COMMENTS ON PROPOSED EDPB RECOMMENDATIONS 01/2020
(DECEMBER 21, 2020)

The United States appreciates the opportunity to comment on the European Data Protection Board (EDPB)'s proposed Recommendations 01/2020 on measures that may supplement transfer tools listed in Article 46 of the General Data Protection Regulation (GDPR) to ensure compliance with EU standards on protection of personal data. In these comments, we first suggest three general interpretive approaches that can be taken in the Recommendations to provide additional clarity for companies (pp. 1-4 herein). We then ask that the EDPB address five specific issues arising in the proposed Recommendations by:

1) ensuring that companies are not required to take actions that adversely affect national governments' responsibility to protect public safety and pursue justice (pp. 5-7);

2) clarifying that data exporters need not assess a destination country government's access to data to the extent that the EU Court of Justice (ECJ) has ruled that the type of data access in question is outside the scope of EU law, in particular access to data for national security purposes that does not impose processing obligations on private entities (pp. 7-11);

3) clarifying that the ECJ's judgment in *Schrems II* permits data exporters to consider *all* current and available information on U.S. privacy protections relating to intelligence access to data, rather than prejudging that those protections are inadequate based on the ECJ's evaluation of the Commission's findings underlying the 2016 Privacy Shield adequacy decision (pp. 11-13);

4) following the "specific circumstances" standard adopted by the Commission in its draft Decision on Standard Contract Clauses (SCCs) (pp. 13-14); and

5) reconsidering data encryption requirements that, if widely adopted, are likely to have serious adverse impacts on public safety and national security in the United States, Europe and other countries around the world (pp. 15-17).

We hope that our comments will serve as a basis for a constructive dialogue between the United States and the EDPB on these important matters. We believe that such a dialogue will promote the adoption of a data transfer regime that is workable for data exporters, consistent with European data protection standards, and respectful of the compelling interest all nations have in conducting law enforcement and national security activities necessary to protect the safety of their citizens and allies.

I. Overview and general proposals

We appreciate the EDPB's effort to provide guidance to companies conducting business outside the EU on the impact of *Schrems II*. That decision has created instability for the U.S. business community, and U.S. companies are urgently seeking greater certainty regarding how personal data may be transferred from Europe to the United States and other non-EU countries. We feel, however, that the Recommendations could provide clearer guidance on how companies may transfer data without violating EU law and incurring exposure to GDPR penalties.

The proposed Recommendations do point out that transfers can be carried out without further concern if an adequacy finding by the Commission is in place under GDPR Article 45, or if derogations are available under GDPR Article 49, but these transfer mechanisms are not available in many cases. As we understand it, there are Commission adequacy decisions in place for only some twelve jurisdictions. And EDPB guidance to date on Article 49 states that derogations are available only in narrow circumstances and must be interpreted restrictively.

As a result, for the vast majority of data transfers, a data exporter would need under the proposed Recommendations to undertake a complex legal analysis of the laws and government practices of each non-EU country in which it does business. The data exporter would need to analyze for each data transfer to a given destination country how that country's investigating agencies may require the data importer to disclose the data transferred, taking into account the country's laws and regulations authorizing government access to data and applicable privacy safeguards and restrictions. This assessment would include evaluating the destination country's intelligence agencies' access to data for national security purposes, for which governing laws or regulations may be opaque, unfamiliar, or difficult or impossible to identify and evaluate based on available information. In effect, each data exporter would be responsible, under extremely challenging conditions, for issuing its own individualized adequacy determination for each non-EU country in which it does business—the kind of determination that the Commission issues only after receiving information directly from, and conducting months of direct consultations with, the non-EU government concerned.

At the end of that burdensome exercise, the data exporter must be able to conclude with high confidence that the detailed requirements set out in the "Essential European Guarantees" (EEGs) of Recommendations 02/2020 have been satisfied.[1] If the data exporter cannot conclude that the EEGs have been satisfied, then it may not transfer data unless supplementary measures cure the deficiency or deficiencies that are present. In that regard, however, a number of the supplementary measures described in Annex 2 of the proposed Recommendations either 1) are applicable to only very limited situations, or the solutions proposed may be infeasible for many situations in which personal data is typically transferred;[2] or 2) are insufficient in themselves to enable the transfer to take place, as the proposed Recommendations concede.[3]

The situation for companies doing business outside the EU thus appears quite bleak, since the Recommendations would require them to engage in a perilous exercise of analyzing complex foreign laws and practices on intelligence activities, with any error giving rise to potential legal liability in the EU. Experience shows that an accurate and thorough analysis of foreign law and

[1] We note that Recommendations 02/2020 on the Essential European Guarantees for surveillance measures do not appear to be open for comment. However, should the proposals made in these comments be adopted, some revisions to them may be appropriate.

