COMMENTS ON PROPOSED SCC DECISIONS
(DECEMBER 10, 2020)

The United States appreciates the opportunity to comment on the European Commission's proposed Decision on Standard Contractual Clauses (SCCs). We appreciate the Decision's overall pragmatic approach to data exporters' responsibility for assessing the laws of the destination country relating to government access to data. In these comments addressing three specific topics in the Decision, we ask that the Commission: 1) show due regard for national governments' responsibility to protect public safety and pursue justice; 2) clarify that data exporters need not assess a destination country government's access to data that is outside the scope of EU law, in particular data access for national security purposes that does not impose processing obligations on private entities; and 3) clarify that when data exporters conduct an assessment of a destination country's laws in light of the specific circumstances of each data transfer, a detailed analysis of the destination country's laws is required only where the data importer has received or is likely to receive requests for disclosure from public authorities.[1] We hope that our comments will serve as a basis for further constructive dialogue between the United States and the Commission on these important matters.

I. The Decision should not adversely affect national governments' responsibility to protect public safety and pursue justice.

The United States has for many years cooperated effectively with the EU and its Member States to confront serious threats to our citizens' safety, including terrorism, organized crime, human trafficking, cyber intrusions and other transnational crimes. This cooperation includes providing mechanisms for transferring electronic data held by U.S. companies from the United States to EU Member States in support of their investigations of a wide range of crimes. Maintaining effective cooperation is important because in the Internet age, detecting, preventing, investigating and prosecuting terrorism and other serious crime increasingly requires access to electronic data that can later become evidence in a judicial prosecution.

We are therefore concerned that the Decision and the clauses in the Annex would appear to require companies to agree to contractual obligations that would impede efforts by investigating agencies of the United States, and in turn of the Member States, to obtain lawful access to data. These provisions would hinder both U.S. investigations and U.S.-EU cooperative efforts to disrupt serious crime, including through U.S. execution of mutual legal assistance requests from Member States. The Commission should consider carefully the justice and public safety missions of governments as well as individual privacy interests before imposing on companies these burdens and obstacles.

For example, the Decision at recital 22 and the Annex at Section II, Clause 3.2(a) appear to require a U.S. company acting as a data importer under an SCC contract to challenge, including in court, any data disclosure request from a government authority if the company

[1] We note that the Decision indicates at footnotes 10 and 11 that it will incorporate by reference the EDPB's recommendations for measures that may supplement transfer tools to ensure compliance with EU levels of protection of personal data. We expect to submit separate comments to the EDPB on those recommendations.

"concludes there are grounds" under U.S. law to bring a challenge and "to exhaust all available remedies to challenge the request." U.S. companies have challenged government disclosure requests in court when they believe they have cause to do so. *Requiring* companies to bring legal challenges whenever possible is quite another matter. The Decision appears to require a legal challenge *whenever* there are "grounds" for one, however slim, novel, unreasonable or immaterial such grounds may be, and even if a company's legal counsel advises that the challenge has little merit. If the initial court rules against the challenge, the company apparently then must "exhaust all available remedies to challenge the request," to include all levels of judicial appeals, regardless of the validity of the initial court's decision. Data subjects, as a third-party beneficiary under the contract, may invoke and enforce these SCC obligations, placing companies at risk of being sued for breach of contract if they disclose data before bringing a challenge and exhausting all appellate remedies.[2]

The proposed Decision could also be read as having the further effect of requiring companies to reject government requests for *voluntary* cooperation in emergency situations, a valuable source of electronic evidence critical to saving lives, including of EU persons. For many years both U.S. and EU Member State authorities have relied on the voluntary cooperation of U.S.-based service providers to produce the content of electronic communications without a compulsory order in emergencies where there is a danger of death or serious physical injury to a person. Covered emergencies include where there is an imminent risk of a terrorist attack, where a child has been kidnapped or is being sexually exploited, or in kidnappings involving death threats. In these situations, Member State authorities must work closely with U.S. authorities to obtain valuable electronic evidence to safeguard EU persons because providers may only disclose the content of electronic communications in emergencies to U.S. authorities. Because there is no legal requirement that providers comply with these emergency disclosure requests, providers could interpret the Decision's requirement to challenge government requests for data when there are grounds to do so, and to exhaust all available remedies, also to require them to exercise their discretion to reject *all* emergency disclosure requests. Others may feel compelled to deny disclosure requests whenever they have any grounds to question the basis for the emergency or demand unreasonable proof of the threat to the life and safety of an individual, wasting time and resources and endangering the lives of those at risk of death or serious physical injury.

