Below is a step-by-step exploration ("showing the work") of how a large network of electric vehicles (EVs)—each equipped with multiple cameras—could, in theory, be used for pervasive, unauthorized surveillance. This discussion is meant as an analysis of feasibility and risks, not a recommendation or blueprint for misuse.

1. Baseline: Typical EV Camera Setups

1. **Cameras for ADAS/Autonomy**
   - **Front-facing** cameras (often multiple lenses) for lane detection, traffic sign recognition, and obstacles.
   - **Rear-facing** camera(s) for parking assist and reverse driving.
   - **Side cameras** for blind-spot detection.
   - Some EVs add **wide-angle "surround view"** systems that give a 360° top-down perspective.
2. **Connectivity**
   - Many modern EVs come with always-on LTE or 5G data connections.
   - Over-the-air updates (for software) and continuous telematics (location, battery usage, etc.) are common.
3. **Data Architecture**
   - The automaker or fleet operator typically collects some camera or sensor data—often in compressed, selective form—to improve self-driving algorithms and vehicle diagnostics.

From a purely technological standpoint, these cameras capture a near-omnidirectional view around the vehicle, especially in aggregate across a moving fleet.

2. How Centralized "Live Feeds" Could Arise

2.1 Data Streams for Legitimate Uses

- **Telemetry and Training**: Manufacturers often gather brief video clips (e.g., a few seconds) for AI self-driving model improvements (e.g., to label complex road scenarios).
- **Remote Diagnostics**: In certain cases, the vehicle can send camera images if there is an error detected (e.g., a collision or sensor malfunction).

2.2 Potential for Expanded Access

- If the backend or fleet-management platform can request raw or near-real-time video from the vehicles without robust privacy controls, then:
  1. **Continuous Streaming** could be enabled: The vehicle's cameras might send higher-quality or constant streams rather than short, event-triggered clips.
  2. **Widespread Coverage**: With a large fleet on the roads, many public areas could be captured from multiple angles.

2.3 Unauthorized or Overreaching Access

- **Central Control Layer**: If a single entity (like the automaker, a fleet-owner, or even a malicious insider) has admin access, they could theoretically:
    1. **Activate cameras in real time** to view specific areas or follow certain vehicles or people on public roads.
    2. **Aggregate feeds** to create a patchwork of coverage, effectively allowing near-omnipresent street-level video in urban areas.
    3. **Leverage location data** (GPS) to target "points of interest," pulling camera feeds from EVs near those points.

3. Technical Feasibility Considerations

1. **Bandwidth Requirements**
    - Continuous high-definition video streams from thousands or millions of vehicles would require immense cellular bandwidth and robust server infrastructure.
    - This cost (and potential network congestion) might limit truly continuous streaming.
    - However, **selective streaming** (triggered by event or region) might still be feasible.
2. **Storage and Processing**
    - Storing and analyzing all that video in real time would require large data centers and advanced analytics pipelines.
    - The required computing resources might make total real-time video logging cost-prohibitive—but partial or live analytics remain plausible.
3. **Integration of Computer Vision/AI**
    - Modern AI tools can recognize faces, license plates, objects, and behaviors in video at scale.
    - If integrated into a central system, scanning for specific people or patterns could become highly automated.
4. **User Permissions and Legal Restrictions**
    - In many jurisdictions, collecting personal data (like identifiable video of people's faces or private property) triggers privacy laws.
    - Automakers and fleet operators often claim they do not store or use raw continuous footage—only short, anonymized, or event-based clips for training.
    - However, if legal or corporate policy constraints weakened—or if a malicious party gained system control—technical capability remains a factor.

4. Likelihood of Unauthorized Surveillance

1. **Corporate or State-Level Motivations**
    - A government might request or mandate real-time or stored footage access under broad legal frameworks (e.g., national security).
    - A corporate entity could theoretically use the data to improve location-based analytics or even monetize it in unethical ways.
2. **Security Vulnerabilities**
    - Hackers or insiders might exploit weak points in the fleet-control infrastructure.

    - If they gain full remote access, they could turn vehicles into roaming “CCTV on wheels.”
    - The bigger the fleet, the bigger the “attack surface,” increasing risk.

3. **Practical Hurdles**
    - **Public Backlash and Legal Exposure**: Automakers risk severe legal and reputational damage if discovered conducting large-scale clandestine surveillance.
    - **Cost vs. Benefit**: Operating vast real-time streams is expensive. Most EV companies are optimizing for cost, so continuous unauthorized feeds might not be seen as profitable or justifiable.

5. Summary Assessment

- **Technically Feasible** in principle:
    - A large fleet of EVs with cameras has near-constant road coverage.
    - Centralized remote access to these cameras can be established if the vehicle–cloud architecture allows.
    - Emerging AI can analyze aggregated footage in real time.
- **Practically Constrained** by:
    - High bandwidth and storage costs for continuous streaming.
    - Regulatory and ethical restrictions (privacy laws, corporate policies).
    - Public relations and reputational risks.
- **Risk Factor**: If privacy protections and oversight are lax, or if an entity with sufficient power/intent wants continuous access, it could be used for widespread surveillance—especially in high-density urban areas.

Final Takeaway

It is **not trivial** to keep all EV cameras live-streaming around the clock, but it is also **not impossible** for a determined operator with the right resources and system privileges. The largest barriers tend to be costs, regulations, and public scrutiny, rather than a fundamental technological limitation. The hardware and connectivity in many modern EV fleets already exist in a form that can be repurposed for near-omnidirectional capture at scale.

Ultimately, unauthorized surveillance on this scale would face legal and ethical challenges. However, from a purely technical standpoint, a centrally controlled, widespread camera network does pose a genuine privacy concern if strong safeguards are not in place.