

"The success of every one of our customers is our priority and we work diligently to produce and maintain the very best training materials in a format that is effective, enjoyable, interesting and easily understood."

Julie Clegg, President Toddington International Inc



TII Logo

Toddington International Inc.

Online Research and Intelligence Newsletter

JANUARY 2014 EDITION

In This Edition:

Featured Article:

- [Technology and Domestic Violence: New Opportunities and Threats in a Familiar \(and Sometimes Unfamiliar\) Landscape](#)

Upcoming Events:

- [Integrated Internet Investigation Training - Calgary: March 10th - 12th](#)
- [OSIRA Inaugural Conference - London: May 7th - 8th](#)

Resources for Investigators and Intelligence Professionals:

- [eLearning "Using the Internet as an Investigative Research Tool"](#)
- [Useful Sites & Resources for Investigators](#)
- [Also of Interest](#)

TII Online Research and Intelligence Newsletter - January 2014 Edition

In this first newsletter of 2014, we'd like to wish our friends, partners and clients a very happy and prosperous New Year.

In this edition of the Online Research and Intelligence Newsletter, we are pleased to present a comprehensive article discussing the impact of technology on domestic violence investigations written by TII President, Julie Clegg. For almost two decades, Julie has been working passionately to address domestic violence and its effects, first as a police officer and then in her position as President of the Ishtar Transition Housing Society in Langley, BC. Julie regularly speaks on issues relating to technology, violence and threat assessment at conferences and training seminars around the world.

As always, we welcome your comments and suggestions for the newsletter as well as submissions from guest writers. Please feel free to [contact us](#) anytime.

Kind Regards,
David Toddington



Integrated Internet Investigations Training: Calgary - March 10th - 12th

With our [3-day Advanced Intelligence Training Workshops](#) in Vancouver and Toronto almost sold out, we are pleased to announce the [Integrated Internet Investigation Training Conference](#) in Calgary, Alberta on March 10th - 12th, 2014.

Our Calgary conference will allow a high degree of flexibility, with delegates being able to attend one, two or all three training days which they can select based on their needs and requirements.

Day One: Digital Privacy and Security

An engaging one-day, plain-english program that will empower you to take control of your data and communications, and enable you to use a variety of freely available tools to protect your static and dynamic data, as well as your online communications.

Day Two: Social Media Investigations

This comprehensive session 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.

Day Three: Financial Crime Investigations

An essential training program for law enforcement and regulatory agencies as well as private sector firms, this new Financial Crime Investigative Process will assist your organization in being more effective in using online techniques and tools to undertake due diligence activities, ensure compliance, recognize and monitor risk, and identifying corporate vulnerabilities.

Package Options

Bronze

- Access to one pre-selected workshop
- 1 month free trial of TII's Premium Resources Knowledge Base
- 7 hours of OSIRA-recognized professional training credits

Silver

- Access to two pre-selected workshops
- 6 month subscription to TII's Premium Resources Knowledge Base
- 14 hours of OSIRA-recognized professional training credits

Gold

- Access to all three workshops
- One-year complimentary subscription to TII's Premium Resources Knowledge Base (a \$299 value).
- One-year free membership to OSIRA
- 21 hours of OSIRA-recognized professional training credits

Platinum

- Access to all three workshops
- One-year complimentary subscription to TII's Premium Resources Knowledge Base (a \$299 value).
- One-year free membership to OSIRA
- 21 hours of OSIRA-recognized professional training credits
- A Brand new, custom-configured, investigation-ready laptop

[Learn More](#)

The logo for OSIRA (Open Source Intelligence and Research Association) features the word "OSIRA" in a large, bold, dark blue sans-serif font. The letters are set against a solid yellow rectangular background.

OPEN SOURCE INTELLIGENCE AND RESEARCH ASSOCIATION

OSIRA Inaugural Conference - May 7th to 8th, 2014

The Open Source Intelligence and Research Association (OSIRA) 2014 conference is now available for registration. Taking place May 7-8, 2014, at the Royal United

Service Institute (RUSI) in London, this 2-day event is limited to just 100 attendees; interest in this conference has been extremely high and seats are already selling quickly.

