



NATIONAL NETWORK
TO END DOMESTIC
VIOLENCE

1400 16TH STREET NW
SUITE 330
WASHINGTON, DC 20036

www.nnedv.org
phone: 202.543.5566
fax: 202.543.5626

**The Testimony of
the National Network to End Domestic Violence
with the Minnesota Coalition for Battered Women**

**Cindy Southworth, MSW
Vice President of Development and Innovation
and Founder of the Safety Net Technology Project at NNEDV**

**June 4, 2014
Hearing of the Senate Judiciary Committee
Subcommittee on Privacy, Technology and the Law
United States Senate
Location Privacy Protection Act of 2014**

A few days before this hearing¹, I received a phone call from Harriet, a 74-year-old retired teacher in California, who heard from her advocate that I was collecting stories about how victims are being impacted by location tracking. This is Harriet's story: Harriet met a charming man in a grief support group and they began dating. He gave her a cell phone. She protested that it was too expensive, but he insisted she accept his gift and use the phone. Things escalated and then he raped her, after which she refused to see him again. He felt no remorse after the assault and called her incessantly and showed up wherever she went. It was uncanny that he knew everywhere she would go – causing her to feel hunted. She turned off the “gifted” phone to experience some relief from his control, but every time she turned it on to see if her family had called, her offender would call moments after she powered on the phone. When she reached out for help, she received a temporary protection order, but unfortunately the judge denied the permanent order saying “there wasn’t enough evidence.” Her only recourse was to leave her community, her friends, and her support system. She called me in hopes that her story could help others. The strength and resilience of Harriet and all survivors inspires me every day.

I. Introduction

Good afternoon Chairman Franken, Ranking Member Flake, and distinguished Members of the Committee. Thank you for inviting me to testify about the importance of location privacy and transparency for victims of domestic violence, sexual assault, and stalking. My name is Cindy Southworth and I am the Vice President of Development and Innovation at the National Network to End Domestic Violence.² I am also representing our member, the Minnesota Coalition for Battered Women.³ I am testifying today on behalf of Harriet and the 7 million victims each year who are assaulted, raped, or stalked by a current or former partner.⁴

¹ Conversation with “Harriet” (name changed to protect the victim’s confidentiality) on May 31, 2014.

² NNEDV is a social change organization dedicated to creating a social, political, and economic environment in which violence against women no longer exists. Founded in 1990 and officially incorporated in 1995, NNEDV represents 56 state and territory domestic violence coalitions who in turn represent nearly 2,000 local domestic violence service providers across the country.

³ The Minnesota Coalition for Battered Women is a well-established, membership organization with over 80 local, regional, and national member programs located throughout Minnesota. The Coalition has existed for 35 years as the state’s primary voice for battered women and has a strong history of effectively carrying out public policy that advances women’s safety and security.

⁴ U.S. Department of Justice, National Institute of Justice and Centers for Disease Control and Prevention. (July 2000). Extent, Nature, and Consequences of Intimate Partner Violence: Findings From the National Violence Against Women Survey. Washington, DC. Tjaden, P., & Thoennes, N.

Table of Contents	Page
I. Introduction	1
Executive Summary of Issues	3
The Safety Net Project at NNEDV ⁵ and the Minnesota Coalition for Battered Women	3
Prevalence and Statistics	4
Benefits of Location Technology	7
II. The Problem: Stalking Apps and GPS Location Tracking by Abusers and Stalkers	7
Family Locator Services	7
Location functionality built into the operating systems of phones and tablets or installed through a car manufacturer	8
Freestanding GPS devices	9
Mobile Apps that Track Location	9
Impact of Location Tracking by Abusers and Stalker	11
Current Legal Recourse	12
III. The Solution: An Overview	13
A. Require consent prior to tracking or sharing location information	13
B. Location tracking must be transparent and visible to the user	14
C. Criminalize the operation, sale, and marketing of technologies whose primary purpose is to surreptitiously track someone's location and facilitate a crime	16
D. Allow law enforcement to seize the proceeds of those sales to fund anti-stalking efforts	16
E. Allow individuals an enforcement option through a VERY modest private right of action	17
F. Require the federal government to gather more information about GPS stalking, facilitate reporting of GPS stalking	17
G. Require the federal government to prioritize funding for GPS stalking prevention, awareness, and detection efforts	17
H. Enact parallel state and Tribal laws to allow local and Tribal level enforcement	18
IV. Conclusion	18
V. Appendix: A Sampling of tracking apps/devices and their features	19

⁵ Cindy Southworth, the Vice President of Development and Innovation at the U.S. National Network to End Domestic Violence (NNEDV) leads the technology, communications, development, and finance efforts of NNEDV. She joined NNEDV in 2002 when she founded the Safety Net Technology Project to address the intersection of technology and violence against women. Through the Safety Net Project, Ms. Southworth works with private industry, advocacy organizations, law enforcement, state and federal agencies, and international groups to improve safety and privacy for victims in this digital age. She has presented over 460 trainings to more than 35,400 advocates, technologists, and justice professionals, including over 25 international presentations and keynote addresses. She has testified before Congress and is on many task forces and committees that address justice, privacy, technology, and safety. Ms. Southworth has a Master's Degree in Social Work and has worked to end violence against women for over 20 years at national, state, and local advocacy organizations. She has spent the past 16 years focusing on how technology can increase victim safety and how to hold perpetrators accountable for misusing technology. Ms. Southworth also serves on the Airbnb's Trust Advisory Board and the Advisory Boards of MTV's A THIN LINE digital abuse campaign, the Privacy Rights Clearinghouse, and the Computers Freedom and Privacy Conference. The NNEDV Safety Net Project is one of 5 organizations internationally that serves on the Facebook Safety Advisory board.

Summary of Issues

- 1) Domestic Violence and stalking impact the entire community at epidemic rates. 1 in 3 women will be assaulted by an intimate partner in her lifetime. 1 in 6 women will be a victim of stalking in her lifetime.
- 2) Location information about victims of domestic violence and stalking is undeniably sensitive, thus surreptitious location tracking devices and apps disproportionately dangerous for these individuals.
- 3) If a victim knows she/he is being tracked or monitored, she/he can take steps to mitigate risk (e.g., leave compromised phone or tracked car at home when she files a police report or meets with a victim advocate).
- 4) National data collected in 2006 (1 year before the iPhone was released, 2 years before the App stores were opened) indicates that Global Positioning Systems (GPS) tracking and electronic monitoring impacted thousands of victims that year, long before the proliferation of “apps.” Eight years later, ninety percent of American adults have a cell phone—the majority of which (58%) are smartphones. A 2012 NNEDV survey of victim service providers around the country found that 72% of them had seen victims who were stalked through the use of a stalking app or GPS or location tracking device.
- 5) If location tracking technology is being used legitimately to monitor children or employees, there is no need for a “stealth mode” or for it to run invisibly. Many reputable family safety and location sharing social networks only function with full notice, consent, and visibility.
- 6) Location tracking technology designed to run in stealth mode is being designed to facilitate stalking and spying. Often these products are marketed to “spy on” or “stalk” your girlfriend/partner/spouse.
- 7) Many vendors boast about the ability to track your girlfriend, partner, or spouse without the victim’s knowledge. Some vendors claim their location tracking product is for monitoring employers or children, yet have the same stalking-focused features as the blatantly advertised “stalking apps.”

