

JOINTS RESPONSES TO THE OPEN CONSULTATIONS OF THE EDPB AND OF THE EUROPEAN COMMISSION ON THE NEW GOVERNANCE OF INTERNATIONAL DATA TRANSFERS

The present document aims at constituting a single answer, by Associazione Culturale Diàlexis, to the following open consultations:

-EDPB 1/2020

-Commission Implementing Decision on standard contractual clauses, which have a common ground, hence they may be dealt with simultaneously.

For understanding our position, it is necessary to recall briefly the historical background of the Commission Implementing Decision, as well as the annexed Standard Contractual Clauses and the draft EDPB's directive, which both are just the last steps of a long lasting legal struggle, which we all are called to comment.

1. From the US Postal Code to ECHELON

European Institutions have correctly singled out international data transfers as one of the core focuses of their duties as a fledging supranational organisation, in particular for what concerns the relationship with the US intelligence legislation. More recently, national and EU leaders have focused still more this concept as "Europe's digital strategical autonomy", and are striving to achieve the latter by promoting European Champions.

Computers and Internet were originally military in nature, and, with priority, intelligence projects. Even the practical functioning of Internet was tested thanks to military funds among DARPA-friendly research centers. Its whole development was paid by the DoD, and the core of their functioning is still defense-related.

The utilization of Internet for "covert operations" was anticipated by the one in nuclear warfare. First of all, the **Anti-missile Defense System** is based on the capability, by Big Data, to forecast, detect, monitor, prevent and counterattack any offensive act of potential enemies. In nuclear warfare, the objective need to act within a span of a few minutes since a nuclear attack renders the intervention of human beings absolutely irrelevant, and, on the contrary, the whole digital system essential. One could say **that all present day digital intelligence is ancillary, in last instance, precisely to the need for an enhanced decision-making capability of computers during a potential Unlimited Warfare attack.** In practice, all patterns of present days' civilization tend to be organized alongside these needs: each citizen is either a tool in the hands of the Apparatus, or an enemy and a target.

Since its beginning, **Mass Surveillance** had been used as part of wartime **censorship** for controlling communications that could damage the war efforts and aid the enemy. For example, during World Wars, every international telegram from or to the United States sent through companies such as Western Union was reviewed by the US military. After the wars were over, surveillance continued in programs such as **the Black Chamber** following World War I and **Project Shamrock** and **COINTELPRO** following World War II.

2.From ECHELON to the Schrems cases

Billions of dollars per year have been spent, by agencies such as the **National Security Agency (NSA)** and the **Federal Bureau of Investigation (FBI)**, to develop, purchase, implement, and operate systems such as **Carnivore**, **ECHELON**, and **Narus Insight** to intercept and analyze the immense amount of data that traverses the Internet and telephone system every day. The Echelon Wikileaks and Prism cases have shown as this surveillance works.

ECHELON, a surveillance program established in 1971 by the United States with the aid of four other signatory states to the UKUSA Security Agreement, also known as “the Five Eyes” has evolved beyond its military and diplomatic origins into "a global system for the interception of private and commercial communications" (mass surveillance and industrial espionage). Former NSA employee Margaret Newsham claims that she worked on the configuration and installation of software that makes up the ECHELON system while employed **at Lockheed Martin**. Britain's *The Guardian* newspaper summarized the capabilities of the ECHELON system as follows:”*A global network of electronic spy stations that can eavesdrop on telephones, faxes and computers. It can even track bank accounts. This information is stored in Echelon computers, which can keep millions of records on individuals.*”Schmidt and Cohen, members of Google’s Board, have written that, in the XXI Century, **Google will substitute Lockheed** in leading America to the control of the world.

In July 2000, **the Temporary Committee on the ECHELON Interception System** was established by the **European Parliament** to investigate the surveillance network. In 2001, the Committee recommended that citizens of member states routinely use cryptography in their communications to protect their privacy. In its report, the committee stated categorically that the Echelon network was being used to intercept not only military communications, but also private and business ones. James Bamford, in *The Guardian* in May 2001, warned that if Echelon were to

continue unchecked, it could become a "*cyber secret police, without courts, juries, or the right to a defence*".

3. After September 11

Since the September 11 terrorist attacks, a vast domestic intelligence apparatus has been built in the USA to collect information using NSA, FBI, local police, state homeland security offices and military criminal investigators. The intelligence apparatus collects, analyzes and stores information about millions of (if not all) American citizens, many of whom have not been accused of any wrongdoing. Under the **Mail Isolation Control and Tracking Program**, the U.S. Postal Service photographs the exterior of every piece of paper mail that is processed in the United States — **about 160 billion pieces in 2012**. The FBI developed the computer programs "**Magic Lantern**" and **CIPAV**, which they can remotely install on a computer system, in order to monitor a person's computer activity. **The NSA** has been gathering information on financial records, Internet surfing habits, and monitoring e-mails. They have also performed extensive analysis of social networks such as Myspace.

