WILMERHALE

The Court of Justice of the European Union Limits the Scope of National Data Retention Laws

DECEMBER 21, 2016

On December 21, 2016, the Grand Chamber of the Court of Justice of the European Union handed down another important judgment regarding data privacy in the European Union. The court held that under the Charter on Fundamental Rights of the European Union, and Directive 2002/58, national data retention laws must be targeted to those data that are strictly necessary to help combat serious crime and must contain substantive and procedural rules governing both the retention of data and the facilitation of access by the government. *See* Joined Cases C-203/15 & C-698/15, *Tele2 Sverige AB v. Swedish Post & Telecomm. Auth.* (Dec. 21, 2016). This case builds on the 2014 judgment in *Digital Rights Ireland and Others* (Joined Cases C-293/12 & C-594/12) concerning the validity of the European Data Retention Directive 2006/24.

The joined cases involved laws from Sweden and the United Kingdom. The Swedish law requires electronic communications service providers to retain for six months certain types of traffic data, including, among other things, those "necessary to trace and identify the source and destination of a communication," location information, and IP address information. *See* Joined Cases ¶ 17. In order to gather intelligence or prevent certain crimes, Swedish law enforcement and security authorities are allowed to access some of the retained data. The British law allows the Secretary of State to issue a "retention notice" requiring a public telecommunications operator to retain "all data or any description of data." *Id*. ¶ 29. Data covered by the law include traffic and other data but not content data. Further, the law allows the government to access these data where it "believes that it is necessary" to protect national security, public safety, or public health, or for other purposes. *Id*. ¶ 33.

The Court concluded that EU Directive 2002/58 governed the challenged laws. Directive 2002/58 provides that certain types of communications data must be processed and stored securely and retained only for as long as necessary. Once retention is no longer necessary, the data must be anonymized or erased. Article 15(1) of that directive allows Member States to require, when it is "necessary, appropriate, and proportionate . . . within a democratic society," that electronic communications service providers retain data for a "limited period" and make it available to Member States for in order to safeguard national security and prosecute crime. *Id*. ¶ 11. But any such requirement can only be used to further the purposes set forth in Article 15(1). It must also comply with the Charter on Fundamental Rights. Articles 7, 8, and 11 of the Charter guarantee the rights to

privacy, the protection of personal data, and freedom of expression, respectively.

According to the Court, a law will pass muster when it allows for "the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned, and the retention period adopted, to what is strictly necessary." *Id*. ¶ 108. Thus, laws must include precise substantive and procedural rules to ensure that the retention of data is "strictly necessary." *Id*. ¶¶ 109-111. They must also contain substantive and procedural rules governing the Member State's access to those data. In particular, a Member State may access only those data of individuals involved in serious crimes, or other data if it might "make an effective contribution to combating" terrorist or other activities threatening national security. *Id*. ¶ 119. And unless there is a "validly established urgency," a Member State cannot access such data unless a court or administrative body has granted permission. *Id*. ¶ 120.

The reasoning of the Court will force a number of other Member States to review their surveillance and data retention laws, taking into consideration the holding that generalized and indiscriminate surveillance is not permissible under EU law. It is also worth pointing out that the Court expressly states that the data in question must be retained within the European Union. *Id*. ¶ 122.

The decision is available here.

Authors

Dr. Martin Braun

PARTNER

martin.braun@wilmerhale.com

+49 69 27 10 78 207