

3 September 2018

We appreciate the opportunity to provide input to decision-makers considering changes to the Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (E-Evidence Regulation) and the Directive on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (E-Evidence Directive).<sup>1</sup> We understand these rules have been proposed to ensure law enforcement and judicial authorities can obtain the electronic evidence needed to investigate and prosecute criminals and terrorists.

Alongside the rapid adoption of mobile technologies, our companies have developed innovative applications and products that improve workplace productivity, accelerate academic achievement, monitor health, and support the global digital economy. Today, the app ecosystem is worth more than €820.9 billion globally and employs 794,000 Europeans. We depend on the ability to conduct business across national borders. Therefore, we support the policy goal of the e-Evidence Regulation and Directive to ensure that conflicts of law do not harm our companies as we comply with cross-border law enforcement investigations.

The global nature of the digital economy has enabled small firms like ours to serve customers and enterprises located around the world. As a result, we routinely receive requests for data from law enforcement agencies (LEAs), within and outside of the EU, necessitating compliance with myriad rules and regulations. This is especially true when transferring data across borders. We support LEA efforts to combat crime and terrorism, and we offer the unique perspective of small and medium-sized enterprises (SME) at the intersection of the global digital economy and governments' request for data for criminal investigations.

As SMEs located across the EU, we believe it is essential for the European Commission (EC) to adopt harmonized regulatory frameworks that allow data to transfer over borders seamlessly. However, it is equally important that lawful access policies foster a relationship of trust between SMEs that collect sensitive data and the consumers who benefit from our digital goods and services. We depend on the trust we have with the people who use and buy our services. We cannot grow our businesses – let alone keep our customer bases – unless we continuously prove that we can be trusted. Therefore, the proposed rules should include appropriate due process and transparency safeguards to protect consumers' private affairs from unreasonable or unlawful intrusion. In their current versions, the EC's E-Evidence Regulation and E-Evidence Directive have the potential to harm our ability to grow and create jobs in the EU if they are not modified to account for small business innovators like us.

---

<sup>1</sup> [https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence\\_en](https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en)

**Aspects of both the Proposed Regulation and its corresponding Directive raise serious concerns for us to maintain our consumers' trust. For example:**

**Maintaining the narrow scope.** Some stakeholders have argued that policymakers should expand the scope of the E-Evidence proposal to include a separate authority to intercept communications. We support the narrow scope of the proposal's application to stored data. Drastically expanding the scope to include intercept authority would require policymakers to conduct a detailed, thorough analysis that would hinder the advancement of the narrow E-Evidence proposal as drafted. We urge you not to expand the scope of this proposal to include the authority to intercept future communications.

**Notice.** The proposed Regulation should clarify that LEAs have an obligation under EU law to provide businesses with adequate notice when they access users' data. We recognize that LEAs may need to impose confidentiality restrictions on European Production Orders (EPOs) in some circumstances, but the Regulation should make clear that this may occur only after LEAs undertake case-by-case assessments to determine whether such restrictions are necessary. Such confidentiality restrictions should be permissible only when an LEA can demonstrate why non-disclosure is required under an objective standard.

**Conflicts of law.** We also have limited resources to devote to situations where a European Production Order (EPO) would cause us to violate the law of another country. We are therefore encouraged that the proposed rules would allow for law enforcement authorities to withdraw the order when there is a conflict. We encourage you to make the rules more explicit in requiring law enforcement authorities and courts to resolve the conflict so that the responsibility for doing so does not fall to the small businesses that receive EPOs. If the process requires input from a foreign authority to assess the conflict, we encourage you to ensure the foreign government has enough time to respond to the request from the Member State court.

**Given the size of our companies and the comparative compliance difficulties with proposed E-Evidence rules, we urge the EC to consider the limitations of SMEs as compared to larger companies with more resources. For example:**

**Provider participation and time limits.** Given the limited resources our small businesses can dedicate to reviewing production orders, we should be given more time to respond to EPOs to fully evaluate their legitimacy and determine whether compliance is possible. The current standard under the Regulation (Article 9) is ten (10) days in routine cases, but six hours in urgent cases. This is simply not enough time for us to respond to orders in every case. We request that the EC revise its standard response period to a "reasonableness" standard so as to better accommodate our relatively small size and economic means.

**Requirements of a Legal Representative.** The E-Evidence Directive requires all companies “established” in the EU to have a legal representative within the Union and places requirements on those representatives that may impose insupportable costs. Specifically, it is unclear under Article 3(1) when the legal representative must “gather[] evidence” for purposes of criminal investigations and how they should do so. The Directive seems to impose an actionable duty on such a representative to constantly monitor the “ebb and flow” of all business activity on the potential that a Member State’s relevant authority may issue us a European Preservation Order Certificate under Article 7 of the E-Evidence Regulation at any time. Most of us cannot afford an extensive legal team or even an in-house attorney due to the cost associated with legal representation. The current iteration of Article 3 may be untenable as it seems to require the hiring of a staff attorney we cannot afford.

