Which streets need help? The ethics of AI pedestrian counts

Camera-based pedestrian analytics and fair street investment in Auckland

The decision and the technology

Suppose Auckland can improve only a few crossings and footpaths. Cameras and software could count pedestrians by location and time, giving a transport team more observations than a short manual survey. Staff could compare those counts when recommending an investment. This hypothetical pilot would inform a funding decision; the responsible council or local board decision-maker would choose the projects (Auckland Council, 2026). Its value depends on both the accuracy of the counts and the fairness of the judgment made from them.

Two ethical risks

First, obtaining anonymous totals can still involve processing identifiable images. Nissenbaum (2004) argues that appropriate information use depends on context: observing a street for design does not justify unrelated tracking. Kitchin (2014) warns that urban data systems can extend surveillance. I would approve cameras only where additional detail from them serves the decision and justifies the privacy cost. Manual surveys or non-imaging counters should be preferred where sufficient. The pilot would need rapid local deletion, limited supplier access and restrictions on reuse. Locations and operating hours should follow the question being investigated.

Second, accurate counts can produce unfair priorities. A busy street may record more pedestrians than an unsafe crossing that people avoid. Footfall would then conceal suppressed demand. Boyd and Crawford (2012) caution that larger datasets are neither complete nor objective. I would give engagement at least as much weight as it does when judging need. For example, a few wheelchair users at inaccessible kerb ramps could indicate an access barrier. Staff should seek evidence from people avoiding the route and explain when safety or accessibility needs justify prioritising a low-count location.

Existing law and the remaining problem

The Privacy Act 2020 governs the collection, notice, security, retention and use of personal information. Information privacy principle 10 restricts reuse, subject to exceptions. The Privacy Commissioner recommends assessing privacy effects before installing closed-circuit television (CCTV) (Office of the Privacy Commissioner, n.d.). The Biometric Processing Privacy Code 2025 requires a check of the actual functions: pedestrian counting is not automatically facial recognition or regulated biometric categorisation (Office of the Privacy Commissioner, 2025). Its transition for existing processing ended on 3 August 2026. A new pilot must establish which rules apply from the outset.

In the European Union, General Data Protection Regulation (GDPR) article 35(3)(c) requires a data-protection impact assessment for large-scale systematic monitoring of public areas. European Data Protection Board (2020) guidance addresses video devices. This offers New Zealand a useful comparative procedure, rather than a direct legal obligation. Privacy compliance still leaves the investment question unresolved: Council must decide how observed use relates to safety, access barriers and unmet need.

A practical approval test

Before procurement, the project sponsor should document the decision, alternatives, processing limits and supplier controls. Privacy and transport staff should assess the necessity. An independent reviewer should compare counts with manual samples across lighting conditions, crowding, and locations. Validation should include children, mobility aids, and crowded scenes, rather than relying on a single overall agreement rate. A system could perform well on average yet miss people whose access needs matter to the decision. Reviewers should record where errors occur and whether they change a priority. Planning staff should separately compare investment rankings with safety audits and community evidence.

The decision-maker should publish the priorities and explain which evidence changed them. Accessible meetings, walk-throughs, and supported submissions could reach residents who are missing from the footage. Questions should address routes avoided and changes that would make them usable.

At a fixed review point, the sponsor should stop or redesign the pilot if processing cannot be explained, counts are unreliable, or additional observations do not support a defensible

investment choice relative to simpler methods. The review should include operating and privacy-control costs before expansion. This limits reuse and adds work, but gives Council a practical test of public value.

There is a real trade-off: longer observation may reveal activity missed by brief surveys, while extending the time people are exposed to recording. Procurement should require the supplier to demonstrate what that extra coverage adds, allow independent checking and disclose any retained images. Council should fund only the observation needed for the decision. A supplier’s offer of greater technical capability is not, by itself, a reason to collect more data.

References

Auckland Council. (2026, September 30). What Auckland's transport changes mean for you. https://ourauckland.aucklandcouncil.govt.nz/news/2026/09/road-ahead/

Boyd, d., & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. Information, Communication & Society, 15(5), 662–679. https://doi.org/10.1080/1369118X.2012.678878

European Data Protection Board. (2020). *Guidelines 3/2019 on processing of personal data through video devices* (Version 2.0). https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en

Kitchin, R. (2014). The real-time city? Big data and smart urbanism. *GeoJournal, 79*, 1–14. https://doi.org/10.1007/s10708-013-9516-8

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 119–158. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/

Office of the Privacy Commissioner. (n.d.). *CCTV*. https://www.privacy.org.nz/resources-and-learning/a-z-topics/privacy-and-cctv/

Office of the Privacy Commissioner. (2025). Biometric Processing Privacy Code 2025 (as amended in 2026). https://www.privacy.org.nz/privacy-principles/codes-of-practice/biometric-processing-privacy-code/

Privacy Act 2020, Public Act 2020 No. 31 (N.Z.). https://www.legislation.govt.nz/act/public/2020/31/en/latest/

Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), 2016 O.J. (L 119) 1. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng