What is OSINT?

BY ERIN BEFFA

Information, some say, is the new oil. Like oil in the early days of the oil boom, important personal and commercial information lies just below the internet's surface. The art and science of finding that information even has a name: Open Source Intelligence (OSINT).

While a few online information sources are relatively well-known (e.g., Facebook), the OSINT analyst goes well beyond these deposits, drilling deeper into the vast reserves of information available on every person, company, and organization.

OSINT isn't "hacking." Trained OSINT analysts *never* intrude into secure realms to locate information; they steal no passwords and breach no firewalls. Instead, they use advanced search techniques and honed research skills to find information hiding in plain sight—information that's freely available to anyone who knows where and how to look.[1]

Lawyers and other legal professionals may be interested to learn OSINT's many uses. This article discusses the science of OSINT and provides an overview of its application within the legal field.

The Staggering Amount of Publicly Available Information

OSINT analysis can reveal a wealth of detail about individual or corporate targets—likely much more information than the target knew or wanted to be publicly available. Using just the first and last name of a person as a starting point, an OSINT analyst dives deep into the available online information for that subject. Through this search, the analyst may identify data points ranging from the subject's mother's maiden name to vehicle VIN to covert social media accounts. The flowchart shows how one basic piece of information can lead to personal details very quickly.

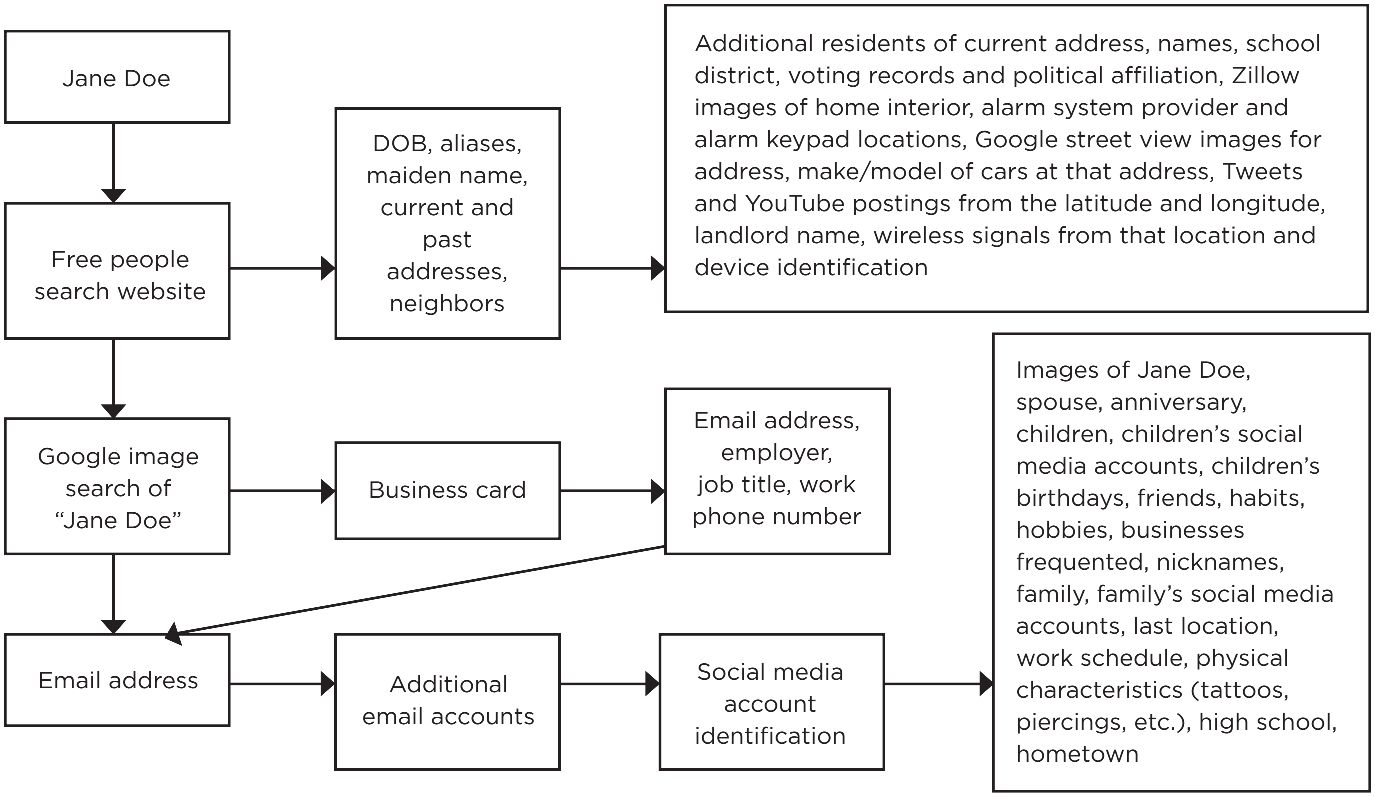
OSINT research can also lead to intelligence about companies, such as working copies of financial details in Excel spreadsheets, PowerPoint presentations detailing company products, building blueprints, proprietary code shared online, or internal memos in PDF format. The amount of proprietary information accidentally posted or left online is astonishing.

