

In this month's Online Research and Intelligence Newsletter, discussion around the use of aliases when conducting online investigations, details on the OSIRA 2nd Annual Global Summit, upcoming TII Training Events and some of the latest resources for the Online Research Professional



Toddington International Inc.
Online Research and Intelligence Newsletter
APRIL 2015 EDITION

IN THIS EDITION:

- [UPCOMING TRAINING: Social Media Intelligence and Investigations](#)
- [FEATURE ARTICLE: "The Name Game" - A Dilemma For Investigators](#)
- [Useful Sites and Research Resources for Online Investigators](#)
- [Article of Interest for Online OSINT Professionals](#)

WELCOME TO THE NEWSLETTER



OPEN SOURCE INTELLIGENCE AND RESEARCH ASSOCIATION

The non-profit Open Source Intelligence and Research Association (OSIRA) is the global leader in OSINT verification and accreditation, industry collaboration and networking, and has been created to share and build upon the decades of knowledge and experience of both its founding Board and its global members.

Bringing together technical and academic industry experts, and experienced OSINT practitioners from the public and private sectors worldwide, OSIRA is dedicated to providing a comprehensive network for research, collaboration, education and industry knowledge sharing.

The [OSIRA Second Annual Global Summit in London on May 7th and 8th, 2015](#) brings together industry leaders and practitioners from around the world, providing key insights into this quickly developing and highly specialized

profession.

Registration is just £300 and the conference promises to be a highly informative event and a great networking opportunity!

Have questions or comments about this newsletter or the services we offer?

Email: contact@toddington.com

Phone: +1 604 468 9222 [UTC -7 hrs]

UK POLICE TRAINING
Internet Research, Intelligence and Investigations

**Avon and Somerset
Constabulary**



Avon and Somerset Police Training and Development Centre
May 5th - 8th, 2015 (4 Days)

Internet literacy and proficiency is now a required skill set for police personnel. Acquiring useful and relevant open source intelligence (OSINT) requires much more than just an ability to surf the web – many valuable sources of intelligence are unknown and untapped by police investigators who simply ‘don’t know what they don’t know’ about finding information online. From routine investigations conducted by frontline personnel to global, tactical and strategic open source intelligence operations, online and social media research and investigation skills are an essential requirement at all levels of an organisation. Aimed at managers, frontline investigators, researchers and analysts alike, this comprehensive five-day training programme will provide detailed instruction in effectively using the internet as an open source intelligence, investigation and research tool and will introduce a number of case studies that will focus on highlighting and correcting some errors that have compromised investigations in the past. With an input on police internet use under RIPA, essential anonymity tools to ensure privacy and security will also be discussed in addition to techniques being used by the criminal element to conceal their identity, location

and illegal behaviour.

Full details and a course brochure available [here](#).

For more information and to book your place on the course [contact us](#).



**SOCIAL MEDIA INTELLIGENCE AND INVESTIGATIONS
JUNE 4TH AND 5TH
VANCOUVER, BC**

A COMPREHENSIVE 2-DAY TRAINING PROGRAM

When it comes to online open source investigations, the vast quantity of information available on social platforms should form an integral part of the overall picture created by open source intelligence gathering efforts.

Real-time, geographically accurate information from a variety of social media and social networks opens up a labyrinth of intertwined relationships, places, interests and possessions that form the nucleus of a myriad of new investigative opportunities.

To recognize, collect and leverage the value of social platform-sourced information, research and investigative professionals must fully understand the limitations, restrictions and legal implications of obtaining, and utilizing, such information in a manner that user privacy expectations, license agreements and other legal limitations are not violated.

Social Media Intelligence and Investigations will introduce research and investigative professionals to a variety of essential tools and techniques necessary to locate, collect and utilize social platform-sourced information, and introduce investigators to the considerations and implications of leveraging this type of information safely and appropriately.

This acclaimed training program will be held at the Pan Pacific Hotel, uniquely located at the heart of Vancouver's downtown waterfront. With the iconic five

sails rising above the Alaska cruise ship terminal and the Vancouver Convention Centre, the Pan Pacific is an unparalleled downtown luxury hotel destination with sweeping views of the Coastal Mountains, Coal Harbour and Vancouver's city skyline, just minutes from the financial district, shopping, theatres, the marina and renowned Stanley Park. Lunch is included and will be served at two nearby, highly regarded restaurants.

