Published on *The Parliament Magazine* (https://www.theparliamentmagazine.eu)



# A square peg into a round hole

Written by Alban Schmutz on 27 November 2018 in Opinion Plus
Opinion Plus

Europe's cloud infrastructure providers support the EU's intentions to crack down on online terrorist content, however policymakers are targeting the wrong players, explains Alban Schmutz.


***Photo credit: CISPE***

With its proposed legislation to proactively monitor customer data online, and so "prevent the dissemination of terrorist content", the European Commission is targeting the wrong players and asking Europe's cloud infrastructure companies to do something that is flatly impossible.

Let me explain why. As our name suggests (CISPE stands for Cloud Infrastructure Service Providers in Europe) we provide the basic infrastructure, the underlying foundations, for European businesses and governments to manage their own data and build their own systems and services.

Imagine the power cables or water pipes in the ground that provide essential but somewhat

workmanlike services to a city and, more importantly, to its many thousands of buildings, businesses, public services and citizens. In the simplest terms, we provide the building blocks for cloud IT.

---

**RELATED CONTENT**

- **Making innovation happen is more than just a motto for the EIT, writes Dirk Jan van den Berg.** **[1]**
- **If Europe wants to compete with China and the US, it needs to invest, writes Paul Rübig.** [2]
- **IEEE | Blockchain A New Digital Revolution: A Parliament Magazine special supplement with IEEE on the opportunities of BlockChain technology** [3]
- **Cybersecurity poses a real, serious threat that must be addressed at EU level, says Mariya Gabriel.** [4]
- **Europe must continue to guarantee the highest hardware resistance levels to cyberattacks, says Stéfane Mouille** [5]
- **Eva Maydell: How the tech revolution is transforming the future of work** [6]

---

The nature of that work means it's not possible, in technical terms, for cloud infrastructure providers to proactively monitor, filter, access, disable and take down a specific piece of content, or otherwise play around with their customers' data.

That data is solely controlled by the customer: cloud infrastructure providers are not controlling what content is put up, how that content is made available to the public, or to whom it is made available by their customers.

We are simply the enablers, the processors (plus a business model founded on the customers' trust that we will not access their data). This is who we are and what we do.

After analysing the proposals and consulting with Member States and the EU institutions, it's become clear the Regulation is wrongly scoped for and should therefore be targeted at social media platforms and online content sharing services.

You see, social media platforms and online content sharing services do have that high level of access and control to their user (customer) data, down to the most granular piece of content.

> "With its proposed legislation to proactively monitor customer data online, and so "prevent the dissemination of terrorist content", the European Commission is targeting the wrong players and asking Europe's cloud infrastructure companies to do something that is flatly impossible"

This means they can delete an individual piece of content or remove an individual user. But we can't do this. It would be like asking the power company to turn off a single light bulb in an apartment without shutting down the entire apartment block or city.

It doesn't make sense. Precisely because they handle the infrastructure side rather than the content side, infrastructure providers can't even distinguish between what is "a piece of content" from what isn't "a piece of content".

To take down a single piece of content, like a photo, they'd need to pull the plug on a whole lot more: taking down an entire social media service, website or customer account, potentially closing down the whole access for many other related legitimate services and, potentially, a disruptively large number of other infrastructure users.

So don't be fooled: despite claims by some filtering technology vendors, there is no silver bullet technology to take down single pieces of content on cloud infrastructures.

For example, 'hashing recognition' technology, which creates digital fingerprint so that a given piece of content is not re-uploaded in another video or social media platform, is technically unfit since cloud infrastructure providers do not have visibility over such content.

> "This is all a bit of a muddle, all be it an extremely well-intentioned one. But good intentions, as we know, do not always lead to the best outcomes"

And there are real risks. The infrastructure (not content) services that we provide are used to drive industry and the economy across the Union. We help power industrial customers who build our trains, planes and automobiles.

Crucially, our infrastructure services enable public agencies and governments to do their work, including the European Parliament and Commission, and extending through city authorities to hospitals, banks, the media, and so on.