Summary of Solutions:

- A. Impose criminal penalties on individuals who use mobile technologies to spy on or stalk individuals.
- B. Require a reminder when location is being used in the background. Abusers and stalkers often consent to the installation of stalking apps on a victim’s phone, and a reminder of the tracking is needed at a future point in order for a stalking victim to become aware of this surreptitious and dangerous location tracking.
- C. Criminalize the operation, sale, and marketing of technologies whose primary purpose is to surreptitiously track someone’s location and facilitate a crime
- D. Allow law enforcement to seize the proceeds of those sales to fund anti-stalking efforts.
- E. Require the federal government to gather more information about GPS/location stalking, facilitate reporting of GPS stalking, and prioritizing training grants for law enforcement.
- F. Require the federal government to prioritize funding for GPS/location stalking prevention, awareness, and detection efforts.

I. Introduction Continued

The Safety Net Technology Project at NNEDV

Founded in 2002, NNEDV’s Safety Net Project focuses on the intersection of technology, stalking, and abuse. The project works to address how technology impacts safety, privacy, accessibility, and civil rights of victims. Safety Net works with communities, agencies, and technology companies to:

- Address how technology impacts survivors of abuse and stalking;
- Educate victim advocates and other professionals on ways to use technology strategically to increase safety;

- Train criminal justice professionals on tactics of technology misuse in the context of domestic violence, sexual assault, dating abuse, and stalking;
- Advise technologists on technology risks and benefits to victims; and
- Advocate for strong policies that ensure the safety and privacy of victims.

Since 2002 the Safety Net team has presented more than 900 trainings to more than 65,000 advocates, law enforcement officials, technologists, and others regarding technology tools, online privacy, and victim safety. Of these trainings, more than 45 were presented outside the United States, including Austria, Australia, Canada, England, Ireland, Lithuania, Mexico, and Portugal. Through in-depth consultations, the Safety Net Project helps police officers and victim advocates on a range of issues, including complex technology stalking cases, implementing new technologies such as smartphone applications, and developing secure online chat systems. The Safety Net Project has responded to more than 13,500 unique requests for assistance, consultation, and resources - averaging over 100 requests each month. The Safety Net Team also works closely with technology companies such as Verizon, Google, and Facebook, and serves on Facebook's Safety Advisory Board.

Minnesota Coalition for Battered Women

The Minnesota Coalition for Battered Women (MCBW) has long been a leader in the domestic violence movement, especially with implementing legislative policy that supports and protects battered women and children. They were one of the first states to adopt a stalking statute in the early 1990s, and in 2010, the Coalition initiated and monitored the passage of several amendments to the stalking statute to update and increase protections for victims. A significant provision in this statute now includes the use of modern technologies being used as a means to stalk a victim. The Minnesota stalking statute (MN Stat §609/748 subd. 2(6)) specifically states that it is a criminal act of stalking if a person *“repeatedly mails or delivers or causes the delivery by any means, including electronically, of letters, telegrams, messages, packages, through assistive devices for the visually or hearing impaired, or any communication made through any available technologies or other objects.”* The Coalition supported the passage of this provision because they received reports from battered women throughout the state that modern technology was being misused by abusers to stalk victims.

Everyone Knows a Survivor: Prevalence and Impact

- 1 in 3 women will experience an assault by an intimate partner at some point in her lifetime.⁶
- 1 in 6 women and 1 in 19 men who will experience stalking in her and his lifetime.⁷
- Seventy-eight percent of stalking victims are women.⁸
- More than half of victims reported losing 5 or more days of work due to stalking, and 130,000 victims reported that they had been fired or asked to leave their job due to stalking.⁹
- A study found that one-fourth of stalking victims reported financial control by the stalker. Sixty-eight percent of the stalkers controlled the victims socially. Virtually all stalkers (98%) attempted to control the victim psychologically.¹⁰

⁶ Black, M.C., Basile, K.C., Breiding, M.J., Smith, S.G., Walters, M.L., Merrick, M.T., Chen, J., & Stevens, M.R. (2011). The National Intimate Partner and Sexual Violence Survey (NISVS): 2010 Summary Report. Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention.

⁷ Katrina Baum et al., “Stalking Victimization in the United States,” (Washington, DC: Bureau of Justice Statistics, 2009).

⁸ Seventy-eight percent of stalking victims are women. Center for Policy Research (1997). Stalking in America.

⁹ Baum, K., Catalano, S., Rand, M., and Rose, K. (2009) Stalking Victimization in the United States. Bureau of Justice Statistics.

¹⁰ Brewster, M. (2003). Power and Control Dynamics in Prestalking and Stalking Situations. Journal of Family Violence. 18(4).

In Just One Day

In just one day in the United States, more than 64,000 adults and child victims are helped by almost 2,000 local domestic violence shelters and outreach offices. Tragically, almost 10,000 times in the same day, a victim found the courage to tell a complete stranger about the abuse perpetrated by someone who was supposed to love her and the overworked and underpaid advocate was forced to say “I am SO sorry, but we don’t have a bed/attorney/counselor available.”¹¹

Homicide Risk

Abusers and stalkers go to great lengths to maintain power and control over their victims. In fact, the most dangerous time for a victim of domestic violence is when she takes steps to leave the abuser.¹² Many victims are stalked relentlessly for years after having escaped from their partners. Batterers who stalk their former partners are the most dangerous and pose the highest lethality risk.¹³ In fact, 54% of femicide victims reported stalking behavior to the police before the victims were killed by their stalkers.¹⁴ Nationwide, an average of 3 women are killed by a current or former intimate partner every day.⁴

Technology Stalking Statistics

It is nearly impossible for the average American to go about his or her daily life without using technology. Technology has become much more than just a convenience or a form of entertainment. Technology is a tool to connect with friends and family, to complete daily tasks, and to educate and learn, whether it’s “to Google” or to take online classes. Americans are increasingly connected – 87% of adults use the internet¹⁵ and are progressively doing more using mobile devices. Ninety percent of American adults have a cell phone (the majority of which (58%) are smartphones) that are being used to go online (63%), download mobile applications (50%), and much more.¹⁶ Domestic violence and stalking occur where we live our lives. For approximately 90% of Americans, that means in person, on mobile phones, and online since the digital world and non-digital world are now so interconnected.

The Department of Justice Office on Violence Against Women funded a Supplemental Victimization Survey to provide in-depth information about stalking. The data was collected in 2006, one year before the iPhone was released in 2007 and before the Apple and Google App stores opened in 2008. Unfortunately, this supplement has not been repeated since 2006, though smaller studies since have also indicate that technology misuse by stalkers and abusers is on the rise.

According to the 2006 data, 34% of stalking victims or a projected 1.14 million people experienced “**following** or spying,” and 32% or a projected 1.04 million people experienced stalkers “**showing up** at places.”¹⁷ In the same study, 7.8% of stalking victims or a projected 246,351 people reported in 2006 that they had been victims of “Electronic Monitoring” and more than 26,000 were projected to have been

11 National Network to End Domestic Violence, Domestic Violence Counts: a National Census of Domestic Violence Shelters and Services. March 5, 2014. www.nnedv.org/census

12 Ronet Bachman and Linda Salzman, Bureau of Justice Statistics, *Violence Against Women: Estimates From the Redesigned Survey 1* (January 2000).