In addition to a host of informative speakers, this event will be an outstanding networking opportunity with public and private sector delegates attending from around the world. Early Bird Registration fee is £100 if paid prior to Feb 28, and £150 thereafter.

[Learn More About OSIRA](#)



Technology and Domestic Violence: New Opportunities and Threats in a Familiar (and Sometimes Unfamiliar) Landscape

Issues around family violence often involve complex physical, mental, emotional, financial, spiritual, cultural and sexual dynamics that can result in a kaleidoscope of impulsive actions and reactions from victims.

Those victims with children can also add responsibility, guilt and a heightened sense of fear into the mix and it can be difficult to visualize an effective escape process, never mind an alternate future.

In the "Information Age" we now live in, the use of technology can provide immediate access to myriad of valuable resources that can assist victims of abuse

Case Examples of Technology's impact on Domestic Violence

- *Mother's location in police safe house revealed by geo-tagged app used by child*
- *Woman killed after search history, examined by abusive husband, revealed she was planning to leave him*

who are considering leaving, or have made the decision to remove themselves and their children from their current situation.

Message forums, live online chat groups, social media and networking sites, help lines, non-profit groups, police and victim support, banking and financial advisors, transition houses and lawyers can all be accessed from any computer or internet connected device that the victim has access to, almost anywhere in the world.

Fast, free access to all this information is unprecedented and can be life-preserving; however, ***it can also be extremely dangerous if the victim does not understand the risks that are associated to the technology they are using, if they do not know how to protect their information or if they are not aware of how their children are using the same technology to communicate with others, including, either directly or indirectly, the abusive party.***

In July 2013, the Domestic Violence Fatality Review Committee (Connecticut) identified the Internet as a growing problem for victims of domestic violence, stating, *"Domestic violence offenders increasingly use the Internet, social media and even global positioning systems, to stalk, terrify and monitor their victims"*

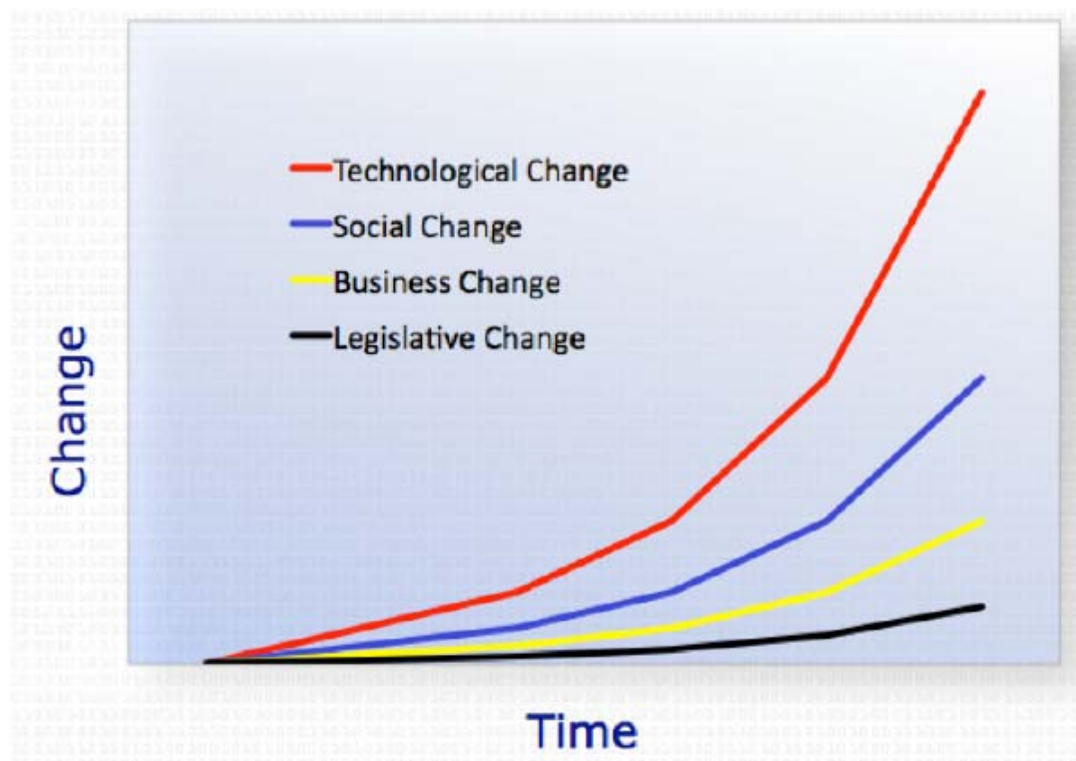
The report went on to state; *"It just keeps getting worse and worse...telephone surveillance, Internet tracking, social media, video cameras, global positioning systems and a plethora of new software is out there."*