The PRISM special source operation system legally immunized private companies that cooperate voluntarily with U.S. intelligence collection. According to *The Register*, **the FISA Amendments Act of 2008** "*specifically authorizes intelligence agencies to monitor the phone, email, and other communications of U.S. citizens for up to a week without obtaining a warrant*" when one of the parties is outside the U.S.. **PRISM** was first publicly revealed on 6 June 2013, after classified documents about the program were leaked to *The Washington Post* and *The Guardian* by American agent **Edward Snowden**.

The **Communications Assistance for Law Enforcement Act (CALEA)** requires that all U.S. telecommunications and Internet service providers modify their networks to allow easy wiretapping of telephone, VoIP, and broadband Internet traffic. In early 2006, USA Today reported that several major telephone companies were providing the telephone call records of U.S. citizens to the National Security Agency (NSA), which is storing them in a large database known as the **NSA call database**. This report came on the heels of allegations that the U.S. government had been conducting electronic surveillance of domestic telephone calls without warrants

Commercial mass surveillance often makes use of copyright laws and "user agreements" to obtain (typically uninformed) 'consent' to surveillance from consumers who use their software or other related materials. **This allows gathering of information which would be technically illegal if performed by government agencies. This data is then often shared with government agencies - thereby - in practice - defeating the purpose of such privacy protections.**

Google-hosted services **many web sites on the Internet are effectively feeding user information about sites visited by the users, and now also their social connections, to Google:**” *Google will also know more about the customer - because it benefits the customer to tell Google more about them. The more we know about the customer, the better the quality of searches, the better the quality of the apps”.*

Facebook also keep this information, as it has been ascertained in the ongoing procedures in front of national regulators, of the Court of Justice and of the Commission.

New features like **geolocation** give an even increased admission of monitoring capabilities to large service providers like Google, where they also are enable to track one's physical movements while users are using mobile devices. With Google as the advertising provider, it would mean that every mobile operator using their location-based advertising service would be revealing the location of their mobile customers to Google. This data is valuable for authorities, advertisers and others interested in profiling users, trends and web site marketing performance. Google, Facebook and others are increasingly becoming more guarded about this data as their reach increases and the data becomes more all inclusive, making it

The CLOUD Act amends the **Stored Communications Act (SCA) of 1986** to allow federal law enforcement to compel U.S.-based technology companies via warrant or subpoena to provide requested data stored on servers regardless of whether the data are stored in the U.S. or on foreign soil.

4.The battle around the US CLOUD Act

In considering the impact of the newly adopted US CLOUD Act, by the **“Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence”**, the **European Data Protection Board (EDPB)** stated that *“By choosing to create a legal avenue under US law for US law enforcement authorities to require disclosure of personal data directly from service providers who fall under US jurisdiction, irrespective of where the data is stored, the US Congress enacts into US law a practice of US governmental entities likely to bypass the Mutual legal assistance in criminal matters treaty (MLAT)² in force between the European Union and the United States of America..... The US CLOUD Act therefore entails the possibility that such electronic communication or remote computer service providers are compelled to answer a request by US law enforcement authorities for the disclosure of personal data that are subject to the provisions of the GDPR. ... The US CLOUD Act thus states an extraterritorial reach of powers under the US **Stored Communication Act....”***

“ This aspect of the CLOUD Act is not compatible with international law:..... ”

Privacy Shield and General Contractual Clauses.

Two conflicting legal logics face each other. From one side, we have **the “traditional liberal-democratic” legal order, embodied in European Law**, which predicates that **any kind of interference in the private sphere is prohibited**. In exceptional cases, as in the case of criminal procedure or of military intelligence, it must be carried out by the responsible authorities, with formal authorizations and documentation, and for a limited period and scope.

From the other side, **we have the American system**, as it has evolved especially since September 11, that considers that **an “unlimited warfare” is under way among, from one side, “Western Civilization”, and, from the other side, “The Rest”**; that the US are **“the policeman of the world”**, and that, therefore, they must **use military instruments for preventing and fighting “terrorists”, who may be even American citizens (like the “Taliban Johnny”)**. Therefore, taking into account the fact that today’s warfare is mainly a digital warfare, **US agencies have the right and the duty to interfere with whichever activity is carried out, by anybody, in the world, for detecting, preventing and striking whichever activity which could result dangerous for “Western Civilization”**.

