"You Can't Handle the Truth!" Separating the Hollywood Myths about Advanced Investigative Techniques from Reality

By Megan Kohls, Research Director- UpStream Intelligence

There are a lot of myths out there about investigative technology - mainly put into our heads by the imaginative thinkers and writers of Hollywood. In shows like Criminal Minds, NCIS, and CSI, whenever an advanced piece of software or equipment is needed to solve that last piece of the puzzle, it just appears like magic, the suspect is identified, and ultimately apprehended.

The reality may not be exactly what you have seen in Mission Impossible, but it is every bit as useful and more accessible than Hollywood would have you believe. In fiction, the best technology is always utilized by government agents and law enforcement. The truth is that most of what Hollywood depicts doesn't exist in the private sector, but the resources that do are very effective and well within reach.

Myth: Investigators can track cell phones in real time using cell towers or software on the phone itself

Reality: This is incredibly illegal! Any kind of tracking device, be it on a phone or a motor vehicle, is against the law in the United States.

With the right permission and chain of custody, forensics on a cell phone or any electronic device can produce evidence invaluable to a fraud or liability investigation. The types of details typically found on a device are location history, messages, photos, videos, and often, deleted content. App data can tell us exactly what the user was viewing, second-by-second, and the device data and diagnostics can give details like whether the phone was face up or face down at a given moment in time.

In one case that came to UpStream Intelligence, forensics were run on a cell phone belonging to the driver of a heavy-duty truck that was involved in a deadly collision. App data showed that, at the time of the crash, a series of SnapChat videos were playing on the device, within the moving vehicle.

Myth: Satellites can be redirected at a second's notice and zoom to show the detail of someone's face

Reality: Satellite owners have the capability to change the focus or path of their assets, and some do offer services that allow customers to pay for the satellite to travel over a specific area, however it is not instantaneous, and is quite costly. In cases where historical images are crucial, archived satellite imagery is easily accessible.

Strict privacy laws govern how detailed satellite imagery can be; the lower the number, the better resolution. Google Maps uses 50cm resolution, and it quickly becomes apparent that the level of detail is suitable for large structures, but not at all able to show details related to small pieces of damage or vehicles, let alone people. The best commercially available satellite images in the US are 25cm resolution, which again, does not get to the level of identifying a person.

A more reliable real-time resource is drone technology, which can be quickly deployed in order to map a location, or record damage following an accident or disaster. Drones are nimble and can map an area in a matter of hours to detail the exact information relevant to a claim or investigation. UpStream Intelligence has coverage within two hours of every major city in the US, making drones a very accessible option.

Myth: You need to be Tom Cruise and have sophisticated technology to break into a warehouse, office building, or headquarters

Reality: Investigators can and have made entry to private facilities when contracted to do so by the owner. Penetration Testing is often thought of in a virtual context to check for breaches in internet security, however the data that is physically accessible is often overlooked.

UpStream Intelligence was contracted by the owner of a warehouse/office facility to determine whether we could gain access to the facility, and if so, what information could be accessed by non-employees. Our team easily made entry into the facility despite standing security protocol and were able to locate and copy sensitive employee HR files, company financial data, and information about customers and vendors. Our work allowed the client to tighten security and prevent a real incident in the future.

Myth: Low quality video or images can be enhanced to be perfectly clear

Reality: Images and video are limited to the level of detail provided by the number of pixels the image contains. The more pixels, the more detail available; ergo, fewer pixels mean less detail and that lack of information is not something that can be enhanced or changed.

Savvy technicians can alter the color or use AI to make informed decisions about what should be in an image - so some level of improvement is available. Another consideration is the most advanced tool of all - the human eye. In one instance, Upstream Intelligence was supplied with grainy dashcam footage of a vehicle that committed a no-touch hit-and-run. Using the experience and knowledge our best surveillance investigators have developed over the years, we were able to determine the make and model of the vehicle and narrow the pool down to three locals with the same color vehicle.

In another instance, we were able to use predictive software to clarify the license plate number of a vehicle that we could then trace back to the owner and submit to the client for a formal interview.

Myth: A single database exists and looking up a suspect or individual requires no ID verification

Reality: The United States is one of very few countries with national background databases which can be used for comprehensive background checks. Furthermore, these numerous resources are commercially engaged in the sale of data and therefore have proprietary data sets. They do not divulge their resources, especially not for specific pieces of data, and they do not guarantee the accuracy of their data. A professional investigator is needed to vet all background information.

When working cases outside of the US, it is important to know what information is readily available to foreign investigators – UpStream Intelligence was asked to locate the next-of-kin for a Honduran National hospitalized here in the US. Despite working with little identifying information, our team was able to work with local investigators to eventually confirm the individual's full name and get the names of possible family members. Ultimately, his estranged daughter was contacted in Europe.

International identity resolution is also paramount to any foreign process service assignment. Some countries allow investigators access to address information, however other countries do not maintain national registers of that data. In those instances, it may be necessary to deploy surveillance investigators who can locate an individual at a potential place of work, residence, or relative's residence.

Myth: There is no software that allows legal professionals to organize notes on jurors during voir dire

Reality: This software does exist! UpStream Intelligence currently partners with JurorSearch during voir dire investigations, allowing us to provide details about potential jurors in real-time. The legal team in court can add their own notes, ask questions, and even mark jurors as struck or empaneled.

The data gathered during voir dire is available throughout the trial, along with social media links to ensure that no information regarding the trial is being shared online. In the rare instance that a juror does step out of bounds and share information that is cause for a mistrial, it can be discovered immediately and the cost of finding out after the trial is over, avoided.

Myth: Financial records and assets hidden by shell companies are both readily available
Reality: Financial records are protected by GLBA, and soft assets require a court order, though there are some instances where assets are required to be listed in detail (such as during a bankruptcy or custody proceedings). The main way to determine whether an individual is being truthful about their quality of life or if they are able to pay on a judgment is by looking at hard assets such as property, equipment, vehicles, and business affiliations.

In regard to businesses, the only entities that are required to share tax information or detailed financial information are publicly traded companies and non-profits. When dealing with a medium-size private company, an investigator must know where to look for financial indicators depending on the industry and state/federal regulatory bodies. Financial indicators can come from much less traditional sources such as lawsuits, new site developments, or acquisitions. The number and caliber of their employees can also indicate the financial status of an entity.

Myth: Only investigators (legally) and criminals (illegally) can get your personal information

Reality: Though the internet is fully entrenched in our daily lives, it is still in its infancy. Privacy law is racing to catch up, but the reality is that we are currently in the wild west when it comes to data security and commercial practices.

Anyone who uses the internet is subject to cookies, which track and report your internet activity back to their place of origination. One website can utilize dozens of cookies - when the data they gather is combined with social media data, sweepstakes/rewards accounts etc., they add up to a $200 billion data industry.

Unfortunately, targeted advertising is not the sole use of this information. People search sites like BeenVerified or Spokeo sell personal addresses, phone numbers, and lists of relatives to anyone with a credit card. Universities across the United States were recently found (by the Dallas Morning News) to be tracking the social media accounts of their students to identify threats such as protests. There is no end to why data is bought, and sold, and stored for future use.

At UpStream Intelligence, we combat this with a unique service called DataShroud. Our specialists review the full online presence of an individual in order to provide a customized internet dossier. We then do a thorough sweep to scrub information from the internet, in addition to advising on how best to manage the content that cannot or should not be removed for professional or personal reasons.