The fact that these types of threats now exist highlights the exponential development of technology, and how the methods used in society today for socializing, communicating and recreation are defining a generation gap wider than has ever been experienced before. These issues can make it much more difficult for victims to ask for, and obtain, support from people who understand the many dynamic methods of victimization that may be used against them.

As recently at the 1980's, police were not inclined to get involved in family violence situations at all, deeming them "civil matters"; fast forward a couple of decades and police officers now find themselves dealing with investigations so complex and steeped in digital evidence that they are quickly becoming crippled by information overload and the increasing pace of a technological revolution unlike anything society has ever seen before.

- ***Youth's real-time social media postings reveal violent incident in progress; police respond and rescue victims***
- ***Numerous women endangered as location of transition house, recorded on GPS, discovered by abusive spouse***

No longer can police officers rely solely on “traditional” investigation and evidence gathering practices; frontline investigators must now also be conversant in the use of social media and networks, electronic evidence gathering, forensic examination of computer systems and digital devices, live online communication, and online privacy and security, or important lines of enquiry may be missed altogether, leaving individuals vulnerable to increased and repeated victimization.



The increasing rate of change in technological development is far outpacing the ability of society and business to adapt to rapidly evolving Information and Communication Technologies (“ICT”). Legislative change, and laws designed to deal with emerging technologies, are even further behind – and the gaps are widening.

A significant challenge facing law enforcement is the cumbersome framework they work within; that is, the legal system. A “blunt instrument” at best, legislation is not designed, or structured, to be highly dynamic or responsive to fast-paced change; the processes for creating new case law, processing appeals, and defining digital evidence, are generally slow and unwieldy, meaning that changes to technological capabilities, privacy considerations and rules relating to evidence and disclosure may sometimes become outdated even during a case’s legal process.

In the late 1990’s, while working as a police officer, I attended a domestic assault

on a mother of two young children. The mother had been stabbed a number of times and had fled the home, leaving her two young children behind in the house with her attacker. Over the next few hours, the children were held hostage while negotiators vied for their release in exchange for cigarettes, alcohol and other such items. What was groundbreaking about this investigation? The negotiations were all carried out by cellular telephone.

When I relocated to Canada in 2004 to undertake my current position, Facebook had only just been invented, the term “social media” was used only by a few technological elites, children did not routinely carry cellular phones and most homes were years from their current state, fully networked with WiFi routers supporting a myriad of connected devices. Gathering evidence in cases of domestic or family violence cases revolved around physical evidence; usually photographs of injuries, telephone records and statements from the victim, any witnesses and the perpetrator.

