Authentication and GPS Tracking

Author : Jeff Welty

Categories : Evidence, Uncategorized

Tagged as : authentication, Evidence, gps, jackson, tracking

Date : June 2, 2014

I've had more and more questions about introducing GPS tracking data in criminal trials. When I think about digital evidence, I think about authentication as the first hurdle. This post summarizes the law regarding the authentication of GPS data.

GPS data may come into criminal cases in several ways: because law enforcement placed a tracking device on a suspect's vehicle; because a suspect was wearing a GPS tracking bracelet as a condition of probation or pretrial release; because law enforcement seized a cell phone or other device containing GPS data from a suspect; and so on. Although each situation presents slightly different considerations, it should often be possible to authenticate such data under Rule 901(b)(1) (testimony of a witness with knowledge that the data is what it is claimed to be), Rule 901(b)(9) (concerning "[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result"), or some combination of the two.

The leading case in North Carolina is *State v. Jackson*, __ N.C. App. __, 748 S.E.2d 50 (2013). The defendant committed a sexual assault while wearing a GPS tracking device as a condition of his pretrial release. The supervisor of the electronic monitoring unit testified regarding how the tracking device worked. The defendant argued that the tracking data was not properly authenticated, but the court of appeals ruled to the contrary. However, the court did not analyze the authentication issue in detail -- instead focusing mainly on whether the data were inadmissible hearsay -- so the opinion is useful mainly for cases that have similar facts.

A few cases from other jurisdictions provide more general guidance. Most courts seem satisfied if a witness with a working familiarity with the GPS system explains how it works, how the data were collected, and what the data mean. *See United States v. Espinal-Almeida*, 699 F.3d 588 (1st Cir. 2012) (ruling that data taken from GPS device seized from boat used for drug trafficking were properly authenticated by the testimony of the lab analyst who examined the device; the analyst provided a "good amount of testimony about the processes employed by the GPS," allowing the court to apply Fed. R. Evid. 901(b)(9), which permits a witness to describe a process or system and thereby authenticate the result of the process or system; the court ruled that expert testimony was not required to authenticate the data, noting that the analyst was "knowledgeable, trained, and experienced in analyzing GPS devices").

Several cases have focused on the qualifications and experience necessary to authenticate the data. Courts generally have ruled that the witness need not be an expert so long as the witness is familiar with the technology. *Id. See also United States v. Brooks*, 715 F.3d 1069 (8th Cir. 2013) (a bank robber was apprehended based on a GPS device that was placed surreptitiously in the loot bag; the trial judge properly took judicial notice of the "accuracy and reliability of GPS technology" generally, and the testimony of an employee of the security company that supplied the device was sufficient to admit the data generated by the device in question; although the witness apparently lacked a "scientific background," he had worked for the company for 18 years, "had been trained by the company . . . knew how the device worked, and . . . had demonstrated the device for customers dozens of times"); *United States v. Thompson*, 393 Fed. Appx. 852 (3d Cir. 2010) (unpublished) (a bank robber was apprehended based on a GPS device that was placed surreptitiously in the loot bag; the GPS data was authenticated at trial by an employee of the security company that supplied the device; he explained how the device worked, and he was properly permitted to testify as a lay witness rather than an expert given that his knowledge was based on his personal experience with such devices).

I'm interested in readers' thoughts about this issue and experiences with different kinds of witnesses used to authenticate GPS data.