The idea that, via a formal bureaucracy of certifications, it would have been possible to skip this substantive contradiction **is a childish trick, which the European Court of Justice has had the merit to disclose**, but which risks to result winning after two Schrems Cases notwithstanding the recent rhetorics of **“European Digital and Strategic Autonomy”**.

5.Schrems I

Based on these facts, **Max Schrems had filed a first complaint against Facebook for storing illegally his data with the Irish Data Protection Commissioner (“DPC”) already in 2013(!)**. The DPC first rejected the complaint as **“frivolous and vexatious”(!!)**. Mr Schrems appealed against the DPC and ultimately won: **In that case, C-362/14 Schrems, the CJEU (“Court of Justice of the European Union”, confirmed his view and ruled that mass surveillance violates European fundamental rights, since it allows massive storage and transfer abroad of European’s data collected without their informed consent. The CJEU struck down the previous “Safe Harbor” system (worked out by Commission and Parliament) that facilitated EU-US data transfers. This system was urgently replaced by the Commission at the last minute with the “Privacy Shield” system in 2016. According to Maximilian Schrems: “Privacy Shield is an updated version of the illegal ‘Safe Harbor’. Nothing in US surveillance law was changed or fixed.”**

After the first CJEU decision on “Safe Harbor”, **Facebook claimed it would not use “Privacy Shield” but, on the contrary, the so-called “Standard Contractual Clauses” (SCCs).** SCCs are a contract between an EU company (here Facebook Ireland) and a non-EU company (here Facebook Inc, in California) in which the foreign company pledges to respect Europeans’ privacy. **The present Decision simply updates the SCC vetoed by the CJEU without any relevant change.**

Under the EU privacy laws (“GDPR”) and the SCCs, a “data export” to a third country is only legal if the exporting company (in this case Facebook Ireland Ltd) can ensure “adequate protection” in the US. In practice, **this turned out to be impossible, because US surveillance laws (such as FISA 702 and EO 12.333) is imposed by the US (and massively enforced by 16 intelligence agencies, as documented by Edgar Snowden).**

Given the situation above and the ruling of the CJEU in the “Safe Harbor” case, Mr Schrems consequently requested the Irish DPC in 2015 to use Article 4 of the SCCs, which allows the DPC to order Facebook to “suspend” the data transfers in individual cases. While the DPC now agreed with Mr Schrems that US surveillance laws violate EU law, they did not take direct action.

6.Schrems II

The DPC, however, did not follow the request of Mr. Schrems, but instead filed a lawsuit against Facebook and Mr. Schrems before the Irish High Court, with the aim to refer the case back to the CJEU - this time on the validity of the SCCs- The Irish High Court complied with the DPC’s request and referred eleven questions to the CJEU, despite the resistance of Mr. Schrems and Facebook (who both opposed the reference for different reasons).

The Court of Justice ruled on July 16, 2020 (Schrems II Case), that the Standard Contractual Clauses and that the transfer of Europeans’ data towards the States, not guaranteeing an adequate protection, is forbidden. So, since almost all providers are US platforms, and the Cloud Act imposes to such platforms to make available the data wherever they are stored, inserting data into the Internet is tantamount as delivering them directly to the US intelligence community.

As stated by EDPB, “The CJEU held, for example, that Section 702 of the U.S. FISA does not respect the minimum safeguards resulting from the principle of proportionality under EU law and cannot be regarded as limited to what is strictly necessary. This means that the level of protection of the programs authorised by 702 FISA is not essentially equivalent to the safeguards required under EU law. As a consequence, if the data importer or any further recipient to which the data importer

may disclose the data falls under 702 FISA49, SCCs or other Article 46 GDPR transfer tools may only be relied upon for such transfer if additional supplementary technical measures make access to the data transferred impossible or ineffective. “

In practice, this means that, according to the DGPR as interpreted constantly by the EUCJ, all transfers of data via internet providers are forbidden. Now, because European citizens and enterprises have been used since a long time to utilize the Internet, and the legal devices like Safe Harbour, Privacy Shield and Standard Contractual Clauses are not valid, most of the current web transactions and operations are illegal

According to Mr. Schrems: “In simple terms: EU law requires privacy, while US law requires mass surveillance. The question is, what happens when an EU company follows US rather than EU law?” (“In Deutschland gilt nicht deutsches Recht”). As Schrems correctly pointed out, the principles of US legislation (mass surveillance as a necessary instrument for maintaining and enlarging the “hidden Empire”, and the opposite principle of the EU (to forbid mass surveillance in defense of citizens’ rights), are at the opposite extremes. And, being Europe in the worse negotiating condition, it could obtain an ,at least partial, victory, only via a very hard fight.