Limited Time Special!

Standard Package: ~~\$1,399~~ **\$999**

Premium Package: ~~\$1,899~~ **\$1,399**

[REGISTER NOW](#) [DOWNLOAD BROCHURE](#)

FEATURE ARTICLE

"The Name Game" - A Dilemma For Investigators



Image by Jack Dorsey via Flickr

By Norm Wilhelm

There is a subject of increasing concern out there for investigators, both old and new. As many persons involved in online investigation, intelligence and research will have realized by now, the Internet has reached the point where it is almost impossible to complete a comprehensive online search process without registering for an account on a website somewhere. Because of the way that information needs to be accessed nowadays, a person conducting a comprehensive online investigation, intelligence or research project will need to have registered for accounts on at least a dozen or more websites.

As a result, each of these persons faces the important question: do I use my real name and personal information? Or will I adopt an alias; also referred to as an alternate identity, a proxy name, a pseudonym, or just what it basically is - a false name. The following paragraphs will address this topic in the form of three questions: *is it illegal to use a false name?*; *is it necessary to use a false name?*; and *what guidelines should be followed if I need to use a false name?*

For your average web surfer, this is a personal choice. There are numerous websites that enforce a policy that you must use your real name and personal information to create an account (note the [Facebook website policy](#)). There are also websites that recommend you don't use your real name and personal information in order to protect your personal privacy (i.e. see the [Transition House Association of Nova Scotia](#) website). What your average person decides to do will be based on their ethics, morals, and desire for privacy of their personal information.

On the other hand, using a false name and false personal information is a serious question for a professional working online, regardless of whether it is for investigation, intelligence, or research purposes. We must consider more than personal choices; we must also consider case law, corporate policies, professional standards, and industry best practices. We may end up in a court of law defending those actions when presenting evidence. A lawyer acting on behalf of our client may have to defend our actions in order to keep the evidence admissible in court. Or worse, the decision to use a false name will be the subject of a news media article condemning this method. None of these situations are ideal, and can lead to tough questions that could have been avoided with some forethought. Consider the following examples:

- [Former Miss NY Takes Match.com to court to find out who's stealing her identity](#) (fake name that was a match for a celebrity)
- [Drug Enforcement Agency sued for fake Facebook account](#) (US government

department set up a fake account using the name of a person they arrested)

- [MPI uses Facebook to send court summons](#) (an investigator created a fake account with a fake profile photo to send a court summons)
- [The real story behind Facebook likes](#) (an American university made 13 fake pages on Facebook, with warnings that the pages were fake)

In each of the categories I created for this article (personal, investigative, intelligence and research) I was able to find at least one news article for each category that had been published within the last year (plus an additional article related to research in Canada from 2011). This clearly indicates that the issue of false names, and the public reaction to the use of false names, is significant and treated as an issue of concern by the media and general public. People react strongly to being impersonated, deceived, or (as one article quotes) 'treated like lab rats'. The search results also indicated to me that I would need additional categories to cover false accounts used for criminal activities, gaming activities, and marketing (all of which have their own angles on the subject, but would be outside the scope of this article).

The heightened public awareness is due to many other reasons, the most significant of which are the number of criminals who use false names to commit illegal acts and fraud; the number of cases of identity theft that are reported; and the increasing number of hacks into major organizations that result in personal information being stolen and even posted publicly on the Internet.

So, to deal with this dilemma, we need to ask ourselves some specific questions, starting with question number one: **Is it illegal to use a false name to create an account?** The answer depends greatly on the country you live in, the state or province you live in, your occupation, your employer, and the purpose of your work. And what kind of activities you are doing with that false name.

There does not appear to be a specific federal law in Canada or the US that currently forbids the use of a false name when creating an online account (although many agencies may and do have specific policy relating to this). There are references to it being illegal for specific occupations in specific states to use a false name, but for the most part it appears to depend mostly on what name you use (explained in detail later on).

To stay on the safe side, each individual investigator, analyst, and researcher, should check their applicable federal and provincial/state laws to ensure there is no specific law against their using a false name. I would point out that people have been arrested in the past for using a false name, and it may only be a matter

of time before it happens again.

