

INVESTIGATING HUMAN RIGHTS VIOLATORS

A primer on how to track down information on individuals and entities in China and Hong Kong



safeguard
DEFENDERS

INVESTIGATING HUMAN RIGHTS VIOLATORS

A primer on how to track down information on individuals and entities in China and Hong Kong

This material is part of

Fighting Impunity: A guide to how civil society can use 'Magnitsky Acts' to sanction human rights violators.

The full guide, ISBN: 978-0-9993706-9-8, is available on Amazon worldwide as paperback, and on Safeguard Defenders website for free as PDF.

Copyright 2020 Safeguard Defenders

<https://SafeguardDefenders.com>

INVESTIGATIVE TECHNIQUES

This section provides information on how to track down data on human rights violators and their businesses. This information has been compiled by corporate due diligence professionals in China and Hong Kong.

1. General

The first step is to build a profile of the perpetrator that uniquely and clearly identifies them. 'Identifiers' help us to confidently identify perpetrators in a Magnitsky filing or any other judicial or regulatory filing.

Collecting identifiers on an individual in China is difficult and risky because as a police state, China is intentionally unclear what is legally public or what is legally private information. In particular, information on officials is often regarded a state secret. Online research can be conducted outside China but it might not be possible to collect a complete list of identifiers online.

Profiling companies or other business entities is usually easier. Publicly accessible official and commercial databases are often enough to accurately identify an organization for judicial filing purposes.

Some 'identifiers' are:

- Their full name (and any variation) – ensure you double check all spellings are correct
- ID and/or passport number
- Name of employer
- Work and home addresses
- Telephone numbers
- Email addresses
- Social media accounts
- Bank account numbers,
- Names of family members

Cost may be a factor in how you decide to go about collecting identifiers. Competent research using free tools and public resources are a low-cost option. Sometimes you may need to pay fees to a commercial search or hire an investigation firm to collect further information to fill gaps.

2. Methodology

Research work will include some or all of the following:

Compile and analyze all the information you already have;

Make a research plan or action plan;

Conduct desktop research, remember to keep a log of each step;

Save all important online information immediately, either as a screenshot or a pdf. Sometimes web pages move or are deleted (and also keep the URL/web-address and mark what time you accessed it);

Make discreet phone inquiries. If necessary, make up an excuse for why you need the information, do not reveal you are planning a Magnitsky submission;

Make discreet field inquiries. If necessary, make up an excuse for why you need the information, do not reveal you are planning a Magnitsky submission;

Analyze all results and write the report.

Maps showing GPS and address of homes, photos of cars or license plate numbers, education background, ownership in any businesses, etc., are all useful information, beyond just name, employer and ID or Passport information. The more the better. Many times the information available will be limited, so the list of identifiers, and other information in this chapter, is a best case scenario, and for you much of this will often be missing.

3. Profiling individuals

In the beginning, you might only have one or two identifiers for the perpetrator, such as their name and their organization name. These are your leads. Gradually gather more information that will allow you to uniquely and accurately identify the perpetrator.

Conduct research in English and in Chinese. You may need to use further languages if the target is connected to a region that uses a different language (for example, Uighur in Xinjiang province).

Don't forget to check if there is a Hong Kong connection to the perpetrator (for example, company incorporation records and real estate information). In this case, remember that spellings in English in Hong Kong generally do not use pinyin Romanization, but one of a number of other Romanization methods. Use the correct spelling to conduct further searches.

Use each new identifier or piece of information on the perpetrator to conduct further research to lead you to additional identifiers. These could be alternative names and addresses, membership in social organizations, names of colleagues or friends, photographs in the media or private social media posts.

Treat everything you find as a new lead. You might come across an online ad or a post in an online forum where the perpetrator has written their phone number (for example a real estate ad or a chat forum about pets or sport). Once you have their phone number, use it as a keyword search term. You will be surprised what it might reveal.

4. Online Tools

Search engines (Clear web). Don't limit yourself to a single search engine. It is vital to use several in each of the languages you are using because different search engines produce different results and therefore different information. Use both Baidu and Google at the very least. If you find a website that is no longer working, visit this site to check earlier versions before it was taken offline.

Deep web searches. Normal search engines like Baidu and Google include only a small part of the information on the internet, maybe as little as 10%. See suggestions for search engines, and a brief explanation what 'deep web' is here.

