August 31, 2017

Comments of

ACT | The App Association
(Transparency Reg. # 7202951387754)
Lighthouse Europe
Avenue Adolphe Lacomblé, 59
B-1030 Brussels

to

The European Commission's Directorate-General for Justice and Consumers (DG-JUST) and the Directorate-General for Migration and Home Affairs (DG-HOME)

on its

# Inception Impact Assessment regarding Obstacles to Accessing Electronic Evidence Across Borders in Criminal Investigations

ACT | The App Association appreciates the opportunity to provide input to the Directorate-General for Justice and Consumers (DG-JUST) and the Directorate-General for Migration and Home Affairs (DG-HOME) on the Inception Impact Assessment regarding obstacles to accessing electronic evidence across borders in criminal investigations.[1]

The App Association represents more than 5,000 app makers and connected device companies across the EU that use mobile technologies to produce innovative solutions that drive the dynamic $143 billion app ecosystem. Without the thriving app economy, the $8 trillion internet of things (IoT) revolution would not be possible.[2] Alongside the global adoption of mobile technologies, our members have been creating innovative products and services that bolster the global digital economy, improve workplace productivity, accelerate academic achievement, and help people lead healthier, more efficient lives. The global nature of the digital economy has enabled our members to serve customers and enterprises located around the world. As a result, our members routinely receive requests for data from law enforcement agencies, both within and outside of Europe. The app developers we represent offer a unique perspective of small business innovators at the intersection of the global digital economy and governments' interest in accessing data for criminal investigations.

## I. General Views of the App Association on Cross-Border Access to Electronic Evidence in Criminal Matters

Roughly 2.5 quintillion bytes of data are created on the internet daily, and our members provide apps or platforms that require the transmission, storage, or processing of that data across international borders. Without clarity regarding how law enforcement may access data stored outside of its borders, businesses of all sizes face serious threats to their operations and success.

Across the EU, our members design and maintain the software components of everything from IoT devices to back-office inventory management. The ability to share and store data in all corners of the globe is an integral part of their business model. In fact, small and medium-sized enterprises (SMEs) that use the internet for global trade have a survival rate of 54 percent, which is 30 percent higher than companies that operate offline.[3] When the laws governing international data storage are unclear and incomplete, it jeopardizes the expansion, and the survival, of these European companies.

---

[1] http://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097_en.

[2] http://actonline.org/wp-content/uploads/App_Economy_Report_2017_Digital.pdf.

[3] WORLD ECONOMIC FORUM, GLOBAL INFORMATION TECHNOLOGY REPORT 2016 41 (2016), *available at* http://www3.weforum.org/docs/GITR2016/WEF_GITR_Chapter1.2_2016.pdf.

We support the European Commission's efforts to address the barriers law enforcement faces when accessing electronic evidence stored across borders. Our members comply with reasonable warrant requests to help public safety officials perform their job effectively. DG-JUST and DG-GROW should provide law enforcement agencies with avenues to efficiently and legally access the data necessary to protect citizens and uphold the law. However, it is imperative that the EC's approach does not impair innovators' ability to bring advanced products and services to the EC.

While cloud computing has the potential to provide SMEs with the ability to expand their business overseas at unprecedentedly low cost, legal uncertainty and retaliatory policies threaten this progress. Without a successful international framework to address cross-border law enforcement needs, nor one to address the digital economy, SMEs face a legally and financially untenable situation in which they must discern which law governs in the context of extraterritorial warrants. For example, when a German court issues an extraterritorial warrant to obtain the communications data of a foreign person that is stored in Italy, the German court's action may conflict with Italian laws. This puts our members in the unfortunate position of either complying with the German court's request and disobeying the Italian jurisdiction's laws, or vice versa. A company should never have to decide which legal framework to follow, and which to violate. Moreover, the legal uncertainty often results in apprehension to partner and invest overseas, hurting the global economy generally and undercutting opportunities for the app developer community specifically.

Technology often evolves faster than the policies and legal processes that govern it, and law enforcement agencies stand to lose without coordinated reform. If policymakers do not resolve legal conflicts with foreign jurisdictions, some governments may stop coordinating their efforts with foreign law enforcement agencies. Moreover, conflicts between legal regimes encourages data localization and shuts off access to data otherwise available to law enforcement. In addition, data localization policies, which seek to toll data flows and fragment the internet, hurt investigations by forcing investigators to make requests through the mutual legal assistance treaty (MLAT) process. Pushing governments to adopt localization regimes would begin a domino effect of governments using technical barriers to prevent access to their citizens' data. The extraterritorial reach of EU laws outside of international legal norms will exacerbate this effect and could risk violating the Budapest Convention on Cybercrime, which requires signatories to offer access to data stored by domestic companies.

We encourage DG-JUST and DG-GROW to provide needed clarity on these legal frameworks to help eliminate the challenges created by this ambiguity. Successfully removing the barriers to electronic evidence stored overseas will ultimately require updating international treaties and domestic laws in a harmonized way. The App Association is committed to working with governments and other stakeholders to address outdated legal assistance treaties and conflicts of law, particularly those that impact the digital economy that is so vital to our members.