Focusing more on the law in Canada, examples indicate that you can be charged with a crime for providing a false name to a police officer; for providing a false name when arrested, or for providing a false name in a court of law (meaning it includes any appearance, even if you are only there as a witness). These apparently fall under sections 129 and/or 139 of the Criminal Code of Canada (obstruction of justice). Persons can be charged for crimes if using a false name to deceive the general public or government agencies. It is 'civilly actionable' (meaning you can be sued) to use a false name to advertise a business, represent a business, claim association with a business, conduct financial transactions, or impersonate the name of an actual person - especially with 'intent to benefit'.

More specifically, it is difficult to say when using a false name is actually illegal to use, especially if it is used as part of 'pretext', a subterfuge used to gain information practiced in the security industry in both Canada and the USA. It would take an entire book to list all of the examples, so here are just a few USA examples that demonstrate why it is important to know which laws apply to your state, occupation and company.

- ***Pettinger v Collection Agency Licensing Bureau (1962, California)***, where a collections officer had his license suspended for using a false name.
- ***NAIC Model Privacy Act (1992)***, enacted by over 20 states as of 2004, with an example of the adaptation being Minnesota Statute 72A.493 (Obtaining Information by Improper Means), where '*An insurer, insurance agent, or insurance-support organization must not obtain information or authorize another person to obtain information in connection with an insurance transaction by: 1) pretending to be someone else; 2) pretending to represent a person; 3) misrepresenting the true purpose of the interview; or 4) refusing to provide identification upon request.*
- ***United States v Drew (2006, Missouri)***, where a person named Lori Drew created a false account on MySpace and was later charged with violations of the Computer Fraud and Abuse Act.
- ***Matthew Lacroix (2010, Rhode Island)***, where a person by this name was arrested in 2010 for creating a fake Facebook account under his boss's name, convicted of using false information and fined \$500.

Here are a few more from Canada, in addition to the one mentioned earlier in this article.

- ***Bill C-299, to amend the criminal code as it related to pretext (2007)***; if passed this would have made the use of pretext techniques illegal in Canada.
- ***Individual Objects To Being Photographed By PI Firm 2008 CanLII 58162 PCC (2008, Canada)***, where private investigators are identified as able to use pretext, but cannot identify themselves as lawyers, doctors, firefighters, police officers, bylaw enforcement officers, armed forces officers, government employees, utility workers, or other licensed professionals.
- ***Researchers use fake Facebook profiles to harvest data from thousands of users (07 Nov 2011)***, where a Canadian university used false Facebook profiles to conduct a study, with approval from their ethics board, but still received complaints about from the general public.

It should also be considered that most websites contain a policy or 'terms of use' page that outlines their stance on the use of false names. Many social media websites have policies against the use of false names. While they cannot charge you with a crime, they can shut down your account or block your IP address if they find you have broken their rules, which can become an irritating obstacle to an assignment in progress with a short timeline.

Many modern court decisions recognize that the general public routinely creates alternate identities online, for a variety of reasons that often have nothing to do with attempting to deceive others. This practice is the use of a 'user name', or 'handle', which is not treated the same as a 'false name'. A website that offers the courtesy of a 'user name' is one that is offering an additional level of privacy, and the practice is often allowed in the website policy. You can pretend to be whoever you want, but you can still get into trouble if the user name violates the website policies, or you are regarded as trying to impersonate someone else.

Many websites will expect that a person will use their real name and personal information whether you want to or not, in order to avoid accusations of deceit, fraud, or obstruction of justice. These include the following types of websites: government databases where you must register for an account; websites where a fee is charged for each article or search; any website where payment for services or products requires charges to be placed on your personal or business credit card.

The fourth point I would consider is the effect of a false name on a chain of custody in the preservation of evidence. The use of false names can seriously complicate situations where custody and preservation are questioned, especially

with the current trend of courts demanding more transparency on the part of online investigators. Judges and lawyers are learning that they need to ask more specific questions about evidence that is being found and preserved, specifically where it was found, how they found it, and what method they used to gain access to it.