Dark web searches. This small part of the internet is not accessible to normal search engines, and can only be accessed using the TOR browser, which anonymizes the user. This is the part of the internet with organized crime, weapon selling, drug smuggling, pedophilia and more. Using the TOR browser is very slow, because it needs to hide you, and therefore the dark web is almost only text based, with basic looking discussion forums. Download the TOR browser on your phone or computer. There are several guides out there to help you get started. This wiki entry has a list of various sites and their TOR addresses. You cannot load these pages with normal browsers, you must connect through the TOR network first. You can search the dark web using this special search engine, when in TOR mode.

Mobile phone number trackers. Search for these online and input the phone number. Most tools will tell you the type of number; the carrier; and the location of the phone. <http://www.ip138.com/sj/> - This site will return where an inputted Chinese mobile phone number was registered (location). On the left-hand side of the home page there are many other categories to search. If this website does not help simply search for similar sites using the search term "手机电话查询".

ID number analysis. There are free online tools available that will use an inputted

Chinese ID number and tell you date of birth, gender, and the place where the ID document was issued (which could be the same as where they live). <https://qq.ip138.com/idsearch/> - This site will return the date of birth, residential address and where the ID card was issued from an inputted Chinese ID number. If this website does not help simply search for similar sites using the search term "身份证号码查询".

Chinese Supreme Court database on legal processes. All legal procedures, except those involving National Security or State Secrets should, theoretically, be listed in this database, located here: <http://wenshu.court.gov.cn/>. If the perpetrator is connected to a criminal case in China, there is a chance it may show up in this database.

Criminal litigation documents and judgments from across China. Although it is not comprehensive, and some information has been redacted, it is a very useful resource and the best website of its type. <http://pkulaw.cn/>

Social media. Social media is one of the richest resources we may have on the perpetrator. Search for them on all possible platforms, especially WeChat, and also search using the names of their close colleagues as that may lead you to your target or even further information on your target. Social media platforms are often used as vanity forums. Even some senior officials may drop their guard and post personal information such as contact numbers, email addresses, names of family members and close friends, alumni connections and photos. Dig deep into every detail. Consider opening a ghost account created under an alias to access the perpetrator's account. A good researcher will have many such ghost accounts.

Social media photos (metadata). Download any relevant photo and then check its metadata. Many times people forget to remove such data, and can include time the photo was taken, what phone was used, but also the exact geographic location (GPS coordinates). Can be great to identify someone's location.

Professional platforms. Chinese-

language sites are more common than their English-language counterparts (such as LinkedIn). Search all possible platforms in Chinese and English, as users may post different information on each site.

Recruitment platforms. Online recruitment platforms, such as www.zhaopin.com, are used by employers to post job ads and by job hunters to post their resumes. Resumes often yield phone numbers, addresses and email addresses. Use the job and education history information to search for colleagues, friends and alumni as well as any named referees. Research these too for additional information on the perpetrator. Recruitment platforms usually require prepayment to view and download resumes.

Alumni groups. Once you know which schools the perpetrator attended, search for whether they belong to any alumni associations. Research the association for further information on them. Consider posing as a prospective employer to contact alumni to dig for more information.

ID numbers. Finding the perpetrator's ID number and/or passport number is often the biggest challenge. Here are some ideas that might help you: if you have their address, check the local property register; if they made any legal filings or public record filings (such as a CCTV senior officer filing a regulatory FARA document in the U.S.), check related documents; if they were involved in any court proceedings, check court documents; if the target has ownership or directorial interest in a company, check the company's public files; and if they have children at school, check school documents.

Corporate searches. Chinese officials and state employees often have connections with businesses. It used to be possible to look for company incorporation records and annual filings from the bureaus of the Administration of Industry and Commerce (AIC) with the help of a local law firm. The AIC is also sometime referred to as the State Administration of Industry and Commerce (SAIC) or the Industry and Commerce Bureau (ICB) has recently merged with the State Administration of Market Regulation (SAMR). In recent years, it has been harder to get information from the AIC, mainly

to protect officials. However, the AIC still provides online search options for company registration information, both free and paid, on which information should be available on all firms across China. You should look through records of shareholders or directors and record basic information such as name, address, contact details, and some basic financials. You should be able to see changes in the shareholding structure over the years. However, this may no longer be possible for some companies.

