The Location Privacy Protection Act of 2012 (S. 1223)

In January 2009, a special report by the Department of Justice revealed that, based on 2006 data, approximately 26,000 persons are victims of GPS stalking annually, including by cellphone.

In December 2010, an investigation by the *Wall Street Journal* revealed that of 101 top smartphone apps, 47 disclosed a user's location to third parties, typically without user consent.

In April 2011, iPhone and Android devices were found to be sending Apple and Google location data, even when users were not using location apps and even though Apple users had no way to stop this.

In June 2011, Nissan Leaf drivers discovered that their cars automatically transmitted their vehicles' location, speed, and destination to many third party websites accessed through the car's computer.

In September 2011, users of Windows Phone 7 smartphones discovered that their phones sent their location to Microsoft when the camera was on—even that app was denied permission to access location.

Later that month, OnStar told its customers that it would continue to track their cars' speed and GPS locations "for any purpose, at any time"—*even if those customers had ended their OnStar service plans*.

In November 2011, consumers learned that smartphones were sending a firm called Carrier IQ location and other information—even though they had never heard of the company and had no way to stop this.

In May and October 2012, the FCC and GAO issued separate reports finding that mobile companies were giving their customers too little information about how their location information was used and disclosed to third parties. The GAO also found that industry self-regulation had been unclear and inconsistent.

Unfortunately, most of these activities are entirely legal. **Even after *Jones*, every time you use the Internet on your smartphone, companies are legally free to give or sell your location information to almost anyone they want—without your consent.** While the Communications Act prohibits wireless companies offering *phone* service from freely disclosing their customers' whereabouts, an obscure section of the Electronic Communications Privacy Act of 1986 explicitly allows smartphone companies, app companies, and wireless companies offering *Internet* service to give their customers' location information to non-governmental third parties—without their customers' permission.

The Location Privacy Protection Act of 2012 (S. 1223), sponsored by **Senator Al Franken** and co-sponsored by **Senators Richard Blumenthal, Chris Coons, Bernard Sanders, Richard Durbin, Robert Menendez, and Dianne Feinstein** will fix this outdated federal law to require companies to (1) get a customer's permission before collecting his or her location data or (2) sharing it with non-governmental third parties. The bill will also (3) raise awareness and help investigations of GPS stalking and (4) criminalize the knowing and intentional operation of "stalking apps" to violate federal anti-stalking and DV laws. *This bill does not concern or affect law enforcement location tracking, which is addressed in other legislation.*

The bill was introduced with the support of a coalition of consumer privacy and anti-domestic violence groups, including the **Center for Democracy & Technology**, **Consumer Action**, **Consumers Union**, the **Minnesota Coalition for Battered Women**, the **National Association of Consumer Advocates**, the **National Center for Victims of Crime**, the **National Consumers League**, the **National Network to End Domestic Violence**, the **National Women's Law Center**, and the **Online Trust Alliance**.