



OSINT *for good*

by Logan Baumunk

WHAT IS OSINT?

Can you remember all of the times you may have inadvertently been in the background of a stranger's photo when walking down a street or passing a local monument? Have you given any thought to who or what is in the background of the last selfie you took? Maybe it was a couple proposing or a young child dropping an ice cream cone. What if it was a robbery suspect fleeing the scene of a crime? What if it was a missile that shot down a plane hours later?

Open-source data is basically any data that is publicly available and can include anything from social media profiles to satellite imagery from a weather database. Knowing how to navigate the endless chaos of information on the internet is the specialty of OSINT investigators. While most individuals may solely focus on what's forefront in a photo or a document, OSINT investigators dig deep behind the scenes. It could be something complex such as geographically locating where a photo was taken because of a building in the background or simply identifying individuals speaking in a video. Open-source investigators are utilizing skills and techniques to fight threats to society including local crime, war crimes, and human trafficking.

WHO IS LEARNING OSINT?: POLICE DEPARTMENTS

A robbery was just reported at one of your local convenience stores. Nobody was hurt, but luckily surveillance video of the incident showed a figure brandishing a firearm at the clerk. While some sections of the video are blurry, there are clear shots of the figure and the car they drove away in.

By analyzing the video, key details can be gathered to assist with identification and locating the offender. Everything from clothing, hair color/style, approximate age, can all be taken and applied to online searches.

If you know where to look, criminals may be forthcoming with their offenses on social media platforms. In a particular case from January 2018, a detective was monitoring social media platforms and uncovered an individual streaming video over Facebook Live that showed him in possession of a loaded handgun and suspected illegal drugs. The detective recognized this individual as wanted criminal by another police department and used the video and online sources to pinpoint exactly where he was currently living. "Based on their observation of the Facebook live video feed, Detectives believed that [the wanted individual] was streaming his video from an apartment located in the 2500 block of Stephenson Circle in Freeport.¹"

What was once a profession with steadfast traditions, investigative journalism is being revolutionized by the inclusion of OSINT search

techniques. Both investigative journalists and OSINT investigators use social media platforms such as Instagram or Telegram to uncover additional leads with their cases.

For example, a neo-Nazi rally was posted to a channel in Telegram at City Hall for the following week and comments are flooding the post from interested attendees. Journalists, police, and OSINT investigators share the capabilities to monitor and investigate deeper into this event. Individuals who plan on attending can be uncovered by photos and usernames. These uncovered members can be found across other social media platforms like Facebook and Instagram. Full names, locations, relatives, and criminal records can be found from previously filed court documents. By utilizing OSINT techniques, an OSINT investigator can map out the entire event with social media coverage and information on attendees. Police can take action from monitoring any intended violence posted to a comment. Journalists can publish confirmed content of the event with evidence of all techniques, and everyone involved.

Amateur open-source investigators brought this technique into the light in 2017 when participants in a Charlottesville, VA white supremacist rally were identified over Twitter. On August 12, 2017, four photos were posted by an account with the username @YesYourRacist showing the faces of the rally attendees. Currently with 50.5K retweets and over 67.4K likes, other Twitter users used matching photos from Facebook and LinkedIn to identify various individuals pictured.² Before these techniques, reporters would need to speak with individuals themselves, taking up valuable time. By utilizing the public on a scale larger than any single person could out in the field, social media search techniques are making it easier for higher quality news to be reported.

INTERNATIONAL OSINT

As of October 2022, it was recorded that there are over 4.74 billion social media users worldwide.³ At a time when humans have never been more connected, social media users have

the ability to share content that would otherwise be missed. A video sharing platform like TikTok boasts over 1 billion global users, may more popularly be known as the harbinger for spiraling trends such as the Tide pod challenge. In regions like Ukraine, social media like TikTok is being used to broadcast and document bombings and war crimes.

Since Russia's invasion of Ukraine in February 2022, there have been 6.8 thousand deaths of civilians while 428 were children.⁴ TikTok videos recorded and published from war torn areas like Ukraine shed light in a way that broadcast news sources cannot. These published videos are amateur recordings showing immediate content rather than compiled data for an article. Within these videos, it was actually proven early on that Russian forces were preparing for an invasion.⁵ Weapons and troops were recorded and posted onto TikTok by the residents of villages they passed through. While media outlets are mired by regulations and other red tape, user-created videos such as these were uncovered by OSINT investigators to directly contradict the mass broadcasted misinformation.