13 Jacqueline Campbell, “Prediction of Homicide of and by Battered Women”, *Assessing Dangerousness: Violence by Sexual Offender, Batterers, and Sexual Abusers* 96 (J. Campbell, ed., 1995). Also: Barbara J. Hart, “Assessing Whether Batterers Will Kill,”(1990) Available at: <http://www.mincava.umn.edu/hart/lethali.htm>,

14 Judith McFarlane et al., “Stalking and Intimate Partner Femicide,” *Homicide Studies* 3, no. 4 (1999).

15 Pew Research, Internet Project, “Internet User Demographics,” www.pewinternet.org/data-trend/internet-use/latest-stats/

16 Pew Research, Internet Project, “Mobile Technology Fact Sheet,” www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/

17 Catalano, Shannan U.S. Department of Justice Office of Justice Programs Bureau of Justice Statistics “Stalking Victims in the United States – Revised” September 2012.

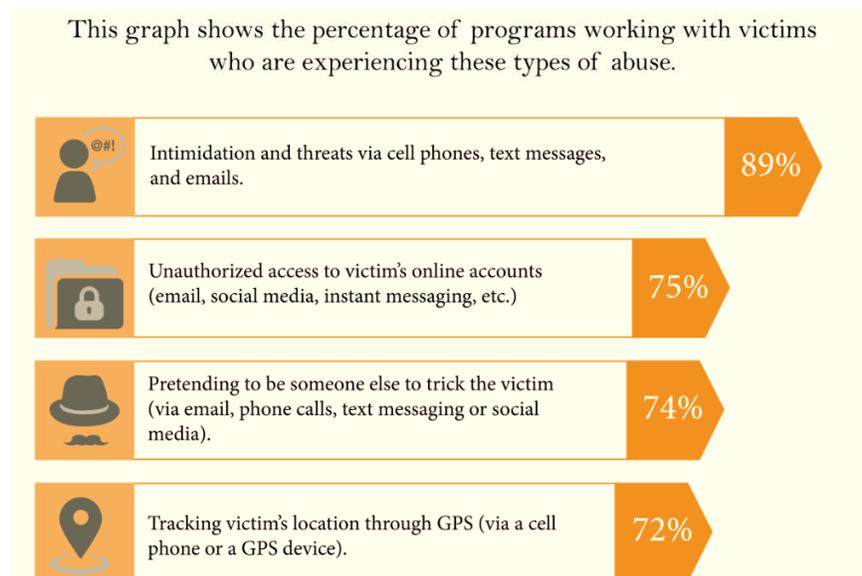
stalked specifically by GPS.¹⁸ Since 2006, the spying and stalking apps have flooded the marketplace, making it even easier for abusers to purchase, install, and stalk. With the growing use of location technology, perpetrators are tracking victims' location more often and in increasingly varied ways.

In 2010 the Centers for Disease Control issued its National Intimate Partner and Sexual Violence Survey. It found that 38.6% of female domestic violence victims and 31% of male victims were “watched, followed or tracked with a listening or other device.” (Note that this survey conflated wiretapping and eavesdropping apps with GPS/location stalking apps).¹⁹

In a 2012 survey of over 750 agencies conducted by NNEDV,²⁰ the vast majority of victim service providers reported that survivors experienced some kind of technology misuse and are asking for help dealing with technology-related abuse:

% of Programs Reported:	Survivors Report the Following Abuse
89%	Abusers harass victims via cell phone
75%	Abusers access victims online accounts without permission
72%	Abusers track victims via GPS

% of Programs Reported:	Survivors Ask for Help on the Following Issues
71%	Safety strategies on using their cell phones safely
62%	Help on managing location privacy
54%	Help on using online spaces/social media safely and privately



¹⁸ Ibid.

¹⁹ Black, M.C., Basile, K.C., Breiding, M.J., Smith, S.G., Walters, M.L., Merrick, M.T., Chen, J., & Stevens, M.R. (2011). The National Intimate Partner and Sexual Violence Survey (NISVS): 2010 Summary Report. Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention.

²⁰ NNEDV, “New Survey: Technology Abuse & Experiences of Survivors and Victim Service Agencies,” www.ovc.gov/news/grantees.html and <http://techsafety.org/blog/2014/4/29/new-survey-technology-abuse-experiences-of-survivors-and-victim-services> (data collected in 2012)

Benefits of Location Technology

Although abusers misuse technology with the intent to stalk and control, the benefits of GPS are undeniable. Location technologies assist all members of the community, including victims and survivors. For example, location devices and apps provide users with maps and directions and can send alerts when hikers are lost while climbing mountains on O'ahu,²¹ or help rescue people after a boating accident off the coast of Charleston, South Carolina.²²

The use of GPS can also help victims. In March 2011, a man was arrested for kidnapping his 4-year-old son outside of a domestic violence center. Police were able to track his movements based upon his cell phone signal. He was taken into custody and the boy was returned to his mother. The man was jailed, charged for assault, and his estranged wife was granted a restraining order against him.²³

II. The Problem: Stalking Apps and GPS Location Tracking by Abuser and Stalkers

Last week a survivor in Indiana reached out for help from a local victim advocate. "Mary" discovered her estranged abusive husband had installed a location tracking app on her phone. She became suspicious when he always called if she varied her routine such as stepping out of her building to buy a sandwich for lunch instead of eating in the building's deli. She asked the advocate to help her figure out what app is on the phone and hoped she wouldn't have to replace her expensive smart phone.

Stalkers misuse location technology to hunt down and/or continuously monitor their victims in several primary ways, including: 1) family locator services, 2) location functionality built into the operating systems of phones, tablets, or cars 3) freestanding GPS hardware devices, and 4) stalking apps sold in App stores or downloaded elsewhere on the Internet.

1) Family Locator Services

Many products are available for the purpose of locating family members via their cell phones. Some of these products are offered through wireless carriers (e.g., Verizon Family Locator²⁴). Generally, locator services provided directly from a cell phone carrier as part of a family plan require some level of authorization to access the victim's account and activate the service. Unfortunately, since most stalkers are former intimate partners, it is sometimes possible for them to find a way to impersonate the victim, access the account, and add these optional location services. Most cell phone carriers, however, have added additional authentication and verification steps, such as automatically sending a text message to the phone informing the user that a tracking application or service is enabled²⁵. Without periodic notification to the tracked phone, the abuser or stalker can turn on the service and surreptitiously track and stalk another adult (the abuse victim) through the locating plan.

²¹ A father and son hiking team were rescued from cell phone GPS after getting lost in the Koolau mountains in O'ahu, Hawaii. www.rmtracking.com/blog/2011/12/12/gps-saves-lives-in-hawaii-and-beyond/

²² Boater Summons Rescue from US Coast Guard with SPOT Messenger April 21, 2010. www.findmespot.com/en/spotemergency/index.php?article_id=626

²³ Terry, Lynne. "Washington Police Used Cell Phone Pings to Zero in on Fugitive in Amber Alert." Oregon Local News, Breaking News, Sports & Weather - OregonLive.com. 2 Mar. 2011. Web. 26 Apr. 2011. http://www.oregonlive.com/pacific-northwest-news/index.ssf/2011/03/washington_police_used_cell_phone_pings_to_zero_in_on_fugitive_in_amber_alert.html

²⁴ http://www.verizonwireless.com/support/faqs/FeaturesandOptionalServices/family_locator.html

²⁵ <https://community.verizonwireless.com/thread/201324>

2) Location functionality built into the operating systems of phones and tablets or installed through a car manufacturer

Most cell phones can be tracked simply due to the way the device is designed and operated. Even without actively using the GPS in the phone, just by triangulating the cell towers—measuring the distance between the phone and the three nearest cell phone towers—the approximate location can be revealed. Wireless carrier companies also have other methods of determining a phone’s location, including GPS information or network usage information that includes location (when connecting to Wi-Fi, for example). In general, the phone must be turned on and be connected with cell towers in order for the carrier to gather location information. This information is typically only available to the wireless carrier and may be obtained by law enforcement with the proper warrants or authorization.²⁶

In addition to the carrier retaining location information, many phones and tablets store location history in the device itself. If an abuser or stalker is able to access the location information on the device, the offender can learn a victim’s daily activities (e.g., if she met with the police or went to the courthouse to file a protection order). For example, for iPhones, the entire location history is stored under “Frequent Locations.” Although there is an option to opt out of the device collecting location history, a survivor will need to know to go beyond the Location Services settings and turn off Frequent Locations under System Services. Many survivors will not know that.

