

Deactivation Is Not Verification

From occupant-controlled surveillance to networked plate readers: why a reported shutdown is not the same as a publicly observable state.

2026.07.20 17:26 DENNIS HEDEGREEN ANALYSE V1.0

[HTTPS://HEDEGREENRESEARCH.COM/ARTICLES/DEACTIVATION-IS-NOT-VERIFICATION/](https://hedegreenresearch.com/articles/deactivation-is-not-verification/)

In Dayton, Ohio, an advanced surveillance system was made visibly blind with black plastic.[1]

The city had suspended its fixed-site automated license-plate reader programme after discovering broader-than-intended sharing with outside law-enforcement agencies.[2] Settings had been changed. Reviews were being planned. Decisions were being reconsidered. But in the draft minutes from a City Commission meeting on 20 May 2026, one sentence turned part of the governance problem into something physical: the commission was looking into putting bags over the Flock cameras “to ensure no data is collected.”[3]

That image is almost too good. A networked camera can read plates at speed, classify vehicles, transmit images through a cellular network, upload them to the cloud, and make them searchable across jurisdictions. [8][9][10] But when the public needs to see that the seeing has stopped, the clearest answer is an opaque cover over the lens.

Deactivated is a reported system state. Covered is an observable physical condition. The first may be true, but the second can be checked from the street.

The Camera Under Human Control

This history does not begin with Flock Safety, and it does not need to begin with the first closed-circuit television system ever built. A more useful starting point is a US patent filed in 1966 by Marie Van Brittan Brown and Albert L. Brown for a home security system using television surveillance.[4]

Their system placed a camera at the entrance to a home. The occupant could see the visitor, speak with them, trigger an alarm, and operate the door lock remotely. It was not an automated license-plate reader, and it was not the first surveillance camera. But the patent repeatedly made its control model clear: the system was under the control of the occupant.[4]

That is a simple relationship. The camera extended the sight of the person inside the home. The person still decided where to look and what to do. The system had complexity, but its authority remained legible. Then the camera learned to read.

From Seeing a Car to Reading It

Historical accounts trace automatic number-plate recognition to the British Police Scientific Development Branch in 1976. The first arrest attributed to detection of a stolen vehicle came in 1981.[5] The important change was not merely a sharper image. The camera was becoming a reader.

By the 1990s, patent literature described roadside systems that did far more than record a passing vehicle. One US patent lineage, beginning with a 1993 filing and granted in 1997, described correcting the perspective distortion of a roadside image, locating the plate, recognising its characters, and comparing the result with valid plate patterns.[6] The object in the image had become structured information.

That made the camera more useful. A human no longer needed to watch every vehicle pass and manually copy every plate. The machine could convert movement into a searchable identifier. It could help find a stolen car, enforce a toll, control access, or build a record of traffic.[6]

It also changed the verification problem. The question was no longer only, “What did the camera see?” It became, “What did the system conclude from what the camera saw, where was that conclusion stored, and who could search it?”

The Reader Becomes a Network

Flock Safety says it launched in 2017 after its founders built a cheaper license-plate reader for a neighbourhood experiencing break-ins.[7] The company did not invent automatic plate reading. Its important move was to make the reader easier to deploy and to connect it to a much larger service.

Two Flock patent applications filed on 1 May 2018 help show the transition. One describes selecting significant surveillance images, applying neural-network filtering, assigning confidence scores, and transmitting selected images over a cellular network.[8] The other describes object-based querying across what the patent calls a “dynamic surveillance network.”[9]

The roadside camera was no longer just a camera. It was a network node.

Flock's own product material makes the design logic explicit. Its cameras can use solar and battery power instead of a local electricity connection. They use LTE instead of local Wi-Fi. Images are uploaded to the cloud. Installation, maintenance, software, and hardware replacement can be bundled into a recurring subscription. Flock explains that customers cannot simply buy the cameras because the company is as much a software company as a hardware company.[10]

That is an effective product design. It removes trenching, wiring, local servers, and much of the customer's maintenance burden. It allows cameras to be installed quickly in places where traditional infrastructure would be expensive. It also removes some of the visible boundaries.

A pair of scissors feels like the obvious answer when a machine should stop. Cut the cable. Break the connection. End the flow. But the cable has already been designed away. The camera has its own power source and its own cellular connection.[10] The absence of infrastructure is one of the product's strengths. It also means the physical route from camera to customer control is harder to see.

A Toggle Is Not a Public Fact

Flock rejects the idea that cities have no control. The company says customers control their data and sharing, that federal sharing is now off by default, and that a local police agency can disable federal sharing with a toggle. It describes audit logs, retention limits, access controls, and other safeguards.[11] Those claims belong in the record.

Dayton's own account is more specific than a general accusation. The city says it discovered that its fixed-site readers had been shared more broadly than intended with outside law-enforcement agencies. It says those sharing settings were progressively disabled, with all outside-agency access disabled by 7 April 2026. The programme remained suspended while an independent review was being prepared.[2]

None of that proves the cameras continued collecting after suspension. That distinction matters. Uncertainty is not evidence of secret operation. A bag over a camera should not be turned into proof that every dashboard, administrator, vendor, or contract was lying.

But the bag still tells us something important. A toggle is visible to the administrator who can access it. A contract is visible to the people who have read and interpreted it. A system status may be visible to the vendor maintaining the device. None of those states is automatically visible to a resident walking past the pole.

The bag is.

