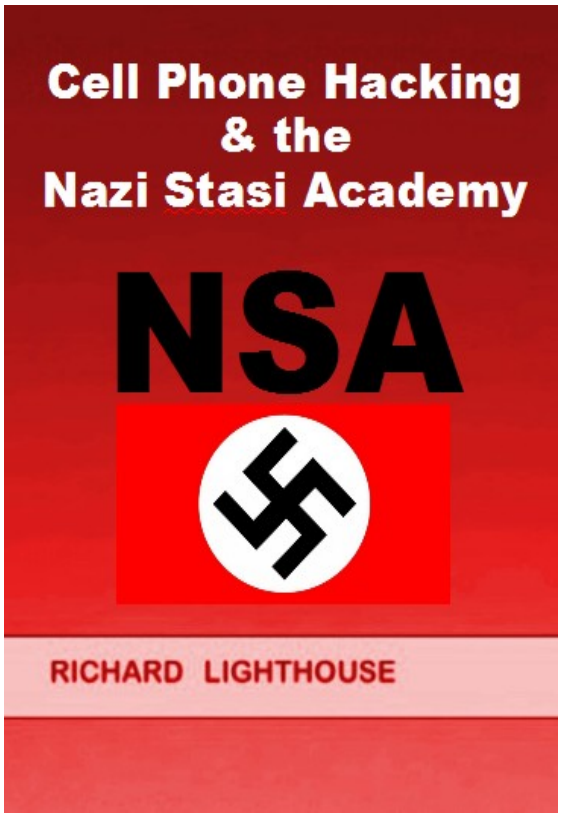

Richard Lighthouse

Cellular Phone Hacking
Published by Richard Lighthouse at Smashwords

ISBN: 9781370681594

efforts in preparing this document, he makes no representations or warranties with respect to the accuracy or completeness of the contents and specifically disclaims any implied warranties or fitness for a particular purpose.

Rev 1b- 22 September 2016
Revision 1c – 22 September 2016
Houston, Texas, U.S.A.

I am a government whistleblower – see my ebooks about the criminal acts of the CIA and FBI. Readers are advised that the NSA may be blocking or restricting access to some of my ebooks, especially outside the United States. Readers are further advised that digital tracking tags may have been placed in my ebooks. Note how slowly the jpg's load into the ebook when viewing. The content of some ebooks may have been altered – still trying to monitor this. If you have tried to contact me, it is possible that emails and phone calls are being blocked (Owenc787 at gmail) 713.three.zero.six.8287

Readers are advised to review the website drjudywood.com which provides compelling evidence about 9-11. Dr Judy Wood and Dr Morgan Reynolds, university professors, filed lawsuits against the US Government for fraud and conspiracy about 9-11. Dr Woods scientific presentation is available at youtube. Readers are also advised to see the movie "Sirius" by Dr Steven Greer, M.D. It is available for free on Netflix, where it is the #1 documentary, and to watch the youtube videos by the Honorable Paul Hellyer, former Canadian Minister of Defense. He has a book titled, “The Money Mafia.”

Also, find my brief educational videos on youtube (Some have been blocked from the search engines).

For more than 4 years, this author has been stalked, harassed, and threatened by US Government agents from the CIA, FBI, and NSA - because of the content of these ebooks. My home has been broken into, repeatedly. In May 2014, my girlfriend was drugged and kidnapped from LaGuardia airport. This is not a joke. My computer, phone, and alarm system have been hacked, including those of my friends and family. It is truly sad and pathetic, these agencies have become criminal organizations. If something happens to me (disappearance, false criminal charges, sudden accident, etc. - my readers can be certain that the FBI and CIA were involved. In my opinion, the Council on Foreign Relations is behind these criminal acts. David Rockefeller is the Chairman.

Cellular Phone Hacking

TABLE OF CONTENTS

Abstract

This short ebook provides some details of cell phone hacking on my iphone. The Internet Protocol (IP) address for the phone is changed on a daily basis. The phone is not shut off. During this entire 30 day period, my phone was physically located in the greater Houston, Texas area. For several days, the IP address showed a location in the middle of Lake Cheney in Kansas. For the Clowns, Idiots, and A*holes, this may be a farcical reference to Dick Cheney, whom is speculated to be the current head of the Majority Intelligence Committee (MAJIC). A table listing the daily changes of my IP address is provided along with the bogus locations. It is likely that the IP address is being altered by the Nazi Stasi Academy (NSA) – a number of recent articles detailing the NSA's obsession with cell phone locations are provided.