The second question to consider is: **Do I really need to use a false name to create an account?**

- For those who have been working online as investigator or analyst, there is an 'old school' mentality that abounds on this subject, that online investigation is 'covert' work that requires never identifying who you really are, never using your real name or personal information anywhere online. However, the growing demand for transparency in presenting online evidence in court is forcing these mentalities out of the corners they have been hiding in. Investigators, analysts and researchers are being asked the very question used to title this point: do we really need to use a false name and personal information? If you can't justify it, the truth might be that you really don't need to be using one. A concern for personal privacy does not always trump the demand for transparency and accountability, as has been demonstrated in several court cases in the US and Canada.
- The more common opinion I have heard over the years is that you should use a false name and false personal information if you are using an account for 'work' (usually investigation and intelligence, but also for journalistic research). This is valid to a certain extent, as we have a right to protect our identity so we can do our work, especially if you are doing undercover work in the private sector or with a law enforcement agency. You also do not want the person being investigated to find out from an alert that a specific person from a specific organization was looking at their account. Researchers and journalists also have valid reasons for using false names as people knowing there is a link to a research study or newspaper article may be reluctant to reveal information.
- However, whatever the circumstances, personal opinions are becoming less important. What is more important is what policy does your employer have on the subject? What policy does your client have on the subject? What rules or guidelines does your industry have on the subject? What does case law say on the subject? It is their approval you should seek and your organizational policy should clearly state what is allowed and what is not allowed. If the policy does not cover the issue, it should be brought up as an issue with the decision becoming part of policy that all employees will be expected to adhere to.

- And are you following these rules, guidelines, and policies? In the end, you should always work with the expectation that your results will be disputed in a court of law, and you should be ready to defend your methods, including the use of a false name.

The third question to consider is: **If I do use a false name, what guidelines should I follow?**

Based on the results of the previous two questions, there will still be plenty of investigators, analysts and researchers using false names to work online in the foreseeable future, for valid reasons. There is already a level of bias and distrust from the general public for those who use false names online to do their work, which must be countered by an arguable level of professional standards. In which case, the following are guidelines that should be borne in mind when choosing a false name. Most of these will be common sense, but others will be the source of future consideration.

- A false name used for legitimate purposes should have some element of individuality to it, so that it can stand alone as an online entity, but not so unique as to be a completely different person from yourself. The point should be to obscure your real identity, not appear to be impersonating someone else.
- The false name should be similar to your original name, but with the spelling of the names different enough to avoid your real name and false name from showing up in the same search results, i.e. when you search for your false last name, you shouldn't see results for your real name in the same set of search results.
- If your last name is too unique, make a simplified version of the name using the first or last two syllables.
- The false name should not use your real first name; instead you could use a middle name or old nickname that you don't normally use.
- Your personal information for your false name should not be exactly the same as you would use for your real name, as many people are clever enough to figure out it is the same person but still close enough that you aren't drastically misrepresenting yourself. For example, if you are male, stay a male in your false name. If you are born in 1970, stay within +/-2 years of that date.
- Blank profile photos are always suspicious, so always have some sort of photo, even if its just a generic scenery shot. Use a photo of yourself, not a

photo of someone else, as that can lead to accusations of impersonation. Wherever possible, always use a photo that you yourself have taken, which avoids copyright issues.

- Providing false location information when creating an account or profile for your false name is trickier. Some account creation formats will check your IP location and will not allow you to enter a false location outside of where you actually are. Where possible, if you really live in one place, your online persona should choose a different city. Avoid using a former home address or work address.
- If you are creating user names and emails to associate with a false online persona, remember that these identifiers may eventually end up being looked at in a court of law. Avoid offensive names and slang, sexual connotations, double entendres, or anything that could be viewed as inciting hatred, opining racism, supporting oppression, bias against sexual orientation, or slandering genders.
- False identities related to undercover work should be planned, reviewed and approved of by the authorities in your organization. This ensures that you are abiding by organization policies and/or client guidelines, in the event that you end up presenting your evidence in a court of law.
- Very important - always use unique email addresses for creating new accounts that cannot be linked to your real person identity. There are still ways of seeing on many social media websites which email address the account was created with and choosing one of your real email addresses tends to defeat the purpose of creating a false name.
- Most important - if you are using a false name to conduct an investigation make sure the false name cannot be confused as a person who is real and known to the subject. This violates current civil case law in Canada and in most of the USA. Law enforcement agencies conducting undercover work have much more flexibility in this issue, as long as the organization knows this is happening and has been approved by the appropriate authorities.
- Just as a final check before putting your false name into use, you might want to do a search and check that there are no negative connotations associated with the name you picked. It would be probably be unwise to select a false name that matches an infamous internet personality, character name, or serial killer, and not know about it.

