THE
NATIONAL LAW REVIEW

EU Releases e-Evidence Proposal for Cross-Border Data Access

Tuesday, May 8, 2018

On April 17, 2018, the European Commission published the e-Evidence Initiative, long-awaited legislation that would create a new framework for European Union ("EU") Member States to access content data and metadata (collectively "e-evidence") across national borders. The European Commission released the proposal less than one month after the United States created its own framework governing cross-border data access in enacting the Clarifying Lawful Overseas Use of Data ("CLOUD") Act. Like the CLOUD Act, the e-Evidence Initiative would provide new tools for law enforcement to obtain data stored across national borders for criminal investigations. Importantly, too, the proposal would enable EU law enforcement authorities to obtain data *directly* from providers—including providers based outside the EU—and potentially regardless of which entity in the provider's corporate structure has possession or custody over the data.

COVINGTON

Article By Covington & Burling LLP
Lauren MoxleyInside Privacy

Communications, Media & Internet
Global
European Union

The e-Evidence Initiative includes two distinct measures: a proposed Regulation and a proposed Directive.

The Proposed Directive

The proposed Directive requires providers of certain online services to maintain a legal representative in the EU. Specifically, it requires every such provider that either (1) is "established" in an EU Member State (*e.g.*, through a subsidiary), or (2) has a "substantial connection" to at least one Member State (*e.g.*, by virtue of a significant number of users there, or targeting its activities to users in Member State), to appoint a legal representative in at least one Member State.

The legal representative must have the capacity to process and fulfill orders from authorities in any Member State to preserve or produce electronic data for use in criminal proceedings—even orders from authorities in Member States in which the provider does not conduct business. If the representative fails or is unable to comply with the order, both the legal representative and the provider it represents may be subject to sanctions.

The Proposed Regulation

The Regulation would create two new legal instruments: a European Production Order ("EPO") and a European Preservation Order ("EPrO"). Member State authorities could use these orders to compel the preservation or production, on a cross-border basis, of four data types: content data, transactional data, subscriber data, and access data. A variety of technology companies would be covered by the Regulation, including electronic communications service providers, cloud providers, social networks, online marketplaces, hosting service providers, and providers of internet infrastructure such as IP address and domain name registries. EPOs and EPrOs would only apply to stored data, however; they could not be used to intercept real-time communications.

Production Orders

The proposed Regulation would empower authorities in one Member State to use an EPO to directly compel a provider in a second Member State to disclose data. EPOs would compel such disclosure regardless of where the data is stored—even if it is stored outside the EU. The provider must respond to an EPO within 10 days, or

within 6 hours where there is "imminent threat to life or physical integrity of a person or to a critical infrastructure," subject to certain exceptions. Authorities may issue an EPO for subscriber or access data for all criminal offenses, but for content or transactional data only for serious offenses (*i.e.*, those with a minimum of a three-year sentence in the issuing Member State, or certain cyber and terrorism-related crimes).

The proposed Regulation includes an "enterprise exception" for EPOs: when authorities seek data that a provider holds on behalf of another company or entity, the EPO may only be addressed to the provider "where investigatory measures addressed to the company or the entity are not appropriate, in particular because they might jeopardise the investigation."

Preservation Orders

Member State authorities could use an EPrO to directly compel a provider in a second Member State to preserve data (*i.e.*, to prevent its deletion), regardless of where the data is stored. Authorities could issue an EPrO for any of the four data types mentioned above, and for all criminal offenses.

Challenging Production and Preservation Orders

Providers may object to EPOs and EPrOs on a number of grounds. For example, a provider may oppose an order if it was not issued by a proper issuing authority, if the provider cannot comply because of *de facto* impossibility, if the provider is not storing the data requested, if the request is not for services covered by the Regulation, or if it is apparent that the order "manifestly violates" the EU Charter of Fundamental Rights or is "manifestly abusive."

In addition, the proposed Regulation establishes two mechanisms though which a provider could challenge an EPO based on a conflict between production obligations under the order and obligations under a third-country law (*i.e.*, one other than an EU or Member State law). First, the provider may refuse to comply with an EPO on the ground that disclosure would force it to violate a third-country law that either protects "the fundamental rights of the individuals concerned" or "the fundamental interests of the third country related to national security or defence." Where a provider raises such a challenge, issuing authorities can request review of the order by a Member State court. If the court establishes that a conflict exists, the court must notify authorities in the third-party country; if that third-party country objects to execution of the order, the court must set it aside.

Second, a provider may refuse to comply with an order because it would force the provider to violate a third-country law that protects interests other than fundamental rights or national security and defense. In such cases, the parties follow the same procedures as above, except that the court, rather than notifying the foreign authorities, conducts a multi-factor analysis to decide whether to enforce the order.

Global Implications

The e-Evidence Initiative would have a number of important policy consequences, not only for EU-based cloud customers, technology companies, and law enforcement authorities, but also for technology companies and cloud customers based outside of the Union. By requiring providers within its scope to appoint a legal representative that can comply with Member State production and preservation orders, the Directive would give law enforcement authorities across the EU the ability to compel providers based outside the EU to produce data—potentially even regardless of which entity in the provider's corporate group has possession or custody over the data. This reading could result in a significant expansion of Member State jurisdiction over digital data held by service providers located outside the EU.

Source URL: https://www.natlawreview.com/article/eu-releases-e-evidence-proposal-cross-border-data-access