



OLR RESEARCH REPORT

November 14, 2011

2011-R-0386

LAW AND LEGISLATION ON CELL PHONE TRACKING DEVICES

By: Kevin E. McCarthy, Principal Analyst

You asked whether any federal or state laws or proposed legislation regulate the sale or use of technologies that track the location of a cell phone. You also requested a discussion of legislative options to address this issue. You were primarily interested in the use of such devices or software by parties other than law enforcement agencies. Your question was prompted by a constituent whose home was burglarized by a person who used this technology to find out when the constituent was away from home.

SUMMARY

Cell phones and other electronic devices generate geolocation information that can be used to determine the (1) location of the devices and their owners or (2) types of activities a person engages in at a particular location. There are a variety of commercially available technologies that allow parties other than service providers to collect and record this data. These technologies can be used for benign purposes, such as tracking a lost child, as well as criminal purposes as apparently happened to your constituent.

We have not found any federal or state laws that specifically address the sale or use of technologies that track the location of a cell phone or other geolocation data. But there is legislation pending in Congress and California in this area.

Four bills (S. 1212, H.R. 2168, S. 1223, and H.R. 1895) have been introduced in Congress this session to regulate the acquisition and use of geolocational data.

S. 1212 and H.R. 2168 (companion bills) make it a federal crime to intentionally intercept geolocation data pertaining to another person or to disclose or use that information. The bills have a number of exceptions, such as collecting information on another person with his or her consent, collecting information in connection with a theft, and foreign intelligence surveillance. The bills modify the Federal Rules of Criminal Procedure to require a search warrant for a law enforcement agency to acquire geolocation information. They allow a person whose geolocation data is intercepted, disclosed, or intentionally used in violation of the bill to recover civil damages.

S. 1223 makes it a federal crime for a nongovernmental individual or entity engaged in the business of offering or providing a service to electronic communications devices from knowingly collecting, obtaining, or disclosing to a nongovernmental individual or entity geolocation information from an electronic communications device without the express authorization of the individual using the device. The bill prohibits the: (1) unauthorized disclosure of geolocation information in aid of interstate domestic violence or stalking and (2) sale of geolocation information regarding children under age 11. On the other hand, it allows geolocation data to be tracked in order to locate a minor child or provide fire, medical, public safety, or other emergency services, among other things. The bill authorizes civil actions by the U.S. attorney general, state attorneys general, and aggrieved individuals for violations.

H.R. 1895 requires the Federal Trade Commission to adopt regulations on the collection of geolocational data from minors. The regulations must require an operator of a website, online service, online application, or mobile application directed to minors to provide clear and conspicuous notice in clear and plain language of any geolocation information the operator collects, how it uses the information, and whether it discloses the information. The operator must obtain a verifiable parental consent before collecting the information from a minor. After collecting the information, the operators must give the parent or a child, upon request, a description of the information collected and the opportunity at any time to refuse to permit the further use or maintenance in retrievable form, or future collection, of information from a child.

Tracking legislation is pending in California. SB 761 requires the adoption of regulations to require a person or entity doing business in California that collects, uses, or stores certain types of data to provide people with a method to opt out of that collection, use, and storage of such information. The bill has more stringent requirements regarding “sensitive information,” which includes the consumer’s location and any information about the individual’s activities and relationships associated with that location, e.g., what an individual typically does at a given location. An entity that willfully violates the regulations is liable to the affected individual in a civil action for actual damages, with a \$100 minimum and \$1,000 maximum, plus punitive damages as the court may allow.

Connecticut law does not specifically address the use of tracking technologies and it is unclear whether current Connecticut law applies. For example, in the case that prompted your question, it could be argued that the burglar violated [CGS § 53a-106](#), which bars the manufacture or possession of burglar’s tools. Other laws that might apply include those that prohibit wiretapping and computer crimes.

The legislature has many options regarding the possession and use of tracking technology. It could modify existing criminal laws to make them apply to certain uses of tracking technologies, create new criminal offenses, or create a cause of action for people injured by the illicit use of the technologies. For example, the legislature could: (1) specify that the possession of the tracking technology by parties other than service providers or law enforcement agencies violates [CGS § 53a-106](#), (2) create a new offense of possessing or using the technology in the furtherance of crimes such as burglary, or (3) make the use or possession of the technology an aggravating circumstance of such crimes as stalking, that subjects an offender to a higher penalty than otherwise applies.

