Adelmann Cybersecurity, LLC
March 14th, 2026

How Kidnappers Choose Their Targets

And How to Avoid Being One

I was able to locate Nancy Guthrie's address and family members in under 30 seconds with one free people search tool. So could you.

Nancy Guthrie, an 84-year-old mother of a notable and wealthy figure, was kidnapped from her home around 1am on February 1st, 2026. **As of March 14th she has not been recovered.** There is footage of a masked, gloved man coming to the door and disabling the camera. This was a seven-figure home in a nice neighborhood outside Tucson, evidence of a highly intentional and targeted crime.

7 Phases of an Abduction:

To understand any situation, every angle needs to be considered. For a complete picture of the crime, the kidnapper holds the most valuable perspective. Thinking like the kidnapper can reveal the how and why of the crime. These are crucial for putting together an investigative narrative. **With an adversarial viewpoint, it is possible to pick up clues and string together conclusions that would otherwise have been overlooked.**

Step 1: Develop your kidnapping motivation and desired outcome.

A kidnapping case can be categorized by the motivation. For an ideological kidnapping case, the goal is to spread a message to as many people as possible in the most convincing way possible. This can be motivated by a political belief or religious reasons, but regardless, the objective is to spread your ideals through a striking and violent act. Imagine kidnapping a notorious journalist for covering a story you don't like as a deterrent for possessing that viewpoint.

Financially motivated kidnappings are very simple: **The perpetrator believes the target has the means and connections for a large ransom to be paid.** Often, a vulnerable member of a wealthy family is chosen because the family deeply cares about the well-being of that person, and they have the means to pay a ransom. Some families opt for kidnapping insurance, though if a kidnapper is aware that you have kidnapping insurance and a ransom will be paid promptly, isn't that more incentive to kidnap? The benefit of kidnapping insurance requires secrecy regarding its existence.

Identifying wealthy families is relatively easy for both criminals and curious minds. Social media and open-source intelligence tools, such as people-search sites, provide scarily accurate information about people's lives. The appraisal value of addresses can be viewed on websites like Zillow, and in some cases, even the property tax amounts are available. These values can be used to estimate a family's financial standing. In a financially motivated kidnapping case, the demands are often made quite soon after the abduction. In the case of Nancy Guthrie, the public has not been made privy to the specifics of these demands, but rather the victim's family has stated "...and we will pay." in a video directed as a response to the kidnapper's demands. *(*link to video)*

Step 2: Identify the target and those who are close to them, who will pay the ransom.

Nancy Guthrie is the mother of the renowned journalist and attorney Savannah Guthrie. This familial connection is identifiable on people search websites, Wikipedia, articles, publications, and likely in interviews. As a kidnapper, I would first identify the financial target, the one who would be compelled to pay the ransom (Savannah in this case), and *then* find the closest connections to her. Siblings are relatively young and active, so it would be harder to physically overpower them. The mother lives alone, outside the city center, and is 84. This identifies a vulnerable, isolated, yet important person to the financial target.

To confirm the strength of any relationship, search social media for either positive or negative mentions of family. Facebook is often public by default, and Instagram is home to infamous individuals as well. Any posts within the last few years, like celebrations and gatherings, will offer clues to relationship strength. Comments on each other's posts will indicate a continued and positive relationship. If there were a public falling out or statements of abuse, it is reasonable to conclude that the person would be a less attractive kidnapping target.

Step 3: Locate the target.

It took me 30 seconds to find the address of Nancy Guthrie. Not from any news coverage of the kidnapping, but the first people-search site that I queried. This is the mother of a notable individual, whose address is public for any curious individual in the world to find. **If you have not explicitly removed your address from the internet and are above the age of 18, unfortunately, you can be found with ease.** *(*Notes on how to remove your information are in the next section)* A kidnapper would search multiple sites to verify the addresses located. On top of this, obtaining images of and around the area when compared with social media posts is a great way to reduce the false positive risk. A kidnapper wants to be sure to kidnap the correct person.

Step 4: Digitally case the residence.