7.The low-profile approach of the Commission (and of EDPB)

The Schrems cases are offering European Institutions and companies the opportunity to reverse the situation at least partially, emphasizing the existence of such basic contradiction, what renders illegal per se the continuation of the present state of things.

Unfortunately, the power relationships between the two banks of the Atlantic are still too unbalanced:

- a)from a cultural and military point of view;**
- b)from the technical and commercial point of view (the OTTs are absolute monopolists);**
- c)from the legal point of view (the US may not be obliged by the EU to abolish their intelligence legislation, which in practice allows them to spy everything and everybody everywhere, and which is essential for their imperial project);**
- d)from the practical point of view, European authorities claim to be unable to get rid from US platforms because there is no European platforms able to do the same things, and in any case free trade would require not to privilege**

European firms. In reality, all of these conditions could be quickly reversed if there would be a political will. Gaia-X, JEDI and Qwant are tentatives in this direction, not exploited up to now.

The choice of the Commission has been to address this issue with a low profile: *“The EU is acting to mitigate such concerns through mutually beneficial international cooperation, such as the proposed EU-US Agreement to facilitate cross-border access to electronic evidence”*. If this approach would be logical in a “normal” situation, it is no more such in the present **“constant emergency” situation**, where all decisions and policies have to be decided within a very short time, even forcing the legal framework (because of the **“Existential Risk”** connected with AI outsmarting Mankind, because the Hair Trigger Alert, because of Global Warming and impending Pandemics). In fact, decisions about vaccines are adopted by the Commission within a few hours.

It is noteworthy that the situation is rendered worse by the fact that **both European Institutions and Member States are still more dependent on the US platforms than citizens and enterprises**, because they have often subcontracted to the OTTS all their digital services, so that the most sensible data of Institutions, authorities, enterprises and citizens are available to the US intelligence community, as proven by many cases of unfair competition of US companies which would not have been possible without economic espionage.

It is sufficient to look at the EDPS directives for communications inside the EU Institutions and the Interinstitutional agreement with Microsoft, for seeing that **Microsoft has much more access to European confidential information than the European authorities themselves**. What is prohibited to European authorities, armies, courts, police, is allowed to the 16 US intelligence agencies. **As the EDPB has noted, there is an inversion of the roles of controller and controlled, what is witnessed by the uncovered plan of Google to destabilize the present Commission.**

It is this what has obliged the Commission to reword the Standard Contractual Clauses, inserting provisions about the controller-controlled relationship, which cannot work because US providers cannot breach the criminal military law of their country.

Long discussions have been made on the ILA, with Microsoft, by journalists, the Commission and the EU Ombudsman. However, taking into account first of all the security character both of the EU rules and of the US laws imposing the disclosure to the intelligence community (without any protection for foreign subjects), it is clear that the Institutions should not have signed such agreement with Microsoft, shall

renegotiate the existing ones and shall be very attentive before signing another. **The mere change of the wording of the SCC does not change anything in the above objective session.**

As soon as the Schrems II decision was adopted on July 16 , **the EDPS issued the Own Initiative Paper concerning the ILA, criticizing the ILA not for its core contents, but for a lot of details unbelievably inequitable, which not even a private company would have accepted.** Immediately thereafter , the EDPB and the Commission have issued new provisions which are simple reeditions of the previous documents invalidated by the EUCJ

The present “standstill” situation is particularly negative for European businesses, which are at disadvantage vis-à-vis their American and Chinese counterparts, for several reasons:

- a)to be exposed a continuous industrial and commercial espionage, which renders almost useless investing in R&D;**
- b)to be subject to inquiries and fines from US authorities;**
- c)not to be able to start businesses on markets already occupied by the OTTs;**
- d)to be obliged to comply with measures (like the ones against Iran), that European authorities have not approved or (like the North Stream) have even sponsored.**

For these reasons, an action is starting for transferring into Europe at least part of the storage of data (“**the Gaia-X initiative**”), whereby Europe would even become the “**trendsetter of Global Debate**”, **exporting its rules. Unfortunately, this precious initiative will certainly not solve the problem, because:**

- a) American providers participating in Gaia-X will still be under an obligation to supply data to the their authorities, even if they will be constrained in servers located in Europe and will be more easily controlled as to the compliance with the GDPR.**
- b) It has been established that also Danish and German intelligence has been spying other Member States on behalf of NSA, i.a intercepting international cables, so that we cannot rely even on the compliance with the Rue of Law by Member States;**
- c) The complex mechanism which should be at the basis of DGPR compliance of Gaia-X has not yet been designed, and we doubt that can work against the hacking capabilities of international cyber-intelligence, unless it is protected by a strong counterintelligence, which requires a tight interconnection among**

judges, police and technicians, strengthening also the criminal sanctions for cybercrimes.