INTRODUCTION

Geolocation data is information generated by electronic devices including cell phones, Wi-Fi equipped laptops, and GPS navigation units that can be used to determine the location of these devices and their owners. A variety of firms use this information for commercial reasons. Cell phone providers use it to route calls to their customers, GPS navigation services companies use it to help their customers avoid getting lost, and other companies use it to provide assorted online services. The Federal Communications Commission requires wireless network providers to give public safety personnel the cell phone GPS tracking location information for E-911 calls that have been made from cell phones.

There are a variety of commercially available products that allow parties other than service providers to collect and record this data. In some cases the uses of this technology are benign, e.g., parents keeping track of their children. On the other hand, the technology can be used for criminal or anti-social purposes. According to the National Center for Victims of Crime (www.ncvc.org), criminals can obtain geolocation data in several ways. These include (1) taking advantage of software installed by the user such as FourSquare, Latitude, or Facebook, that provide opt-in location tracking services on smart phones and other mobile devices and (2) covert third party applications installed by the offender, such as MobiSpy, which secretly record and report the victim's location.

LAWS AND LEGISLATION

Federal

S 1212 and H.R. 2168. The Geolocational Privacy and Surveillance Act (the GPS Act) amends the federal criminal code to prohibit intentionally:

1. intercepting geolocation information pertaining to another person;
2. disclosing to any other person such information, knowing that it was obtained in violation of the bill; or
3. using geolocation information, knowing that the information was obtained in violation of the bill.

It makes exceptions for interceptions involving:

1. information acquired by a provider of covered services (electronic communication service, remote computing service, or geolocation information service) in the normal course of business;
2. federal officers, employees, or agents conducting foreign intelligence surveillance;
3. persons having given prior consent;
4. public information;
5. emergency information;

6. theft; or
7. a warrant.

The bill allows geolocation data to be obtained, with a warrant, in connection with a criminal investigation. However, it makes it a crime to disclose this information to any other person, knowing that it was obtained in connection with an investigation, with intent to improperly obstruct, impede, or interfere with the investigation.

The bill prohibits use illegally obtained information, and evidence derived from it, as evidence. But, it allows investigative or law enforcement officers and a state's principal prosecuting attorney to intercept and use such information under specified emergency circumstances.

The bill also prohibits acquiring geolocation information of a person for protective activities or law enforcement or intelligence purposes except with a warrant issued under the Federal Rules of Criminal Procedure or the Foreign Intelligence Surveillance Act. It directs the United States Sentencing Commission to review the federal sentencing guidelines and policy statements applicable to persons convicted of fraud and related activity in connection with obtaining certain confidential phone records information.

The bill sets penalties for violations of its provisions. It also allows a person whose geolocation information is intercepted, disclosed, or intentionally used in violation of the bill to recover actual or statutory damages from the person who committed the violation. The statutory damages are \$100 per day or \$10,000, whichever is greater. The court can also award punitive damages.

The Senate bill, introduced by Senator Wyden, is currently before the Senate Judiciary Committee. The House bill, introduced by Representative Chafetz, has been referred to Subcommittee on Crime, Terrorism, and Homeland Security of the House Judiciary Committee.

S. 1223. The Location Privacy Protection Act of 2011 amends the federal criminal code to prohibit a nongovernmental individual or entity engaged in the business of offering or providing a service to electronic communications devices from knowingly collecting, obtaining, or disclosing to a nongovernmental individual or entity geolocation information from an electronic communications device without the express authorization of the individual using the device. It defines

“geolocation information” as any information concerning the location of an electronic communications device and used to identify or approximate the location of the electronic communications device or the individual using the device. The bill makes exceptions for:

1. locating a minor child or providing fire, medical public safety, or other emergency services;
2. transmitting the geolocation information to the individual or another authorized recipient; or
3. uses expressly required by states, regulations, or appropriate judicial process.

The bill requires an entity that provides geolocation information to: (1) provide notice that geolocation information relating to an individual is being disclosed to another individual and (2) inform an individual on how he or she may revoke consent to the collection, receipt, recording, obtaining, and disclosure of geolocation information relating to him or her.

The bill authorizes civil actions by the U.S. attorney general, state attorneys general, and aggrieved individuals for violations, subject to specified limitations.

The bill prohibits: (1) the unauthorized disclosure of geolocation information in aid of interstate domestic violence or stalking, and (2) the sale of geolocation information regarding children under age 11.