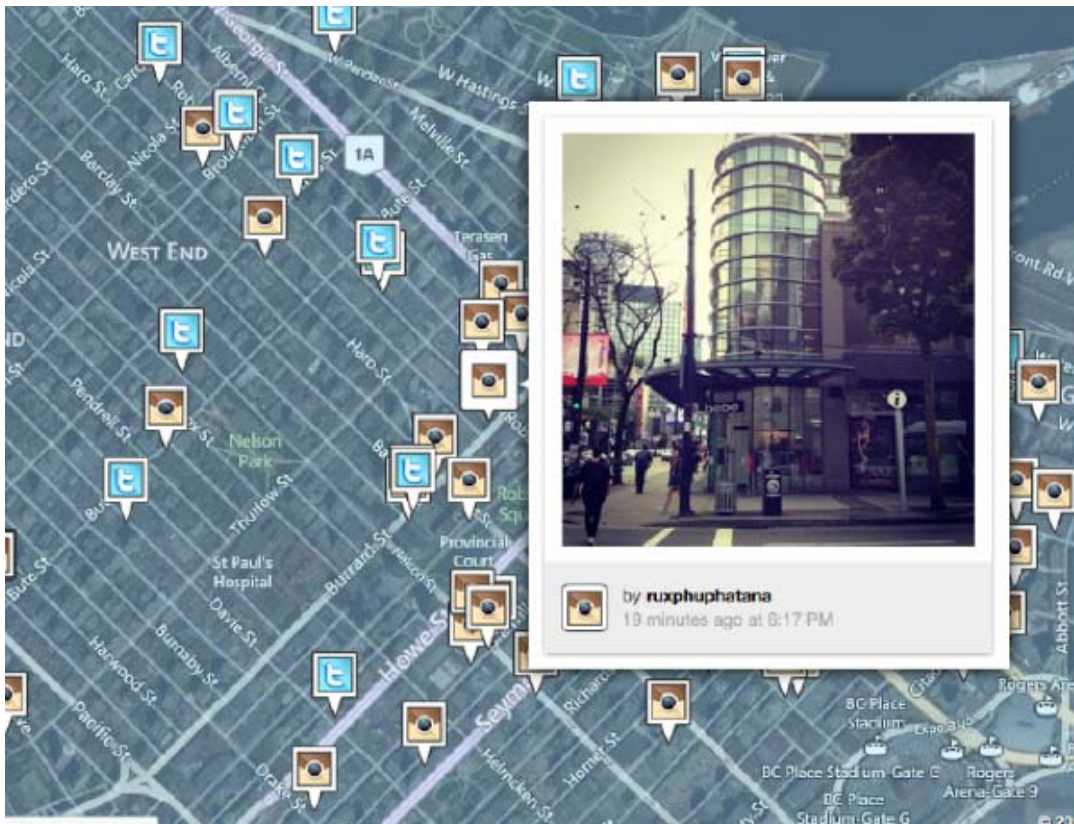
Depending on the specific type of criminality involved, if any of the traditional elements were absent from the available evidence, a case had a very low likelihood of making it to the courtroom and the victim was at risk of being victimized all over again. Many women who had suffered ongoing physical, sexual and emotional abuse failed to speak out, knowing it would be a “word-against-word” situation that they had little chance of “winning”.

In less than a decade, our world has become so digitally connected that most of what we do, both on and off line, is monitored, tracked or linked in one way or another. The majority of us carry recording, tracking and communication devices on our person all the time, in the form of our smart phones. We can use these devices to record the words or actions of another without that person being aware that they are being recorded; we can transmit data automatically using “apps” and pre-configured settings, and we can communicate with others using voice commands that don’t require us to touch our phones at all. These can all be life-saving assets for victims of family violence if used correctly, effectively and surreptitiously.

Conversely, when we use our computers and other devices to search for information online, those machines will typically store information about the keywords we search and the sites we visit. The sites we visit on the other hand, also store a vast amount of information about us that could be used to specifically identify us. Sites such as Google and Facebook gather and analyze so much of our personal information, they are able to present us with targeted, personalized content whenever we visit either their sites or those of their affiliates.

Some of this information can be located and viewed by anyone who has access to the computers and/or devices we use, sometimes whether they know our password or not, depending on how the computer has been configured. Anyone with access to our computers or networks, whether at home or at work, may also be able to view our Facebook status updates, details of our private message and our web based email, without ever gaining direct access to any of those accounts.

