The Location Privacy Protection Act of 2011 (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 without user consent.

In April 2011, consumers learned that iPhone and Android smartphones were automatically sending Apple and Google information about the smartphone's whereabouts—even when users were not using location applications and, in Apple's case, even though users had no way to stop this collection.

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.

Many people know that after *Jones*, the government has to get a warrant to GPS track someone. What most Americans don't know is this: **Even after *Jones*, federal laws <u>allow</u> the companies that get location information from their customers' cellphones and smartphones every day to give that information to almost anyone they please—<u>without</u> their customers' consent.** While the Cable Act and the Communications Act prohibit cable companies and phone companies offering telephone service from freely disclosing their customers' whereabouts, an obscure section of the Electronic Communications Privacy Act (18 U.S.C. § 2702) allows smartphone companies, app companies, and even phone companies offering wireless Internet service to freely share their customers' location information with third parties without getting their customers' permission first.

This doesn't make sense: when a person uses a smartphone to place a phone call to a business, that person's wireless company can't disclose his location information to third parties without first getting his express consent. But when that same person uses that same phone to look up that business on the Internet, his wireless company can legally disclose his location to anyone other than the government.

The Location Privacy Protection Act of 2011 (S. 1223), sponsored by **Senator Al Franken (D-Minn.)** and co-sponsored by **Senators Richard Blumenthal (D-Conn.), Chris Coons (D-Del.), Bernard Sanders (I.-Vt.), Richard Durbin (D.-Ill.), Robert Menendez (D.-N.J.), and Dianne Feinstein (D-Cal.)** is a narrowly-tailored bill that would close current loopholes in federal law by requiring any company that may obtain a customer's location information from his or her smartphone or other mobile device to (1) get that customer's express consent before collecting his or her location data; and (2) get that customer's express consent before sharing his or her location data with non-governmental third parties. The bill also contains provisions to (3) increase understanding and facilitate the investigation of crimes that involve location data misuse. Finally, it (4) creates focused criminal penalties for the worst abusers of location technology, including the knowing and intentional use of so-called "stalking apps" to violate federal anti-stalking and domestic violence laws.

The bill is supported by a coalition of consumer privacy and anti-domestic violence groups. The provisions of the bill are modeled on existing privacy protections in federal law and best practices of leaders in the smartphone market.

For more information or to co-sponsor the Location Privacy Protection Act of 2011 (S. 1223), contact Alvaro Bedoya at 4-1024.