The next step is casing the residence. Without leaving the computer, Google Street View can show vehicles that park in the driveway or on the street. License plate numbers are a critical piece of information that can be used to track the movements of a vehicle. Thankfully, on large sites like Google Street View, they are blurred. Generally visible attributes like home security signage, fences, hedges, and locks provide invaluable information for would-be intruders. Some questions this research aims to answer are:

Does the power need to be cut to avoid alarms? Is the front of the home too well protected by cameras? Is it a gated community? Where can the kidnapping vehicle park? Are there cameras on neighbors' houses or on the street? Can you see evidence of pets that could be loud or dangerous? How far away is the police station? How many different roads could you leave the area by?

Every single one of these can be answered from Google Street View and Google Earth. If a kidnapper searches hard enough, floor plans of the home can pop up online if it was constructed or renovated recently.

Step 5: Plan the logistics of abduction.

How will a kidnapper transport and store the victim? A simple question that requires intense forethought. We have established earlier that harming the victim in any permanent way jeopardizes the operation. **Then how will the kidnapper manage disobedience?** Must they sedate the victim or restrain them? How do you ensure the victim doesn't leave traceable evidence at the scene of the crime? Do you walk or carry the victim to the vehicle? Are they

placed in the front seats, back seats, or storage compartment? If a victim has a condition that needs regular management, such as diabetes, the kidnapper has to keep up with treatments. This may limit the time and distance traveled between stops and require obtaining supplies.

The big problem is the geographical logistics of transport. With satellite images, cameras everywhere, tracking algorithms, and thermal imagery, how do you take someone forcefully from their home and bring them to a secure location you control? Blend in.

The art of invisibility is challenging but rewarding. If you are able to blend into the crowd, you can break the traceability of your crime very early on. Choose the most common, boring car. Choose the most mundane time to transport the victim, say rush hour on a Tuesday evening. Be slow and methodical. If none of your actions are out of place from what anyone else does, it is hard to trace anything. Do you have an inside man who delivers for Amazon? Hide the victim in a delivery truck and order a package to the keep site ahead of time. Nothing looks out of place.

An additional strategy to include is unpredictability. The idea is to produce so much noise and misdirection that the true plan is lost like a needle in a stack of other needles. **Decoy vehicles stretch search efforts even thinner.** Providing false tips and leaving red herring evidence can distract investigators from the true plan. Behaving unlike other kidnappers (which requires research into the subject) makes it unlikely that the plan will be deduced very quickly by investigators. When you break down a sophisticated crime like this, it does gain a cinematic quality.

Step 6: How do you store and hold the victim?

Storage of the victim is nearly as complicated. The kidnapper presumably has a life outside of holding someone hostage, and will need to travel to and from the keep-site. The kidnapper must obtain the essentials of healthy survival for the victim, including necessary medications. Does the victim need to have a regular procedure done that can only happen in a physician's office? **A kidnapper becomes a caregiver when the hostage is in their possession, but will do no more than keep them alive.**

Preventing escape and self-harm are large challenges for kidnappers to overcome. A hostage who escapes places the kidnapper at risk of discovery, and eliminates any possibility of a ransom payment. Something considered less often is the threat of self harm. **A hostage may realize the leverage they hold is in their own life, and threaten to jeopardize that in the pursuit of freedom.** As a kidnapper being able to recognize a bluff from a genuine threat is vital to the operation, and would likely have done some amount of psychological research.

Physically restraining the hostage may give them more reason for self harm as they lose hope even though they will prevent escape attempts. As a kidnapper you must balance the risks of these two possibilities for the specific hostage you are holding.

Step 7: How do you get paid?

In order for this endeavor to be a success, you **need to walk away with the ransom**. This introduces a number of challenges to overcome. First, how can you ensure a safe mutual transfer? You must have built up enough trust for the ransom to be paid ***before*** you release the hostage. Secondarily, what format will you receive the money in? Every option has its pros and cons.

Cash is quite bulky for large ransoms and the bills are serialized. Additionally, trackers and ink packs are often used to later apprehend the criminal. Physical gold is better because of its density and lack of traceability, though large sums of gold will be hard to exchange for fiat currency, and it is still heavy to carry around.

Crypto seems like a better option, have the ransom paid to a brand new wallet, send it through a mixer, and you have clean coins. It is not this simple. The Bitcoin blockchain (public ledger of all transactions made) can be easily

analyzed and retroactively traced to identify stolen tokens. Even when using a mixer, there are emerging methods of tracking the movement of crypto using artificial intelligence flagging subtle patterns. I do not personally know how these algorithms work, nor how effective it is, but **an intelligent criminal may not take that risk**.

