The Lone Wolf
Technical Journal
Volume 1 Issue 1
April 6, 2010

This issue contains:

Executive Summary of an FBI Law Enforcement Bulletin on secret recordings of suspects.

Whether in a prison cell, interrogation room, or the back seat. of a police car, suspects left seemingly unattended with a co-conspirator, friend, or total stranger often seize the opportunity to discuss or lament their current predicament. Very often, incriminating statements are made. Law enforcement officers who put themselves in a position to hear and record suspects' conversations, either by planting a listening device or by posing as a co-conspirator, friend, or stranger, are apt to obtain very valuable incriminating evidence.

The surreptitious recording of suspects' conversations is an effective investigative technique that can withstand both constitutional and statutory challenges. Law enforcement officers contemplating the use of this technique should keep the following points in mind:

1. Because the technique does not amount to "interrogation" for purposes of Miranda, it is not necessary to advise suspects of their constitutional rights and obtain a waiver prior to using this technique.

2. To avoid a sixth amendment problem, this technique should not be used following the filing of formal charges or the initial appearance in court, unless the conversation does not involve a government actor, the conversation involves a government actor who has assumed the role of a "listening post, or the conversation pertains to a crime other than the one with which the suspect has been charged.

3. To avoid both fourth amendment and title III concerns, suspects should not be given any specific assurances that their conversations are private.

4. Law enforcement officers should consult with their legal advisors prior to using this investigative technique. This will ensure compliance with State statutes or local policies that may be more restrictive than the Federal law discussed in this article.

In any subsequent prosecution, the government is likely to be confronted with a vehement constitutional and statutory attack to the admissibility of such damaging evidence. Specifically, the defense is likely to argue that the surreptitious recording of the suspects' conversations violated fights guaranteed by the fourth, fifth, and

sixth amendments to the U.S. Constitution, as well as certain protections afforded individuals under Title III of the Omnibus Crime Control and Safe Streets Act.(Crawford, 1993)

To be successful, a challenge to the admissibility of surreptitiously recorded conversations based on the fifth amendment self-incrimination clause would have to establish that the conversations in question were the product of unlawful custodial interrogation. Because statements made to individuals not known to the defendant as government actors do not normally amount to interrogation for purposes of the fifth amendment, this challenge is destined to fail. (Crawford, 1993)

Stanley v. Wainwright is one of the original cases to deal with a fifth amendment challenge to the admissibility of surreptitiously recorded suspect conversations. In Stanley, two robbery suspects were arrested and placed in the back seat of a police car. Unbeknownst to the suspects, one of the arresting officers had activated a tape recorder on the front seat of the car before leaving the suspects unattended for a short period of time. During that time, the suspects engaged in a conversation that later proved to be extremely incriminating. (Crawford, 1993)

On appeal, the defense argued that the recording violated the rule in Miranda. The Court of Appeals for the Fifth Circuit, however, summarily dismissed this argument and found that the statements were spontaneously made and not the product of interrogation. Miranda warnings are unnecessary if the suspect is conversing with someone who either is, or is presumed by the suspect to be, a private individual. Because suspects in this situation would have no reason to believe that the person to whom they are speaking has any official power over them, they have no reason to feel the compulsion that Miranda was designed to protect against. (Crawford, 1993)

In Kuhlmann v. Wilson, the Supreme Court held that placing an informant in a cell with a formally charged suspect in an effort to gain incriminating statements did not amount to deliberate elicitation on the part of the government. In doing so, the Court made the following statement:

"Since the Sixth Amendment is not violated whenever--by luck or happenstance--the State obtains incriminating statements from the accused after the right to counsel has attached,' a defendant does not make out a violation of that right simply by showing that an informant, either through prior arrangement or voluntarily, reported his incriminating statements to the police. Rather, the defendant must demonstrate that the police and their informant took some action, beyond merely listening, that was designed deliberately to elicit incriminating remarks."

As a result of the Supreme Court's decision in Kuhlmann, the mere placing of a recorder in a prison cell, interrogation room, or police vehicle will not constitute deliberate elicitation by the government. Instead, to raise a successful sixth amendment challenge, the defense has to show that someone acting on behalf of the government went beyond the role of a mere passive listener (often referred to by the courts as a "listening post") and actively pursued incriminating statements from the suspect. Anyone in police custody should beware of hidden cameras and tape recorders in: Back seats of police cars, Prison Cells and Interrogation rooms. (Crawford, 1993)

Police can legally record a suspects conversation with anyone other than a policeman without a miranda warning and without notice. Whenever your in a government controlled environment, KEEP YOUR MOUTH SHUT! Being put in the same area as a co-defendant is a well known and documented police tactic.