**Requirement to use EPOs.** Our businesses utilize cloud-based services that allow us to store data remotely, often in a Member State closer to our customers but different from our primary place of business. However, the due process requirements for investigations involving digital data vary widely by Member State. When the E-Evidence rules take effect, to ensure legal consistency, we believe the Regulation should require EU Member States to use EPOs instead of other national measures. Compliance with a variety of different measures—some of which may conflict—will require too many resources and damage our ability to focus on growing our business, creating jobs, and innovating our services.

**Reach comity agreements with the United States.** With the U.S. government’s recent passage and implementation of the Clarifying Lawful Overseas Use of Data (CLOUD) Act, we are encouraged that the E-Evidence proposal would empower Europe to enter into a comity agreement with the United States. We believe that the only solution to both encourage the free flow of data and facilitate law enforcement access to data is through comity agreements. We hope that the EU and the United States will reach such an agreement expeditiously.

We appreciate the opportunity to share our views on this matter and would welcome further occasions to more thoroughly share our experiences and input on the points raised above. Thank you in advance for your time and consideration on this important issue, and we look forward to engaging with you further during the course of the legislative process.

Sincerely,

**ACT | The App Association**

Morgan Reed

President

**Barefoot Studio**

Augustin van Rijckevorsel  
CEO  
*Belgium*

**Oh Bibi!**

Stanislas Dewavrin  
CEO  
*France*

**SolidQ**

Fernando Guerrero  
CEO  
*Spain*

**Tap Tap Interactive Retail Solution**

Christophe Verbeiren  
CEO  
*Belgium*

**Wyres**

Brian Wyld  
CTO  
*France*

**IPlytics**

Tim Pohlmann  
CEO  
*Germany*

**Apps-Garden**

Bartosz Wróblewski  
CEO  
*Poland*

**Andaman7**

Vincent Keunen  
CEO  
*Belgium*

**Tapptitude**

Gabriel Dombri  
CEO  
*Romania*

**Kowo**

Nicolas Rampelbergs  
Managing Partner  
*Belgium*

**Free Drive**

Gaetan Raevens  
CEO  
*Belgium*

**Birdiz**

Hamza Khelf  
CEO  
*France*

**Blügle**

Augustin van Rijckevorsel  
CEO  
*Belgium*

**ISPY Coffee and Water**

Poppy Morris  
CEO  
*United Kingdom*

**Delox Florals**

Delia Chadwick  
CEO  
*United Kingdom*

**Drone Bulgaria Ltd**

Ivan Kolev  
CEO  
*Bulgaria*

**Stirling Ackroyd**

Chris Chidgey  
CEO  
*United Kingdom*

**Giglioitti Ltd**

Charles Seadon  
Co-founder  
*Ireland*

**Qualia Systems**

Chadi Abou Karam

CEO

*France*

**Tribox EU S.p.r.l**

Maxime de Caritat

Co-founder

*Belgium*

**L'Escapadou**

Pierre Abel

CEO

*France*

**Clé Privée**

Pascal Paluel Marmon

CEO

*France*

**Creo Group**

László Grad-Gyenge

CEO

*Hungary*

**Fast Lease**

Cédric Alexandre

CEO

*France*

**Edtap**

Tom Montgomery

CEO

*United Kingdom*

**Quorum**

Florent Barré

CEO

*France*

**Almédia**

Gilles Noeppel

Chef de projet

*France*

**Egylis**

Tanguy de Pommereau

CEO

*France*

**Nouss**

Fernando Guerrero

CEO

*Spain*

**Dafilog S.a.r.L**

Daniel Fichter

CEO

*France*

**Fundshop**

Florian de Miramon

CEO

*France*

**Dimensional Studio**

Marc Kruzik

CEO

*United Kingdom*

**SupportFi**

Leonard Recope de Tilly-Blaru

CEO

*France*

**Corporation Pop**

Dom Raban

CEO

*United Kingdom*

**Pixel Pitch**

Brilius Povilas

Web Developer

*Lithuania*

**Matsuu**

Robert Kwiatkowski

CEO

*Poland*

**Seele Games**

Céline Pecheur

Co-founder

*France*

**CCCP**

Frédéric Forest

Co-founder

*France*

**Lawrenza**

Yves d'Audiffret

CEO

*France*

**Fluicity**

Julie de Pimodan

CEO

*France*