



West Virginia State Privacy Office

Privacy Tips

May: Wearable Devices & Location Tracking



Fitness trackers and smartwatches collect biometric data (heart rate, sleep) and GPS data (where you run, walk, or work). While useful for health, this data is often shared with third-party "marketing partners."

For government workers, broadcasting your daily routine and precise location can create a "pattern of life" that reveals sensitive information about your agency's operations or your personal security.

Your Action:

- Open the app associated with your wearable (like Fitbit or Garmin).
- Go to the "Privacy" settings and turn off "Precise Location" when you aren't actively tracking a workout.
- Review the "Data Sharing" section and opt-out of sharing your metrics with third-party researchers or advertisers.

**Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.*