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

**For the Hearing of the Senate Judiciary Committee**
**Subcommittee on Privacy, Technology and the Law**
**United States Senate**
**Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy**

**May 10, 2011**

***Introduction***

Chairman Franken, Ranking Member Coburn, and distinguished Members of the Committee, the National Network to End Domestic Violence, on behalf of its member coalitions including the Minnesota Coalition for Battered Women, thanks you for the opportunity to submit testimony on this important issue. The National Network to End Domestic Violence (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.

In 2002, NNEDV's Safety Net Technology Project was launched nationally to educate victims of stalking, sexual and domestic violence, their advocates and the general public on the strategic use of technology to increase personal safety and privacy. For the past nine years, the Safety Net Project has been providing training, education, support and technical assistance for domestic violence victims and their advocates as they navigate the benefits and challenges of the Internet and other forms of technology. One issue the Safety Net Project has long focused on is survivor safety and privacy in an increasingly networked and mobile world. The Safety Net Project provides ongoing trainings, tools, and advice that helps victims increase and maintain their online and mobile privacy when using social networking sites and location based and social location sharing services. We also train victim advocates, law enforcement, lawyers, prosecutors, and others how to recognize and hold abusers accountable when they misuse technology, such as global positioning system (GPS) or spyware programs, to monitor and stalk.

NNEDV works closely with our 56 member coalitions, including The Minnesota Coalition for Battered Women. The Minnesota Coalition for Battered Women is a well-established, membership organization with 83 local, regional, and national member programs located throughout Minnesota. The Coalition has existed for almost 30 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.

Minnesota 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 most recently, 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 sudb. 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 in 2010 because they received reports from battered women throughout the state that modern technology was being misused by abusers to stalk victims.

As we address the Committee's questions it is critical to point out that technology does not cause stalking. If a victim removes all technology from her life, her controlling abuser will simply resort to utilizing

non-technological means to harass, monitor, and stalk. However, since technology is prevalent in our lives, stalkers and abusers use this readily available tool to facilitate their harm and control. Abusive partners want control and power over the victim. In fact, the most dangerous time for a victim of domestic violence is when she takes steps to leave the abusive relationship.[1] Women who are separated from their abusive partners are 3 times more likely than women who are divorced and 25 times more likely than married women to be victims of violence at the hands of an intimate partner.[2] 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.[3] In fact, 54% of femicide victims reported stalking behavior to the police before the victims were killed by their stalkers.[4] Eighty percent of women who are stalked by former husbands are physically assaulted by that partner and 30 percent are sexually assaulted by that partner.[5]

Stalking is an extremely dangerous event for victims and it can be equally dangerous for those around. The abuser who knows the location of a shelter program in which the victim is residing and seeking safety can target the entire shelter and put all the residents at serious risk of harm. The Minnesota Coalition for Battered Women recently surveyed their 83 member programs and received numerous accounts of how batterers misuse modern technology to further monitor, control, and intimidate women. Batterers misuse various forms of technology in conjunction with one another to optimize the level of control and power over their victims.

When victims are harmed by abusers who misuse technology, some people suggest that the victim get rid of the technology to prevent the stalking or harassment. For some victims who are in the process of planning to leave an abuser, changing phone numbers, getting rid of a cell phone, or discontinuing social networking or location sharing sites may actually increase suspicion by the abusive partner and increase the risk for violence. Sometimes when an abuser's ability to remotely track a victim is interrupted, the abuser escalates his violence in an attempt to regain control over the victim. There are additional reasons why "simply discontinuing" her use of technology might result in greater harm to a victim. For instance, many victims with disabilities use technology to decrease barriers, assist with activities in their daily lives and facilitate or enable communication with the outside world. In these instances, it may be impossible or very difficult for the victim to stop using the technology, despite the fact that the stalker might be misusing it to monitor or control her.[6]

## ***Mobile Technology's Benefits to Victims***

As technologies converge, mobile phones are able to do so much more for victims who are fleeing violence. Victims can use technology to call 911, take pictures of an abuser who violates a no-contact order, send and receive emails from supportive family member, search for help on the Internet, and map directions in real-time. This instant access to information has made it easier for victims of domestic violence to seek and find safety from abuse. From their mobile devices, victims can locate a domestic violence program in their community, reach out for support, find information about protection orders, and search for housing and employment opportunities. In addition, mobile devices have enabled survivors of abuse to stay in touch with their families and friends and find support in new communities, which often helps reduce isolation, an integral part of an abusive relationship. For people experiencing violence who are Deaf or have a disability, accessible mobile devices and relay services can decrease barriers and ensure access to help at crucial moments. For example, people who are Deaf can use a web browser or Instant Messaging program on a mobile phone to