What the Bag Verifies

An opaque cover does not delete previously collected data. It does not terminate a contract. It does not erase a database, disable every radio, settle who owns the hardware, or prove that every component behind the lens is inactive.

The bag does not verify deactivation. It verifies obstruction.

That is narrower. It means the lens is physically covered and the camera no longer has its ordinary unobstructed view. It does not mean every technical or contractual question has been answered.

That narrowness is not a weakness. It is what makes the act honest.

The history of surveillance technology is often told as a history of increasing capability. The camera gained reach. Then memory. Then character recognition. Then databases. Then automated search. Then cellular connection. Then network scale.

The plastic bag exposes the missing parallel history: how does the public verify that each capability has stopped?

Every generation made the camera better at verifying who passed. None of those improvements necessarily made it easier for the public to verify that the camera had stopped watching.

That is why the black bag matters. It is not sophisticated. It does not need an account, an audit interface, a vendor statement, or an interpretation of contract language. It turns a remote system claim into a visible physical limit.

The camera learned to recognise the car. The city still needed plastic to make the camera's blindness visible.

— Dennis Hedegreen, trying to see the structure

Sources

1. Jason Koebler, 404 Media, “Cities Are Covering Flock Cameras With Trash Bags,” 28 May 2026. [404 Media](https://www.404media.co/cities-are-covering-flock-cameras-with-trash-bags/) (<https://www.404media.co/cities-are-covering-flock-cameras-with-trash-bags/>).
2. City of Dayton, “Dayton ALPR Cameras Community FAQs.” [City of Dayton](https://www.daytonohio.gov/1368/Dayton-ALPR-Cameras-Community-FAQs) (<https://www.daytonohio.gov/1368/Dayton-ALPR-Cameras-Community-FAQs>).
3. City of Dayton, draft City Commission minutes, 20 May 2026. [Draft minutes](https://www.daytonohio.gov/AgendaCenter/ViewFile/Minutes/05202026-1624) (<https://www.daytonohio.gov/AgendaCenter/ViewFile/Minutes/05202026-1624>).
4. Marie Van Brittan Brown and Albert L. Brown, “Home security system utilizing television surveillance,” US Patent 3,482,037, filed 1 August 1966 and granted 2 December 1969. [US3482037A](https://patents.google.com/patent/US3482037A/en) (<https://patents.google.com/patent/US3482037A/en>).
5. European Secure Vehicle Alliance (ESVA), memorandum PF 11 submitted to the UK Parliament’s Protection of Freedoms Bill Committee, section “The History of ANPR.” [Memorandum PF 11](https://publications.parliament.uk/pa/cm201011/cmpublic/protection/memo/pf11.htm) (<https://publications.parliament.uk/pa/cm201011/cmpublic/protection/memo/pf11.htm>).
6. James F. Frazier, Craig C. Reinhart, and James F. Alves, “Automated license plate locator and reader including perspective distortion correction,” US Patent 5,651,075, assigned to Hughes Missile Systems Co, filed 30 August 1995 with priority from 1 December 1993 and granted 22 July 1997. [US5651075](https://patents.google.com/patent/US5651075) (<https://patents.google.com/patent/US5651075>).
7. Flock Safety, “Introducing Flock’s national and statewide law enforcement search network.” [Flock Safety](https://www.flocksafety.com/blog/introducing-law-enforcement-network) (<https://www.flocksafety.com/blog/introducing-law-enforcement-network>).
8. Garrett Langley and Matt Feury, “Method and system for capturing and storing significant surveillance images,” US Patent 10,559,200, assigned to Flock Group Inc, filed 1 May 2018 and granted 11 February 2020. [US10559200B1](https://patents.google.com/patent/US10559200B1/en) (<https://patents.google.com/patent/US10559200B1/en>).
9. Garrett Langley and Matt Feury, “System and method for object based query of video content captured by a dynamic surveillance network,” US Patent 10,795,933, assigned to Flock Group Inc, filed 1 May 2018 and granted 6 October 2020. [US10795933B1](https://patents.google.com/patent/US10795933B1/en) (<https://patents.google.com/patent/US10795933B1/en>).
10. Flock Safety, “Frequently Asked Questions,” sections on power, connectivity, cloud upload, ownership, maintenance, and subscription. [Flock Safety FAQ](https://www.flocksafety.com/faq) (<https://www.flocksafety.com/faq>).
11. Flock Safety, “Why Are Some Flock Cameras Being Removed by Cities?” 2026. [Flock Safety](https://www.flocksafety.com/blog/why-are-some-flock-cameras-being-removed-by-cities) (<https://www.flocksafety.com/blog/why-are-some-flock-cameras-being-removed-by-cities>).

RELATION MEMORY

RETURNS TO [Recognition Is Not Verification](#) · Returns to the original distinction between a reported answer and verified knowledge, now applied to whether a surveillance capability has stopped.

MATURES FROM [Surface Is Not Verification](#) · Extends the distinction between visible surface and proof into the physical observability of a covered camera.

EXTENDS [Recognition Is Never Verification](#) · Carries the same discipline into shutdown claims: uncertainty about operation does not verify secret collection.

EXTENDS [Recognition From Above Is Not Verification](#) · Moves from what a surveillance system claims to recognise to how the public can observe that its ordinary view has been obstructed.

CANONICAL URL: [HTTPS://HEDEGREENRESEARCH.COM/ARTICLES/DEACTIVATION-IS-NOT-VERIFICATION/](https://hedegreenresearch.com/articles/deactivation-is-not-verification/)

PDF VIEW GENERATED: 2026-07-20T15:26:18.931Z