In closing, you can take all the proper precautions, get all the required approvals, and follow all the proscribed guidelines and rules, but you never can tell if something will still trip you up. As an example, there is the story of a Jonathan

Paradis that occurred in mid-2014. In a case of mistaken identity, Mr. Paradis was confused with a criminal having a similar name, despite his protests. This could happen to anyone else with their real name; creating additional false names increases the irony of being mistaken for someone else who is actually being sought by law enforcement agencies (as in [this article](#)).

Norm Wilhelm is a former member of the Department of National Defence. His prior work resulted in his being employed at a number of sites across Canada, as well as traveling to a dozen countries around the world in support of Canadian, UN, and NATO operations. In addition to working with local and federal law enforcement departments, he has also worked with members of numerous foreign intelligence, security and law enforcement agencies. His final position was as the senior political and military intelligence analyst for the Canadian NORAD Headquarters, as well as being a resident subject matter expert on several intelligence and security-related topics. After serving the country for 20 years he retired and subsequently entered the private sector. With a background in intelligence and security operations, information management, and research and analysis, Norm is active in general investigations and open search research at Toddington International Inc.

This article is for discussion purposes only and is not intended to address specific legal concerns nor should it be relied upon as legal advice. Online investigators and researchers should ensure that they are in compliance at all times with the legislation and policies that govern them.



USEFUL SITES AND RESEARCH RESOURCES for Online Investigators

<http://www.uszip.com> - US Zip Code Information

<http://www.mxtoolbox.com> - A useful MX record, DNS, blacklist and SMTP diagnostics site

<http://hashtagify.me> - Social media hashtag search tool

<http://www.heapr.com> - Google, Twitter, Wikipedia and Wolfram Alpha search engine

<http://bunkrapp.com> - Web presentation application (alternative to PowerPoint)

<http://www.myallsearch.com> - Choose from Bing, Google, Dogpile, DuckDuckGo, Ask and other search engines

<https://www.blippex.org> - Search engine based on anonymity

<https://instagr.in> - View Instagram posts, and filter by locations and tags

<https://witkit.com> - Encryption-oriented collaboration platform

<http://twiangulate.com> - Analyze Twitter connections between friends and followers

<https://lastpass.com> - Password manager, compatible with multiple browsers and operating systems

<http://metaki.com/alerts> - Real-time Twitter hashtag alerts

<http://geosocialfootprint.com> - View your geospatial footprint and issues with your current sharing habits

<http://www.digitalattackmap.com> - Digital Attack Map, indexing top DDoS attacks worldwide

<http://goo.gl/U2DWty> - Social Analytics: Chrome extension that allows you to see how many times a page has been shared on social media

<http://map.ipviking.com> - Live map tracks cyber attacks in real-time

https://www.google.com/advanced_patent_search - Google Advanced Patent Search

<http://www.picsearch.com> - Image search engine

[Visual Ping](#): Chrome extension that notifies users of changes to a website

<https://probatesearch.service.gov.uk/#wills> - Search UK wills dating back to 1858

<http://flashchatapp.com> - Chat app for "instant, private and anonymous" messaging

<http://archive.org/web/web.php> - Internet Archive: Wayback Machine

<http://www.tchat.io> - Search Twitter posts via hashtags

<http://ban.jo/search> - Social media content and news aggregator, with "trending events" and other search features

<http://www.oninstagram.com> - Search Instagram users and posts by country

<http://visibletweets.com> - Search tweets by keyword or username (visualized results)

<https://followerwonk.com/analyze> - Analyze a Twitter user's followers

<http://www.cra-arc.gc.ca/chrts-gvng/menu-eng.html> - Registered charity search (Canada)

<http://ctrlq.org/first> - Find out who tweeted it it first

<http://www.flashearth.com> - Flash Earth: Mapping utility with satellite and earth views

<http://keywordtool.io> - Keyword Tool: Provides keyword suggestions for Google, Bing, and YouTube

<http://www.coeverywhere.com> - Search for real-time, geo-tagged social media posts and see what's trending

<https://www.getsafeonline.org> - Online safety resource for protecting yourself, your computers and mobile devices