---

[1] Ronet Bachman and Linda Salzman, Bureau of Justice Statistics, *Violence Against Women: Estimates From the Redesigned Survey* 1 (January 2000).
[2] Ronet Bachman and Linda Salzman, Bureau of Justice Statistics, *Violence Against Women: Estimates From the Redesigned Survey* 1 (January 2000).
[3] 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),
[4] Judith McFarlane et al., "Stalking and Intimate Partner Femicide," *Homicide Studies* 3, no. 4 (1999).
[5] Center for Policy Research, *Stalking in America*, July 1997
[6] 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.

make calls via IP Relay to hotlines or 911. In summary, new technology and mobile technology can benefit many victims.

Cell phones can be a lifeline for battered women and victims of sexual assault and stalking. Enhanced 911 features of cell phones provide operators with critical location information of a victim. Cell phones have also been beneficial in helping victims and finding abusers. In 2005, a young woman in Maryland used text messaging to get help while being kidnapped by her ex-boyfriend. Hiding the phone between the passenger seat and the door, she texted her sister who called 911 and relayed the license plate number and other crucial information. The woman was rescued by New York police. [7]

In March 2011, a man was arrested for kidnapping his 4-year-old son outside of a domestic violence center, where, fearing for her safety, the boy's mother had gone to seek help in obtaining a restraining order. By quickly working with the man's cell phone service provider, police were able to track his movements based upon his cell phone signal. He was taken into custody without incident 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.[8]

## *Past Harm to Victims from Abusers and Stalkers who Misuse Mobile Technologies*

Although it is obvious that mobile devices can be quite helpful they can also store or provide sensitive information about the user's activities, communications, and location. As technology evolves, stalkers and abusers quickly misuse it for nefarious purposes. Years ago, abusers who enforced rigid control over their victims' movements would check the odometer on the car to discover, by noting the excessive mileage, whether the victim had dared venture to the grocery store when the abuser had forbidden any trip beyond picking up the children at school. Enhanced technologies have provided more sophisticated tools for the same behaviors and crimes.

In a recent case in Northern St. Louis County, MN, an advocate reported that a woman who entered the domestic violence program located within a county building received a text message from her abuser within five minutes of entering the building. The abuser asked why she was in the county building. The woman was extremely frightened and the advocate helped her obtain an Order for Protection (OFP) at the local courthouse. After filing the OFP, the woman received another text message asking why she went to the courthouse and if she was filing an OFP against him. The only device the woman had on her was her smart phone and they later concluded that her abuser was tracking her via a location tracking application or service on her phone.

In another situation in Minnesota, an immigrant woman from Thailand who sought emergency housing in a metro area domestic violence shelter discovered that her American citizen husband had used a location tracking application or service on her phone to monitor and control her whereabouts. The Thai woman came to America with a limited understanding of the American judicial system and spoke very little English. Her only family in the United States was her husband who was physically, emotionally and psychologically abusive towards her. He even went so far as to apply for an Order for Protection against his Thai wife in order to further manipulate and control her. Finally, through the police, she was able to escape her abusive husband and seek shelter at the local domestic violence program. While staying at the shelter, her abusive husband sent her text messages asking why she was there and told her to come home. He would call taxi cabs to wait for her outside of the shelter at all hours of the day until she was relocated to another location. The Thai woman did not know her husband used her cell phone to monitor her whereabouts but she did suspect he was monitoring her. It seemed too coincidental that he would randomly show up at places where she was going or he would know where she had been during the day. It wasn't until she arrived at the shelter that she realized her abusive husband was using an application on her cell phone to track her. Battered women who are limited English

[7] Lee, Jennifer. "Cellphone Messages Lead Police to Abducted Maryland Woman." *The New York Times - Breaking News, World News & Multimedia*. 11 June 2005. Web. 26 Apr. 2011. <http://www.nytimes.com/>.
[8] 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

proficient (LEP) are often some of the most vulnerable battered women and they need additional safeguards to protect them against abusers.