The requirement in the Decision to challenge government disclosure requests whenever possible would place an enormous litigation burden on companies to essentially automatically challenge a wide range of disclosure requests, and would also place a commensurately heavy burden on governments to enforce each such request. Such a relentless wave of unmeritorious challenges could dramatically impede critical

[2] In the U.S. legal system, federal trial court decisions may be appealed both to a U.S. Court of Appeals and again to the U.S. Supreme Court, and there are additional appellate procedures (e.g., requests for rehearing, requests for rehearing *en banc).* Other countries have similarly extensive appellate options. The Decision could be read to require *a company to avail itself of all these procedures*, regardless of the validity of the initial court's decision or the likelihood of success. U.S. law provides for judicial sanctions for "frivolous" litigation, and the Decision might place companies in the position of being required to pursue litigation that would result in such sanctions.

law enforcement investigations by authorities in the United States and in EU Member States, which rely on mutual legal assistance requests to the United States for access to electronic evidence needed to protect public safety. Taken even further, this hostility to routine and necessary government disclosure requests could have a chilling effect on regulatory oversight of many U.S. and EU institutions, such as the oversight of financial sector enterprises and the safety of financial markets. Given the critical role that financial supervision plays in identifying money laundering, terrorist financing, and other financial crimes, for example, this regulatory oversight also relates directly back to public safety.

We submit that that these provisions should be removed from the Decision, and the responsibility for making fundamental legal judgments and litigation decisions should be left to the companies. Alternatively, these provisions should be amended to require companies to assess the lawfulness of government requests and to challenge those they believe both to be clearly unlawful under the law of the destination country and where the alleged unlawfulness materially impacts the individual rights of a data subject. The Decision should expressly exempt emergencies from any contractual obligations under an appropriate standard.

Next, if a U.S. company does accept, or a court confirms, the legality of a government disclosure order or request, the Annex at Section II, Clause 3.2(c) would require the company to provide the government no more than "the minimum amount of information permissible" in response to the request. To be clear, we expect companies to disclose only information that is responsive to a lawful government request. The Decision, however, by imposing a contractual obligation on a company to disclose only the "minimum" amount "permissible," would create an incentive for companies to withhold information otherwise reasonably viewed as responsive, again at risk of being sued by the data subject for breach of contract for disclosing any information the company might have "permissibly" withheld. Orders and requests often seek identified categories of data and information because investigators cannot know in advance precisely what data or information is in the providers' possession. Accordingly, there is always some degree of discretion in interpreting and applying a government request for data, and the Decision would put a thumb on the scale against the interests of public safety. As noted above, requiring providers to resist all requests in court could also have serious negative consequences for voluntary cooperation in response to emergency disclosure requests, as "the minimum amount of information permissible" to disclose in that context is always zero. If this approach is maintained, the Decision could hinder effective government investigations relating to serious violations of law in the United States and Europe and again place litigation burdens on companies by essentially mandating that companies adopt an uncooperative, obstructive approach to disclosure requests.

Finally, the Decision at recitals 17, 21, and 22, and the Annex at Section II, Clauses 3.1(a)(i), 3.1(b) and 3.1(c) would require a U.S. company to notify the data subject, the data exporter, or the supervising authority about government disclosure requests, the authority requesting the data, the legal basis for each request, whether requests were challenged and the outcomes of the challenges, the responses provided by the company, and any related inability to comply with the SCCs. These notification obligations represent a dangerous imposition on companies who currently, in most instances, responsibly exercise discretion as to whether to inform their customers of government requests. The vast majority of major U.S.-based

electronic communications service providers, for instance, have developed policies establishing a baseline requirement to notify their customers of government requests, subject to reasonable exceptions. For instance, many U.S. providers will not inform customers of requests in child exploitation cases or if there is legitimate threat to the safety of others. The forced notification regime envisioned by the Decision and Annex makes no evident allowance for such reasonable exceptions to notification.

