Written Testimony of

Detective Sergeant Ben A. Finley
Johns Creek Police Department – Johns Creek, Georgia

Before the House Committee on Energy & Commerce
Subcommittee on Communication and Technology
"A Legislative Hearing on Seven Communications Bills"

April 13th, 2016

Chairman Walden, Ranking Member Eshoo and Members of the Subcommittee: My name is Detective Sergeant Ben A. Finley from the Johns Creek Police Department in Johns Creek, Georgia. I am a 20 year veteran of law enforcement and I am currently the Supervisor of the Criminal Investigations Division in my department. The majority of the crimes I investigate are internet/cyber related crimes. Over the last couple of years I have had quite a bit of experience and success investigating Swatting/Hoax 911 calls in which Spoofing technology was utilized.

First let me say it is both an honor and a privilege to be here before this committee this morning to provide testimony on this important issue. Some of the issues I will speak on today will include swatting/hoax 911 calls and the use of spoofing technology. Before we start I want to make sure everyone understands exactly what I'll be talking about.

Swatting/Hoax 911 Calls: This is the act of calling and deceiving an Emergency Service/ 911 Center with the report of a false report of an ongoing critical incident. The calls usually contain reports of Active Shooters with multiple people dead or injured- Persons held hostage – Bombs/ IED's and threats to fire upon and kill law enforcement upon their arrival. Calls of this nature not only require a large law enforcement response but it diverts other critical resources as well. No one is immune from these acts from Hollywood celebrities – Members of Congress and just regular everyday people.

Call Spoofing: Caller ID "spoofing" occurs when a caller deliberately falsifies the information transmitted to your Caller ID display to disguise their identity. Spoofing is often used as part of an attempt to trick someone into giving away valuable personal information so it can be used in fraudulent activity or sold illegally. It is also used in many Swatting/Hoax 911 calls. There are some legitimate uses for spoofing numbers such as a business like a domestic violence shelter, rape crisis center etc. Some spoofing services even offer the ability to disguise and change your voice from male to female and add background noises.

IP Spoofing: IP Spoofing is a technique used to gain unauthorized access to machines, whereby an attacker illicitly impersonates another machine by manipulating IP packets. IP Spoofing involves modifying the packet header with a forged (spoofed) source IP address, a checksum, and the order value. Internet is a packet switched network, which causes the packets leaving one machine may be arriving at the destination machine in different order. The receiving machine resembles the message based on the order value embedded in the IP header. IP spoofing involves solving the algorithm that is used to select the order sent values, and to modify them correctly. (Source: iplocation.net)

Example #1:In 2014 I was the lead investigator in a multi-state and international swatting investigation that involved a serial swatting suspect who had swatted 40+ cities in the US and Canada. This individual had terrorized multiple families all over the USA and was responsible for hundreds of thousands of dollars of wasted time and resources by local and federal law enforcement officers responding to these fake incidents. He used VoIP (Voice over Internet Protocol) phone services (Skype – Google Voice etc.) anonymizer websites, spoofing technology and multiple email and social media profiles to hide himself.

During my investigation I was able to link this one individual to all of these swatting cases here in the United States. I also uncovered the fact that my suspect lived in Canada. I then contacted the FBI Atlanta Field Office- Cyber Program to get their assistance. With the help of FBI Atlanta we contacted the Royal Canadian Mounted Police in British Columbia, Canada and coordinated our efforts to stop this individual. We found out the suspect was very well known to them as well for swatting in their country.

After all the legal aspects were worked out between our two countries, the Canadian Crown Counsel (Canadian Courts) agreed to have our cases transferred to them for prosecution of the suspect. The suspect was then arrested and charged in their court system with our offenses as well as the charges he faced there in Canada. The suspect eventually pleaded guilty to a majority of the counts against him and was sentenced to jail time in Canada.

Example #2: During the same time period I was investigating another Swatting/Hoax 911 incident involving an individual from the North East United States. In his swatting hoaxes he was used several layers of spoofing technology. He started with a spoofing phone app that he ran through his own personally created spoofing website and then onto a nationally known spoofing company. He also incorporated VoIP (Voice over Internet Protocol) phone services as well (Skype-Google Voice etc.). As you can imagine, it took quite some time to sort through all of this and get to the offender. Along with this multi layered spoofing, the suspect had also used voice disguising software to alter his voice in hopes that he could remain undetected. All of this spoofing technology allowed him to do multiple swatting/hoax 911 calls all over the country until he was finally identified.

