Are mobile devices (including cell phones) tracking devices under 18 U.S.C. § 3117?
(Relevant excerpts from January 13, 2011 memo)

(1) Does defining cell phones and cell-site-simulators as tracking devices conform more clearly to the statutory language of 18 U.S.C. § 3117, and ECPA more generally?

On its face, 18 U.S.C. § 3117 seems to clearly encompass cellular phones. Although there is strong legislative history from ECPA's passage in 1986 suggesting that Congress originally intended to encompass only standard beepers, the plain language of the statute is clear enough that there is likely no need to reach the legislative history. Arguing against this is difficult, and will only get more difficult going forward as geo-location increases in accuracy.

(2) How strong is the risk that judges will be more likely to require a warrant simply because a mobile device is called a "tracking device?"

There is clearly a strong correlation between a conclusion that mobile devices are tracking devices and a warrant requirement. Of the eleven cases that conclude that phones constitute tracking devices, nine also require a warrant, and of the seven that conclude they are not, six approve hybrid orders. Several courts explicitly tied the two facts together, such as by concluding that, because a cell phone is a tracking device, "probable cause is the appropriate standard."

At the same time, it is important to note that the government did not indicate that mobile devices were tracking devices in these cases – this line of argument was brought up by defendants, in amicus briefs, or by the judges themselves. While there does seem to be some connection between tracking devices and probable cause requirements, judges may well see tracking devices whether we call them that or not.

(3) Are courts moving toward defining mobile devices as tracking devices already?

Out of twenty-one cases dealing with prospective CSLI decided since 2005, eleven clearly concluded that mobile phones were tracking devices, seven concluded they were not, and the remaining three had mixed conclusions. More recent cases, however, have predominantly concluded that cell phones constitute tracking devices when used as such. Of 6 cases dealing with prospective CSLI since 2008, all but 1 clearly concluded that the phones constituted tracking devices, while the final case distinguished based on the relative accuracy of CSLI. Further, all but one required that a warrant be provided to get the information sought, and the sixth concluded that magistrate judges had the discretion to demand warrants if they felt it appropriate. Some of the judges that decided recent cases are less sympathetic to our issues, but the trend is still marked.

Based on clear statutory language and case law, warrants are not always required to use tracking devices. Nor is it impossible to use a 2703(d) order to access records stored by a service that provides mobile devices that may be tracking devices. Nevertheless, both of these conclusions have been asserted in rulings over the last five years in the context of concluding that cellular phones are tracking devices. While we already address the possibility that mobile devices could be tracking devices in the alternative, focusing more on this argument could provide us with a better opportunity to shape the regime that may govern if courts continue to trend as they have been.

Pros and Cons of Cell Phones as Tracking Devices

Pro	Con
(1) If communications from phones to determine location fall outside the pen/trap statute, we could potentially use cell-site simulators, at least in public/passive more, without a pen/trap order. (2) Conforms more clearly to the statutory language of 18 U.S.C. § 3117. (3) Easier drafting of warrants seeking phone location. (Although this is really only an added convenience – we have not really been challenged on this issue) (4) The search and seizure warrant form requires us to identify the district in which the phone is located; the tracking device warrant form only requires us to identify the district in which the device is installed (5) The search and seizure warrant form requires us to identify the property to be searched and items to be seized; the tracking device warrant form does not. (6) The tracking device warrant form includes a pre-written order to the provider to comply. This holds more weight than the custom order-to-comply that we usually draft and include.	(1) Judges may be more likely to seek warrants for location information from mobile "tracking devices." (2) Signals from a tracking device aren't "electronic communications" under 18 U.S.C. § 2510(12)(C). This could make it harder to use ECPA process to get non-voice communications directly from mobile devices. It could also limit the applicability of the Wiretap Act, and cause similar problems accessing data from third-party apps that track users' location. (Google Latitude) In this situation, we either need only a grand jury subpoena to get the information in question (a standard that is unlikely to be upheld), or we could find ourselves needing to meet a probable-cause standard. This could be ameliorated (but not fully resolved) if we argue that mobile devices are only tracking devices when used as such. This argument has been repeatedly noted favorably in recent opinions, and would likely be persuasive. (3) Along the same lines, if we cannot use an ECPA warrant to get cell-phone location information, then we cannot get the warrant in any district, but rather will have to determine where the phone is located and then get the warrant in that district. [See discussion in next section for more details.] (4) If a cell phone is a tracking device, this further burdens the hybrid order, because we're getting location and relying in part on a pen/trap that intercepts electronic communications. (5) This would reverse our long-standing claims that phones are not tracking devices.

The benefits of relying on 2703 when obtaining warrants for cell-phone location information.

CCIPS believes that it is appropriate to rely on both 18 U.S.C. § 2703(c)(1)(A) and Rule 41 to obtain a warrant for prospective cell phone latitude/longitude information. This approach provides substantial jurisdictional benefits. If law enforcement can rely on § 2703(c)(1)(A), the warrant may be issued by "a court of competent jurisdiction," which will include "a court with jurisdiction over the offense being investigated." 18 U.S.C. §§ 2703(c)(1)(A), 2711(3). If a court must rely on Rule 41 alone for jurisdiction, law enforcement will have to establish that the court has authority to issue the warrant under Rule 41(b), which is likely to require applying for the warrant in the district where the phone is located. This requirement will be particularly troublesome when law enforcement has no idea where the phone is located, but it will also create some difficulty when the phone is located in another district.

CCIPS's approach is supported by the language of § 2703(c)(1)(A): "A governmental entity may require a provider of electronic communication service . . . to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the government entity – obtains a warrant . . . ." Prospective latitude/longitude warrants fall within this language.

Warrants are used prospectively in other contexts, including video surveillance, tracking devices, and, prior to the pen/trap statute, pen registers. CCIPS believes that § 2703(c)(1)(A) warrants, like other warrants, may have prospective effect. Indeed, the argument for prospective application of § 2703(c)(1)(A) warrants is substantially stronger than the argument for the hybrid theory (i.e., combined pen-trap/2703(d) order for cell-site data). There is no direct statutory linkage between 2703(d) orders and the pen/trap statute, a flaw often cited by decisions rejecting the hybrid theory. *See, e.g., In re Application*, 396 F. Supp. 2d 747, 761 (S.D. Tex. 2005) ("the text of neither the Pen/Trap Statute nor the SCA mentions such hybrid treatment for cell site data"). In contrast, § 2703(c)(1)(A) explicitly invokes warrants – it states that the government may compel a provider to disclose information pertaining to a customer when the government "obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure."

If a magistrate rejects CCIPS approach, the government can seek a traditional Rule 41 warrant. But if a magistrate accepts CCIPS's approach, the government should be entitled under *Leon* to good-faith reliance on the magistrate's decision. Moreover, the CCIPS position may reduce litigation risk. For example, an AUSA might seek an order under Rule 41 only based on a mistaken belief that the phone was in the district. If the phone turns out to be outside the district, there would be substantially less litigation risk had the AUSA also relied on § 2703(c)(1)(A).