Some of these provisions suggest there may be exceptions to the notification obligations, but they do not indicate the basis for such exceptions, referring only to a company's obligation to notify "to the extent possible" or recognizing the company may not be "in a position to notify." The laws of many countries, including the United States and EU Member States, provide grounds for restricting or delaying such notifications for sound reasons, including safeguarding public safety and maintaining the integrity and confidentiality of the investigation. In the United States, for example, the government may apply to a court to obtain a protective order barring notification of the customer and others if it can demonstrate that notification could endanger the life or physical safety of an individual, cause targets to flee or destroy evidence, or seriously jeopardize the investigation. 18 U.S.C. § 2705(b). To avoid creating conflicting legal obligations, the proposed Decision and Annex should be amended in a way that appropriately and reasonably balances the interest in ensuring notification of affected parties with legitimate government interests in protecting the public and investigations from the harm that notification can cause. As part of the amendments, these provisions should explicitly recognize that notification is not required when prohibited by law.[3]

Amending the Decision to show due regard for both public safety concerns as well as individual privacy interests is appropriate for data transfers from the EU to countries like the United States with democratic legal systems, a commitment to the rule of law, and a longstanding and deep history of law enforcement and national security cooperation with EU Member States. For data transfers to those countries, there is no need for SCC clauses to impose on companies obligations to contest and impede government requests whenever possible based on a principle that cooperation with the government in this context should be at an absolute minimum. Notably, data disclosure requests from EU Member States to EU-based companies are not subject to such requirements under EU law. Applying those requirements solely to non-EU countries is discriminatory. It could also result in substantial harm to public safety—in the EU and the United States—by undermining longstanding and productive relationships between governments and the private sector, which have always been subject of course to appropriate constraints based on the rule of law. We do not believe these harms are a necessary result of EU law. Rather, the Commission should find ways to protect individual privacy rights while at the same time allowing governments to carry out their responsibility to conduct lawful investigations to protect public safety and bring wrongdoers to justice.

[3] For example, the SCC Decision of 2010 was clearer in this regard, imposing on a data importer a contractual obligation to notify the data exporter of government disclosure requests only "unless otherwise prohibited, such as [via] a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation." A broad clause along these lines, recognizing exceptions where notification is prohibited law, should be set out in the Decision and made clearly applicable to all of the notification obligations imposed on the data importer.

II. The Decision should clarify that data exporters need not assess government data access that is outside the scope of EU law on data protection, in particular data access for national security purposes that does not impose processing obligations on private entities.

The proposed Decision would require data importers to notify data exporters about two different types of government access to transferred data: Primarily, for example at recital 22 and Annex Section II, Clause 3.1(a)(i), the data importer would be obligated to notify the data exporter when the destination country's government obtains access to transferred data by invoking national laws authorizing the government to require the data importer to disclose the data, such as through a compulsory disclosure request or production order. In addition, however, recital 22 and Annex Section II, Clause 3.1(a)(ii) would require a data importer to notify the data exporter if it "becomes aware of any direct access by public authorities to personal data transferred" pursuant to the SCCs in accordance with the law of the destination country.

