CLOUD STORAGE AND DUE PROCESS:
A Defense Attorney's Perspective

David Aylor, Esq., Charleston, SC, USA

This report presents the current picture of American jurisprudence on the balance between LEA's access to stored personal data and the property and privacy rights of the data's owners. It starts with the developing case of federal agents accessing Microsoft's data on servers in Dublin, Ireland. Next, it discusses the most recent U.S. Supreme Court case, *U.S. v. Jones*, on LEA access to personal positioning data, to present the background over which later inferior courts have ruled on similar matters, such as LEA access to cell phone tower data that determines a defendant's positions during his alleged crimes. Finally, it presents some international implications of this emerging picture, both of U.S. relations with members of the Council of Europe and of ongoing negotiations between Council members and nonmembers.

In Microsoft's case, the federal Stored Communications Act (SCA) allows the U.S. to obtain a warrant for unopened emails stored for less than 180 days. The SCA section states, in effect, that the U.S. must show probable cause.

Microsoft argued that federal courts aren't authorized to give warrants for search/seizure of a party's property outside U.S. territory; that the SCA limits the scope of an SCA warrant to existing rules; therefore, U.S. can't search Microsoft property located in Ireland.

The Court ruled that an SCA warrant is obtained like a search warrant (upon showing of probable cause), but is served like a subpoena (U.S. orders party to produce information, rather than commandeering party's property to retrieve or search for the information); thus, the subpoena principle of custody, control, and possession controls. Where the served party has the data in its custody/control, it has the legal obligation to produce it to the U.S. This ruling avoids practical obstacles to effective law enforcement and conflict with the intent of the PATRIOT Act which was to define the "location" of stored data by its ISP's location rather than that of the hard drive on which data is stored.

In *U.S. v. Jones,* the Supreme Court ruled that the U.S. violated a right to privacy (from unreasonable searches) when it put a GPS transmitter on Jones's car and used 28 days' location data to prosecute him. It did so on both property and privacy bases, and it distinguished the "private" character of this ostensibly "public" data (in that it was akin to a constable riding in the car for 4 weeks).

Lower courts since *Jones* have used its reasoning to protect defendants where the government tried to get both past and future cell tower use data on a sub-probable-cause showing. The Sixth Circuit in *U.S. v. Davis*, 754 F.3d 1205 (June 11, 2014), *vacated by U.S. v. Davis*, 573 Fed. Appx. 925 (Sept. 4, 2014) (to be reheard *en banc*) held that Davis had a privacy right in his historical cell tower location data where he reasonably expected his whereabouts to remain private, and that the U.S. must show probable cause to get a warrant for the data, despite the U.S.'s argument that the SCA allows them to get a court order to obtain the data on a sub-probable-cause showing of "special, articulable facts" that there are reasonable grounds to believe that the records or other info sought are relevant and material to an ongoing criminal investigation.

The Southern District of California, in *U.S. v. Espudo*, F.Supp.2d 1029 (S.D. Cal. 2013), held that *future* cell tower location data also was only obtainable by the U.S. on a probable cause showing for a warrant, despite the U.S.'s claim that such data was "historical" and thus under the ambit of the SCA, and that the ECPA Pen/Trap and CALEA statutes, which banned getting physical location data for cellphone users by a low standard of "mere certification by the U.S. that data is relevant to ongoing investigation," didn't preempt the SCA's permission for the U.S. to get the data. Rather, such future location data was not addressed by any federal law and so was controlled by the default probable-cause standard.

However, courts like these two have granted the U.S. immunity from their holdings because *Leon* allowed good faith exceptions to apply to the exclusionary rule of evidence. Because in both cases the U.S. operated under the good faith belief in the validity of the warrantless court-orders to get the data at issue, and in the constitutionality of the SCA's sub-probable-cause clauses, the defendants were denied relief. Only moving forward are these courts' jurisdictions under notice that this sort of data requires a warrant based on probable cause.

Where U.S. citizens and LEAs have competing tools to protect or access stored data (MLATs, SCA/other statutes, private third party contracts with foreign data-hosts, subpoena "custody" doctrine), the proliferation of international cloud storage may tip the balance in favor of citizens. Where nations' IT laws and due process traditions differ greatly (ex., India, China, U.S.), how do negotiations establish a common ground over which to build mutually beneficial cyber/cloud security solutions?