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.[9] Numerous cases of GPS stalking have arisen since then. In 2010, an Arizona man stalked his wife using a location service before allegedly murdering their two children and shooting himself.[10] 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. [11]

It is difficult to determine the prevalence of cases involving misuse of mobile technology. Although research is beginning to emerge, victims of stalking often do not know all of the methods a stalker uses to gain information. Victims' unsubstantiated reports are likely to be disbelieved and offenders are unlikely to disclose their illegal stalking tactics. Additionally, many stalking cases are never reported to law enforcement, so reliance on police reports will, again, provide an underestimate. Research from data collected in 2006 shows that more than 1 in 4 stalking victims reported that their stalker used some form of technology to stalk them.[12] Of those who were aware and able to report being stalked electronically, 83 percent reported being stalked by email or instant messaging. Additionally, 46 percent reported that the stalker used a camera to monitor their actions, and 10 percent reported that GPS technology was used to monitor them.[13] With the growing use of mobile location-based services, it is our experience that perpetrators are location-tracking victims more often and in increasingly varied ways. Paradoxically, when crimes are committed using digital technology, there is often digital evidence that can assist in investigating and prosecuting the abusers.

## *Harm to Victim from Abusers and Stalkers who Misuse Mobile Technologies*

This committee has expressed an interest in learning about location tracking through mobile devices and location-based services used in mobile phones and other devices. As mentioned earlier, mobile devices that have location services can be quite helpful, particularly in cases where law enforcement can use that information to locate someone who dials 911 or is missing. For victims, GPS-enabled mobile devices allow them to use applications that list nearby shopping, hospitals or police stations, provide quick real-time directions, and more. However, the location capability of GPS also has risks when it is misused.

Stalkers may misuse technology and enable location products offered through a wireless phone service provider or install location tracking applications onto GPS-enabled cell phones,. 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 extra authentication and verification steps, such as automatically sending a text message to the phone informing them that a tracking application or service has been enabled. For this reason, stalkers may favor third-party location tracking applications (available in some app stores or via Internet) because some of these tracking applications and services do not provide as much notice to the consumer or verification that consent to track has been obtained. There are ways 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.

---

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

[10] 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. <http://online.wsj.com/article/SB10001424052748703467304575383522318244234.html>.

[11] Ibid.

[12] Baum, K., Catalano, S., Rand, M., & Rose, K. (2009, January). Stalking Victimization in the United States. *Bureau of Justice Statistics Special Report. NCJ 224527.* 1-15.

[13] Ibid.

Another method in which an abuser may attempt to discover sensitive victim information is through call history and other data collected by cell phone service providers and devices. Risks regarding information stored on the device is highest for victims who have not yet fled and have regular contact with the abuser who can, with physical access to the phone, track the extent to which victims may be reaching out for help and trying to plan an escape. The location data collected by cell phone service providers is not typically accessible to the general public. Generally law enforcement must subpoena the cell phone provider for that information.

Sometimes, the mobile device stores location information. For example, certain iPhone and iPad devices may automatically store a file with historical location information of the Wi-Fi hotspots and cell towers nearest where you have been. When this historical data is viewed by an abuser, there is a risk that an abusive partner could use this file to see where the victim has been. It is yet unclear all the ways a technology-savvy abuser might attempt to misuse this data, however the information in this file might provide information about where the victim has been going versus real-time location tracking of the victim. For example if a victim is secretly visiting a domestic violence center but told her abuser that she was across town at the library, the historical location information might alert the abuser to her plans to leave. While this sort of location information on a device can reveal information the victim wants to hide from her abuser, if an abuser is monitoring and controlling the victim to that extent, it is unfortunately likely that the abuser is also using other technologies to control and monitor the victim possibly even including spyware or keystroke loggers on the victim's home computer or smart phone.

As technologies converge, and voice, data, and location are offered by one mobile device, the information these devices collect and store can be revealing. At the same time, some benefits of this technological convergence can be helpful for survivors seeking to use their mobile device to call for help, search the Internet for critical legal information, and use location services to identify the nearest police department. To support the privacy of all consumers, including the safety of victims, it is critical that companies be transparent about what data is being collected, when it is collected, what application or service is using the data, who the data is shared with, and how long the data is stored. Companies must also allow consumers to choose what information can or cannot be collected and with whom that information will or will not be shared.