The implication is that the data importer and exporter are responsible for assessing not only how a destination country government may invoke its laws to compel the data importer to disclose data, but also the extent to which the country of destination might obtain non-compulsory "direct access" to the data, during or after transfer, without any disclosure, processing of data, or even awareness by the data importer—for example, unilateral access obtained for national security purposes by intelligence agencies. Recent jurisprudence of the Court of Justice, however, reveals that EU law does not limit comparable data access activities of EU Member States' intelligence services, nor does it provide for privacy protections for such access against which a data exporter could assess a destination country's law and practice. Moreover, requiring data exporters to assess this type of hypothetical data access by a destination country would impose an impossible burden on data exporters and make data flows subject to disruption based on rumors and conjecture.[4]

We recognize that the judgment in *Schrems II* could be interpreted to extend the "essentially equivalent" standard for SCC transfers to non-compulsory access to data overseas for national security purposes, which U.S. intelligence agencies may conduct pursuant to Executive Order 12333. However, the Court's judgment on this issue remains ambiguous,[5] and the Court failed even to address the threshold issue of whether non-compulsory government data access falls within the scope of EU law on data protection, an issue which its Advocate General in the case, Saugmandsgaard Øe, analyzed in detail.[6] In assessing which types of U.S. national

[4] The situation might be different if the Commission is stating that the data importer need notify the data exporter only when it has actual awareness of direct surveillance of the data transferred pursuant to the SCCs. While we would still have doubts regarding the application of EU law if this were the intent, such an approach would at least be more feasible for companies to implement. See discussion at pp. 6-7 below.

[5] For example, the Court began its review of data access under EO 12333 and FISA 702 by citing the derogation in the Privacy Shield framework permitting participating U.S. companies to disclose data "to the extent necessary to meet [U.S.] national security [and other government] *requirements*." *Schrems II*, judgment §§ 164-65 (emphasis supplied). But EO 12333 authorizes no compulsory access, so there can be no "requirement" on the basis of EO 12333 alone for a company to disclose any data to the U.S. government.

[6] *Schrems II*, Opinion of Advocate General Saugmandsgaard Øe §§ 201-30.

security data access would be governed by the General Data Protection Regulation if undertaken by a Member State, Advocate General Øe opined that EU law does not "apply to national measures relating to the collection and use of personal data that are directly implemented by the State for the purposes of the protection of national security, without *imposing specific obligations* on private operators. In particular, as the Commission claimed at the hearing, a measure adopted by a Member State which, like EO 12333, authorized direct access by its security services to data in transit, would be excluded from the scope of EU law."[7]

Since its July decision in *Schrems II*, the Court of Justice has ruled that EU Member State measures to access data without imposing processing obligations on data holders are outside the scope of another EU data protection law, Directive 2002/58 (the "e-Privacy Directive"). In its judgment in *La Quadrature du Net and Others* of October 6, 2020 (*LQdN*), the Court considered what scope of data access by Member State governments falls within the scope of the e-Privacy Directive, in light of Article 1(3) of that Directive which excludes from its application activities which fall outside the scope of EU treaties.[8] The Court decided that the e-Privacy Directive applies only to national measures *requiring* data holders to process data,[9] but not to direct access of data by Member State authorities.[10] The Court likewise ruled that the General Data Protection Regulation does not apply to such direct access.[11] Finally, while the Court stated that its ruling was subject to the application of the EU Law Enforcement Directive, the Law Enforcement Directive expressly excludes from its application national security activities and thus does not apply to the national security data access under discussion here.[12]

---

[7] *Id.* §§ 209-11 (emphasis supplied).

[8] *LQdN and others* (joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:6), judgment §§ 86-104.

[9] The Court's conclusion in *LQdN* built upon the similar analysis by the Advocate General in that case, Campos Sánchez-Bordona, whose opinion the Court cited (§§ 98,101). Advocate General Sánchez-Bordona concluded (§§ 79-80 of his opinion) that "[t]he range of public authority activities that are *exempt* from the general [EU legal] regime governing the processing of personal data" include government activities that are "intended to safeguard national security and are undertaken by the public authorities themselves, without *requiring* the cooperation of private individuals and, therefore, *without imposing on them obligations* in the management of businesses."

[10] *LQdN*, judgment § 103 ("By contrast, where the Member States directly implement measures that derogate from the rule that electronic communications are to be confidential, without imposing processing obligations on providers of electronic communications services, the protection of the data of the persons concerned is covered not by Directive 2002/58, but by national law only . . . .").

[11] *Id.* § 102 ("It follows that the above interpretation of . . . Directive 2002/58 is consistent with the definition of the scope of [the GDPR], which is supplemented and specified by that directive").