In addition, the bill directs: (1) the National Institute of Justice to conduct a national study to examine the role of geolocation information in violence against women; (2) the Office on Violence Against Women director to establish a task force to assist in the study's development and implementation; (3) the Federal Bureau of Investigation, in conjunction with the Bureau of Justice Assistance, to create a mechanism using the Internet Crime Complaint Center to register complaints of crimes aided by use of geolocation information; and (4) the U.S. attorney general to develop a national education curriculum to ensure that all courts, victim advocates, and state and local law enforcement personnel have access to information about relevant laws, practices, procedures, and policies for investigating and prosecuting the misuse of geolocation information.

The bill, introduced by Senator Franken, has been referred to the Senate Judiciary Committee.

H.R. 1895. The Do Not Track Kids Act of 2011 requires the Federal Trade Commission to adopt regulations on the collection of geolocation data from minors. It prohibits the operator of a website, online service, online application, or mobile application directed to minors, or an operator having actual knowledge that it is collecting such information from minors, from collecting such information in a way that violates the regulations.

The regulations must require an operator to:

1. provide clear and conspicuous notice in clear and plain language of any geolocation information the operator collects, how it uses the information, and whether it discloses the information and
2. establish procedures or mechanisms to ensure that geolocation information is not collected from minors except in accordance with the regulations.

When collecting geolocation information from a minor, the operator must:

1. obtain a verifiable parental consent before collecting the information;
2. after collecting the information, give the parent, upon request, a description of the information collected and the opportunity at any time to refuse to permit the further use, maintenance in retrievable form, or future collection of information from a minor;
3. give the same notice and opportunity to a child who is 13 to 17; and
4. provide a way to obtain any information collected from a minor, if it is available to the operator when the parent or child aged 13 to 17 makes the request.

The consent or authorization is not required to collect geolocation information, to the extent permitted under other provisions of law, needed to provide information to law enforcement agencies or for an investigation on a public safety matter.

The regulations must also prohibit an operator from discontinuing service provided to a child:

1. under 13 based on refusal of his or her parent to permit the further use or maintenance in retrievable form, or future online collection, of geolocational information from the child by the operator, to the extent that the operator can provide this service without such information or
2. aged 13 to 17 based on his or her making this refusal.

The bill bars states and local governments from imposing any liability for commercial activities by operators in interstate or foreign commerce connected with covered activity or action that is inconsistent with the bill. The bill also provides that an operator and its agent may not be held to be liable under any federal or state law for any disclosure made in good faith and following reasonable procedures in responding to a request for disclosure of geolocational information under the bill.

The bill, introduced by Representative Markey, has been referred to the Subcommittee on Commerce, Manufacturing, and Trade of the House Committee on Energy and Commerce.

California

A bill working its way through the California legislature would result in the regulation of the collection, use, or transfer of “precise geolocation information” and other information such as e-mail addresses by companies that are doing business in California. [SB-761](#) requires the state attorney general, in consultation with the California Office of Privacy Protection, to adopt regulations to require a person or entity doing business in California that collects, uses, or stores online data containing covered information from a consumer in the state to provide the consumer with a method to opt out of that collection, use, and storage of such information. Covered information includes such things as an individual’s Internet activity and personal information such as his or her street and e-mail address.

Under the regulations, the covered entity must disclose to a consumer certain information relating to its information collection, use, and storage practices. The bill prohibits a covered entity, to the extent consistent with federal law, from selling, sharing, or transferring a consumer’s covered information. The bill does not apply to entities that do not track

“sensitive information,” which includes the consumer’s geolocation and any information about the individual’s activities and relationships associated with that geolocation, e.g., what an individual typically does at a given location.

A covered entity that willfully fails to comply with the regulations is liable to the affected individual in a civil action in an amount equal to the sum of the greater of any actual damages, but no less than \$100 or more than \$1,000, plus punitive damages as the court may allow. The covered entity is also liable to the individual for the costs of the action together with reasonable attorney’s fees as determined by the court. The civil action must be commenced within two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

CURRENT CONNECTICUT LAW

Connecticut law does not specifically address geolocational tracking and it is unclear whether current law addresses the use of technology to track a cell phone’s location or other geolocational information. In the case that prompted your question, it could be argued that the burglar violated [CGS § 53a-106](#), which bars the manufacture or possession of burglar’s tools. Under the statute, burglar’s tools are:

...any tool, instrument or other thing adapted, designed or commonly used for advancing or facilitating offenses involving unlawful entry into premises, or offenses involving forcible breaking of safes or other containers or depositories of property, under circumstances manifesting an intent to use or knowledge that some person intends to use the same in the commission of an offense of such character.