Some devices also have a “find my phone” feature or are running a security software that allows the user to find their phone if it is lost or stolen. For the iPhone specifically, if the “find my phone feature” is turned on and if the abusive party has access to the victim’s iCloud or online account, then they can monitor where the phone is in real time (not just historical location data), in addition to whatever information is stored in the iCloud. When NNEDV works with victims and advocates, we recommend that users put a passcode lock on their phone, and turn off location tracking in the settings if they don’t need it or want it. However, with all safety strategies, survivors should only use them if it won’t create suspicion from an abuser and potentially increase danger and risk.

In addition to smart phones, location information on navigational systems, such as OnStar, can be misused in order to stalk or monitor someone.²⁷ Family Link is an optional add-on service to the operator-assisted emergency response and navigation services offered by OnStar.²⁸ Subscribers can log on to OnStar’s Family Link Web site to view a map with the vehicle’s location at any time. They can also schedule e-mail or text alerts to update them periodically on the location of the automobile on specific days or times.²⁹

While fleeing to a Texas shelter, a victim stopped at a truck stop. OnStar disabled her car for no known reason. Police arrived and called OnStar to verify that the car was NOT stolen. The victim entered the shelter on Friday and in the middle of the night her car horn started randomly going off. It happened again each night. Monday morning, the abuser called the victim, said he knew she was staying in the shelter and threatened her. She felt protected on the secure shelter campus where her car was inside the gates, however she had to work with a local dealership and the police to get the OnStar disabled so the car horn stopped waking all of the families in shelter at 2am. ~ Advocate in Texas

²⁶ Lee, Kaofeng & Olsen, Erica. (2013) Cell Phone Location Privacy and Intimate Partner Violence. Domestic Violence Report, August/September 2013, Vol. 18, No. 6.

²⁷ Fraser, C., Olsen, E., Lee, K., Southworth, C. and Tucker, S. (2010), The New Age of Stalking: Technological Implications for Stalking. Juvenile and Family Court Journal, 61: 39–55. doi: 10.1111/j.1755-6988.2010.01051.x

²⁸ <https://www.onstar.com/web/portal/family-link?g=1>

²⁹ <http://www.cnet.com/news/want-to-know-where-your-teen-is-ask-onstar/>

3) *Freestanding GPS Devices*

Abusers can also use free-standing devices to monitor and stalk their victims. These GPS devices can be Portable Navigation devices (e.g., Garmin) or small tracking devices marketed to track equipment, merchandise, or equipment and be installed surreptitiously by the abusive party.



Other GPS-type tracking systems include small devices designed to be hidden under the car or inside the dashboard, and are often marketed as “Covert GPS Trackers.” Some of these products are marketed for apparently legitimate use: parents can track their teens’ cars to ensure that their teen goes where they say they are going and parents will be alerted if the car goes beyond a predetermined area or is speeding. Parents can reprimand their teen driver by using the product to remotely flash the dome light or honk the horn of the tracked automobile. Other products are more blatant about its purpose: Bluewater Security Professionals brazenly pitches, “By installing a vehicle tracker in the car of your husband or wife, you will be able to track their every move and tell what his or her true location is. It would be as if you were sitting right next to them in the passenger seat.”

A survivor in Missouri, “Gia” suffered years of horrific sexual violence and abuse. She was finally able to break away, moved to an undisclosed location, varies her routes to and from places, and minimized her online presence. Recently she was visiting a friend and the perpetrator showed up unexpected with a van borrowed specifically with the intention of abducting her. Fortunately she was able to escape. She has had her vehicle checked repeatedly for the tracking device that led the perpetrator to her. So far, nothing has been found on the car, so she is trying to find a tech unit that will examine her phone for her. Gia finally felt safe after years of terror and she is back to looking over her shoulder at all times. ~ Advocate in Missouri

4) *Stalking apps sold in app stores or downloaded elsewhere on the Internet*

One of the most comprehensive ways a stalker can track a victim is by installing a tracking program or spyware onto the victim’s cell phone. In most cases the abuser will need physical access to the phone in order to install a monitoring program. This can occur if the abuser or an accomplice of the abuser has access to the phone or if the survivor inadvertently installs such a program without knowing what it does.

Many location tracking applications and services (some are available in app stores or via the Internet) do not provide notice to the target/victim or verify that consent to track has been obtained by the person being tracked. Stalkers can install a location-tracking application on to the victim’s phone without the victim’s knowledge. Depending on the type of application, the stalker can then monitor the location of the victim’s phone via a website or his cell phone to monitor the real-time or historical movement of the victim’s phone.

Despite the marketing claim that these location services or applications are for parents to locate their teenage children or an elderly parent, most of these services focus on the ability to operate in “stealth mode,” mention that it’s possible to use these services to “catch a cheating spouse,” and highlight the fact that the target will not know the app is running. Most of these apps have additional features beyond disclosing the location of the cell phone. Some features allow the monitoring person (potentially, the abuser) to be notified if the targeted person goes outside of a certain geographic boundary (known as “geofencing”), be notified if the targeted person goes to or leaves a certain place or address, be sent notifications of a targeted person’s location at specific times, or see a history of where the targeted person has gone throughout the day or week.

Below are two screen images of “HelloSpy,” a tracking product that promises to: **“Silently monitor text messages, GPS locations, call details, photos and social media activity. View the screen and location LIVE!”** HelloSpy also claims to have over 250,000 customers, with plans ranging from \$19.99/month to \$119.99/year. If their numbers are accurate, this stalking app has brought in a minimum of \$4,997,500 (if all customers purchased the cheapest 1-month plan).

This notable alleged “family safety” product also has a continuous animated image on their main webpage showing a scene from the movie *Cruel Intentions* where a man roughly shoves a woman off the bed, head first.³⁰

HelloSpy: Your Mobile Phone Spy Solution

You may have a thousand reasons for wanting to monitor your kids OR employees on their mobile phone but you only need one tool to get all the answers you need: HelloSpy *Mobile Phone Spy Software*. All you need to do is: Discreetly install our advanced spy software on most the smart phone you want to monitor and then login to your HelloSpy user account to access:

- Real-Time Location Tracking Even When In Buildings
- Complete Call History Log
- Pictures Sent or Received
- Full Contact Details
- Complete Text Message Log
- Remotely Enable Spy Call to Listen to Live Surroundings of the Phone
- And More...