Use in the Legal Field

For legal professionals, OSINT may be the key factor in the outcome of a case. Below is a broad overview of some of the most common law-related applications.

Identifying Key Players

OSINT analysts can help lawyers locate and gather information about witnesses, potential plaintiffs, and other key players in a case.


Jane Doe
Free people search website
DOB, aliases, maiden name, current and past addresses, neighbors
Additional residents of current address, names, school district, voting records and political affiliation, Zillow images of home interior, alarm system provider and alarm keypad locations, Google street view images for address, make/model of cars at that address, Tweets and YouTube postings from the latitude and longitude, landlord name, wireless signals from that location and device identification
Google image search of "Jane Doe"
Business card
Email address, employer, job title, work phone number
Images of Jane Doe, spouse, anniversary, children, children's social media accounts, children's birthdays, friends, habits, hobbies, businesses frequented, nicknames, family, family's social media accounts, last location, work schedule, physical characteristics (tattoos, piercings, etc.), high school, hometown
Email address
Additional email accounts
Social media account identification

Using a compendium of tools, techniques, and resources, the OSINT analyst can turn the first informational "hint" into a full dossier of potentially valuable details.

Lay witnesses are often the most difficult to identify and yet essential to a case. Image analysis is one tool used to identify unknown witnesses. Given the popularity of social media and widespread camera use, there are likely photos or video of a potentially crucial event to an active case. But it's very common for people to overlook the information contained in a single image. OSINT analysts can pivot off small details to identify locations, describe the time frame, and name participants.

OSINT analysts can also locate people who lived in a particular area during a specific time frame. Such information can help locate witnesses or find possible plaintiffs in a class action suit.

Finding an expert witness to testify is another use of OSINT research. A more advanced review could reveal significant detail regarding the expert's past work and credibility. OSINT analysts may find incidents of disreputable behavior or details that discredit an expert witness.

Locating people with other shared characteristics, such as particular school affiliations or medical conditions, is yet another use of OSINT research. This can be useful when identifying class action plaintiffs or persons associated with a subject of interest. While traditional skip tracing can assist in locating service of process targets, OSINT techniques go well beyond what is available in standard credit reporting files.

Performing Due Diligence

Anyone involved in acquisitions understands the time and energy required to build a comprehensive dossier on a subject. OSINT research for corporate merger and acquisition activity can help identify assets, historical business changes, high-risk insecure data systems, staff who may be a liability, and fraudulent activity.

For example, analysts may review historical satellite images of a property for evidence of significant structural changes or repairs. If a property has undergone significant updates while the owner claims bankruptcy, this may indicate potential fraud. Social media, such as Tweets originating from the latitude and longitude of a particular address, can also reveal fraudulent activity.

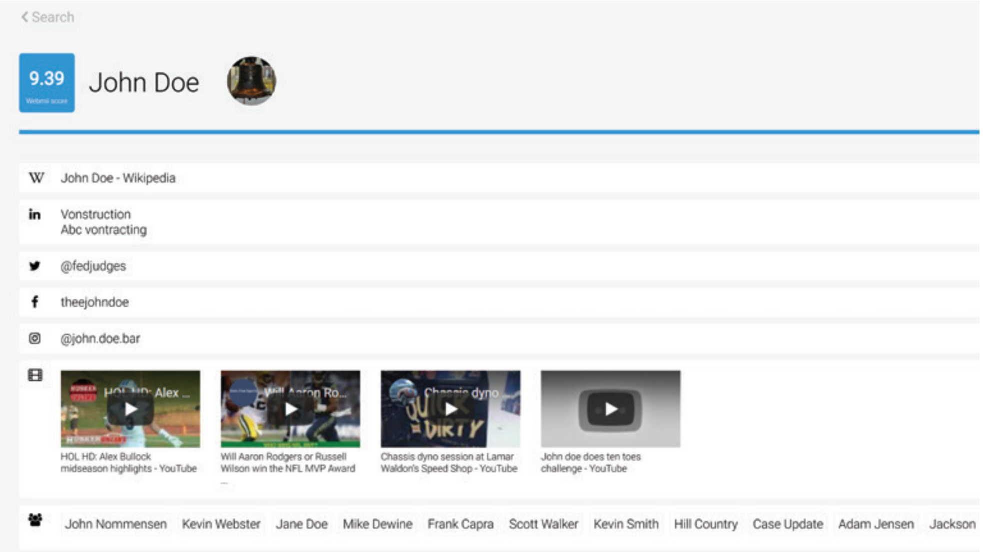
Performing company due diligence is an intensive task, but OSINT analysts can help lighten the load.