## ***Protecting Victims***

To increase victim safety and privacy, whenever possible, NNEDV works with an impressive array of technology companies to incorporate privacy features into their products. Many technology companies, including AOL, Facebook, Google, Loopt, Microsoft, Twitter and Verizon, have proactively solicited NNEDV's input and feedback before releasing new products. Apple recently contacted NNEDV and we hope that Apple will continue to work with us to increase privacy for all consumers including enhanced safety for victims.

NNEDV has worked closely with wireless phone carriers such as Verizon and third-party Location Based Service (LBS) applications such as Loopt and Google Latitude to ensure that an abuser cannot turn on a location tracking service on the victim's phone without the victim's knowledge. With special consideration to victim safety, some third-party location-sharing applications even allow a victim to manually set her location so if her abuser forces her to share her location while she is still in the relationship and risking violent retribution, she can manually set a false location and then secretly travel to meet with a victim advocate, a police officer or an attorney.

In this digital age, any company that is rolling out services that use a consumer's personally identifiable information or location should proactively identify and address risks for victims of domestic and sexual violence, stalking and abuse. This is not only good business but it can save lives. For example, since 2007, NNEDV has worked with Google to ensure that the confidential addresses of domestic violence shelters are removed from Google's Street View and the Google Maps application. NNEDV has also assisted Verizon, Google, Loopt and other companies in working to prevent stalkers and abusers from misusing products and in creating user privacy and notification options for location-based services and other products. We welcome

further opportunities to assist Apple and other companies on mobile privacy options that enhance the privacy of all consumers, especially those with heightened safety concerns.

Technology companies that develop location tracking tools or applications that rely on location tracking to improve their functionality or speed can help protect victims by ensuring that the consumer has notice of the information collected, whether that information is transmitted in real-time, and the length of time for which location information is retained. To best protect victims, and comply with industry standards, cell phone service providers, application developers, and device manufacturers should follow the Wireless Association's (CTIA) *Best Practices and Guidelines for Location Based Services.*[14] These guidelines "rely on two fundamental principles: user notice and consent."[15]

Users should 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 LBS portion must be conspicuous."[16] 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 pre-paid 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."[17] 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. This may be 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. As CTIA's *Guidelines* suggest, "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."[18] 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.

When developing products that may track or share location or other sensitive information, device manufacturers and application developers should consider and proactively address and minimize potential misuses of their product. They should consult with organizations, such as NNEDV and its member coalitions, that work with victims to determine how similar products have been misused in the past and work closely with technology companies to identify low cost, but high impact notifications which might alert a victim to monitoring or stalking. Relatively simple safeguards can be added to help prevent misuse of the product and unauthorized

[14] 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
[15] Ibid.
[16] Ibid.
[17] 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
[18] Ibid.

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, Loopt, Foursquare, Twitter, Yelp, Dictionary, 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. Robust verification and authentication processes will also help prevent illegitimate access to information.

Finally companies should develop processes that will respond to and support victims quickly when technology is being misused by abusers or stalkers to harm. Companies should create an accessible and responsive process that provide clear and quick information to users about how their technology works, how to work with either the company or law enforcement to stop the abusive behavior, and resources that can provide assistance to victims.

## *Conclusion*

Mobile devices have, undeniably, become an amazing safety tool for victims of violence and stalking. Knowing that one can summon help with the press of a single key can provide incredible peace of mind to a victim of stalking or abuse. Unfortunately, mobile devices can also be misused by abusers to stalk, monitor, and locate victims. By working together with groups like NNEDV to protect those most vulnerable to misuse of their location and personally identifiable data, a variety of companies in the mobile industry have demonstrated a commitment to minimizing any possible risks and maximizing benefits for all consumers are fully considered. NNEDV recommends first, that all mobile providers and application developers follow the Wireless Association's (CTIA) *Best Practices and Guidelines for Location Based Services*[19] and second, that companies work proactively with organizations such as NNEDV that specialize in addressing how technology impacts victims to anticipate and address potential harms before they ever occur. When companies proactively design safety and privacy options into their products and services with victims clearly in mind, they help victims of domestic violence, sexual violence and stalking stay alive and be better protected, and they prevent abusers and stalkers from easily misusing their products to further perpetrate abuse and harm. Designing privacy, notice and consent into mobile devices, applications and services that use location or personally identifiable data will keep us all – victims, the victim's family and friends, police officers, and community members – safer. It is good business and it may save lives.

[19] 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