THE SEVENFOLD INCREASE IN EMERGENCIES AT AT&T

In its response to Ed Markey's questions about law enforcement requests for cellphone data, AT&T attributed the growing number of requests it gets to its expanding customer base.

> To keep these numbers in perspective, AT&T serves over 103,200,000 wireless customers (in 2007, by contrast AT&T served just over 70,000,000 wireless customers).

But that can't explain the entire increase: only one category of request—requests like orders and warrants requiring court oversight—has gone up at or below the 47% increase in AT&T's customer base. All other categories have increased at a faster pace.

	2007	2011	Increase
Customers	70000000	103200000	47%
Subpoenas (Criminal)	63100	131400	108%
Orders/Warrants	36900	49700	35%
Rejected Surveillance Orders	425	965	127%
Exigent Requests (PSAPs)	23200	65500	182%
Exigent Requests (Non-PSAPs)	1800	13800	667%

What's particularly striking is how many more non-PSAP (that is, non 911 call) exigent requests AT&T has gotten: a more than sevenfold increase.

Now, AT&T doesn't explain how it treats such requests legally or practically. By comparison, US Cellular cites the language from 18 USC 2518(7)—including language permitting the release of information for "conspiratorial activities threatening the national security interest"—in its exigent request section (see Exhibit 1, page 1); that law requires requestors to submit paperwork for the order or warrant within 48 hours. Sprint cites 18 USC 2702(c)(4) explicitly, which doesn't include the time limit; but Sprint imposes one itself, even while

emphasizing providing this information is voluntary.

> For example, Section 2702(c)(4) of the SCA permits Sprint to comply with law enforcement requests in emergency situations when Sprint believes there is an emergency involving danger of imminent death or serious physical injury. In those circumstances, our processes require law enforcement to fax in a form which we use to authenticate the law enforcement requestor and to help verify that an appropriate emergency exists. After being satisfied that the statutory requirements have been met, the Sprint analyst will comply with the request but only for 48 hours, providing law enforcement with sufficient time to obtain appropriate legal processes. To be clear, in these particular circumstances, providing information to law enforcement is not required and Sprint could decide that it will not comply with these emergency requests. Sprint has determined, though, that on balance it is in the interest of our customers and members of the general public who may be at risk to comply with emergency requests, particularly since they often involve very serious life-threatening situations such as kidnapping, child abduction and carjacking.

AT&T doesn't cite the law directly, but its description matches 2702(c)(4) and therefore would not legally require a follow-up application. Verizon cites 2702(c)(4) explicitly.

Note that this means AT&T, Verizon, and Sprint are treating cell location as a record, not content. Sprint provides this—sort of—explanation for it.

> Nonetheless, there are circumstances,

> which are outlined in the applicable statutes, where information can be disclosed to law enforcement with the consent of the customer or in certain emergency situations. In those cases, Sprint still requires appropriate documentation, and although it may not be a legal demand, per se, it is legally permissible for Sprint to provide the information under the statute, as discussed herein.
>
> [snip]
>
> Sprint has business records that contain information on the location of a wireless device based on that device's proximity to nearby cell towers. The information in Sprint's records is often referred to as "historic" or "stored" location as it is customer information of a historic nature that is stored by Sprint for its own business purposes. For example, Sprint uses this information for certain billing, taxing, network troubleshooting and capacity planning purposes. Sprint also has the capability to determine the location of a cell phone in real time by using GPS technology.
>
> The location information contained in Sprint's business records is not basic subscriber information as defined by the statute but is information Sprint has relating to its customers' mobile device usage. Consequently, a court order based on "specific and articulable facts" is required prior to disclosure of that information to law enforcement.
>
> [snip]
>
> There is no statute that directly addresses the provision of location data of a mobile device to the government.

The explanation doesn't really say whether it

treats a GPS reading as a stored record or not—probably because that's where this interpretation gets dicey.

Sprint goes on to suggest Congress provide some clarity about this cell location data. (It also note the government interprets the law to require the cell company to provide not just the target caller location, but also the "location of associates on a call with the target.")

Not so AT&T, which seems to be giving this information out like candy in the name of exigent circumstances. And unlike Sprint, it's not clear AT&T (or Verizon) imposes any requirements on how long such emergencies can last.

But then, it's not just AT&T. The government, too, seems to want to declare a permanent state of emergency so it can get all our cell data anytime it wants.

Update: Transcription error fixed per joberly.

Update: Table corrected per Anchard.