<http://www.ljseek.com> - Search engine for LiveJournal blogs

<https://sumall.com> - SumAll: All-in-one social media monitoring and analytics

<https://www.tunnelbear.com> - VPN allowing users to avoid access restrictions and browse the internet privately

<https://my.abine.com/#/register> - Blur: Secures the personal information you

share online

<http://privacygrade.org> - Search privacy "grades" for Android apps

<http://www.openwebanalytics.com> - Free, open source web analytics software

<http://www.journalmap.org> - Location-based, scientific literature/research search engine

<https://addons.mozilla.org/en-US/firefox/addon/lightshot> - Easy-to-use and convenient screenshot tool (Firefox add-on)

<http://hola.org> - Security-oriented VPN browser add-on that claims to let users bypass internet censorship & restrictions

<https://getpocket.com> - Save web articles for later viewing

<http://piwik.org> - Open source web analytics platform

<http://www.ssrn.com/en> - Social Science Research Network & e-Library

<http://globaledge.msu.edu> - Global business knowledge resource portal

<http://networking.ringofsaturn.com/Tools/traceroute.php> - Online traceroute tool

<http://blekko.com> - Web search engine and social news platform with categorized results

<http://www.bizdb.co.uk> - BizDb: Free UK companies search (detailed results)

<http://usersearch.org> - Search for a user by username, email address, and more

<http://www.emergent.info> - Website debunking internet rumors in real-time

ARTICLES OF INTEREST
for the Internet Research Professional

[Privacy matters: How to hide and stay invisible on the internet](#)

[The Face Detection Algorithm Set To Revolutionize Image Search](#)

[How social media hashtags work](#)

[How cyber-cops are taking the fight to online fraudsters](#)

[Using Social Media in Immigration Cases](#)

[Lies, Damn Lies and Viral Content: How News Websites Spread \(and Debunk\) Online Rumors, Unverified Claims and Misinformation](#)

[Facebook Can Now Track Online Searches Out of App](#)

[Five Best File Encryption Tools](#)

[How to See If Your VPN Is Leaking Your IP Address \(and How to Stop It\)](#)

["Privacy loss intrinsic": Warnings over smart device privacy](#)

[Our expanding personal profiles compiled from our online activities: "The Moral Hazard Of Big Data"](#)

[Searching for tweets gets easier with Google, Twitter partnership](#)

[More Privacy: Social Media Apps You Should Be Using](#)

[How To Safely Share Passwords With Others Who Need Them](#)

[Child watch: The apps that let parents 'spy' on their kids](#)

[This is how easy it can be to get people's medical information and credit card number](#)

[From the Pew Research Center: "Social Media Update 2014"](#)

[How to hide your online identity with a VPN service](#)

[The Cobweb: Can the Internet be archived?](#)

[Top Big Data and Analytics Trends for 2015](#)

[10 Useful Google Search Tips](#)

[Use this URL to find "in-depth" articles on Google](#)

[Researchers Use Siri to Steal Data From iPhones](#)

[How Facebook Knows You Better Than Your Friends Do](#)

[2015 Trends in Big Data: Real Time](#)

['Silk Road Reloaded' Just Launched on a Network More Secret than Tor](#)

[The Best Tools for Finding Information When Google Isn't Enough](#)

[LinkedIn Search: Finding People and Jobs More Quickly](#)

[Browsing In Privacy Mode Isn't As Secure As You Think](#)

[How Twitter Tracked the French Terror Suspects](#)

[10 Must-Know Instagram Tips](#)

[The Enormous Implications Of Facebook Indexing 1 Trillion Of Our Posts](#)

[How to record your desktop, tablet, or smartphone screen](#)

[Taking Screenshots on Windows, Mac, Android and iOS Devices](#)

["Mac Users: 10 hidden Mac features you might not know about"](#)

["Facebook's New Search Function: Useful or Creepy?"](#)

["The Founder's Guide To Email Security"](#)

["Facebook Now Lets You Search For Specific Posts"](#)

["Blackphone details incoming features for PrivatOS and a new privacy-focused app store"](#)

["What Is End-to-End Encryption?"](#)

[3 Tips to prevent becoming a victim of online fraud](#)

[Rankings of encrypted messaging programs](#)

[Your Twitter history is now public and everything you have ever posted is searchable](#)

["Fitbit activity data as evidence in court"](#)