Crawford, K. (1993). Surreptitious recording of suspects' conversations. *FBI Law Enforcement Bulletin*, *62*(9), 7.

A technical overview of "Red Boxes" and their use in theft of telecommunications service.

Telephone hackers, commonly called "phreakers" have been manufacturing a device for years allowing them to avoid paying for long distance telephone calls. This device is commonly called a red box. The device exploits the lack of a tone filter on the payphones microphone.

Specifically the red box generates tones are a combination of a 1700 Hz & 2200 Hz tone played together. One 66 ms tone represents a nickel. Two 66 ms tones separated by a 66 ms interval represents a dime, and a quarter is represented by five 33 ms tones with 33 ms pauses.

Red boxing relies on the ACTS system, to ensure the ACTS system is used, dial 1010288 immediately before dialing 1 and the number with the area code. This will manually select AT&T as your long distance provider. Other long distance selection codes will work, the phreakers sole goal is to have the ACTS system handle the payment.

Courtesy of Phrack Magazine, the following is an explanation of the most common piece of hardware used during the 1990's to generate red box tones.

> To make a Red Box from a Radio Shack 43-141 or 43-146 tone dialer, open the dialer and replace the crystal with a new one.
> The purpose of the new crystal is to cause the * button on your tone dialer to create a 1700Mhz and 2200Mhz tone instead of the original 941Mhz and 1209Mhz tones. The exact value of the replacement crystal should be 6.466806 to create a perfect 1700Mhz tone and 6.513698 to create a perfect 2200mhz tone. A crystal close to those values will create a tone that easily falls within the loose tolerances of ACTS.
>
> The most popular choice is the 6.5536Mhz crystal, because it is the easiest to procure. The old crystal is the large shiny metal component labeled "3.579545Mhz." When you are finished replacing the crystal, program the P1 button with five *'s. That will simulate a quarter tone each time you press P1. (Voyager, 1995)
>
> *Note from author, the "P1" button refers to the speed dial "number one". Using speed dial ensured your tones were played at the proper speed. Additionally, when using a 6.5536 Mhz crystal the batteries must be fresh. Dying batteries will generate an audible tone, however the tone will not meet ACTS specifications and will not work.

Red boxes are currently effective at circumventing standard payphones in the United States. While some electronics manufactures have sold microphone filters designed to eliminate the use of a red box through the microphone, the use of a red box is relatively rare and the installation of countermeasures would not be cost effective for the phone company. The advent of cell phones has

somewhat phased out this interesting device however, it is still a viable method for obtaining free telephone calls at payphones.

Additional information is easily found online, phonelosers.org a group specializing in phreaking is still operating as of 2010 and their website offers detailed information. In the event a particular payphone has a muted or filtered microphone it is possible to still use your red box by splicing onto the telephone line entering the payphone, thus bypassing the filter. Considering the effort, it would generally be easier to find another payphone.

Voyager (1995). The #hack faq. Phrack Magazine, 6(47), Retrieved from http://www.phrack.com/issues.html?issue=47&id=6

Burglar tips from professional burglar Jack Maclean

Did you park in the driveway of the place you burglarized, in front of the residence, get dropped off, or park a distance away?

A. Seventy-two percent said that they parked a distance away, which is why you always want to call the police every time you see somebody in front of your condominium, townhouse, or residence who walks completely away from the area after parking. That's what I used to do when I just got started. This is why the police always check out cars parked in shopping mall lots after hours. Burglars think nothing of parking somewhere, and then walking a couple of miles or so, eventually working their way back to the car. If you ever see anybody park on the side of the street between your house and the next one, and walk down the street, call the police. When they arrive they will run the car license through the computer. If it's stolen or looks suspicious for any reason, they will put a stakeout team on it and wait for the culprit to get back and question him. Burglars are caught all the time like this. Twenty percent said that they got dropped off, which is the professional way of doing things. If you see anybody getting out of a vehicle and walk or run between residences, call the police at once. They don't mind coming to your area and checking these things. That's their job, and you'd feel a lot worse if you didn't call and somebody's house in the area got hit. Six percent said that they would park in the driveway of the house they were going to hit. These are the guys that plan on lugging off whatever they can. Again, if you see something that doesn't look right— call the police. Two percent said they would park in front of the place. I don't know why. Perhaps for a fast getaway.