All these activities would, potentially, be jeopardised if Infrastructure-as-a-Service (IaaS) providers remained in scope of the proposed legislation, with such companies not technically able to deliver the measures laid out. If such technologies were to be developed in the future, infrastructure providers would be required to snoop on all data entrusted to them by individuals, corporations and public institutions, even when such data is not normally available to the public.

The measures would require accessing every single piece of data owned by the infrastructure customers, which might include law enforcement emails, highly sensitive intellectual property (IP) such as design files for an aircraft manufacturer, genomic databases or perhaps details of power plant operations, and in doing so undermine the security and confidentiality of sensitive content that was never intended to be available to the public.

So this is all a bit of a muddle, all be it an extremely well-intentioned one. But good intentions, as we know, do not always lead to the best outcomes.

In our best-case scenario, IaaS providers are hoping the co-legislators will carefully reconsider the Regulation before the train leaves the station, which means exempting cloud infrastructure companies (clearly the wrong players) and building a set of workable measures that enable us to address, in the most effective and proportionate ways, the terrorist threat we face as a society.

You can view the CISPE press release on the proposed EU Regulation on Terrorist Content Online **here** **[7]**and the full position paper **here** **[8]**

**About the author**

Alban Schmutz is CISPE Chairman and VP Strategic Development & Public Affairs at French cloud computing company ,OVH

**Tags**
Digital Agenda [9]
European Commission [10]
Internal Market [11]
**Categories**
Business and industry [12]
AI and robotics [13]
Data privacy [14]
Digital single market [15]
Internet of Things [16]
Defence and Security [17]
**Twitter Link**

---

Read more on:

Facebook [18]

Twitter [19]

Website [20]



---

ResearchDods
EventsDods
Training

**Media & publishing titles**

Politics HomeThe HouseThe Parliament
MagazineHolyrood
Total PoliticsPublic Affairs NewsCivil Service
World
PublicTechnology
Training
JournalDods Parliamentary CompanionVacher's Quarterly The European Union and Public Affairs Directory

**Dods events**

Westminster BriefingDigital Health & Care ScotlandMEP AwardsThe Skills SummitScottish Public Service AwardsPublic Sector Procurement SummitPublic Sector ICT SummitCyber Security SummitCyber Security 2017Training Journal Awards

**Partnership events**

The Health and Care Innovation ExpoCivil Service LiveCivil Service

**Links**
[1] https://www.theparliamentmagazine.eu/articles/partner_article/eit-digital/individuals-make-innovation-reality
[2] https://www.theparliamentmagazine.eu/articles/news/digital-recipe-european-success
[3] https://www.theparliamentmagazine.eu/articles/magazines/ieee-blockchain-new-digital-revolution
[4] https://www.theparliamentmagazine.eu/articles/opinion/how-eu-building-robust-and-secure-digital-environment
[5] https://www.theparliamentmagazine.eu/articles/partner_article/euro-smart/eu-must-continue-guarantee-highest-hardware-resistance-levels
[6] https://www.theparliamentmagazine.eu/articles/opinion/how-tech-revolution-transforming-future-work
[7] https://cispe.cloud/website_cispe/wp-content/uploads/2018/11/18112--CISPE_PR_Illegal_content_Regulation_Final.pdf
[8] https://cispe.cloud/website_cispe/wp-content/uploads/2018/11/CISPE_Position_Illegal_Terrorist_Content_Regulation_20181126.pdf
[9] https://www.theparliamentmagazine.eu/tags/digital-agenda
[10] https://www.theparliamentmagazine.eu/tags/european-commission
[11] https://www.theparliamentmagazine.eu/tags/internal-market
[12] https://www.theparliamentmagazine.eu/categories/business-and-industry
[13] https://www.theparliamentmagazine.eu/categories/ai-and-robotics
[14] https://www.theparliamentmagazine.eu/categories/data-privacy
[15] https://www.theparliamentmagazine.eu/categories/digital-single-market
[16] https://www.theparliamentmagazine.eu/categories/internet-things
[17] https://www.theparliamentmagazine.eu/categories/defence-and-security
[18] https://www.facebook.com/TheParliamentMagazine/
[19] https://twitter.com/parlimag
[20] http://www.theparliamentmagazine.eu/