Introduction

For more than 4 years, my phone, computer, alarm system, truck, and anything electronic in my possession has been routinely hacked and harassed. The three-letter agencies behind these crimes are seeing the walls quickly close in around them. It is only a matter of time before the global hacker community overtakes these criminals and their agenda. They are outnumbered by a much larger majority.

Cell Phone IP Location for 713.306.8287

The phone and service were both obtained in Houston from MetroPCS, a subsidiary of TMobile. This phone was located in the greater Houston area during this entire period, but the IP address is altered almost every day. On the one day that it shows in Houston – I was never within 10 miles of that location (29.6929, -95.5261). Although this table does not cover every day, it covers the 22 days when I remembered to check it. These 22 days were captured as screen shots to my iphone 5.

Cell Phone IP Locations

IP Address	City	Date	
172.56.16.222	Los Angeles, CA	7/19/2016	
172.56.16.222	Los Angeles, CA	7/20/2016	
208.54.4.254	Ontario, CA	7/21/2016	
172.56.17.2	Universal City, CA	7/25/2016	
172.58.41.44	Spokane, WA	7/26/2016	
172.58.41.33	Kent, WA	7/27/2016	
208.54.4.225	Ontario, CA	7/29/2016	
172.56.16.188	Los Angeles, CA	7/30/2016	
172.56.17.255	Universal City, CA	8/01/2016	
208.54.4.208	Los Angeles, CA	8/02/2016	
208.54.4.208	Los Angeles, CA	8/03/2016	(LA City Hall) 34.0544, -118.2440
208.54.4.208	Los Angeles, CA	8/04/2016	"
208.54.4.211	Los Angeles, CA	8/05/2016	
172.56.17.16	Los Angeles, CA	8/08/2016	
208.54.4.198	Los Angeles, CA	8/09/2016	
208.54.4.198	Tustin, CA	8/10/2016	
172.56.15.106	Houston, TX	8/11/2016	29.6929, -95.5261
172.56.40.31	Los Angeles, CA	8/12/2016	
172.56.40.100	Los Angeles, CA	8/13/2016	
172.56.40.15	Los Angeles, CA	8/14/2016	
172.56.40.15	Los Angeles, CA	8/15/2016	
172.56.40.5	Los Angeles, CA	8/18/2016	

Table 1. IP Location Data. Note that the IP geolocation information was wrong 100% of the time.

Here are the statistics for correct IP geolocation addresses from:

GeoIP2 accuracy by city:

United States 87%- correct 12%- incorrect 2%- unresolved

My IP location was wrong 100% of the time (I was in Pearland, Texas on the morning of 11 August). This is statistically meaningful. Note that the prefix and pattern of the IP addresses are 208 and 172. There is also a noticeable pattern in the daily IP numbers. Based on similar statistics from other providers, it is clear that my IP location is being manually hacked and altered. In my opinion, this is likely being done by the NSA (the Nazi Stasi Academy).