## II. Views of the App Association on Specific Objectives and Policy Options From DG-JUST and DG-HOME to Address Cross-Border Access to Electronic Evidence in Criminal Matters

In the Inception Impact Assessment's discussion of objectives and policy options, DG-JUST and DG-HOME offer a variety of paths forward, ranging from maintaining the status quo, to adopting a new legal framework, to initiating negotiations with other key governments. Below, we offer reactions and recommendations to the proposed policy options:

- We agree that maintaining the status quo – doing nothing new to address cross-border access to electronic evidence in criminal matters – is insufficient, and will intensify the growing legal uncertainty and accountability issues.
- Before initiating an ambitious legislative effort, we urge the EC and all EU Member States to resolve the inefficiencies of the MLAT process by dedicating funding for its modernization. We believe the EU is well-positioned to serve as a global leader in this effort.
- We strongly support the EU "[i]nitiating negotiations with key partner countries such as the United States in order to enable reciprocal cross-border access to electronic evidence, in particular on content data, and including appropriate safeguards."
- We support the EC's use of Art. 82 of the Treaty on the Functioning of the European Union as the basis for legislation to address obstacles in accessing electronic evidence across borders in criminal investigations. In addition, we urge that any legislation requiring EU Member States' law enforcement authorities to provide a justification for their requests for electronic evidence be consistent with the Charter of Fundamental Rights.
- We believe suggested legislative solutions to address law enforcement access to electronic evidence across borders should carefully consider the costs that would be borne by SMEs and develop measures to reduce these costs and burdens. For small business service providers located outside of the EU, appointing a legal representative in the EU alone may represent an unsustainable cost, and could effectively prevent companies from doing business in the EU or with EU subjects.

- The App Association continues to engage with key governments to create a predictable, transparent, and balanced framework for law enforcement access to electronic evidence across borders. For example, the App Association supports S. 1671, the International Communications Privacy Act (ICPA), currently pending in the U.S. Senate. We believe ICPA would remove conflicts between U.S. and foreign jurisdictions over U.S. law enforcement agencies' access to data pertaining to foreign citizens stored outside the United States. The current legal ambiguity in the United States plagues small business tech firms as they work to reach overseas markets. Varying circuit courts disagree on the scope of U.S. law enforcement's authority to access such data, and the courts alone are unlikely to adequately resolve the issue. A legislative solution is needed. In addition, we encourage DG-JUST, DG-HOME, and leading data protection authorities (DPAs) to examine ICPA and advise whether it would remove conflicts that may arise between U.S. law and the pending General Data Protection Regulation (GDPR). This guidance would be immensely valuable to Congress in its evaluation of the sufficiency of ICPA's provisions.
- Should the EC use legislation to develop a new legal framework, any requests from non-EU service providers (discussed in Legislative option 1) should be permitted only when channeled through internationally-agreed processes or when the non-EU service provider resides in a country subject to such processes. The extraterritorial reach of EU laws that do not adhere to international legal channels are likely to result in retaliatory steps by non-EU countries and could damage the interests of the EU. In addition, allowing law enforcement authorities to issue "production orders" would represent a shift in policy to enable "production requests;" we suggest that such a shift be clearly and publicly justified from a legal and policy perspective.
- Any framework developed by the EC should strictly avoid data localization requirements. Data localization requirements provide no demonstrated public safety benefit and can result in serious declines in imports and exports, reduction of an economy's international competitiveness, and the compromising of potential domestic economic diversification. Further, most SMEs do not have the resources to build or maintain unique infrastructure in every country in which they do business, effectively excluding them from commerce.

- The creation of a framework that would enable "law enforcement to access e-evidence pursuant to a set of safeguards and measures to mitigate cross-border effects, without cooperation of a service provider or the owner of the data, through a seized device or an information system" (Legislative option 2) could significantly alter service providers' ability to control the data they hold and would jeopardize trust between the private sector and law enforcement and between service providers and their customers. Further, it implicates service providers' ability to utilize strong technical protection mechanisms to ensure end user security and privacy. Should such an EC framework require that "backdoors" be built into encryption algorithms for the purposes of government access, it would undermine both the safety and security of data, as well as the trust of end users. Moreover, "backdoors" could create vulnerabilities exploited by unauthorized parties, further undermining law enforcement's interests. The App Association strongly advises the EC to avoid this approach.
- Should a new framework be developed through legislation, we agree that it should provide "a common understanding of types of electronic evidence and service providers that fall within the scope of the measures proposed" (as described in Legislative option 3). Without commenting on the kinds of electronic evidence to be included or the service providers that would fall within the scope of a new framework, it is vital that both are defined to provide the basic information organizations need to comply with the framework. Such a framework would be appropriately scoped by limiting its applicability to EU-based service providers.

## III. Conclusion

The App Association appreciates the opportunity to provide the important insight of the small business software developer industry regarding obstacles in accessing electronic evidence across borders in criminal investigations. We commit to work with the EC, law enforcement, and other stakeholders to ensure that law enforcement can protect citizens across the EU, while affording them with the many benefits of the app economy.

Sincerely,

Morgan Reed
President

Brian Scarpelli
Senior Policy Counsel

Graham Dufault
Director of Government Affairs

Joel Thayer
Associate Policy Counsel

ACT | The App Association
(Transparency Reg. # 7202951387754)
Lighthouse Europe
Avenue Adolphe Lacomblé, 59
B-1030 Brussels