No one will ever know that you are tracking them because our advanced *Mobile Phone Spy Software* remains completely hidden from the user. From the moment you install the spy software onto the mobile phone you wish to monitor, all of the phone data is available to you via your HelloSpy user account. Starting for around \$0.30 a day, HelloSpy makes it easier and more affordable than ever to get the answers you want and deserve to know!



[Sign Up NOW !!!](#)

Step by Step:

- >> [How to install on iPhone/iPad target.](#)
- >> [How to install on Android phone.](#)

On another HelloSpy webpage, there is a photo of a man grabbing a woman’s forearm (see image below). The woman has visible abrasions on her face. Next to this photo is a list of the features of HelloSpy, including: Track Phone Location, Read Phone SMS Remotely, See Call History, and more.





Quick Features List

- Track Phone Location
- Read Phone SMS Remotely

There are other apps that offer additional monitoring and spying features, in addition to location tracking. These programs are known as cell phone spyware or monitoring software. Cellphone spyware allows the abusive person to monitor all activities that occur on the phone, including all messages sent and received, apps downloaded, phone calls, voicemail received, and location information. Some spyware will even allow the monitoring person to call the phone and, without the user realizing, use the cell phone as a listening device to hear conversations occurring around the user. These products do not send any notifications to the user to inform them that their location is being tracked or even that the product is installed on their phone.

³⁰ <http://hellospy.com/mobile-phone-spy.aspx?lang=en-US>

Cellphone spyware is widely available and easy to install. The abusive person just needs a few minutes with the phone.

These apps are often brazenly marketed to stalkers, sometimes briefly mentioning employee monitoring and child safety -- almost as an afterthought or cover story -- and heavily focusing on the features that will help you "spy on your spouse".



Impact of Location Tracking by Abusers and Stalkers

As more users adopt mobile technology, abusers and stalkers are misusing that technology. The Apps and devices noted above are developed and advertised directly to stalker and certainly makes it easier to facilitate these crimes. In some tragic cases, GPS devices and apps may have actually aided the offender in locating the victim to commit murder, or the location tracking was one piece of an overwhelming list of controlling tactics that preceded a victim's death.

In 2004, a stalker in California purchased a cell phone with location tracking service expressly for the purpose of tracking his ex-partner. He attached the cell phone to the underside of her car and was only caught when the victim saw him under her car changing the cell phone's battery.³¹ Numerous cases of GPS and location stalking have arisen since then.

In 2009, in Seattle, a man used the location service on his estranged wife's phone to track her to a local store. After finding her speaking to a man there, he shot and killed their five children and himself.³²

In 2010 in Delaware a divorced father installed a GPS device on his ex-wife's car after the judge issued a Protection From Abuse Order against him. He also left 120 voicemails on his 5-year-old's cell phone in just one evening, including one where he called his daughter an "inconsiderate little bitch."³³

In Philadelphia, on Sunday, June 20, 2010, Sean Burton installed a tracking device on his estranged wife's new partner, James Stropas' car. Between time of installation and Monday morning, the location of the device was checked via the laptop in Burton's van 147 times. Using the GPS to hunt down Stropas, Burton murdered James Stropas in a parking lot by stabbing him over 70 times.³⁴

In another tragic 2010 case in Scottsdale, Arizona, Andre Leteve used the GPS on his estranged wife's phone to stalk her before he shot and killed both of their children, 15-month-old Asher and 5-year-old Alec.³⁵

³¹ Boghossian, N. (2004, September 4). High-tech tale of stalking in the 21st century. LA Daily News, p.N1

³² Ibid.

³³ Family Court of Delaware/WestLaw/Jan. 12, 2010

³⁴ DiGiacomo, Marlene. Man convicted of killing Oaks resident and war vet Stropas. Montgomery News. Monday, March 28, 2011 <http://www.macombdaily.com/20110325/accused-pennsylvania-murderer-recalls-bloody-struggle-with-wifes-lover>

³⁵ Scheck, Justin. "Stalkers Exploit Cellphone GPS." Business News, Finance News, World, Political & Sports News from The Wall Street Journal - Wsj.com. 3 Aug. 2010. Web. 26 Apr. 2011.

In 2011, Dmitry Smirnov methodically stalked and murdered his former girlfriend after first researching whether Illinois has the death penalty. After determining that the state had abolished the death penalty, he drove to the Chicago area, attached a GPS device on the victim's car, and followed her for several days. He sat by her car in her office parking lot and murdered her when she left work. During the murder, he had to stop and reload his gun in the middle of shooting her.³⁶

In 2013, in Petaluma, California a man used a smartphone application to track a victim through her cellphone.³⁷ He tracked her to a friend's house and was arrested when he assaulted her.

Current Legal Recourse When Location Tracking is Used to Harm Victims

Fortunately, stalking is a crime in all 50 states, the District of Columbia, the U.S. Territories, and there is even a Federal stalking law. Unfortunately, many stalking laws do not address the use of location tracking devices or apps. Some judges have interpreted using location tracking software over a period of time as stalking, but the initial installation may not be considered a crime. Crimes that violate the federal stalking and cyber stalking laws are rarely charged, probably due in part to the high burden in the statutory language and the limited resources of the FBI and U.S. Attorneys.

The Electronic Communications Privacy Act (ECPA)³⁸ prohibits the manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices, however it does not cover devices that surreptitiously track location information. Many of the comprehensive Stalking/Spy apps that I have included in my testimony very likely violate ECPA since they manufacture, send, advertise, and promote the use of a surreptitious interception device – and some of their features intercept electronic communications; it's important to note, however, that there are apps that track only GPS location and do not offer eavesdropping capabilities – and are hence not clearly prohibited under federal law. Unfortunately, I am only aware of one instance of the U.S. Department of Justice indicting a manufacturer of SpyWare.

In August 2005, United States Attorney Carol C. Lam of the Southern District of California and John C. Richter, Acting Assistant Attorney General for the Criminal Division, U.S. Department of Justice, indicted Carlos Enrique Perez-Melara -- the creator and marketer of a spyware program called "Loverspy" - and four others who used Loverspy illegally to break into the victims' computers and illegally intercept the electronic communications of others.³⁹

“Purchasers would then select from a menu an electronic greeting card to send to up to five different victims or email addresses. The purchaser would draft an email sending the card and use a true or fake email address from the sender. Unbeknownst to the victims, once the email greeting card was opened, Loverspy secretly installed itself on their computer. From that point on, all activities on the computer, including emails sent and received, web sites visited, and passwords entered were intercepted, collected and sent to the purchaser directly or through Mr. Perez's computers in San Diego. Loverspy also gave the purchaser the ability to remotely control the victim's computer,

³⁶ Huffington Post, Dmitry Smirnov Pleads Guilty, Gets Life In Stalking Murder Of Ex-Girlfriend Jitka Vesel. First Posted: 07/23/11 Updated: 09/22/11 www.huffingtonpost.com/2011/07/23/dmitry-smirnov-pleads-gui_n_907839.html

³⁷ CBS San Francisco and Bay City News Service. Petaluma Man Arrested For Stalking Woman. November 13, 2013 <http://sanfrancisco.cbslocal.com/2013/11/13/petaluma-man-arrested-for-stalking-woman/>

³⁸ 18 U.S. Code § 2512 Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited

³⁹ U.S. Department of Justice, Press Release. August 26, 2005 <http://www.justice.gov/criminal/cybercrime/press-releases/2005/perezIndict.htm>

including accessing, changing and deleting files, and turning on web-enabled cameras connected to the victim computers. Over 1,000 purchasers from the United States and the rest of the world purchased Loverspy and used it against more than 2,000 victims. Mr. Perez's operations were shut down by a federal search warrant executed in October 2003.⁴⁰

On November 5, 2013, the FBI announced the addition of Mr. Perez to its Cyber's Most Wanted List and is seeking information from the public regarding his whereabouts.⁴¹ (Mr. Perez fled the country at the time of his indictment.) Mr. Perez was indicted for manufacturing a surreptitious interception device; sending a surreptitious interception device; advertising a surreptitious interception device; advertising and promoting the surreptitious use of an interception device; intercepting electronic communications; disclosing electronic communications; and unauthorized access to a protected computer for financial gain.