["Digging deeply": Online search tips for conducting business research](#)

["These Are the Least Secure Messaging Apps"](#)

[ShadowCrypt: "Brings Encrypted Messaging to Facebook, Twitter, and Any Other Website"](#)

[Useful 19 LinkedIn tips and tricks you may not be familiar with](#)

[Organized crime groups utilizing social media to further their interests](#)

["Be Mindful Of What You Post On Social Media: What Goes Online Stays Online!"](#)

[Checking Social Media Privacy Settings: Facebook, Instagram, Twitter, Google+, LinkedIn, & Pinterest](#)

["Make Research Easier With These Five Tools"](#)

["The in-depth guide to using Pocket"](#)

["There's More to Search than Google"](#)

["Using Analytics to Improve Fraud Detection: The Role Big Data Can Play in Real-Time Fraud Management"](#)

["Hidden camera fingerprints link photos to individuals"](#)

["How to Research Your Competition on Facebook"](#)

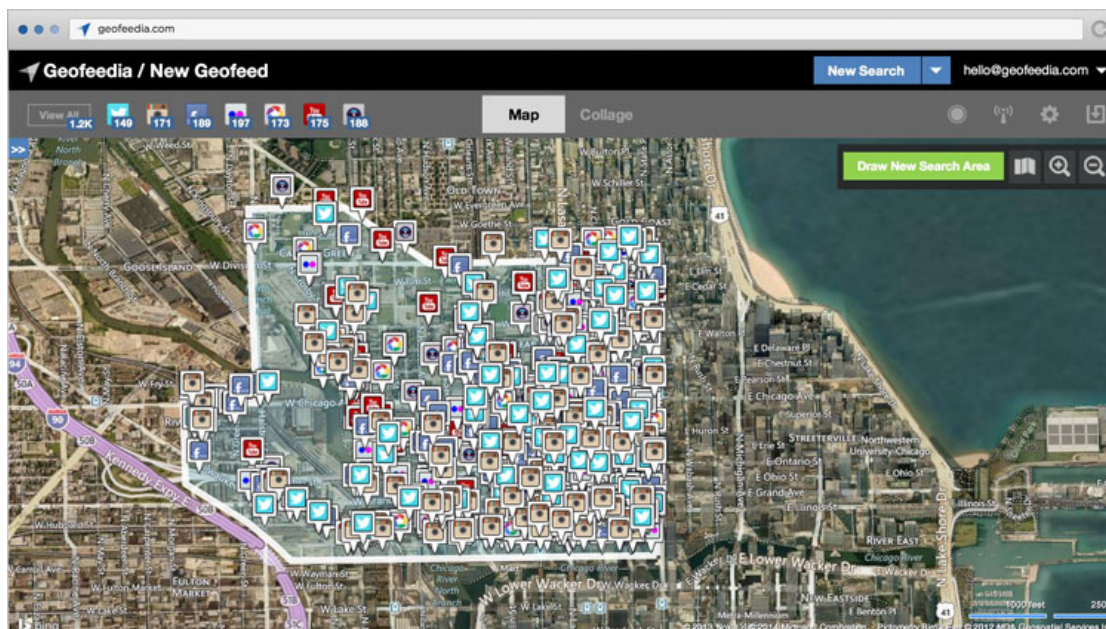
["10 Important URLs That Every Google User Should Know"](#)

The TII Online Research and Intelligence Newsletter is brought to
you by Geofeedia



Location-based Social Media Search, Discovery and Analytics for Public and Private

sector.



About the Internet Research and Intelligence Newsletter

At TII, we are committed to keeping our clients well-informed of the latest developments in Internet Intelligence and Online Research tools, techniques and trends.

If you find the Internet Research and Intelligence Newsletter useful, please feel free to pass it on. If you have suggestions as to how we can improve, or would like to submit an article for publication, [please contact us](#).

To subscribe to the newsletter, simply visit [our website](#).

TII makes all efforts to comply with Canada's Anti-Spam Legislation (CASL). To unsubscribe from this newsletter, please click on the link below or [contact us directly](#).

[follow on Twitter](#) | [friend on Facebook](#) | [forward to a friend](#)

Copyright © 2015 Toddington International, All rights reserved.

[unsubscribe from this list](#) | [update subscription preferences](#)

