The Testimony of
Detective Brian Hill
Criminal Investigations Division
Anoka County Sheriff's Office

For the Hearing of the Senate Judiciary Committee
Subcommittee on Privacy, Technology and the Law
United States Senate
Location Privacy Protection Act of 2014

June 4, 2014

Introduction

Chairman Franken, Ranking Member Flake, and distinguished Members of the Subcommittee, my name is Brian Hill and I thank you for the opportunity to appear before the Subcommittee to testify about law enforcement's support of the Location Privacy Protection Act of 2014.

Background and Expertise in Cyberstalking Investigations

I am a Detective with the Criminal Investigations Division (CID) of the Anoka County Sheriff's Office in Minnesota. I have been working in my role as a Detective with the Criminal Investigations Division since 2008 and am responsible for the investigation of domestic violence and criminal sexual conduct cases, suspicious deaths, homicides, missing persons, and fatal motor vehicle accidents occurring in our county. We serve the fourth most populous county in Minnesota and have developed an extensive digital forensics lab which is one-of-its-kind in our state.

I am a Computer/Mobile Device Forensic Examiner/Investigator trained by the Minnesota Bureau of Criminal Apprehension, the Federal Bureau of Investigation, and the Secret Service. I have a Cell Phone Technology and Forensic Data Recovery Certification (CTF), Advanced Cellular Technology & Smartphone Forensics Certification (+SMART), Access Data Bootcamp Certification (FTK), Access Data Certified Examiner (ACE) and Access Data Mobile Examiner (AME). I am a member of the High Technology Crime Investigators Association (HTCIA). I also serve on the Board of Directors of the Minnesota Chapter of HTCIA as the 1st Vice President. Additionally, I served in the Air Force Reserves

from 1997 to 2006 in the 96th Airlift Squadron and was deployed from March 2003 to March 2005 for the wars in Iraq and Afghanistan.

GPS "Stalking Apps": Widespread, Serious Safety Threat

The use of "stalking apps" to perpetrate cyberstalking poses serious safety risks to victims of domestic violence.

I worked with a victim a couple years ago where she suspected that her estranged boyfriend must have put some type of spyware on her phone. She stated that he would know things about private conversations that she had over the phone and in text messages. Also he would show up randomly at locations where she was. I did an exam of her phone and was unable to get a full data extraction off of the phone and unable to determine if there was any spyware. Later, she brought in her computer for me to look at and I was able to find that the program FlexiSPY was accessed on the computer. I was then able to show that the program was installed on her phone and was able to work with her to get a new phone and set up new email accounts on a safe computer.

After stealth cyberstalking has begun, regaining safety is a difficult and expensive process for victims. On top of the trauma of surviving domestic abuse, victims are economically and socially impacted. They often must buy new phones, computers, and other technological equipment to be rid of the stealth stalking apps – although there are never any guarantees. Additionally, as we all become more accustomed to using our phones to work, bank, text, email, access social media, search the internet, and pay bills, stealth cyberstalking not only financially impacts victims, but can serve as a tool to isolate victims from all of the functions and social connections their phones provide – including isolating them from being able to reach out to domestic violence advocates or law enforcement. If victims want to be rid of stealth stalking apps they must create new email accounts and change all passwords and security questions – although, again, there are never any guarantees. It is terrifying for victims to know that they will never really know if the stealth stalking apps are gone or if they will reappear after being removed. This means victims' privacy and peace of mind continue to be violated, often long after they have bought new phones or changed their passwords.

These harrowing victim experiences are more and more commonplace through the proliferation of stalking apps. As I have been performing digital forensic examinations since 2008, I continue to discover new apps, especially as they become cheaper and more readily available. For instance, our office is

currently investigating an attempted murder in the context of domestic violence. When we examined the victim's phone, we discovered Ti-spy, running in stealth mode on her mobile device. Ti-Spy is an internet company that advertises itself as parental monitoring software. The software costs just $7 per month and can be installed on any Android smartphone. The software advertises that it can track text messages, calls, GPS locations, and basically access any data contained on the phone that the software has been installed on.

As in the case of discovering Ti-spy, I typically become engaged in a forensic investigation after victims, their domestic violence advocates or law enforcement detect the unsettling signs of digital wrongdoing. They notice a pattern of the abuser knowing all kinds of information about where a victim is and what she is doing, when there is no way the abuser should know those things. In the last 3 years, the mobile forensic examinations I conduct have increased exponentially – by 220%[1] – and I only investigate felony level domestic violence crimes in just one out of 87 counties in Minnesota. We currently average 30 forensic exams per month, again only on felony level cases.