Legal Loophole for Location in ECPA

Many location tracking stalking apps that only capture and disclose location would not violate ECPA, since ECPA does not cover location interception alone. This legal loophole allows app and device developers to create products that track and share a victim's location, 24 hours a day, as she goes to the police department to file a report, the courthouse to apply for a protection order, and the undisclosed and highly hidden domestic violence shelter to an abusive individual. More specifically, while ECPA requires user consent before a company shares the contents of that user's communications, the law allows a commercial entity to share a user's location information without his or her consent. As noted above, there are many location tracking "Stalking Apps" that only capture and disclose location, which would not violate ECPA, since ECPA does not cover location interception alone.

III. The Solution

A. Require consent prior to tracking or sharing information

Technology companies that develop location tracking tools or applications that rely on location tracking to improve their functionality can help protect victims by ensuring that the consumer has notice of the location information collected, whether that information is transmitted in real-time, who has access that information, and the length of time for which location information is retained. These concepts are not new – robust notice and truly informed consent has been best practice since the Fair Information Practices were articulated in the 1970s.⁴² In 2010, The Wireless Association (CTIA) published industry "*Best Practices and Guidelines for Location Based Services*."⁴³ These guidelines "rely on two fundamental principles: user notice and consent."⁴⁴

Survivors of abuse and all users must be informed about how their location information will be used, disclosed, and shared. This process should be prominent, transparent, and easy to understand. As noted in CTIA's *Guidelines*, "Any notice must be provided in plain language and be understandable. It must not be misleading, and if combined with other terms or conditions, the Location Based Service (LBS) portion must

⁴⁰ Ibid.

⁴¹ U.S. Department of Justice, Press Release. November 5, 2013 <http://www.fbi.gov/sandiego/press-releases/2013/fbi-seeks-information-regarding-several-cyber-fugitives>

⁴² <http://bobgellman.com/rg-docs/rg-FIPShistory.pdf>

⁴³ CTIA. *Best Practices and Guidelines for Location Based Service*. Volume 2.0. March 23, 2010. Available at: http://files.ctia.org/pdf/CTIA_LBS_Best_Practices_Adopted_03_10.pdf and www.ctia.org/policy-initiatives/voluntary-guidelines/best-practices-and-guidelines-for-location-based-services

⁴⁴ Ibid.

be conspicuous.”⁴⁵ Knowing how and when their location information (via mobile device) is gathered and shared will help empower victims to develop strategies to minimize their vulnerability and determine whether or not it is safe to carry their mobile phone and/or to purchase a new phone that will provide greater privacy and safety.

Users must have the opportunity to actively and meaningfully consent to the use, disclosure, or sharing of their location information. Meaningful consent must be prominent, succinct, and very easy to navigate. “Pre-checked boxes that automatically opt users in to location information disclosure, or choice mechanisms that are buried within a lengthy privacy policy or a uniform licensing agreement ordinarily would be insufficient to express user consent.”⁴⁶ Consent is especially critical when the product or application does not require location information in order to function. For example, some mobile internet browsers may retain location information regarding past wireless access points users have accessed. This may allow the device to more quickly access wireless internet in the future when an individual returns to that location. However, this is not critical to the functioning of the device. The device can search anew for internet access each time the user visits that physical location. While this will take more time, some consumers would prefer an increased wait time to having the device maintain unencrypted location log files for an unspecified amount of time. This may be especially true for victims of stalking and domestic violence, who have very real concerns about their personal safety.

Consumers can only truly consent when they have been provided with enough information to gain a full understanding of the collection, transmission, and retention practices and policies of the applications and services they use. Again CTIA’s *Guidelines* agrees: “All entities involved in the delivery of LBS, including wireless carriers, device manufacturers, operating system developers, application aggregators and storefront providers, should work to educate users about the location capabilities of the devices, systems, and applications they use as well as to inform them of the various privacy protections available.”⁴⁷ When consumers understand all elements of their devices and applications, they can make fully informed decisions that may enhance the privacy of many users and increase the safety of some especially vulnerable consumers, including battered women and consumers with low literacy and/or limited English proficiency.

B. Location tracking must be transparent and visible to users

Consent is critical, but consent alone is insufficient. It is common for abusers and stalkers to install tracking apps or devices without the knowledge of the victim/user/target of the tracking. Since the device cannot know if the actual user is consenting or if perhaps a stalker consented during a surreptitious install, a reminder that the user’s location is being tracked is critically needed.

Relatively simple safeguards can be added to help prevent misuse of the product and unauthorized access to information. For location-based services, this could take the form of periodic text messages, splash notification, or an ever-present icon to notify and remind the user that a tracking application is on the device. It can also take the form of a central transparent place to view all device features and additional applications that are requesting use of your mobile phone’s location. The iPhone, for example, lists all applications (e.g. Camera, Maps, Twitter, Yelp, etc.) that want to use location services and provides the user with an easy way to turn the location services on or off for the entire phone or for any individual application.

⁴⁵ Ibid.

⁴⁶ Ibid.

⁴⁷ Ibid.

If location tracking technology is being used legitimately to monitor children or employees, there is no need for a “stealth mode” or for it to run invisibly. The reputable family safety and location sharing social products only function with full notice, consent, and visibility. Location tracking technology designed to run in stealth mode is being designed to facilitate stalking and spying. In 2005, the AntiSpyware Coalition, consisting of major anti-spyware companies, software developers, and non-profit groups, created a consensus definition of spyware, which stated that tracking software, done covertly is spying” .⁴⁸

Excerpt from the Definitions:⁴⁹

The table below lists some technologies that have been used to harm or annoy computer users. It is important to note that with proper notice, consent, and control some of these same technologies can provide important benefits: tracking can be used for personalization, advertisement display can subsidize the cost of a product or service, monitoring tools can help parents keep their children safe online, and remote control features can allow support professionals to remotely diagnose problems.

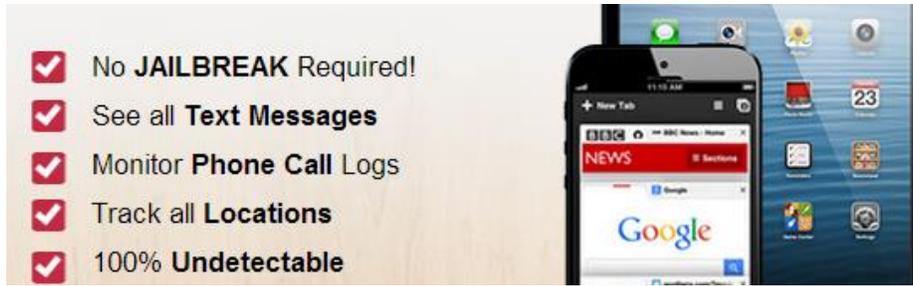
For example, the underlying technology that enables a keylogger is Tracking Software. Tracking Software can both harm and help a user. When a keylogger is installed and executed covertly, it is spying. On the other hand, a keylogger can be used for legitimate purposes with clear consent, such as letting an IT help desk remotely assist a user in problem diagnosis. An underlying technology typically becomes unwanted when it is implemented in a way that provides no benefit to -- or actively harms -- authorized users.