If the data that we have control over can be so insecure, what about all the data that we have no control over, such as data generated by others that reveal information about us? When our children access certain applications on their mobile phones, tablets, laptops, desktops or gaming devices, those applications and devices can reveal information about their physical location, their friends, school, family, recreational activities and social networks.



Images can reveal huge amounts of information including time and date of creation, type of device used, and exact geographical location. Sites such as Geofeedia (<http://www.geofeedia.com>) can reveal real-time, geotagged social media postings made from devices with Geo-location services activated, as is often the default setting on cell phones and devices, revealing exactly what was said or seen, at what time, at what location, and by whom.

So what will the future bring in terms of technology and how will it impact family

and domestic violence situations?

In the next couple of years we will see more widespread use of facial recognition technology, mobile interaction devices such as Google Glass and the widespread inter-connection of devices, appliances and processes that will link independent facets of our lives together in unimaginable ways. These changes could go as far as to fundamentally affect how people interact and ultimately, how society functions, as a whole. Would you behave differently if you knew that everything you said and did could be recorded by anyone at any time? Would you feel safer or more vulnerable if your mobile device shared information about you continually? Would you self-censor or would you welcome the opportunity to be heard?

Those victims of violence who are able to understand these technologies, have access to them and utilize them for assistance and protection may find that they are able to remove themselves from dangerous situations more quickly and effectively than ever before, while gathering their own evidence and preventing recurrences of violent situations. Technology can be a very valuable asset in accessing social services, arranging financial assistance and alternative housing, and staying in touch with critical support networks, while maintaining privacy, security and well-being.

For the tech-savvy abuser, they will have an ever increasing array of options to intimidate, victimize and closely watch their targets in ways like never before.

This exponential change and growth in technology is only going to continue, and to expedite. Those that are not able, or inclined, to embrace these changes in technology may quickly find themselves unable to fully participate in society on a number of levels, and those in service industries, that are relied upon to help and advise others, may find that their services become outsourced or even obsolete as they will no longer be in a position to provide relevant, timely and effective assistance to those that need it.

The most effective way forward is to educate those responsible for providing protection and assistance to victims of violence and abuse so they can provide appropriate, accurate advice, ensure evidence is not lost or compromised and help vulnerable victims protect themselves, their family, their property and their livelihood.

Julie Clegg, President

Toddington International Inc.



eLearning: "Using the Internet as an Investigative Research Tool"

The most comprehensive and up-to-date Internet Research e-Learning program available anywhere, "Using the Internet as an Investigative Research Tool" is designed to enable investigators, researchers and intelligence personnel to find better online information, in less time, at less cost, with less risk".

For a fraction of the cost of a classroom based training course, our flexible and interactive virtual classroom environment allows candidates to progress at their own pace and competency level with a qualified personal instructor on hand at all times to ensure success. Initially launched in 1998, this highly acclaimed and continually updated online course has been successfully completed by over six thousand investigators and knowledge workers around the world.

"This information packed course was comprehensive, well-constructed and presented in a format which takes the student through the steps of learning on-line skills at a pace which allows for good understanding of the materials presented. I would highly recommend (and have done) that anybody interested in this area take this course. I was particularly impressed at the balanced and easily understood way in which the various areas were covered. This is a course which someone with a reasonable level of computer skills can take and become proficient in without having to have years of IT expertise, and yet come away with a high level of knowledge of the principles of Online Investigative research. This approach gives the student the confidence to challenge themselves and improve, which is the best recommendation for any kind of course."

(Comment from recent e-Learning attendee)

Group discounts and licensing options for private and public sector organizations are available.