Locks

For years, Medeco was the only company that made pick-proof locks, and consequently had the only lock worth buying. A pick-proof lock literally is one that can't be opened by a locksmith—or burglar— using standard lock-picking tools or drills. There's a spring-loaded guard in the lock cylinder itself that prevents the insertion of anything in the keyhole other than a properly fitting key.

Golf Carts

Golf carts are very good for patrolling smaller areas. Condominiums, townhouses, and small residential communities sometimes utilize them for inexpensive, quiet operation. From a burglar's point of view they're thought of as "dangerous." In the past, I eluded many police cars and circling planes because of their operational noise. On the other hand, I was nearly caught several times by either police or security guards in golf carts. They are designed to be quiet, and they are. Once a burglar knows that certain areas are patrolled by golf carts, there's a good chance he will not work that area any longer.

If you heard a TV or stereo on in a home as you were walking around it, but could not see in because of closed curtains, would you still hit the dwelling?

A. The purpose of this question is to find out if the longtime myth of leaving something going inside to make noise would actually scare the burglar away. I had 15 percent say that they would still hit the place after first knocking on the front door to see if anybody was home. The other 85 percent said they would leave. The key to the plan of noise in an unoccupied home is to make sure that no one can see inside even a tiny bit. The noise is only half the game; the complete curtain coverage is the other half. Your whole family should make a game of it and shut all the curtains in the entire house and then go outside and try to find the slightest space where anyone can see in. If there is one, your closed curtains have no effect at all.

What would you say are the best places for hiding valuables? Where were the places that you wouldn't spend time searching?

A. Eighty-one percent stated that safes of good quality were hiding places that they didn't bother messing with. They're speaking about safes of good quality. That means if one burglar can pick it up and lug it out of your residence while smoking a cigarette, it's not good quality. That would be called a burglar's delight. Why? Because they know you had enough faith in it to purchase it in the first place, so you must have had enough faith in it to use it to store your valuables. Easy pickin's! *Safes are only as safe as their installations.* Second choice was hiding things, in this case money, in a book and putting the book on a shelf with many other books. It's too time consuming to bother with.

Where would you look first for the goods in a residence?

A. This was almost another landslide victory, with 95 percent stating that as soon as they would enter a home, or apartment, or condominium or whatever kind of residence they were burglarizing, the master bedroom would be the first place to look for the goods. I fell into that category, too, stepping into a home and walking right past any and everything to get to the master bedroom. It's the worst place in the world to hide anything of great value.

Have you ever looked under the mattress or under beds for anything?

A. This is one of the worst places that a person can hide something. Ninety percent stated that they looked under beds and in between mattresses. I have found many ladies' handbags with cash inside them slipped under beds, along with guns, clubs, vibrators, and dirty magazines. I never did a job during which I wouldn't check under the beds. It's a bad place to put anything but dust and slippers.

While in a home, in a closet, would you take time to go through every single pocket of the clothes hanging up?

A. Thirty-five percent said yes, which is hard to believe. If they even saw some of the walk-in closets I've seen—that looked like clothing stores—they would have needed sleeping bags. The other 65 percent said they wouldn't go through them all. I would hide anything in a pocket of a rack full of clothes, provided there were at least thirty garments hanging in that closet, which is well under what the average person has. I feel it's a safe place. Clothing hanging over a chair or draped across something is just the opposite. Never leave anything of value in those pockets.

Did you ever pull books off a shelf, looking for valuables inside?

A. Only 25 percent stated that they have pulled a few books off shelves at times and gone through them. Seventy-five percent said that it takes too much time.

Would you take TVs, radios, stereos, etc. if, as you were picking them up, you saw I.D. numbers engraved on them?

A. Seventy-five percent said they would take them anyway. Engraving I.D. numbers on property does not prevent your local burglar from taking it, but it does help in the recovery of your property. So it is a very good idea to engrave, or in some way mark your property, either with your social security number or your name and address. Equipment for doing this is at your police station and local crime-watch headquarters.