Monero is completely private by default. There is no public ledger of transactions and the authorities will only know the address of the recipient address. If you move the crypto to another wallet you control, they are safe in their privacy. The problem is that a ransom payer will have a really difficult time buying large sums of Monero at one time. It is banned from many major exchanges and peer-to-peer swaps only offer small amounts per transfer. Similarly, Monero is only widely accepted for payment on dark web onion shops. It will be hard to liquidate a large ransom paid in Monero.

My point here is not to say there is any best way of receiving or paying a ransom, but more that there are always reasons why a criminal will make certain demands. Knowing how the criminal wants the money can give investigators clues to what will happen to the money in the immediate future.

Lessons and Outcomes:

In reality, experts do not know what happened or how it was planned. This plan was executed well enough that the FBI, weeks later, is begging the public for information. A family was torn apart, and as of today, has not been made whole again. It is a cruel and disgusting act for the shallow objective of money. I hope for everyone's sake that Nancy Guthrie is returned safely, as soon as possible, and I extend my sympathies to the family. I cannot imagine the pain this has and continues to cause. *(link to FBI tip site)* *(Article explanation)*

The primary lesson to be learned from this is that these types of crimes are carried out with rigorous planning. **These criminals are experts and should not be expected to make mistakes**. The best way to stay out of trouble is to avoid becoming a target or to reduce the information available about you. As the saying goes, "an ounce of prevention is worth a pound of cure."

How to Protect your own family:

I do not intend to judge or state that not enough care was taken by the Guthrie family, but rather to explore what people can do going forward to protect themselves and their loved ones from similar situations. We should not have to be concerned about these things, but we live in an imperfect world.

Widespread address availability:

What sticks out to me the most is the widespread availability of addresses. Many people are unaware that they can be found so easily, and many more do not see it as a substantial safety concern. If you are able to remove your address from the internet, it makes any would-be criminal's life many times harder. Make yourself hard to find. The additional benefit of removing your address is that **the value of someone's home can be used to infer their level of wealth**. In this kidnapping case, this means validating someone's ability to pay a ransom.

For those wondering how all these sites get your information in the first place, the short answer is everywhere. Most commonly public data is scraped from local registries of deeds, court documents, digitized phone books, and voter registrations. These companies will then buy data from private companies where data is aggregated from utility bills, online accounts, magazine subscriptions, and other similar data aggregators.

Ways to remove your address from the internet:

Removal of personal information from the internet is a straightforward but tedious process. Unless you are lucky enough to be European, or live in California (after the DROP platform starts to be enforced), a request for removal must be submitted to each company and/or website hosting your information. You must follow the policies and procedures of the sites in question, and have **essentially no legal backing**. There are software companies that offer these services, but I assure you, they will not get everything. There are people-search websites that require you to verify your identity as part of the removal process, and a third-party software company cannot do this on your behalf. If you hire a professional firm to do these removals for you, they will require information and some participation from you. If not, **you are being taken advantage of**.

Steps can be taken to prevent the casing of the home, as mentioned in the previous section, even while your address is public. Google and Apple may blur your residence on their databases upon request. *(link to Google blur explanation)* Apple’s process requires you to email them with a request to censor a face, license plate, or house that you own. You can email mapsimagecollection@apple.com.

Data poisoning:

Despite anyone's best efforts, information that was once on the internet tends to reappear. To defend against the inevitable resurgence of sensitive information, experts will employ a strategy known as data poisoning. **This process introduces fake or altered data onto people search websites and other databases in order to overwrite or obscure the true information.** If the public knows that I was born in 1996, but they find ten different dates of birth for me in that year, it will be hard to determine which is correct, if any. This strategy understands that an entirely invisible public profile is near impossible to maintain and will look suspicious to anyone investigating. It is better to have a few fake believable bits of information, than nothing at all. On top of protecting yourself, wasting a criminal's time with wild goose chases gives them less time to go after a vulnerable person.

Real Data	Poisoned Data
34 South Main St, Castor MS	45 Main St, Castor MS
828 445 9281	828 454 8912
James Richard Doe	James Ronald Doe
January 8th 1965	January 18th 1956

**This data has been adjusted to remain believable, but enough to be unhelpful for would-be attackers.*

How to mitigate the risks of Social Media:

Social media leaves it up to the end user to protect themselves. The presence and usage of social media itself is not an issue; I have and use a number of social media profiles regularly. The issue is with what you allow others to see. Do not post pictures of your vacation **while you are still on vacation**. Do not include house numbers, street signs, notable buildings, or identifiable landmarks when posting images from or near your home and place of work. Do not post the school your children attend.