For more information and immediate sign up, visit: <http://www.toddington.com/etraining>

Useful Sites & Resources For Investigators

- <http://shipspotting.com/ais/index.php>
Live AIS & satellite ship tracker
- <http://gwitter.com/>
Fairly intuitive Twitter search tool, searchable by Twitter user
- <http://worldcam.com/>
Worldcam: Great search tool for finding Instagram photos from specific venues
- <http://languagemonitor.com/>
Global Language Monitor for information on words and language use around the world
- <http://whathashtag.circuloajo.es/>
Utility that lets you enter a keyword and find out the most popular related hashtag
- <http://knoema.com/>
Search engine for free data, statistics and visualizations
- <http://crimereports.com/>
Crime reports by location - available for Canada, US & UK
- <http://urlchecker.o2.co.uk/urlcheck.aspx>
Status checker lets you see if a website has been blocked under the new UK internet content regime
- <http://gpsvisualizer.com/geocode>
Utility for converting an address into latitude and longitude coordinates
- <http://geochirp.com/>
GeoChirp: Twitter search by topic and geolocation
- <http://tweetpaths.com/maps>
Map that lets you plot geotagged tweets for a particular Twitter user
- <http://search.nerdydata.com/?homeLogo>
Source code search engine, indexing HTML, Javascript, CSS and plaintext
- <http://twitter.com/search?q=geocode>
Twitter search by geolocation
- <http://telepathwords.research.microsoft.com>

Find out if your password really is as strong as you think

- <http://www2.etown.edu/vl/>
The WWW Virtual Library: International Affairs Resources
- <http://efind.com>
Search engine claiming to allow secure, anonymous and private browsing without tracking
- <http://plagtracker.com/>
Easy-to-use plagiarism checking utility, great for academics and website curators
- [EPI-Search](#)
Find relevant web research resources via related/similar search
- <http://sameid.net/>
Reverse search by analytics IDs (limited to 5 searches per day)
- <http://convoflow.com/>
Real-time social media conversation tracker
- <http://getsyme.com>
Syme - a Canadian-based encrypted social network that allows you to share with only those you decide to
- <http://Bitcoins.com>
Site explaining what a Bitcoin is
- <http://nearbytweets.com/>
Geolocation-based and keyword searchable Twitter monitoring tool that displays local tweets
- <http://monitor.wildfireapp.com>
Social media analytics and monitoring tool
- <http://hshtags.com/>
Social media hashtag search engine
- <http://sharedcount.com/>
Tool for tracking URL shares, likes and tweets
- <http://itpints.com>
Real-time search providing YouTube, Google News, Google Plus, Friendfeed, Reddit, Vimeo and Flickr results
- <http://who.int/research/en/>
World Health Organization's research portal for data and statistics
- <http://tweetbeep.com/>

Utility for receiving Twitter alerts

- <http://symbols.net/>
Website that claims to be "the web's largest resource for symbols, signs and flags"
- <http://lexisweb.com/>
Search engine for researching legal content
- <http://search.motherpipe.com/>
Search engine in beta mode that claims it does not track users or use cookies

Also of Interest

- iBeacons - Coming to a grocery store near you <http://goo.gl/S1DIxe>
- UK Social media statistics from the start of 2014 <http://goo.gl/Dk1yHr>
- 'Narrative Authentication' - An alternative to the password? <http://goo.gl/wvI3PH>
- Online Privacy: We Are The Authors Of Our Own Demise <http://goo.gl/qILEjk>
- The Internet of Things Is Wildly Insecure — And Often Unpatchable <http://goo.gl/a597n9>
- Twitter Map Tracks Users Ringing in 2014 Around the Globe <http://goo.gl/843CwN>
- Facebook allegedly scanned users' private messages, now facing lawsuit <http://goo.gl/4RXSiz>
- Get notified when your password has been stolen <http://goo.gl/4fDikM>
- 2013 Twitter Glossary <http://goo.gl/5QT0Za>
- Perform multiple searches without opening multiple tabs using the web app Searchlet <http://goo.gl/Lw8Fej>
- Deleting one's Facebook activity is apparently not very easy to do <http://goo.gl/9ef4ns>
- Wondering if your Snapchat account information was leaked? Here's how to check... <http://lookup.gibson>
- Latest figures for Pew Research Center's Internet Project <http://goo.gl/VF0uyO>