[2] For example, regarding use cases 1-6 in Annex 2, use of pseudonymized data or split or multiparty processing will often either be infeasible for typical business needs, while the use cases of data transiting a third country and protected recipients do not address the most typical situations data exporters confront.

[3] *See, e.g.*, Annex 2, § 95 and subsequent examples.

practice in this area can be difficult if not impossible to accomplish.[4] Even larger data exporters that have the means to hire foreign counsel in multiple countries will likely confront problems in obtaining thorough assessments in this area, in particular for countries whose governments are not committed to public transparency about intelligence activities. Even if a government does provide transparency concerning its rules and activities governing access to data for national security purposes, different legal interpretations may be possible, or no clear assessment under EU law may be apparent. The situation is even more difficult for small- or medium-sized entities, which may not be able to hire foreign counsel, and any effort to analyze foreign laws and practices themselves may be particularly susceptible to error.

We do not think it necessary to place data exporters in this position in order to comply with *Schrems II.* We propose below three general approaches, which we believe could be reflected in the Recommendations, and which would at least ease the burden imposed on the data exporter: 1) applying increased flexibility regarding the use of Article 49 derogations; 2) applying a flexible interpretation of "essential equivalence" absent an adequacy finding by the Commission; and 3) issuing guidance adopting restraint in subjecting data exporters to fines and other corrective measures when their actions were based on reasonable conclusions drawn when analyzing the available information on foreign law and practice.

First, with regard to derogations, the EDPB has stated on a number of occasions that the derogations contained in GDPR Article 49 must be interpreted restrictively; for example, many derogations may only be used for processing activities that are occasional and non-repetitive.[5] In our prior comments, we have expressed concern that this interpretation appears to be in tension with the text of Article 49 itself.[6] The EDPB's interpretation also appears to be in tension with the text of paragraph 202 of the *Schrems II* judgment, where the Court of Justice states: "in view of Article 49 of the GDPR, the annulment of an adequacy decision such as the Privacy Shield Decision is not liable to create [] a legal vacuum." If derogations are to be narrowly restricted, and many are available only in occasional and non-repetitive situations, it is difficult to see how the Court could have concluded that Article 49 provides meaningful relief from the annulment of the Privacy Shield adequacy decision. In light of these considerations, we ask the EDPB to reconsider its past interpretation of the available scope of derogations and adopt a more flexible approach in the Recommendations.

Second, both the Court of Justice and the EDPB have stated that third country privacy protections do not have to be "identical" to those afforded in the EU in order to be considered "essentially equivalent,"[7] and the Recommendations should show similar deference. We feel

[4] As noted in footnote 24 of Recommendations 02/2020, the term "legislation" is broader than acts of legislatures and includes administrative regulations, policy documents imposing requirements and related directives issued by executive authorities, as well as jurisprudence (which may have the same force of law as legislation enacted by the legislature). To the extent that data exporters are required to carry out the task of analyzing a destination country's legal regime, the analysis would be incomplete if only acts of legislatures are considered. This, of course, makes the task of the data exporter even more difficult.

[5] In addition to the proposed Recommendations, see, *inter alia*, Guidelines 2/2018 at 4-5; Guidelines 2/2020 § 7.

[6] Comments of the United States on EDPB Guidelines 2/2020 at 2, at link.