People with bad intentions will use all of this against you in a heartbeat. If a thief sees your whole family is on vacation, the house is empty and unprotected. If a kidnapper finds multiple addresses of yours online, but sees you posting in the front yard of one year-round, they just verified the location.

Spam and scam mail are becoming harder to identify with the adoption of AI. An individual can blackmail you, threaten you, or pretend to be an institution you trust, like a child's school. Does this not scare you? Our homes and families are exposed through what we willingly place in public.

My last recommendation is to set any and all profiles to private if you are willing and able to do so. I say this last because it does not invalidate the previous recommendations, and **I recognize that many people are not willing or able to make some profiles private.** Keep in mind that comments, profile pictures, and some content posted before you set the account to private will still show up publicly.

Meta-data Harvesting:

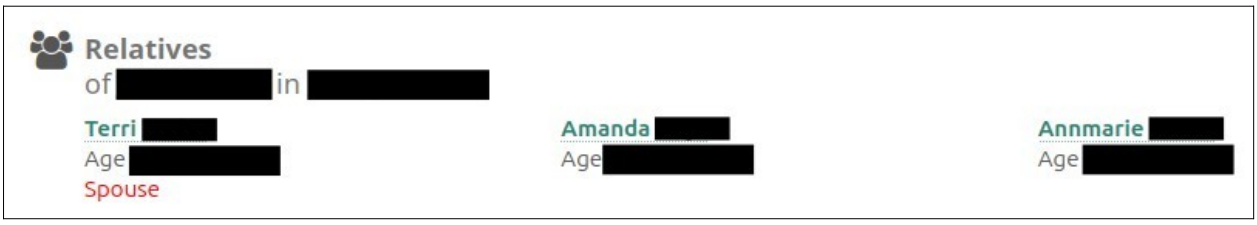
Anytime a photo is taken on your phone, it stores data within the photo on the date and time it was taken, the device used, the GPS coordinates the photo was taken at, and the camera settings. All of this data is usually invisible to us, but with simple software anyone can decode it. This is Meta-data. This data is stored as EXIF (Exchangeable Image File Format) and is standard across major smartphone and camera manufactures.

Most modern devices will have settings to limit meta data capture, *(iOS guide | Android guide)* but I strongly encourage getting software designed to scrub meta-data before distribution. You will need to retroactively remove or alter the meta-data of images already taken. Some social media applications, like Instagram, will automatically scrub meta-data but please do not rely on this to keep you safe.

Impact of the family unit:

One person can do everything right, but those around them may still compromise their safety. If you live in a home with a spouse, adult children, your parents, or roommates, **your information becomes tied to theirs**. On people-search websites, you can often search by address in addition to by name, phone number, and email.

You become exposed when your roommate posts pictures with you even if you remove your information from the internet. These sites have sections dedicated to linking the information of family members and associates. I speak of this not only so you can protect yourself, but so you can protect those who you care about. Your safety improves their safety, and theirs improves yours.



Having good digital security does not exempt you from the benefits of physical security.

Physical security is a separate topic entirely, but still very important to cover. You must have reasonable standards of safety, both physically and digitally, to protect yourself. An untraceable individual missing a front door is likely to be made a victim of opportunistic crimes. Opposite to this, a person who lives in a fortress but is agnostic to digital safety is prone to being manipulated, tricked, and fooled into letting the harm come to them. **It pays to be well-rounded in every aspect of our lives, and safety is no different.** Standard physical security tips:

- Keep your doors locked even while in the house. Use a deadbolt if present.
- Replace the screws in the strike-plate of exterior doors with 3" screws. (the metal plate that the door bolt contacts VIDEO)
- Keep windows shut and locked when not in use.
- Identify quick points of ingress and egress in the case of an emergency.
- Keep cars in a locked garage so license plates are not readable. (if applicable)
- Communicate with the other residents of the home about your time and method of arrival.
- Establish what to do in emergency situations with the residents of the home.
- Do not open the door to a knock. Identify who is knocking and why beforehand.
- Install exterior cameras and/or motion-detected lights.
- An alarm system can be useful, but be mindful of the privacy trade-offs.
- Sweep your home for bugs, microphones, and cameras.
- Get a loud dog. Large or violent dogs are easily subdued by a treat.