Would you steal guns from inside a home?

A. Another landslide. Ninety percent of the 300 inmates said yes, they would steal guns whenever they found them. Citizens all over the world buy guns for their protection at home and a good percentage of them are stolen from their own homes, and used for robberies, gang fights, murder and every other crime committed with guns. What good is

a gun if it's not near your bed, right? But you saw earlier that hiding things under beds and in between mattresses is useless. That leaves end tables on each side of the bed. I always checked those places, frequently finding guns there. Where should you hide guns? Good question! I would say on the floor, behind a dresser or chair. I never looked there, and in my many discussions with burglars I have never heard of anybody else looking there. Put the weapon by your bed at night and hide it every morning. It wouldn't take any more time than slipping the old dentures back in.

GOOD HIDING PLACES	POOR HIDING PLACES
Buried containers	Master bedrooms in general
Dropped ceilings	Any sliding drawer
Washing machines	Any cabinets with hinged doors
Clothes dryers	Phony electrical outlets
Garbage cans	Medicine chests
Hollowed-out books	Under mattresses
Behind and under un-upholstered chairs	Refrigerators and freezers
In pockets of clothes hanging in a closet	In pockets of clothing draped across

Prime Time for Burglars

There are actually a lot of periods that can be identified as prime time for burglars. Smart ones, for instance, will find out when the local police force changes shifts. When that happens, there tend to be fewer squad cars out on the street. So it won't hurt you to know the same information, and be more careful at those times. Burglars also love it when there's a huge fire or other disaster in the general vicinity. That way the cops are off paying attention to civil needs, thus giving the burglar a better chance of not getting caught.

Would you rather have rainy weather or nice weather for doing burglaries?

A. I preferred rainy, windy, lousy nights for doing burglaries. It covered up the noise if any was made, the footprints if any could be left, and made for poor aftermath investigation work, along with poor visibility from cars. Besides, what police officer really wants to get out of a warm dry car to get wet? There are a few, but for the most part they would rather stay dry. Fifty-five percent agreed with my way of thinking. The other 45 percent were fair-weather burglars. So even though you can get hit any time, don't rule out rainy days or nights. Burglars don't have holidays or rain dates. They'll work any time. (Maclean, 1983)

Maclean, Jack. *Secrets of a supertheif*. 1st edition. New York, New york: Berkley Books, 1983. unk.. Print.

TrueCrypt, and the 5th amendment saved my life.

This isn't meant to be advertising for or against computer encryptions. Facts are, I encrypted my computer and it saved my life, my reputation and everything I have.

In February 2004 my house was raided by the FBI. They came with the full van and armed agents. They rushed in, presented a warrant and mentioned they had proofs somebody here had downloaded child pornography. Now understand this: this isn't a whole child pornography is good / child pornography is bad story. I don't know if people who watch child pornography turn into pedophiles or not (I don't think they do). I am not saying what I did was good, or even legal.

I had downloaded some child pornography. Not a lot of it, maybe 30 pictures. I am NOT sexually attracted to children and promptly deleted most of them. Since I had a large pornographic collection, there might have been a few I wasn't able to find, and delete. I never watched these pictures or masturbated to them. That being said, I accept my responsibility of downloading them. One thing I should say: I downloaded them all in one day, without knowing it was actual pornography (i.e. downloaded a file that wouldn't indicate it contains child pornography).

They promptly took my computer, my external external hard drive and my laptop. They took my parents' computer as well. I was detained for interrogation, and I was smart. The very first thing I said, even before the interviewer dropped his pen, is "I want my attorney." Note: I had no attorney. I was bluffing. The officer said "Sure," took a few notes, and asked me for a few details "to file the case." Yes, he tried to trick me into talking, or at least starting to talk. I immediately repeated: "I want my attorney." That is the ONLY thing I said. I wanted to yell at him "I DON'T GIVE A SHIT ABOUT YOUR FILE" but I did not.

He eventually complied, asked for his details, at which point I said I did not have an attorney but was in the process of finding one. However, I wanted a public defender. They charged me with possession of child pornography, mentioning my computer as proof. Inside, I laughed a bit, knowing what was waiting. I was formally charged, set bail, paid it, and let out. And then began a quite dramatic - but funny - turn of events. When you file charges in my state, the defendant has the right to a speedy hearing AND, of course, a preliminary hearing. I expressed my rights fully (eventually hired an attorney, my public defender didn't do much).