[7] *Schrems II*, judgment § 94; EDPB, Recommendations 02/2020 § 49.

that the EDPB must acknowledge the varying but legitimate pathways different democracies adhering to the rule of law have taken to balance government needs for data access to protect their citizens with the need to protect individual privacy interests. In particular where there is no Commission adequacy decision in place for a country, the EDPB should not adopt a position that subjects a data exporter to a potential penalty for having reached a good faith, reasonable conclusion based on all reasonably available information regarding "essential equivalence," even if a supervisory authority may subsequently disagree. The statement in paragraph 1 of the proposed Recommendations that the "right to protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights" underscores the need for balancing the right to protection of personal data with other fundamental rights laid down in the Charter, including rights relating to property, professional life, conducting a business, and general economic interests, as well as the rights to life and to liberty and security of individuals. A more flexible interpretation of "essentially equivalent," in which differences are acknowledged and accounted for, would strike a balance between these rights. For example, where the Court has imposed certain standards in EU Member States, the EDPB should not issue guidance requiring identical standards outside the EU where other safeguards may accomplish a similar result. It should instead afford assessments of destination countries the flexibility inherent in the concept of "essential equivalence."

Third, we believe it is within the competence of the EDPB to provide guidance on the imposition of fines or other corrective measures by supervisory authorities (such as suspending or banning transfers deemed to be non-compliant) in a manner that alleviates reasonable concerns of data exporters. Currently, data exporters have no clear understanding of how severely supervisory authorities will apply the GDPR penalty structure. Many exporters fear they will be subject to significant penalties even for inadvertent, good-faith errors or misunderstandings about foreign laws and practices, about which it may be difficult to find information and over which reasonable minds can differ. By placing burdens on data exporters in the Recommendations without also including guidelines that assuage concerns that penalties will be quite severe, their difficulties are compounded at a cost to international trade. This lack of guidance may generate a tremendous chilling effect on international data transfers, as companies will have little certainty as to whether their assessments of complex foreign laws and practices will withstand challenges, and whether massive fines will be levied. We therefore recommend that the EDPB issue guidelines that will provide predictability by making clear that penalties will not be excessive if companies acting in good faith reach conclusions that are later rejected.

Each of these three proposals addresses issues as to which there is little interpretive jurisprudence, leaving data exporters facing substantial risk, and consequently threatening disruption to any data-based commerce between the EU and all other countries. There is accordingly an urgent need for the EDPB to provide flexibility that alleviates the plight of data exporters until such time as the Commission issues additional adequacy determinations, and judicial rulings provide additional guidance, including on whether the laws and practices of numerous countries around the world provide protections "essentially equivalent" to EU standards. We call on the EDPB to provide such flexibility now to avoid adverse consequences to the EU's economy, research and development, and relations with other jurisdictions.

II. Proposals concerning specific aspects of the proposed Recommendations

Beyond the above general proposals, we identify and discuss below five specific points as to which we believe changes to the Recommendations are needed.

A. The Recommendations 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 a range of 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 that is held by U.S. companies from the United States to EU Member States in support of their investigations of serious 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 proposed Recommendations call for 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. This 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 EDPB 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 proposed Recommendations at paragraph 112 call for data importers to agree to "challenge," including in court, any data disclosure request from a government authority if the data importer "concludes that there are grounds" under the law of the destination country to do so. As discussed in our recent comments to the Commission,[8] 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 proposed Recommendations appear 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. Data subjects, if made third-party beneficiaries under the contract, could invoke these obligations, placing companies at risk of being sued for breach of contract for disclosing data before bringing a challenge.[9]

This guidance 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

[8] Comments from the U.S. government on Proposed SCC Decisions at 1-4 (10 Dec. 2020), at link.

[9] U.S. law provides for judicial sanctions for "frivolous" litigation, and the proposed Recommendations might place companies in the position of being required to pursue litigation that would result in such sanctions.

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 proposed Recommendations' requirement to challenge government requests for data whenever there are grounds to do so, 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.

This requirement to challenge government disclosure requests whenever possible, by requiring companies essentially to challenge automatically a wide range of disclosure requests, would place an enormous litigation burden on companies, and a commensurately heavy burden on governments to enforce each such request. Such a relentless wave of unmeritorious challenges could dramatically impede critical 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 impact could likewise harm public safety.

We submit that that these provisions should be removed from the Recommendations, 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 Recommendations 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, paragraph 112 of the proposed Recommendations calls for the data importer 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 proposed Recommendations, however, by calling for a contractual obligation 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 Recommendations as proposed 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 Recommendations 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.

Amending the Recommendations to show due regard for 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 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 governments of 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 of course always been subject to appropriate constraints based on the rule of law. We do not believe these harms are a necessary result of EU law. Rather, the EDPB 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.