All of these steps can substantially reduce the likelihood and success rate of threats against you, but it is important to remember that any protection will only stall a determined adversary. **Effective protections will give you enough time for the authorities to get involved and prevent any harm from coming to your family.** There is nothing that can bring your risk down to zero, but we can get close. Anyone offering you a guarantee is either ignorant or deceitful.

How Open Source Intelligence Can Solve This Crime:

Though the kidnapping has already occurred, the relevance to cybersecurity is still present. Open Source Intelligence (OSINT) is gathering information from publicly accessible data. This is a fundamental component of any investigation, despite the authorities having access to additional data through closed sources. The FBI accepts tips, and even now, both the authorities and the Guthrie family are offering large sums of money for information leading to the recovery of Nancy.

Below are some examples of the types of ways open source intelligence can be used in this kidnapping case:

1. The kidnapper and the victim are human. What patterns can we look for?

The humanness of a perpetrator and a victim means there are certain regular actions that must be taken. Clues can be intuitively gathered from this. Assuming the kidnapper has some shred of decency or a weak bladder themselves, **how long (far) could they go before stopping for the restroom?** What restrooms fall within that area? Where are the nearest cameras to these restrooms?

This is an example of what questions we can ask and answer with open source intelligence. OpenStreetMap, Google Earth, and other software have robust searching and mapping capabilities that anyone can use for free. There are growing databases of cameras on streets and on homes that we can have access to, though usually only the authorities will have access to the actual camera feeds.

2. Searching the internet for evidence of motive.

A strategy that can be deployed both proactively and retroactively is screening the internet for cause. If a person of interest has a social media presence, the **comments could include threats or hate towards them**. This is not itself a crime. People have the right to express whatever they think, but if a crime did occur, or is believed to occur in the near future, looking into the origin of these strong comments could produce meaningful leads.

Even more subtle things to watch out for would be obsessive accounts, stalking type behavior, and spillover to the tangible world. If letters start appearing at someone's doorstep, this can be cause for concern. If a car seems to drive by the home an inappropriate number of times, again, this can be cause for concern. Depending on how far ahead a violent act is planned, the perpetrator may not be covering the tracks before the final decision to conduct the crime is made.

3. The victim is only valuable if kept alive.

The victim of kidnapping is the entire store of value. If they are harmed in any permanent way or die, the value goes to zero, and the consequences increase drastically. Kidnappers are incentivized to take care of the victims. With this in mind, we can look for the specific needs of a victim. Do they take daily medicine? Does it require a prescription to fill? How many days of supply can you get at one time? Are there dietary restrictions or supplements that need to be obtained?

The unique combination of requirements for a victim (an elderly woman is likely to require more precise care than a 24-year-old) means that if the kidnappers need to store the victim for longer than their existing supplies last, they will be forced to purchase more. Stores keep records of sales, and for prescription drugs, a prescription is required.

The likely outcome here is where the authorities privately contact pharmacies and stores in a certain radius, and ask for any receipts that contain the items they are tracking. Often, stores will also have video footage, payment records,

and possibly even a record of a prescription. This information can all be used to trace the identity of the perpetrators as well as the rough location where they are storing the victim. This is a less open strategy, but individuals can inform the proper authorities of what combination of items should be flagged, where, and when.

4. Value of Crowdsourcing investigations.

From the perspective of the authorities, the value of crowdsourcing is immeasurable. **This is why photos of suspects are publicized, and why we have any information about the situation.** The more eyes and ears able to identify clues, the more likely they are to retrieve the victim. Online communities such as Tracelabs.org are groups of skilled individuals dedicated to working on cases such as these. Reddit has been known to geolocate obscure images in minutes after upload.

Everyone has a unique perspective and a unique skillset. The one out of 100 million input that someone gives could be the difference between a family being reunited with their mother or not. There is no cost to involving the public, but there is an opportunity for incredible upside. **Each of us has something to add.** Whether that be publicity to the situation, a new perspective, an idea to try, or a friend of a friend who knows someone. We can all make a difference.

Report prepared by:
Griffin Adelmann
Founding Partner, Adelmann Cybersecurity, LLC
Griffin@adelmanncybersecurity.com
+1 (646) 883 5096