Strengthening Security

Securing client data (and the firm's reputation) is a growing concern in the current era of mega breaches and citywide ransomware lockouts. A malicious hacker can take down a company out of spite or for financial gain via crypto-ransomware. But an organization cannot address security issues it doesn't know about.

OSINT research can help identify internal and external security weaknesses so a firm can harden its security posture and reduce the risk of online attacks. Examples of OSINT security risks include:

- company emails in use on the dark web;
- images of physical keys and badges found online;



< Search

9.39 Webmii score

John Doe

- John Doe - Wikipedia
- Vonstruction
Abc vontracting
- @fedjudges
- theejohndoe
- @john.doe.bar
- HOL HD: Alex Bullock midseason highlights - YouTube
- Will Aaron Rodgers or Russell Wilson win the NFL MVP Award …
- Chassis dyno session at Lamar Waldon's Speed Shop - YouTube
- John doe does ten toes challenge - YouTube

John Nommensen · Kevin Webster · Jane Doe · Mike Dewine · Frank Capra · Scott Walker · Kevin Smith · Hill Country · Case Update · Adam Jensen · Jackson

A targeted search for "John Doe" using WebMii.com.

- outdated website security certificates;
- leaked documents with executive signatures;
- former staff revealing sensitive details on internal review forums; and
- open FTP servers, PDF, and DOC files unsecured on company-hosted websites.

Isn't OSINT Just Googling?

Google is a great search engine, but OSINT research goes far beyond Google. To say OSINT is "Googling on steroids" would almost be accurate.

To understand OSINT, one must first understand the limitations of major search engines like Google. Google does not possess the ability to search everything online. The Google search engine works by indexing information it crawls from online sources. The information brought up from a Google search is the result of Google's proprietary algorithm. While the amount of information held in Google's data centers is staggering, it is far from all the information available. A 2014 article estimated that Google had indexed just 4% of the information on the internet.[2]

Typical internet browsing traffic does not wholly exist within Google. You may navigate to YouTube for videos, LinkedIn for the last name of that guy from Sales you only refer to as "Bob," or your Outlook app to check your email. Yet when many internet users start an online search of their digital footprint, the search often begins and ends with Google. OSINT analysts go deeper by using additional analysis tools.

Often, an OSINT analyst will start with a single piece of information, such as a person's name or email address. Pivoting off the smallest details reveals more and more personal information regarding an individual that can be crucial for the subject and any malicious attacker.

Enumerating a target's online presence is another primary task for OSINT analysts, who employ specific techniques and tools for precise account identification. For example, the analyst might use a social media identification site such as WebMii.com to search across a variety of social media platforms. This can lead to coworkers, friends, family, school associations, email addresses, additional businesses, assets, hobbies, patterns of behavior, physical locations for the subject, and more.

OSINT analysts can also help users begin to understand their own digital footprint and the implications of the widespread availability of their personal information. The potential for exploitation of this information is boundless. Every individual and corporation should understand their digital footprint.

Conclusion

The collection, analysis, and identification of publicly available information is the heart and soul of open source intelligence. Beyond a deep understanding of Google capabilities, OSINT analysts flex a wide range of known sites, tools, and techniques to uncover valuable information regarding a subject. As the amount of information online continues to grow, OSINT research will only become more valuable to firms and other businesses. CL

Erin Beffa is an Open Source Intelligence professional at Digital Silence in Denver, where she leads the OSINT Practice. Her expertise in OSINT is well-recognized in the field, including her receipt of a Black Badge as the winner of the NolaCon tech conference's OSINT event. In addition to assisting clients across a wide range of intelligence assignments, she volunteers with the Innocent Lives Foundation, Trace Labs, and Operation Safe Escape. She also works with the National Child Protection Task Force in the search for missing and exploited children.

Coordinating Editor: Joel Jacobson, joel@rubiconlaw.com

NOTES

[1] Because OSINT only searches publicly available resources, the information gained is by definition "public" information. Even if an individual or company expected or preferred that the data remain confidential or private, the OSINT analyst did not transgress any technical (e.g., "hacking" an account) or legal (e.g., Terms of Service violation) barriers to obtain the information, and thus there is no known privacy or other legal breach inherent in the OSINT process. OSINT analysts also understand fundamental evidentiary requirements, and the information located is generally admissible subject to ordinary foundation and hearsay requirements. Similar rules apply for information gathered from the dark web. As long as the researcher follows specific rules of conduct when accessing the data, passive collection of information on the dark web is legal and within the realm of OSINT.

[2] Rosen, "The Internet You Can't Google," *Tennessean* (May 2014) https://www.tennessean.com/story/money/tech/2014/05/02/jj-rosen-popular-search-engines-skim-surface/8636081.