Flood of Geolocational Privacy Legislation Introduced in June

June 22, 2011

June has seen a flood of activity on Capitol Hill seeking to protect consumer geolocational privacy. Within a few days of one another, three bills were introduced that, if enacted, would require consumer consent before geolocation information attained through mobile devices can be collected, used or disclosed to third parties. On June 14, 2011, Rep. Jason Chaffetz (R-UT) and Rep. Robert Goodlatte (R-VA) introduced the *Geolocational Privacy and Surveillance Act* (GPS Act) (H.R. 2168) in the House and, on June 15, 2011, Sen. Ron Wyden (D-OR) introduced companion legislation in the Senate (S. 1212). Similarly, on June 16, 2011, Sen. Al Franken (D-MN) and Sen. Richard Blumenthal (D-CT) introduced geolocational privacy legislation of their own - the *Location Privacy Protection Act of 2011* (S. 1223). In the Senate, the Franken-Blumenthal bill and GPS Act were referred to the Judiciary Committee while, in the House, the GPS Act was referred to the Judiciary and Permanent Select Intelligence Committees. This advisory will highlight the key provisions of the GPS Act and Franken-Blumenthal bill.

Collection and Use of Data

Notably, both the GPS Act and Franken-Blumenthal bill prohibit the collection, use or disclosure of consumer geolocation data without consumer consent or satisfying one of a number of exceptions. The GPS Act and Franken-Blumenthal bill can be read broadly enough to protect real-time and archived geolocation information. Both bills create exceptions for the collection of geolocation information in emergencies. The GPS Act also creates exceptions for data collected in the normal course of business, surveillance authorized by FISA, to investigate device theft or fraud, to enable parents to track their children and for information that is otherwise publicly-available. The Franken-Blumenthal bill exempts common carriers as well as cable service providers from the bill.

Scope

The GPS Act is broader in scope than the Franken-Blumenthal bill, applying to federal and state government entities as well as commercial service providers while the Franken-Blumenthal bill is limited to commercial service providers. Significantly, the GPS Act places checks on governmental tracking. The GPS Act prohibits federal or state law enforcement from tracking an individual's location through mobile devices without first obtaining a warrant based on probable cause.

Investigation of Privacy-Related Harms

The Franken-Blumenthal bill also calls for greater study on the harms caused by invasion of geolocational privacy. The bill would direct the National Institute of Justice to issue a report examining the role of geolocation data use in stalking and violence against women. The bill would direct the U.S. Attorney General to develop curricula for law enforcement and courts to investigate the misuse of geolocational data and directs the FBI's Internet Crime Complaint Center to register crimes that were aided by geolocation information.

Penalties

Both bills would impose criminal and civil penalties for unlawful collection, use and disclosure of geolocation data. Under the GPS Act, violators could face criminal penalties of up to 5 years in prison compared to 2 years under the Franken-Blumenthal bill. The Franken-Blumenthal bill would impose criminal penalties on mobile applications intended for stalking and for selling children's geolocational data. Both bills create a private cause of action for individuals to sue violators for statutory and punitive damages as well as attorney's fees. However, the GPS Act imposes steeper civil penalties - $100 for each day of a violation or $10,000, whichever is greater - compared to the Franken-Blumenthal bill - not less than $2,500 per violation. Both bills empower the states and Federal government to enforce consumer data protection.

Conclusion

These bills build on the growing legislative record on privacy and data security but are unique for their keen focus on protecting geolocational privacy. Geolocational privacy is emerging as a chief privacy concern in Congress and among consumers in light of recent media reports and developments, including revelations regarding geolocational information collection practices at Apple and Google. Communications service providers, mobile application developers and device-makers that utilize geolocation data need to be aware of these developments and the potential implications for their business models and data flow processes. For more information on geolocational privacy, please see our Kelley Drye Advisory regarding the Federal Communications Commission's June 28, 2011 public forum on consumer privacy and location based services (LBS) tracking.

Kelley Drye & Warren LLP

Kelley Drye & Warren's Privacy and Information Security practice is a leader in advising clients on privacy and information security issues and has been at the forefront of developments in this growing area of the law. Our attorneys regularly counsel clients regarding all aspects of privacy and data security compliance, including drafting and amending privacy and information security policies, advising clients on interpreting their own policies, crafting data security programs for clients, performing privacy and/or data security audits of existing business practices, drafting agreements with third parties regarding their obligations in connection with handling clients' customer data, and representing clients in connection with federal and state regulator privacy investigations regarding their privacy and data security practices.