The police - and FBI - had one problem. My hard drives were all encrypted.

Even my laptop was encrypted. Back home, I took care to properly destroy anything that could ever get me in trouble - even letters I wrote as a child. The police had rapidly checked for more evidence, but as they wouldn't find anything, they did not take the time to look for drugs, drugs equipment and other evidences for other crimes. Two weeks later I got a call from someone claiming to work for the FBI. Apparently they were unable to decrypt my hard drives and required my help. I told them to talk to my attorney. I was summoned in and the only thing I told them was "I want my attorney".

They wanted the password We know you encrypted your data. We even know which program you used. By law, you are required to decrypt the data. I replied, “I want my attorney”.They complied, my attorney came (at high cost) and the situation was re-explained to him (I, of course, already told him the situation, and he recommended not helping them a damn). He told them they had no legal stand.

The FBI formally ordered me to decrypt my data, threatening to charge me with terrorism, and I refused one last time. I was jailed again for a night and new charges were pressed for obstruction (i.e. refusing to help on an investigation). Fast-forward a week, I get a formal plea bargain. Ten years as a sex offender, six years probation, if I recognized guilt for possession of child pornography. The other charge would be drop. Quite a good deal, huh? My public defender STRONGLY told me to accept as the conviction rate was "nearly 99%". My attorney told me to invoke my 5th amendment and refuse any cooperation.

Fast-forward to the preliminary hearing. The judge has to decide whether or not there is enough evidence to prosecute me. He asks for the investigator, who explains the situation, and for the forensic expert. To make a short story, they mention my IP clearly downloaded child pornography. Looks like I'm finished, except for one thing. It has been so long between the download and the raid it was hard to prosecute me on the IP address alone. The records were old, incomplete, poorly filed. My attorney did a good job making the forensic expert admit "mistakes were possible”.

Then came my turn. The expert told the judge they could not find any trace of child pornography because my hard drives were encrypted. He said it was a clear proof I "was hiding something probably worse" at which point he was promptly stopped by my attorney (speculation is not accepted in court). The judge agreed. The expert closed his statement by saying that I had not only encrypted my hard drives, but external drive and laptop.

Then came my turn. The judge summoned me, asked me a few questions, and finally asked: "Why did you encrypt your hard drive?" Think fast. What could I reply!!! "For safety and privacy, your honor. In case of theft." Then the judge asked, "Why do you refuse to decrypt your data?" The $1,000 question (note: this is not exactly what was said, just how I recall it). What can I say? Quick, a word with a lawyer. Then, the genius answer: **"Your honor I would like to invoke my 5th amendment" The judge simply replied, "Alright".**

Oh, the irony of 5th amendment. If you don't invoke it, you have to incriminate yourself. If you do invoke it, you indirectly admit guilt. Of course that can't be used against you, but whatever. There were a few more statements, and eventually the prosecution had nothing. The judge took a moment to think, then said two words that would change my life. "Case dismissed" due to "lack of evidence". I was ecstatic and the prosecution was furious. They closed the file. The judge was about to end the audience when I said:

> "Your honor, they still have my computer. I want it back!"
> "You just had a criminal case dismissed."
> "It's my stuff. I want it back"
> "Very well. Your town's police department has 30 days to give you your material back. Audience finished".

I was very happy. I felt I added to the insult with that last request. The prosecution party couldn't believe it, after all that work.I got my stuff back and it took me a full month before I dated to open my computer again. I was afraid they put a bug or would still try to harass me or incriminate me. I feared they were waiting for me to decrypt me to charge me again. I waited one whole month, then decrypted the file - saved the files I wanted to keep then formatted it all, writing random 0's and 1's.

So this is it. TrueCrypt certainly saved my life, reputation and money. Without it, there is no doubt the police would have found the pictures, and convicted me. I would be on the same registry as rapists and pedophiles - all this for a mistake of mine. But encryption - and refusing to give up despite the threats of being charged with a much more serious crime - kept me free. (Anonymous, 2010)

Anonymous,"http://m.reddit.com/r/IAmA/comments/afib1/truecrypt_and_the_fifth_amendment_saved_my_life/." *Truecrypt, and the 5th amendment saved my life*. Reddit, 01/2010. Web. 6 Apr 2010.