[12] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, art. 2(3)(a) & recital 14 (explaining that the Directive should not apply to the processing of personal data in the course of activities that fall outside the scope of Union law, such as activities concerning national security or the activities of agencies or units dealing with national security issues).

In sum, under *LQdN* no EU legislation governs the direct access by Member State authorities of personal data for national security purposes—not the e-Privacy Directive, not GDPR, and not the Law Enforcement Directive. Since EU law does not limit and provides no privacy protections relating to EU Member States' direct access to personal data for national security purposes, a data exporter would have no comparative standard by which to assess whether privacy protections offered by a destination country for the same type of activities are "essentially equivalent" to protections required by EU law. The Commission should interpret the *Schrems II* decision in a manner that does not impose a double standard under which non-EU countries' measures are subject to strict EU data protection rules while comparable Member State measures are not subject to EU law at all. Such an interpretation would be discriminatory and inconsistent with the Court's ruling that appropriate safeguards under Article 46 of the GDPR "must ensure that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection *essentially equivalent* to that guaranteed within the European Union by that regulation, read in the light of the Charter."[13] We recommend that references to governments' "direct access" to data without imposing processing obligations on private entities be removed from the Decision.

There is an additional compelling, practical reason to exclude non-compulsory data access for national security purposes as a factor to be taken into account. If data exporters are required to assess how governments engage in such secret activities, they would face an impossible task. Many countries conduct unilateral intelligence activities outside their territory to protect their national security. Where a country's intelligence agencies do not exercise jurisdiction permitting them to compel disclosure of information, they must rely on non-compulsory, and frequently clandestine, means to obtain information. Data exporters would have no factual basis to assess such clandestine intelligence activities with any reliability. Even in democracies adhering to the rule of law, intelligence activities conducted abroad through such non-compulsory methods often must be kept secret. Requiring data exporters to take into account this type of data access would have the perverse result of punishing countries like the United States who have taken substantial measures towards transparency[14] and rewarding others who have chosen to keep their involvement in such activities secret.[15] Perhaps most troubling, non-democratic, authoritarian regimes that obtain non-compulsory direct access not only to data

[13] *Schrems II*, judgment § 105 (emphasis supplied).

[14] In 2015, the U.S. Office of the Director of National Intelligence ("ODNI") issued "*Principles of Intelligence Transparency*" which guide U.S. intelligence agencies on making information about intelligence activities and oversight publicly available in a manner that enhances public understanding while continuing to protect information that, if disclosed, would harm national security. ODNI, *Principles of Intelligence Transparency for the Intelligence Community* (2015), at link. ODNI also created an internet site called "*IC on the Record*" that provides public access to information related to intelligence activities, including thousands of pages of documents on intelligence-related matters. ODNI, *IC on the Record*, at link.

[15] Countries vary substantially in their commitment to transparency of national security data access and related measures taken. *E.g.*, EU Fundamental Rights Agency *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU—Volume II: Field Perspectives and Legal Update* (2017) at 87 ("Member States and oversight bodies take very divergent approaches when it comes to the regulations and/or practices aiming to provide for the transparent functioning of the oversight system"), at link.

outside their jurisdiction, but within it as well, with no public transparency whatsoever, would be in a more favorable position under EU law than transparent democracies.

Assigning data exporters responsibility to assess such hypothetical access to data by intelligence services would make global data flows subject to disruption based on speculation and accusations. Parties interested in impugning intelligence activities are at liberty to criticize and make unsubstantiated allegations.[16] Many intelligence services, on the other hand, including in the United States and the EU Member States, are unable to respond to such allegations, in light of policies not to confirm or deny specific intelligence activities.[17] As a result, if data exporters and Member State supervisory authorities are required to assess government access to data that is not based on processing obligations imposed on private entities, data flows in and out of the EU would be subject to disruption based on speculation and allegations made in media reports.

In view of these considerations, we submit that the sections of the Decision indicating that data exporters are responsible for assessing government access to data obtained without imposing processing obligations on private entities should be removed.

