

# LEVERAGING

# THE STATE OF SURVEILLANCE



by Stephen Roper  
*DigiStream Investigations®*

## THE INTERSECTIONS OF SURVEILLANCE(S)

In 2018, surveillance comes in many forms and serves many purposes. Closed circuit television networks (CCTVs) installed in banks and stores provide security from both external and internal threats of theft or danger. Police body and dashboard cameras act as measures of self-surveillance to protect citizens and enforce accountability. Another form of self-surveillance, through social media's many methods of content creation, promote brands and lifestyles. Then there are traffic cameras, stationed to ensure rules of the road are followed and conditions maintained.

And as these and other manifestations of modern-day surveillance continue to expand, they also intersect. A tweet detailing an accident on Sunset Boulevard is corroborated by video from a red-light camera. Someone curious about the storage time of security camera footage in a grocery store poses the question to friends on Facebook. More and more, online activity and tangible evidence are colliding, making an understanding of how to leverage all surveillance-types vital for today's investigators.

## RECORD RETENTION RATE(S)

Visit any CCTV-chatroom or message board and it becomes apparent people all start at the same question: how long is footage obtained by CCTV cameras actually kept?

A fender-bender occurs in an IKEA parking lot and is caught by an outdoor camera surveilling the entrance to the store. Is that footage kept by the business for as long as, say, a red-light camera capturing not only someone running a traffic light but t-boning another vehicle in the intersection? Can that video be retrieved? Is any of it public record or all of it?

Recognizing the need to establish protocol for the retrieval of pertinent footage from both public and private entities, DigiStream elected to conduct

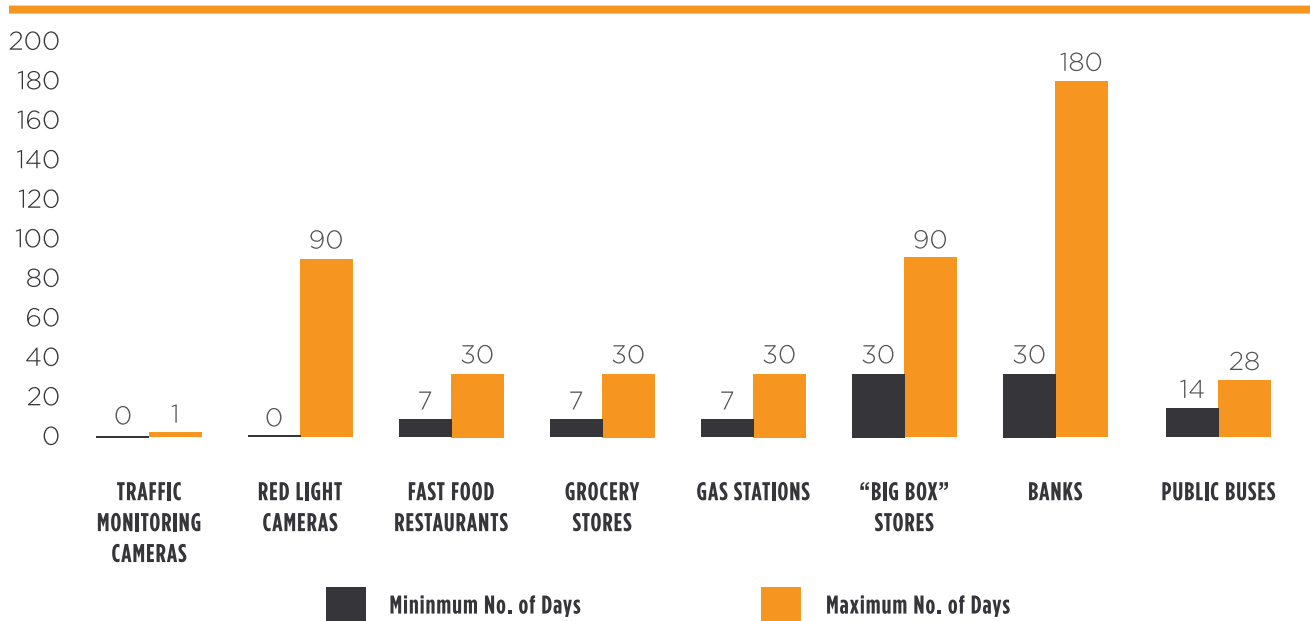
a national survey of over 30 facilities across 8 states to determine best practices. Locations were chosen by their possessing outward-facing security cameras and the first, most obvious question to answer was whether or not desired video would be available days, months, or even years after the incident in question.

For starters, an approximation of a CCTV network's storage rate can be determined by asking four questions:

1. How many cameras?
2. Their resolution?
3. Their frame rate?
4. Their frequency of recording, i.e. 24/7 or motion?

With this basic information obtained, a “CCTV record time calculator” can be used to determine the likelihood the video sought-after is still available. If the CCTV network’s “specs” remain unknown, the below survey of facilities reveals average retention rates of footage:

#### AVERAGE RETENTION RATE RANGE BY FACILITY TYPE



## THE INTERSECTIONS OF SURVEILLANCE(S)

As a general rule of thumb, private businesses like those canvassed in the survey will require a subpoena if police have not obtained the desired footage already. Additionally, identifying retention rates with stores, restaurants, and gas stations is best done in-person as questions about a business’s security system from an anonymous phone-caller will not be met with the most accommodating or illuminating of responses. This is especially true of smaller businesses like gas stations and fast food restaurants, where contacts stated any information regarding security video storage would be released in-person and not over the phone; “Big Box” stores and banks, by comparison, will direct inquiries to Loss and Prevention and/or corporate legal teams prepared for these types of requests.

For public entity CCTV networks like traffic cameras, there are several distinctions to consider when predicting the possibility of retrieval and planning the approach:

1. What type of camera recorded the incident? As illustrated in the above graph, traffic monitoring cameras have very little, if any, storage as most are live-streaming for observational purposes. But if an accident was caused by an alleged traffic light infraction, the possibility of obtaining footage is greater due to the higher retention rate.
2. Is this footage considered public record or require a subpoena? This is where jurisdictions’ sensibilities on what the public has a right to reveal themselves,

much like individuals' privacy settings on social media accounts. Generally, if the department being contacted retrieved footage from a private entity itself it will be considered material to a case and require a subpoena. However, if the department's own CCTV network captured the desired footage a public records request should prove satisfactory.

## THE BIGGER PICTURE IS THE TOTAL PICTURE

Surveillance is everywhere, voluntary and not, and to paint a complete picture one must tap all available sources to buttress against any dispute of simple fact. One tweet or Instagram photo does not prove an accident occurred or someone was at fault, but leveraging that online content into witness testimony and actual video suddenly transforms conjecture to truth. The networks to obtain information are in place, it's just a matter of knowing where and how to get it.