Some of these spoofing companies and anonymizer websites that these individuals use are located in foreign countries that have none or very limited data retention policies. They maintain no logs of the users; they accept untraceable currency (Bitcoin – Darkcoin etc.) and are generally non-compliant with any request from law enforcement requesting user logs and records.

During my investigations I have traced these individuals to countries such as Russia, Germany, Amsterdam, Hong Kong any many others.

Even if we have an MLAT (Mutual Legal Assistance Treaty) with that nation, it is still a very difficult task to get the information you need in a timely manner.

Victim Impact of Swatting: Most of the time the news coverage on Swatting/Hoax 911 calls deals primarily with the call that was received, the alleged incident that was reported and the amount of Police, Fire and EMS equipment that responded to the fake call. In a lot of these cases there are real victims that suffer some intense emotional distress and trauma.

In one of the swatting incidents I investigated, a male caller called into our 911 center and said "**Alright, I killed the Mom, I killed the Dad and I killed the little boy in the house. I got the little girl right here. " I … I need $30,000 dollars or I'm killing her too".**

The only people present in the home that day were a Nanny and babysitter. There were two small children in the home at the time of the swatting call. Mom and Dad found out by friends calling them and telling them they saw on the news where something horrible had happened at their home. Imagine as a parent you get that call and you rush home thinking that your entire family has been killed. You arrive and see multiple Police vehicles lining your street. Officers with rifles pointed at your house. EMS crews with stretchers out in the street beside the ambulances on standby for casualties.

I was there and saw the Mother as she was running through neighbor's yards trying to get to her home. She was in a panic, totally distraught with a look of horror on her face. We had to physically restrain her and tell her that her children were fine and they were sitting in the back of our Fire Chief's vehicle. To see the raw emotion pour out of that woman as she embraced her children and sobbed out loud affected every one there. That's when you realize the impact that these swatting hoaxes can have on its victims. It truly makes you angry to know that someone did this for fun. It motivates you to want to find the person who did this act. It also makes you wonder what type of person would derive some type of enjoyment out of doing this to people.

There are quite a few other crimes I have investigated that involve criminals using spoofing technology to scam citizens out of their money and personal identifying information.

IRS Scam: This is the one that is the most prevalent this time of year. Scammers will call unsuspecting people and claim to be IRS agents and tell the victims they have outstanding tax debts and they have to be paid now to avoid jail time, deportation etc. The scammers will usually have the victim's last name and last four of their Social Security number which will further convince the victim the call is legitimate. Also if the victim checks the number that appears on their caller ID they will find that the number is a real phone number to the local IRS division. The criminals use readily available spoofing phone apps and spoofing websites to further their criminal activity by making the legitimate number appear on the victim's phone.

Arrest Warrant Scam: This is a growing scam that is reaching victims all over the country. The victim will receive a phone call from a person who impersonates being a local police officer from the victim's home area. The phone number that appears on the potential victim's phone will be a legitimate number to their local Police or Sheriff's Office from their area. The Police Impersonator will then tell the potential victim there is an arrest warrant out for them for an unpaid debt, missed jury duty or some other infraction. The Impersonator claims they can get the warrant dismissed if the victim will send the fine amount by Western Union or Green Dot Card. After the victim realizes they have been scammed it is too late. This is yet another instance in which criminals use phone spoofing apps and spoofing websites to further their criminal enterprise.

These are just a few examples of criminals that utilize spoofing technology to facilitate their crimes.

I hope this has given you a little better understanding of what all goes on in these situations.
These are not harmless "pranks' as some may describe them. When you see the toll it takes on families that have gone through some of the situations you will understand.

We do need good legislation to deal with this issue. As our technology increases so will these incidents. It is important to note that criminals will always update their techniques to use the most recent technology to help further their criminal enterprise. They will always use and abuse any new technology to help them exploit companies or people. At the end of the day the American people are going to look to both of us for help. They'll look to people like you to make the laws and to people like me to enforce them.

I thank you for your time today and again for the honor and privilege of being here to speak to this committee on this legislation. Thank you.

Sergeant Ben A. Finley

Johns Creek Police Department- Georgia