Underlying Technology	Description of Underlying Technology	Why the Underlying Technology May Be Wanted	Why the Underlying Technology May Be Unwanted	Common Terms for Well- Known Unwanted Varieties
Tracking Software	Used to monitor user behavior or gather information about the user, sometimes including personally identifiable or other sensitive information.	May be used for legitimate monitoring: e.g. by parents or companies. May be a necessary component of adware that is linked to wanted software. May allow customization	Done covertly, tracking is spying May collect personal information that can be shared widely or stolen, resulting in fraud or ID theft. Can be used in the commission of other crimes, including domestic violence and stalking. Can slow machine down May be associated with security risks and/or loss of data.	Spyware (narrow)* Snoopware Unauthorized Keylogger Unauthorized Screen Scraper

“Emma” fled to Minnesota from the other side of the country, seeking safety. Her stalker found her anyway, shattering her sense of safety. From 1,400 miles away, he would text message her that he knew exactly where she was and who she was with. She couldn’t figure out how he knew where she was. Then, on a day she took a trip outside of the rural Minnesota County where she lived, he showed up out of nowhere. She was terrified. Soon after, he moved to Minnesota. The stalking got worse. Emma and her advocate went to her cellphone carrier and law enforcement. Everyone said: you’ve got GPS tracking spyware on your phone – that’s how he knows your every move. But the police didn’t have the technology and training to examine the phone or remove the stalking app. ~ Advocate in Minnesota

⁴⁸ Anti-Spyware Coalition agrees spyware definition. SC Magazine. November 3, 2005 www.scmagazine.com/anti-spyware-coalition-agrees-spyware-definition/article/32584/

⁴⁹ <http://www.antispywarecoalition.org/documents/definitions.htm>



C. Criminalize the operation, sale, and marketing of technologies whose primary purpose is to surreptitiously track someone's location and facilitate a crime

It is currently a crime to manufacture, distribute, possess, and advertise electronic communication intercepting devices.⁵⁰ It is past time to also criminalize intercepting tracking location in addition to electronic communication.

Enactment of new federal and state criminal statutes criminalizing bad acts that misuse location technologies will have several positive effects. First, enacting new criminal statutes will empower law enforcement officials to target emerging, technology-aided forms of stalking or abuse and focus the criminal justice system's efforts towards penalizing bad acts. This may be especially valuable in the case of stalking or domestic violence where it is often the case that a series of escalating behaviors are a prelude to an ultimately tragic event. Equipping law enforcement with new statutes and new, potent penalties may allow for interventions before tragedies occur. Second, the enactment of these statutes may give victims and their lawyers and advocates new opportunities to seek out prosecutions, thereby empowering individuals that otherwise may feel powerless. Holding abusers and stalkers accountable will have a significant, beneficial effect for some victims and may help deter escalating abuse or break the cycle of abuse they are suffering. Third, it will help eliminate marketing of technologies that are designed to facilitate stalking and similar abuses.

HelloSpy is the most powerful mobile phone spy and tracking software that lets you monitor ALL the activities of any iPhone or Android phone. HelloSpy is super easy to install on the phone you want to monitor. It starts uploading the monitored phone's usage information and its exact location instantly which can be viewed by logging in to your HelloSpy user area from any computer(or smartphone) in the world within minutes. This state-of-the-art application works in stealth mode which means that it will never be found on the target cell phone.

D. Allow law enforcement to seize the proceeds of those sales to fund anti-stalking efforts

No one should profit from encouraging or enabling criminal acts, and stalking app and device developers are creating and selling crime-facilitating products with abandon. Federal law (18 U.S.C. § 2513) provides that entities who violate the prohibition on wiretapping (18 U.S.C. § 2511) and the prohibition on making a device whose primary purpose is wiretapping (18 U.S.C. § 2512) can have the devices used to commit those violations forfeited. Funds seized from companies promoting stalking and abuse should go to support prevention, awareness, and training to help end stalking and abuse.

⁵⁰ 18 U.S. Code § 2512 Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited

E. Allow individuals an enforcement option through a VERY modest private right of action

The proposed protections for victims will be of little use without effective enforcement mechanisms. The Attorney General has limited resources and not every division can prioritize resources for prosecution. Individual victims must be able to obtain recourse. It is also in the interest of public safety for the entire community, not just for an individual stalking victim, to hold accountable developers who willfully and knowingly develop and market apps and devices to facilitate crime.

Since the penalties proposed in the bill are capped globally at \$1 million for accidental acts or omissions, and \$2 million for intentional or willful violations, these amounts would be de minimis to any large reputable company; however, the amounts could be a vital incentive to counter the potential profits an unscrupulous developer may earn by marketing and selling to stalkers.

Please note that many small businesses carry liability insurance that would likely cover non-willful violations. Small businesses are typically required to carry insurance if they want to take out a lease or loan, and per some contracts.

F. Require the federal government to gather more information about GPS stalking, facilitate reporting of GPS stalking

NNEDV supports gathering more information and statistics while recognizing the staggering financial cost to doing comprehensive national supplemental studies. In early 2004, staff from the U.S. Department of Justice Office (DOJ) Office on Violence Against Women (OVW) worked with the DOJ Bureau of Justice Statistics (BJS) to develop a special survey on stalking. At the time, the most recent data were nearly 10 years old and there was a critical need for more detailed information about victims of stalking, offenders who commit stalking, victim interaction with the criminal justice system, and the monetary cost of stalking to victims and society in general. OVW and BJS agreed to work in partnership to develop a “stalking supplement” to the National Crime Victimization Survey (NCVS).

In the absence of a comprehensive national study, many smaller studies and surveys have shown an increase in the incidence of technology misuses corresponding to the increase by the broader community of technology use.

G. Require the federal government to prioritize funding for GPS stalking prevention, awareness, and detection efforts

20% of stalking victims stated the police took no action when contacted.⁵¹

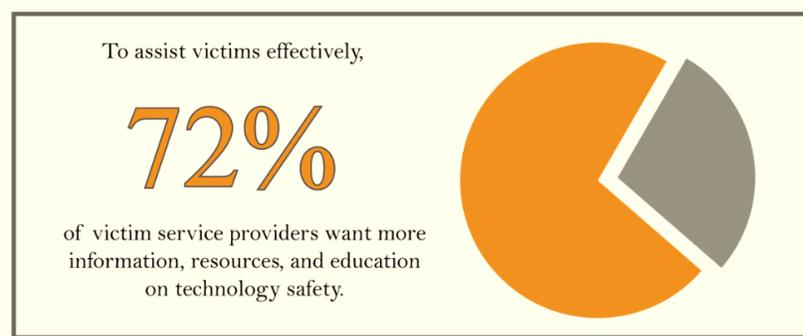
NNEDV has trained over 65,000 police, prosecutors, victim advocates, judges, and other professionals in the past 12 years on the safe use and misuse of technology. Given the high rate of turn-over in these demanding and underpaid professions, ongoing technology training is needed – even in communities that were trained recently. NNEDV is able to accept one training invitation for every two-three training requests that we have to turn down. Every ballroom filled with officers and advocates equals thousands of victims who will have a trained support system that understands location privacy and technology stalking. Unfortunately the demand for training far exceeds the

“Spyware that can easily be installed on mobile phones is often used by abusers and stalkers to track or contact women who have filed protection orders against them. Police need to be aware of these technologies and the role they can play in stalking and domestic violence situations.” Orvena Gregory, Second Chief, Sac and Fox Nation (Oklahoma)

⁵¹ Center for Policy Research, Stalking in America, July 1997

funded training resources. NNEDV's Safety Net Team could double our staff from two full-time trainers to 4 full-time trainers and still need to turn down far too many training requests.