- Beware: Your 'digital tattoo' will not disappear from the web, says cyber security firm <http://goo.gl/Nohw9r>
- The Evolution of the Password — And Why It's Still Far From Safe <http://goo.gl/ITljE8>
- Hackers Pair SnapChat Numbers with Users on Mass Scale <http://goo.gl/pe8ZpV>
- Study: Facebook is "dead and buried", being replaced by simpler networks <http://goo.gl/GW6D6M>
- 2013 Big Data trends <http://goo.gl/EHwVte>
- Best 2013 Firefox add-ons <http://goo.gl/Dqfz2n>
- Get notifications from websites using only your browser <http://goo.gl/f9yKnb>
- Facebook privacy and user habits <http://goo.gl/vY03Tf>
- According to Stanford Researchers, connecting metadata with usernames is not hard to do <http://goo.gl/YtZ0OT>
- Inside Microsoft's Digital Crimes Unit <http://goo.gl/9fA01B>
- How to set up your browser so all your favorite sites open upon launch <http://goo.gl/Krpybn>
- Using Big Data to combat human trafficking <http://goo.gl/YtohBK>
- Harvard student alleged to have sent bomb threats identified despite using Tor <http://goo.gl/K9O5bX>
- Consider the implications of a facial recognition app for Google Glass <http://goo.gl/oiHFaw>
- The tools helping investors monitor Twitter sentiment and predict changes in the market <http://goo.gl/T7BX0L>
- The most searched-for term on Google UK in 2013 was ... <http://goo.gl/WvqTP2>
- 2013 Google search breakdown: Top 10 trending, "what is", and "how to" searches <http://goo.gl/r5qhjV>
- Bing vs. Google - Five ways Bing is better than Google <http://goo.gl/hwp8Qa>
- Facebook privacy - Three things you should know <http://goo.gl/5dVcYL>
- Great Google Maps feature: Click anywhere on a map to obtain longitude

- and latitude coordinates <http://goo.gl/M1ExVC>
- How much is your private data worth? <http://goo.gl/4VqPZE>
 - A list of the worlds 40 most popular social networking sites <http://goo.gl/qR2DNy>
 - Social media facts for Western Europe <http://goo.gl/DJYcYq>
 - Taking "helicopter parenting" to another level with child tracking smart watch <http://goo.gl/1MsTKs>
 - How has social media evolved over the past 5 years? <http://goo.gl/bRUdAA>
 - Top Bing searches in 2013 <http://goo.gl/S5w1Ta>
 - 16 useful Google Drive tips <http://goo.gl/gJmSKZ>
 - Why we're so bad at picking passwords <http://goo.gl/WfISW6>
 - Inside a Bitcoin Mining Operation in Hong Kong <http://hongwrong.com>
 - Litecoin: The digital currency growing faster than Bitcoin? <http://goo.gl/hMwPm0>
 - Guide to Gmail's latest updates <http://goo.gl/ssw6th>
 - Bing improves image search <http://goo.gl/ocUjYu>
 - Computer uses images to teach itself common sense <http://goo.gl/BwxLk0>
 - Is the intelligence community missing the larger problem, an inability to "think big"? <http://goo.gl/4PTPX8>
 - Security "best practices" vs. what actually works <http://goo.gl/Q5TOax>
 - Definitive guide for Twitter terms and symbols <http://goo.gl/diQv25>
 - Connect, empower, share - Keeping teens safe online <http://goo.gl/apxJqm>
 - Disruptions: A Digital Underworld Cloaked in Anonymity <http://goo.gl/HGiZFC>
 - Using social networks and big data to identify trends in hopes of reducing violence <http://goo.gl/Cstei0>
 - Guide to the invisible web <http://oedb.org/ilib>
 - US judge rules there is no expectation of privacy for P2P data <http://goo.gl/LcB7Zt>
 - Google Flight Search lets you save and access flight information on all of your devices <http://goo.gl/FyVn4E>

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

Copyright © 2014 Toddington International, All rights reserved.

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