III. The Decision should clarify the practical implications of its direction that data exporters should take into account the "specific circumstances" of each transfer where the data importer receives no disclosure requests from public authorities.

The United States commends the Commission for its holistic, pragmatic approach to the data exporter's responsibility for assessing the laws of the destination country relating to government access to data. In particular, at recital 20 the Decision directs data exporters to consider the totality of the "specific circumstances" surrounding each transfer of personal data, including, among other factors, "any relevant practical experience indicating the existence or absence of prior instances of requests for disclosure from public authorities received by the data importer for the type of data transferred . . . ."

As explained above, it is only necessary to take into account government data access that is compulsory and imposes data processing obligations. A data importer would obviously be aware of this type of data access. If a data importer has never received a data disclosure request from a government, recital 20 indicates it should be able to rely on that fact to conclude that any actual risk of such access to the personal data it handles is negligible. This enables the data importer to focus pragmatically on the

[16] For example, allegations have been repeatedly made in leading French newspapers that intelligence agencies of the government of France have been intercepting international communications data by tapping submarine telecommunications cables. *Quand le gouvernement remanie discrètement les lois renseignement*, LIBÉRATION (19 June 2018), at link; *Les câbles sous-marins, ces autoroutes du Web prisées par les espions*, LE FIGARO (2 July 2015), at link; *Comment Sarkozy et Hollande ont autorisé une vaste surveillance d'Internet*, LE MONDE (1 July 2015), at link.

[17] EU Fundamental Rights Agency, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU—Mapping Member States Legal Frameworks* (2015) at 66 (referring to Member States' "'neither confirm nor deny' stances"), at link .

concrete impacts a transfer of personal data will have on individual privacy, as opposed to engaging in a speculative exercise about theoretical possibilities.

The United States encourages the Commission to highlight the practical implication of its pragmatic approach directing companies to take into account the specific circumstances of the underlying transfers. For example, the vast majority of U.S. companies doing business in the EU do not, and have no grounds to believe that they, deal in any data that is of any interest to U.S. intelligence agencies. Given U.S. policy not to gather intelligence for purposes of assisting U.S. companies commercially,[18] companies trading in ordinary products or services, and whose EU-U.S. transfers of personal data involve ordinary commercial information like employee, customer, or sales records, would have no basis to believe U.S. intelligence agencies would seek to collect that data.

In particular, only a very small number of U.S. companies have ever received orders to disclose data under Section 702 of the Foreign Intelligence Surveillance Act, the form of compulsory process of concern to the Court of Justice in *Schrems II*. The Commission's direction that data exporters should take into account the specific circumstances of each data transfer shows an awareness and sensitivity to these kinds of facts. Highlighting this implication would alleviate unfounded anxiety in the business communities—both in the United States and in the European Union—over the impact of the *Schrems II* decision on their enterprises.

In sum, the United States encourages the Commission to emphasize that data exporters need to conduct a detailed analysis of the destination country's laws only if the data importer either has or believes it is likely to receive requests for disclosure from public authorities. The Commission should emphasize the importance of data exporters focusing on actual risks to data privacy given the specific factual circumstances of the context of each transfer. Taking this step would greatly alleviate the concerns on the part of the vast majority of companies engaged in transatlantic commerce. If the data they handle is of no interest to the U.S. intelligence community, the possibility of such access to personal data should be of no interest to European privacy regulators. To restore trust between European privacy regulators and the business communities on both sides of the Atlantic, the Commission should make this clear.

IV. Conclusion

We appreciate the opportunity to provide these comments and our views regarding the Decision on SCCs and their impact on data exporters' responsibility to assess privacy protections relating to government access to data in destination countries. We would welcome meeting with the Commission to engage in a direct and more detailed dialogue on these matters.

[18] *E.g.*, Presidential Policy Directive 28, "Signals Intelligence Activities" § 1(b) (17 Jan. 2014) (signals intelligence "shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose"); *id.* § 1(c) ("It is not an authorized . . . purpose to collect such information to afford a competitive advantage to U.S. companies and U.S. business sectors commercially"), at link.