/body-area-networks-ban/
- NIST, IEEE 802.15.6 propagation models: https://www.nist.gov/publications/propagation-models-ieee-802156-standardization-implant-communication-body-area-networks
- RAND, The Internet of Bodies (RR-3226): https://www.rand.org/pubs/research_reports/RR3226.html
- RAND, "The Internet of Bodies Will Change Everything" (2020): https://www.rand.org/pubs/articles/2020/the-internet-of-bodies-will-change-everything-for-better-or-worse.html
- RAND, "Are We Ready for the Internet of Bodies?" (2021): https://www.rand.org/pubs/articles/2021/are-we-ready-for-the-internet-of-bodies.html
- Figures 3–4: Mary Lee, RAND, "Internet of Bodies: Our Connected Future" (2022): https://nationalpress.org/wp-content/uploads/2022/11/Mary-Lee-Internet-of-Bodies-Presentation.pdf
- Figure 1: Hahn et al., arXiv:2201.06354 (2022): https://arxiv.org/abs/2201.06354
- Figure 2: World Economic Forum (2020): https://www3.weforum.org/docs/WEF_IoB_briefing_paper_2020.pdf
- FDA recall, Medtronic MiniMed: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfres/res.cfm?id=175194
- FDA, Section 524B cybersecurity FAQs: https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity-medical-devices-frequently-asked-questions-faqs
- FTC, Health Breach Notification Rule: https://www.ftc.gov/business-guidance/resources/complying-ftcs-health-breach-notification-rule-0
- FTC, GoodRx (2023): https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising
- Duke Sanford, data brokers and mental health data (2023): https://techpolicy.sanford.duke.edu/data-brokers-and-the-sale-of-americans-mental-health-data/
- FTC, GM/OnStar complaint (2025): https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-takes-action-against-general-motors-sharing-drivers-precise-location-driving-behavior-data
- FTC, GM/OnStar final order (2026): https://www.ftc.gov/news-events/news/press-releases/2026/01/ftc-finalizes-order-settling-allegations-gm-onstar-collected-sold-geolocation-data-without-consumers
- Naperville Smart Meter Awareness v. City of Naperville (7th Cir. 2018): https://law.justia.com/cases/federal/appellate-courts/ca7/16-3766/16-3766-2018-08-16.html
- EFF on the Naperville ruling: https://www.eff.org/deeplinks/2018/08/win-landmark-seventh-circuit-decision-says-fourth-amendment-applies-smart-meter

Graphics are reproduced with attribution for non-commercial educational use. Ask the copyright holder before republishing.

Wireless Device Complaint

Pocahontas County Commission · Privacy Resolution, Item 7 · File with the County Clerk, 900 Tenth Avenue, Marlinton, WV 24954

No measurement is required. You may use any radio-frequency meter or detector, of any make, or file without one. A complaint can't be refused or delayed because of the instrument used. Fill in what you can and leave the rest blank.

A. Resident

Name	
Address of the property	
Phone / email	
Owner or tenant?	☐ Owner ☐ Tenant (landlord's name: _____)

B. The equipment

Where it is (room, outside wall, pole, etc.)	
What it is, if known	
Make / model / serial number	
FCC ID on the label	_____ ☐ No FCC ID found ☐ Couldn't check
Who installed or operates it, if known	
When it was installed (approximate)	
Did you give informed consent to a wireless transmitter?	☐ No ☐ Not that I know of ☐ I agreed to service but wasn't told it transmits wirelessly
Photos attached?	☐ Yes, number of photos: ____ ☐ No

C. What you noticed

Meter or detector used (any kind), or "none"	
What it showed	
Does the signal stop when the device is unplugged?	☐ Yes ☐ No ☐ Not tried (Unplug only equipment you're allowed to; ask the operator to switch off anything else.)
Was the device connected to internet or phone service at the time?	☐ Yes ☐ No ☐ Not sure
Could your phone or computer see or join a network from the device?	☐ No network visible ☐ Visible but couldn't join ☐ Yes, joinable ☐ Didn't check
Date(s) observed	

D. Location

Approximate distance from the Green Bank Telescope	_____ miles ☐ Not sure
How determined	☐ Map printout attached ☐ GPS / mapping app ☐ Estimate

E. Volunteer screening record (optional; filled in by the screener)

Screening is done only at the resident's written invitation. The screener measures only and does not open, unplug or alter equipment owned by a utility or service provider. Method: see the Measurement Procedure.

Screener's name and contact	
Resident's written invitation	☐ Signed below in Part F ☐ Separate note attached
Date / time	
Instrument / serial / calibration date	
Filters, preamplifiers or attenuators used	
Measuring distance from the device	_____ ft
Peak reading, device on (unit)	
Reading, device off (unit)	
Frequencies identified, if known	
Converted field strength (µV/m), and "at least" value after rated error	

F. Statement and signature

I state that the information above is true to the best of my knowledge. I did not give informed consent to a wireless transmitting device as described above. ☐ I invite the screener named in Part E to take measurements at my property. ☐ I agree to allow an independent tester arranged by the Commission or the Prosecuting Attorney to examine and measure the equipment at a time we agree on.

Signature: _____ Date: _____

For the County Clerk

Log number / date received	
Forwarded to the Prosecuting Attorney (date)	
Forwarded to the Attorney General's Consumer Protection Division (date)	
Confirmation requested (date / by whom)	

WHAT I BOUGHT: A DOORBELL.



WHAT I GOT:

- **Face recognition on whoever comes to my door**
- **A line for police to request my video**
- **A company that decides when police see it without asking me**