As Euractiv puts it, *“the main danger for Gaia-X and its ambition to develop a competitive European cloud infrastructure and technological sovereignty is a different one: It is “corporate capture” – the reliance of many of the founding members of Gaia-X on US and Asian technologies, such as OpenStack or Kubernetes.*

If the objective of the EU and national governments is to invest to build up EU technological competence through Gaia-X, it has to assure that Gaia-X does not turn into a trojan horse for the GAFAM hyperscalers to siphon off public funding for creating the envisioned federated data infrastructure with US and Asian technology providers.

With the Gaia-X summit highlighting participants [from](#) IBM Cloud, Microsoft Azure, Amazon Web Services and Google and OVH cloud announcing to become a strategic integrator of Google Cloud, one has to wonder how much the founding Gaia-X industrial members, led by interim CEO Hubert Tardieu of Atos, a strategic partner of Google, are actually interested in developing European technological sovereignty over tapping into the market potential of a federated data infrastructure.

As a telltale sign, Google’s Gaia-X representative during the summit cited the company’s adherence to the SWIPO code of conduct as Google’s definition of supporting fair competition in the European cloud market. SWIPO is an initiative that the French CIGREF association, representing the 100 largest French companies and public administration, and also a Gaia-X member itself, [labeled as a clear failure of corporate self-regulation](#), stating that:

‘Cigref can only acknowledge the failure of the self-regulation process of the cloud market in Europe. This failure is essentially the result of a systemic asymmetry of skills, resources and objectives between some of the world’s leading cloud service providers, on the one hand, who defend the core of their business and their ability to lock in their customers, and on the other hand those users whose lobbying in this area is not their business.’

‘None of the proposals made by Cigref members to improve the SaaS code of conduct and the subsequent governance of codes of conduct by the legal entity have been taken into account, in defiance of the SWIPO Working Group’s governance rules’

One has the impression that among Gaia-X founding members, [the](#) key principles of Gaia-X: (#4) digital sovereignty and self-determination and (#5) free market access and European value creation have little or no priority, and that the project – while providing a vision for data portability and protection – is actually an elaborate exercise of window dressing and lip

service to swoon European and national governments into providing significant additional revenues for US technologies.”

8.Strategical autonomy

Being privacy on the Internet strictly connected with military, political and commercial intelligence, it is clear that a genuine data protection will not be reached until also a full scale defense autonomy of Europe will exist (the “strategical autonomy”).

This is not a reason for not doing anything. The only correct approach not the Schrems II would be to indicate **a timing-schedule for a well defined phase-out of US control, coordinated with the general Strategical autonomy of Europe as requested by French President Macron** (and for the temporary permission of data transfers under certain conditions during the different phases according to principles like the “red”, “orange” and “Yellow” zones for Covid-19) Taking into account the deadlines set by our competitors, an in first instance by China, the correct Phase-out period should last about 15 years. In the meantime, Europe should construct, always in phases, its Strategical Autonomy(cultural, intelligence, technological, military, political, economic).

It is obvious that, immediately, compliance with the Schrems II decision is not possible, because of the long standing business relationships and the inexistence of a new technical means for a stronger data protection, which Gaia-X is promising. A temporary period, let’s say, of 6 months, could be covered by a fine-tuning of the SCC as the one proposed by the Commission, and, contemporarily, the creation of new European-controlled storage facilities in Europe, but, immediately after that, a further period should be initiated, when the new Gaia-X-type technologies could be experimented. During both periods, a further technology should be worked out with a EU financing, which should guarantee a complete firewall of data going outside the EU space, as well as a military, judicial, infrastructural and criminal protection against any further transfer.

Always in the meantime, Europe should:

- a) invest in a wholly autonomous digital ecosystem, of which today there is no trace at all;
- b) create a European Technology Agency and a European ICT code, encompassing citizens rights, public-private cooperation, cyber-defence and cyber-intelligence, financing, antitrust, tax, privacy, intellectual property rights;
- c) propose to the US and to China a deal, whereby no country will spy the data of

the others, and agreed upon technological standards, If President Biden is willing to “work with Europe”, he should start from this point.