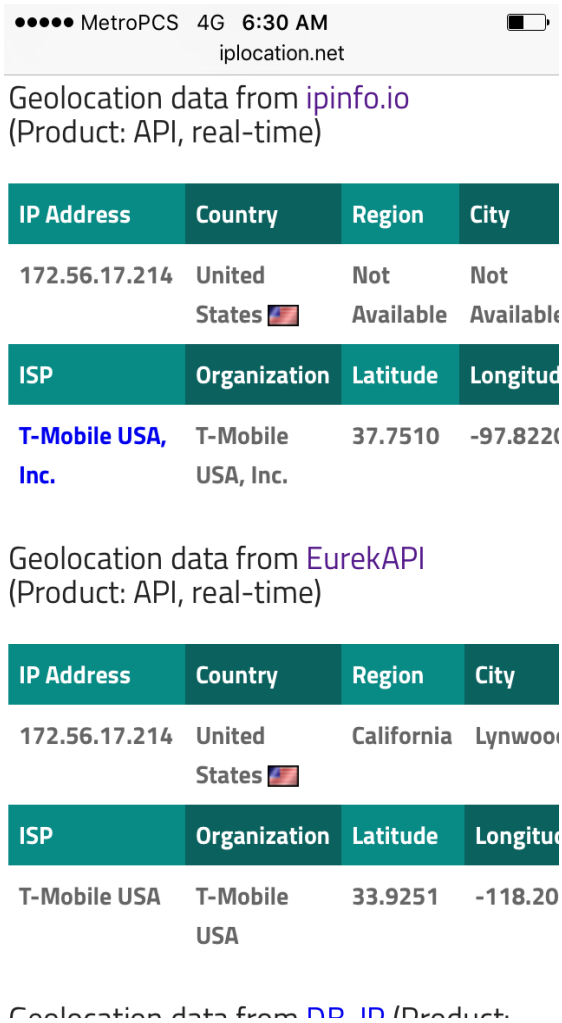

Figure 1. Between 27 August and 31 August 2016, my IP location showed Geolocation data as 37.7510, -97.822; which is in the middle of Lake Cheney in Kansas. Apparently, no cell phone tower has a name there.

Some of the headlines from the Washington Post in 2013, before the newspaper was bought by Jeff Bezos (Amazon):

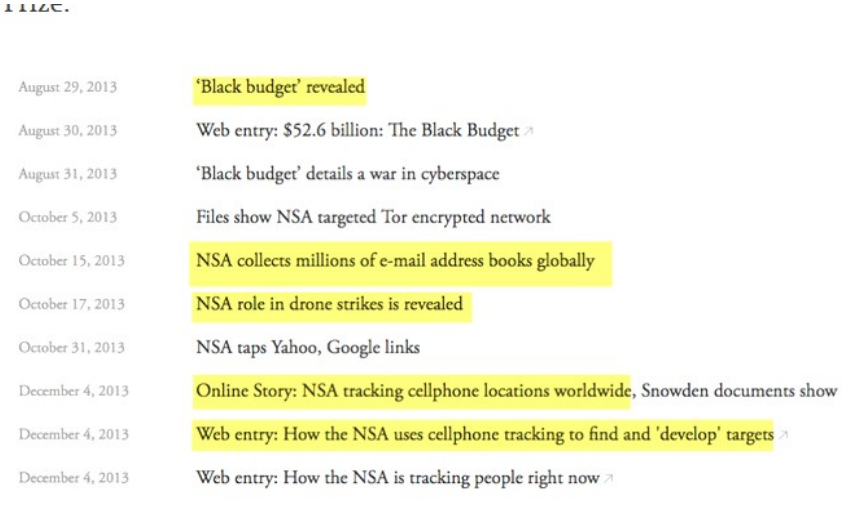

Figure 2. A summary of Washington Post headlines about cell phones and emails from 2013.

Conclusions

This short ebook shows some of the cell phone hacking and harassment that has likely been done by government agencies. In my opinion, the Council on Foreign Relations is behind these criminal acts.

Readers are encouraged to read the associated technical papers at smashwords.com, lulu.com, amazon, barnandnoble, kobo.com, and apple ibooks.

Acknowledgments

Acknowledgments: The author gratefully acknowledges Seth, Jane Roberts, and Rob Butts for their significant contributions.

About: The author holds a Master of Science (M.Sc.) degree in Mechanical Engineering from Stanford University.
Author bio is available at:
www.smashwords.com/profile/view/RLighthouse

Contact:
owenc787@gmail.com 713.three-zero-six.8287
RLighthouse1 –at- fastmail point fm

Funding:
This research was generously supported with a grant from the Foundation Opposed to Academic Puffery (FOAP).

References

This is a living document. The author reserves the right to make corrections and changes.