Training is needed and has been requested by officers and advocates in all states, U.S. Territories, and Tribal communities. A 2012 survey found that 72% of victim service providers want more training and resources on technology stalking and safety.⁵²



H. Enact parallel state and Tribal laws to allow local, state, and Tribal level enforcement

NNEDV is hopeful that the Location Privacy Protection Act of 2014 will become a model for state legislatures and for NNEDV's member state domestic violence coalitions to develop state complementary laws. Such state laws could expand the enforcement from federal to state law enforcement since the overwhelming majority of stalking and domestic violence investigations are completed by local police and corresponding charges are filed by local prosecutors.

IV. Conclusion

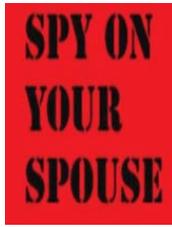
NNEDV supports innovation and has seen countless positive ways that technology, when developed thoughtfully, can increase the safety and support for survivors of abuse and stalking. We are proud of the close working relationship that we have with technologists and we thank Verizon, Google, Facebook, Apple, and the Application Developers Alliance for consistently working with us to increase survivor safety. The Location Privacy Protection Act of 2014 will narrowly impact a handful of bad actors that design or operate products created and sold to facilitate terrifying crimes. Senator Franken, thank you for your tireless and ongoing efforts to end violence against women. Thank you to Ranking Member Flake and the entire committee for your long support of VAWA and these important location protections for survivors.

After getting a protection order "Beth" began seeing her abuser everywhere. As a nurse, her scheduled days to work were variable, and she did not always go straight home, so she really didn't feel her whereabouts were "extremely predictable." Beth took her phone for service, and explained everything to them. The phone had applications running on it that they were unfamiliar with. Unfortunately Beth's reports of stalking were not believed. It took her ex brutally bludgeoning her almost death for them to take her seriously. Beth survived that attack. Her ex was convicted of 1st degree attempted murder and is now serving a decades-long sentence. ~ Advocate in Minnesota

⁵² NNEDV, "New Survey: Technology Abuse & Experiences of Survivors and Victim Service Agencies," www.ovc.gov/news/grantees.html and <http://techsafety.org/blog/2014/4/29/new-survey-technology-abuse-experiences-of-survivors-and-victim-services> (data collected in 2012)

A Sampling of Tracking Apps and Devices Marketed to Stalkers

Track My Spouse Cell Phone
 (Bibacory) - April 26, 2013
 Lifestyle
 Install Add to Wishlist
 This app is compatible with your device.
 ★★★★★ (60) 8+1 +154



GPS Tracking Devices
 Easily Hidden Real Time GPS Trackers & Loggers

TrimTrac Pro Real Time GPS Tracker
 > VIEW DETAILS

Silver Cloud Cover Realtime GPS Tracker
 > VIEW DETAILS

Spy Software for Cell Phones
 Silently Monitor Calls, SMS, Contacts and GPS Location

BUY NOW
 100% Undetectable

stealthGenie

Flexispy Gives You Total Control Of Your Spouse's Cell Phone Without Them Knowing

Install FlexiSPY on the cell phone you want to monitor — it then works invisibly in the background, continually sending you information about everything that is happening on your spouse's cell phone.

Shop All Items

SilverCloud Tag Live View Personal Real Time GPS Tracker
 Silver Cloud Cover Realtime GPS Tracker / Tracking Device for car / vehicle
 Covert Real Time Tracker SilverCloud Synch Hidden GPS Tracker - Always Tracking Device
 Micro Tracker II Real Time GPS Covert Tracking Device

AccuTracking
 Eyes at Your Fingertips ... Low Cost GPS Tracking Service for Everyone

HOME SERVICES FEATURES DEMO STARTER KIT PRICING LOGIN FAQ SUPPORT FORUMS

• [knowledgebase](#) [Will it work in the car trunk, indoors, underground?](#)

A Sampling of Features and Different Spying and Stalking Devices

Question: Is the application invisible?
Answer: mSpy works in stealth mode.
 It does not display any icons and appears on the device application database under different names (system processes), which leaves virtually no chance for the user to identify this software. Moreover, there are neither logs stored on the target device nor pop-up messages ever showing up on the main screen.

<p>Specialized For Spying On Instant Messages</p> <p>FlexiSPY is the only spy software that can spy completely on WhatsApp, Facebook, Skype, Viber, WeChat, LINE, & BBM</p>	<p>Call Interception</p> <p>Listen & record live phone call conversations as they happen. No other spyphone can do this</p>
<p>SMS Tracker</p> <p>Read SMS & email messages to see what they're saying</p>	<p>Bug Their Room</p> <p>Listen in on their phone's surroundings & hear what's really going on behind closed doors</p>
<p>Cell Phone Tracker</p> <p>Are they really where they say they are? Pinpoint their exact location & find out</p>	<p>Spy On Mobile Phones</p> <p>Monitor any mobile phone & get the data you need right on your computer & phone</p>
<p>Password Cracker</p> <p>Read the passcodes & passwords contained in any Android, iPhone or iPad, so you can access their services directly. A feature</p>	<p>More Features Than Any Other Product</p> <p>FlexiSPY has over 150 features which is more than any other spy product - many of which are totally unique. Other products claim to be the most powerful.</p>

GPS Location, Cached Location, Network Location, Cell Tower Location

Battery Saver
 Make three long clicks in top left screen corner and you will be able to access GPS-tracker settings.
 BATTERY SAVER is running...

Spy On Email

The user can easily go through all the emails that get handled via the target cell phone. So if you doubt that your employee might be carrying the crucial information out via emails. Click below for more features.

[View Incoming / Outgoing E-mails](#)

- ✓ 5 min download from web
- ✓ 100% undetectable
- ✓ Records 5 Key activities
- ✓ View remotely from Web
- ✓ 1 view for all devices

Unit1 Dec 20 2005 04:38:51 PM
 Speed: 4 mph
 Heading: S

Unit2 Dec 21 2005 09:19:49 AM
 Speed: 17 mph
 Heading: SE

Track GPS Location

With the inbuilt GPS device, the GPS Software of Imobispy efficiently traces and records all the GPS locations of the monitored cell phone. Click below to view features.

[View current GPS location](#)

Android Spy Software
 100% Undetectable - Monitor Android Devices Remotely

Monitor iPhone Without a Jailbreak!
 View Text Messages, iMessages, Locations and more!

Monitor Internet Activities

This feature will enable the user to get through all the websites that the monitored cell phone user has browsed. Click below for more features.

[URL Tracking](#)