- Search by company name only on this government website. <http://gsxt.gdgs.gov.cn/>. (this website is only available if your IP is inside mainland China, you can use a VPN to connect through a Chinese server.)
- This non-government website consolidates AIC and other corporate information records into a database that is also searchable by an individual's name. This could help you identify corporate affiliations. You will need to register and may also need to pay a subscription fee. www.qichacha.com

If you cannot find the perpetrator from this information, you can also try:

- Prospectuses. These should contain details of all shareholders (including for BVI entities) and for companies listed in China.
- Annual reports. These should disclose family relationships if more than one family member is involved in the company.
- Company reports. Most listed companies must file a report when certain shareholders cross investment thresholds and they should disclose who the ultimate beneficiary is. These can sometimes provide personal information.
- Chinabond.com.cn. This site lists prospectuses for loans, financial statements and other information on many mainland Chinese and Hong Kong companies, including unlisted ones that have been involved in bonds or loans. Sometimes this

- includes information on shareholders. Note that searching this site can be quite time consuming.
- Offshoreleaks.icij.org. This site lists hidden offshore entities. English only.
- Children abroad. Many Chinese officials and state employees send their children overseas to study and also to set up a base through which they can channel assets into real estate or bank accounts for example, in case they ever need to flee China in the future. Research the possibility that the perpetrator has children overseas. You might find their name on assets in Canada or the U.S.

Restrictions

In 2013, due diligence and anti-fraud consultant Peter Humphrey from the UK and his wife were arrested in Shanghai and falsely imprisoned for illegally acquiring citizens' information.

Since then, using the pretext of privacy protection, China has introduced more restrictions on collecting information on officials and it has become increasingly harder to conduct private investigation or due diligence work in the country.

The law was also amended to prohibit the gathering of private information from any source at all, which includes public online sources. This means that any research conducted in China on an individual is at risk of arrest and imprisonment, especially in sensitive cases.

Banned methods. China has made illegal certain investigatory methods once commonly used by private investigators (other countries also restrict these):

- Accessing mobile phone records (calls and texts);
- Tracking someone's location via their mobile phone signal;
- Accessing detailed profiles of individuals from incorporation files;
- Blanket real estate searches using an individual's name;
- Accessing border entry and exit records;
- Accessing client databases from service companies (e.g. airlines);
- Accessing bank records;
- Accessing criminal records

5. Conducting Research from Hong Kong

Hong Kong still has a relatively more liberal environment for conducting investigations and due diligence work despite the steady deterioration of its autonomy and human rights and encroachment on its judicial independence.

In Hong Kong, business licenses can be issued without providing detailed description of business activities. In Hong Kong, private investigation companies are not banned but you are required to apply for a license and comply with privacy laws. There is much more information on public record than in mainland China and so investigations here are easier and much safer.

The public records listed below can be legally accessed after paying a moderate fee, or for free. Visit in person, search the online database or hire an agent to conduct the search for you.

- Directorships. Input the name of the perpetrator to check whether they are an individual or shareholder of a Hong Kong-based company.
- Incorporation records. Kept in a company's registry, these will list the names and addresses of shareholders and directors, and either a complete or partial record of their ID or passport number, and names of company secretaries. The ID number may be a Hong Kong ID or their PRC ID. Access to this information often requires a fee.
- Annual returns. Kept in a company's registry, these will contain updates in incorporation such as changes in shareholding structure, shareholders and directors. Note: The street address of a Hong Kong incorporated company is often a corporate secretarial services company and not an operational address. Also, shareholders of Hong Kong companies are sometimes offshore companies (such as BVI or

Cayman Islands) with the ultimate beneficiary shareholders concealed.

All the above you can search at Hong Kong Companies Registrar (English and Traditional Chinese). The most basic searches are free, but for more details, there are some (very) limited costs involved.

- Hong Kong-wide real estate. You can search against a name to trace property ownership transactions. Usually these only include transactions above a certain value (for example, HKD5 million).
- Real estate ownership. Search for the ownership details of a property.
- Litigation searches. Search judicial registries for litigation records.
- Criminal records. There are privacy restrictions attached to searching criminal records in Hong Kong, but local press report on most criminal trials, so try searching media.
- Marriages and deaths. Limited search is available on records of marriages and deaths.

These searches are best performed by a trained public records specialist and so you may want to hire a search company or private investigation firm based in Hong Kong to help. You may also contact Safeguard Defenders for recommendations.

Additional information that be good to have, but which there are no legal means to get, is for:

- Banking records. Attempting to retrieve banking records in Hong Kong without a court order is a criminal offence.
- Telephone call records. These are protected by privacy laws and obtaining them without a court order is a criminal offence.

INVESTIGATING HUMAN RIGHTS VIOLATORS

A primer on how to track down information on individuals and entities in China and Hong Kong

For more resources, see the full manual:

[Fighting Impunity: A guide to how civil society can use 'Magnitsky Acts' to sanction human rights violators.](#)

For more resources related to this, and many other subjects, see [Publications](#) and [News](#) respectively on Safeguard Defenders website.

Copyright 2020 Safeguard Defenders

<https://SafeguardDefenders.com>