1. Richard Lighthouse, CIA Agents in Camp Logan Neighborhood, Smashwords.com; 2016.

2. Richard Lighthouse, CIA Offices, Smashwords.com; 2016.

3. Richard Lighthouse, Presidential Directive 51 & FEMA Prison Camps, Smashwords.com; 2016.

APPENDIX

All Washington Post articles:

1. NSA tracking phone locations on 'planetary scale'

Documents obtained from Edward Snowden show the agency tracks most cellphone users worldwide.
Max Ehrenfreund | National Security | Dec 5, 2013
The National Security Agency is monitoring the locations of most of the world's cellphones, examining billions of records daily in an effort to identify associates of surveillance targets, Barton Gellman and Ashkan Soltani report. Documents describing the bulk collection were given to The Washington Post by former NSA contractor Edward Snowden. Senior intelligence officials said that the program, known as CO-TRAVELER, does not operate inside the United States, but U.S. cellphones used abroad are visible to the system. The NSA has little interest in most of the world's population, but it collects information about where they are anyway to identify people who may be associated with those who the agency believes are dangerous:

2. Agencies collected data on Americans' cellphone use in thousands of 'tower dumps'

Law enforcement made more than 9,000 requests last year, a congressional inquiry has revealed.
Ellen Nakashima | National Security | Dec 8, 2013 Federal, state and local law enforcement agencies conducting criminal investigations collected data on cellphone activity thousands of times last year, with each request to a phone company yielding hundreds or thousands of phone numbers of innocent Americans along with those of potential suspects. Law enforcement made more than 9,000 requests last year for what are called "tower dumps," information on all the calls that bounced off a cellphone tower within a certain period of time, usually two or more hours, a congressional inquiry has revealed.

3. How the NSA uses cellphone tracking to find and 'develop' targets

December 4, 2013 3:04 PM EST - The National Security Agency gathers location data from around the world by tapping into the cables that connect mobile

networks globally and that serve U.S. cellphones as well as foreign ones. (Osman Malik / The Washington Post)

4. NSA tracking cellphone locations worldwide, Snowden documents show

By Max Ehrenfreund December 5, 2013
The National Security Agency is gathering nearly 5 billion records a day on the location of cellphones around the world. Ashkan Soltani, a Washington Post contributor and an independent privacy and security researcher, sat down with The Post's Alice Rhee to explain. (Thomas LeGro/The Washington Post) The National Security Agency is monitoring the locations of most of the world's cellphones, examining billions of records daily in an effort to identify associates of surveillance targets, Barton Gellman and Ashkan Soltani report. Documents describing the bulk collection were given to The Washington Post by former NSA contractor Edward Snowden.

5. NSA address book spying in one FAQ
The NSA is sweeping up the contact information of thousands of Americans. Here's how they do it.
Ashkan Soltani | Business | Oct 14, 2013
The NSA is engaged in bulk collection at key internet access points controlled by foreign telecommunications companies and allied intelligence services. Slides show that the information is being collected from at least 18 collection points known as "SIGADs" or Signals Intelligence Activity Designators. The documents and intelligence officials say all the collection of contact information takes place outside U.S. territory. But the distributed nature of modern web infrastructure means that communications between an American user and a U.S. webmail provider (such as Google) could still flow outside the United States, where there are fewer legal restrictions on NSA surveillance. The contact lists of Americans also cross the NSA's international collection points when they live or travel overseas.

6. NSA collects millions of e-mail address books globally
October 15, 2013
The National Security Agency is harvesting hundreds of millions of contact lists from personal e-mail and instant messaging accounts around the world, many of them belonging to Americans, according to senior intelligence officials and top-secret documents provided by former NSA contractor Edward Snowden. The collection program, which has not been disclosed before, intercepts e-mail address books and "buddy lists" from instant messaging services as they move across global data links. Online services often transmit those contacts when a user logs on, composes a message, or synchronizes a computer or mobile device with information stored on remote servers. During a single day last year,

the NSA’s Special Source Operations branch collected 444,743 e-mail address books from Yahoo, 105,068 from Hotmail, 82,857 from Facebook, 33,697 from Gmail and 22,881 from unspecified other providers, according to an internal NSA PowerPoint presentation. Those figures, described as a typical daily intake in the document, correspond to a rate of more than 250?million a year. (The article features a video of President Obama boldly stating that the NSA is not collecting American's emails.)

*Using the NSA's logic, that American's emails are only "incidentally collected and not targeted" - if you shoot someone with a gun incidentally, so long as you didn't target them, you haven't violated any laws or Constitutional Rights.