By law, manufacturing or possession of burglar’s tools is a class A misdemeanor, punishable by up to one year’s imprisonment, a fine of up to \$2,000, or both.

Arguably, it could be considered a form of wiretapping. [CGS § 53a-187](#) defines “wiretapping” as the intentional overhearing or recording of a telephonic communication or a communication made by cellular radio telephone (cell phone) by a person other than a sender or receiver, without the consent of the sender or receiver, by means of any instrument, device, or equipment (other than normal operation of a telephone corporation and the normal use of the services and facilities it furnishes under its tariffs). The law does not address whether the transmission of location information by the cell phone constitutes “a

communication made by a cellular radio telephone” and we have found no case law on this issue. Under [CGS § 53a-189](#), a person is guilty of eavesdropping when he unlawfully engages in wiretapping. Eavesdropping is a class D felony, punishable by one to five year’s imprisonment, a fine of up to \$5,000, or both.

Under [CGS § 53a-251](#), a person commits computer crime when he or she:

1. intentionally makes or causes to be made an unauthorized display, use, disclosure, or copy of data residing in, communicated by, or produced by a computer system by accessing the system or causing it to be accessed;
2. intentionally or recklessly and without authorization (a) alters, deletes, tampers with, damages, destroys or takes data intended for use by a computer system, whether residing within or external to a computer system, or (b) intercepts or adds data to data residing within a computer system;
3. knowingly receives or retains data obtained in violation of these provisions; or
4. uses or discloses any data he knows or believes was obtained in violation of these provisions.

[CGS 53a-250](#) defines a computer system as a computer, its software, related equipment, communications facilities, if any, and includes computer networks. It is not clear whether a cell phone is a computer system, but it appears that “smart phones” may be because they have many of the capacities of computers, such as browsing the Internet, sending and receiving e-mails, and performing mathematical calculations. If so, it would appear that intentionally making a copy of data communicated by the phone, including geolocational data would constitute a computer crime. Computer crimes carry penalties ranging from a class B misdemeanor to a class B felony, depending on the conduct and the amount of property damage caused.

LEGISLATIVE OPTIONS

The legislature has many options to discourage the inappropriate use of technologies that collect or store geolocational data. It could modify existing criminal laws to make them apply to the prohibited use of tracking technologies, create new criminal offenses, or create a cause of action for people injured by the illicit use of the technologies. These options are not mutually exclusive.

Modify Existing Criminal Laws

The legislature could adopt legislation that specifies that the unauthorized possession or use of cell phone tracking technologies violates existing provisions of the law. For example, the legislature could specify that:

1. these technologies, except when possessed by service providers, law enforcement agencies, or other authorized users, are burglar's tools;
2. the intentional interception of geolocational information from a cell phone or similar device constitutes wiretapping; or
3. "smart phones" and similar devices constitute a "computer system" for purposes of the computer crime laws.

In the latter option, the legislature might want to specify a minimum penalty, since the interception of geolocational data does not necessarily result in economic damages.

Under current law, it appears that tracking another person's location by use of cell phone tracking technologies does not in itself constitute stalking in violation of [CGS §§ 53a-181c](#) through [53a-181e](#), since one of the elements of these crimes is that the perpetrator follow or lie in wait for the victim. The legislature could specify that following can be accomplished by technological as well as physical means.

Create New Criminal Offenses

The legislature could adopt legislation based on the bills currently being considered by Congress and in California. It could also criminalize the possession or use of the tracking technologies in furtherance of a specific crime (e.g., burglary, robbery, or stalking) or crimes in general. Similarly, it could make the possession or use of the technologies in

connection with a crime an aggravating condition leading to an enhanced penalty. This would be similar to the enhanced penalty for crimes such as assault, kidnapping, and manslaughter committed with a firearm.

Create a Cause of Action

The legislature could create one or more causes of action allowing a person whose location was tracked using the technologies the ability to sue the person tracking him or her. For example, the legislature could specify that such tracking constitutes an intentional infliction of emotional distress.

Alternatively, the legislature could restrict the possession and use of the tracking technologies and allow an individual to sue a person who violates these provisions for damages. For example, the legislature could adopt a provision similar to that in S. 1212, which allows a person whose geolocation information is intercepted, disclosed, or intentionally used in violation of the bill to recover actual or statutory damages from the person who committed the violation. The statutory damages are \$100 per day or \$10,000, whichever is greater. The court can also award punitive damages.

KM:ts