Diving deeper into these videos, an OSINT investigator could analyze various key details. They can then be compiled and utilized into searches to conclude specifics including makes or calibers of guns, military rank, and unit numbers. Bellingcat, a Netherlands-based investigative group specializing in fact-checking and OSINT, has led the charge with publishing findings from the invasion uncovered through OSINT. With the amount of violence perpetrated against civilians in Ukraine, Bellingcat has sourced posts and photos from social media platforms like Twitter and Telegram to document the carnage.

One set of photos posted to Telegram on December 9, 2022, shows the documented wreckage of a residential building in a Kharkiv suburb from a strike.⁶ Three other posts show the aftermath of the shelling of Donetsk which killed 7 people and damaged surrounding homes.⁷

Beyond the validation and accuracy of documenting these posts and photos, investigative groups like Bellingcat preserve this data as a break in the clouds. In the sources of their data, they include, "This level of verification is intended to indicate where incidents took place, when and where there are reasonable visual indications of civilian harm. Our investigation plan for the collection of this material and its uses are informed by the Berkeley Protocol on Digital Open-Source Investigations. These incidents are also being collected and archived at a forensic level for potential evidentiary use in the future."⁸

OSINT V. TRAFFICKING

During your normal day to day article browsing and social media scrolling, it is very likely that you have encountered advertisements. These advertisements may highlight a miracle pill that will help you lose 20 lbs. with ease or maybe a skin care product that will melt away wrinkles. You may have also seen an advertisement that attempted to provoke you with something like "Women in your area are desperate for attention." Included with these ads are two or three pictures of individuals provocatively situated to grab your attention. Would you know for certain that the pictured models are over 18 years old?

While some of the advertisements may show models over the age of 18, it's been reported that victims of commercial sex trafficking were introduced at the age of 15.⁹ Groups like Guardian Group enlist volunteers with comprehensive OSINT skills to combat sex trafficking. Focusing on the sale and exploitation of women and children, techniques are used to identify victims and confirm the ages of those pictured in such advertisements.

Clicking on the advertisement listed above, you are brought to an escort website that will show you additional photos, possibly a phone number, and their location. OSINT investigators can use this information to positively identify and uncover additional online content to corroborate whether or not this individual is a victim of

trafficking. This information can then go to law enforcement to contribute to the safety of youth.

WHERE THERE IS LIGHT

Whether it's close to home or reaching across borders, no detail is irrelevant for OSINT investigators. The next time you scroll down Facebook or like a photo on Instagram, think about how many eyes are on your profile.

If your Facebook account is public, has anyone posted a Happy Birthday message? Anniversary? Do you have your location and education fields updated in your info section? What about public photos of your pets and their names? Have you considered how easy your password is to be guessed? The National Cyber Security Centre said 15% of the population used pets' names, 14% use a family member's name, and 13% pick a notable date.¹⁰

How much of your daily life you are leaving open for those with OSINT skills without the best intentions? As Masashi Kishimoto wrote, "In this world, whenever there is light, there are also shadows."

-
- 1 <https://www.thefreelibrary.com/Wanted+Teen+Arrested+After+Getting+Away+Location+On+Facebook+Live-a0522351117>
 - 2 <https://techcrunch.com/2017/08/13/fascists-called-out-on-twitter/>
 - 3 <https://datareportal.com/social-media-users#:~:text=Analysis%20from%20Kepios%20shows%20that,since%20this%20time%20last%20year.>
 - 4 <https://www.statista.com/statistics/1293492/ukraine-war-casualties/>
 - 5 <https://www.washingtonpost.com/world/2022/02/11/russia-ukraine-military-videos-tiktok/>
 - 6 <https://ukraine.bellingcat.com/?id=CIV1701>
 - 7 <https://ukraine.bellingcat.com/?id=CIV1695>
 - 8 <https://ukraine.bellingcat.com/?id=CIV1695>
 - 9 https://www.thorn.org/wp-content/uploads/2018/06/Thorn_Survivor_Insights_061118.pdf
 - 10 <https://www.bbc.com/news/technology-56680790>