Lack of Resources & Awareness Undercut Law Enforcement Response to Cyberstalking

While my department deals with only felony cases, stalking apps are frequently used in misdemeanor and gross misdemeanor domestic violence cases. Most local law enforcement, however, do not have the resources, staffing time, training, or forensic equipment to examine mobile devices for GPS stalking apps operating in stealth mode.

Investigating cyberstalking is labor intensive and requires expensive specialized equipment. Anoka County is fortunate to have eight tools we use for forensic examinations.[2] Anoka County also has dedicated staff to perform the investigations.

Other law enforcement agencies may have one exam tool, at best, and little to no dedicated staff time to conduct the forensic examinations. If agencies rely on just one tool or rely only on what is visible on a victim's phone, they are potentially receiving just 5% of the data off a phone and thus, losing a large amount of potential evidence that can be helpful in keeping victims safe. Because of Anoka County's resources, we frequently have detectives and domestic advocates from other counties requesting that we

[1] Anoka County Mobile Phone Exams as reported by the Anoka County Sheriff's Office: 2011 – 171 exams; 2012 – 240 exams; 2013 – 377 exams; 2014 YTD through April – 119 exams.

[2] Katana – Lantern; Cellebrite Ultimate – UFED TOUCH; Cellebrite - Classic; Susteen – Secure View; Microsystemation – XRY; Oxygen Forensics Suite; Accessdata – MPE Plus; Paraben – Device Seizure.

perform exams for cases in other jurisdictions. In fact, federal agencies have also asked us to perform forensic exams for them.

This resource problem is so widespread that in a recent survey conducted by the Minnesota Coalition for Battered Women in conjunction with Minnesota Court Administration, advocates indicated that cyberstalking was the number one priority for law enforcement training in the protective order context. Because technology is frequently used to stalk victims and violate protective orders, law enforcement's awareness and capacity to respond to victim reports is key to safety and accountability.

To address the need for training on cyberstalking, I have worked closely with the Minnesota Coalition for Battered Women, and its 80+ member programs, in developing and conducting several trainings and curricula. Since 2009, I have trained over 3,000 domestic and sexual assault advocates, prosecutors, judges, general crime advocates, corrections officers, law enforcement, and community members in Minnesota and around the country. The trainings have focused on (1) the use of technology in intimate partner stalking; (2) securing and gathering evidence in technology assisted crimes; and (3) the use of technology in violations of protective orders.

Our efforts have borne fruit, but strained resources and a lack of awareness continue to undercut law enforcement's ability to recognize and respond to domestic violence victims' increasing reports of cyberstalking. This erodes victim trust in the criminal justice system. A common abuser tactic in domestic violence is to convince the victim she is crazy. There are few things that will drive you crazy more than a victim reporting that she believes he is using stealth stalking apps only to be told: we don't believe you or we don't have the resources to examine your phone. When law enforcement can't effectively identify and respond to cyberstalking reports, victims stop reporting the crimes and abusers win.

A Meaningful Solution to Cyberstalking: The Location Privacy Protection Act of 2014

The Location Privacy Protection Act of 2014 is a major step in addressing the proliferation of stalking apps in the context of domestic violence, by banning the development, operation, and sale of GPS stalking apps. This is important because in order to combat this issue we need to go after the companies that make and market these applications. It comes down to economics, and if we make it unprofitable for the companies to make these programs, then we can help ensure that abusers don't have access to them.

Secondly, the bill supports victim safety by requiring that stalking apps running in stealth mode alert the user and request permission to run. It requires that *all* apps get permission to collect or share location information, making sure that a stalking app can't disguise itself as an employee, or family tracking app – or simply as a flashlight app.

In my opinion, the most important part of the Location Privacy Protection Act of 2014 is that apps will be required to notify the user a second time – 24 hours or seven days after installation – about the tracking implications. This allows for a victim to be notified when the perpetrator doesn't have access to the phone. If this notice only applied to stalking applications, they would just simply change the name of the app or market it in a different way. Just like in human trafficking when Craigslist no longer allowed certain ads, the company backpages.com emerged and began to offer those ads. This Act would address such evasion of the law.

Finally, the Act will bring national public awareness to this serious and widespread issue by requiring that the federal government gather more information about GPS stalking, facilitate reporting of GPS stalking, and prioritize training grants for law enforcement.

I urge you to support the Location Privacy Protection Act of 2014.

Thank you again to the committee for reviewing my testimony and for your support of law enforcement's efforts to keep domestic violence victims and our communities safe.