B. The Recommendations should clarify that data exporters need not assess government access to data to the extent that the ECJ has ruled that the type of data access in question is outside the scope of EU law on data protection, in particular access to data for national security purposes that does not impose processing obligations on private entities.

The proposed Recommendations advise data exporters, when assessing whether privacy protections for a data transfer meet EU standards, to take into account two different types of government access. Data exporters are primarily directed to assess how the destination country government may obtain access to the transferred data by invoking its national laws authorizing the government to require the data importer to disclose the data, such as through a disclosure order. However, other sections of the proposed Recommendations (paragraphs 43, 75, 117) call for assessing government access to data *not* based on such disclosure requirements under national laws, and potentially not even while the data is held by the data importer. For example, paragraphs 43 and 117 refer to government access to data that may occur "without the data importer's knowledge." Paragraph 75 refers to a government obtaining access to data "[i]n transit by accessing the lines of communication used to convey the data to the recipient country."

The implication is that a data exporter is responsible for assessing not only how a destination country government may invoke its laws to require data importers to disclose data,

but also how any other government access to the data may occur, during or after transfer, without any compelled disclosure or processing of data, or even awareness by the data importer—for example, unilateral access obtained for national security purposes by intelligence agencies. However, as we have discussed in our recent comments to the Commission,[10] requiring assessments of this type of data access is inconsistent with recent judgments by the Court of Justice, would impose an impossible burden on data exporters, and would make data flows subject to disruption based on rumors and conjecture.

We recognize that the judgment in *Schrems II* could be interpreted to extend "essentially equivalent" comparative assessments to non-compulsory government access to data for national security purposes, which U.S. intelligence agencies may conduct outside the United States pursuant to Executive Order 12333. However, the judgment remains ambiguous on this issue,[11] and the Court failed in *Schrems II* 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.[12] In assessing which types of U.S. national security data access would be governed by the GDPR 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."[13]

Since its July decision in *Schrems II*, the Court of Justice has similarly ruled that EU Member State measures to obtain access to personal 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.[14] The Court decided that the e-Privacy Directive applies only to Member State measures *requiring* data holders to process data,[15] but not to direct access to data by Member

---

[10] Comments from the U.S. government on Proposed SCC Decisions at 5-8 (10 Dec. 2020), at link.

[11] For example, the Court began its review of data access under EO 12333 and Section 702 of the Foreign Intelligence Surveillance Act 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.

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

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

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

[15] The Court's conclusion in *LQdN* built upon the analysis by the Advocate General in that case, Campos Sánchez-

State authorities.[16] The Court likewise ruled that the GDPR does not apply to such direct access.[17] 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.[18]

In sum, under *LQdN* no EU legislation governs direct access by Member State authorities to personal data for national security purposes—not the e-Privacy Directive, not GDPR, and not the Law Enforcement Directive. Since EU law provides no privacy protections relating to EU Member State governments' 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 EDPB should not interpret *Schrems II* to create a double standard under which non-EU countries' direct access measures are subject to strict EU data protection rules while comparable Member State direct access 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."[19] We recommend that references to governments' "direct access" to data without imposing processing obligations on private entities be removed from the Recommendations. Otherwise, data exporters will be placed in the impossible situation of assessing whether privacy protections relating to foreign direct access measures are "essentially equivalent" to a non-existent EU standard.

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."

[16] *LQdN and others*, 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 . . . .").

[17] *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").

[18] 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).

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

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, unbounded by the geographical pathway of their transfers. 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, or to compare it to intra-EU clandestine practices. Even in democracies adhering to the rule of law, intelligence activities conducted abroad through such non-compulsory methods are typically 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 that have taken substantial measures towards transparency[20] and rewarding others who have chosen to keep their involvement in such activities entirely secret.[21] Perhaps most troubling, non-democratic, authoritarian regimes that obtain non-compulsory direct access not only to data outside their territory, 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 destination countries' intelligence services would make global data flows subject to disruption based on speculation and rumor. Parties interested in impugning intelligence activities are at liberty to criticize and make unsubstantiated allegations.[22] 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 their need to protect fragile intelligence activities, which forms the basis for policies not to confirm or deny specific intelligence activities.[23] As a result, if data exporters and Member State supervisory authorities are required to assess government access to

---

[20] For example, 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.

[21] Countries vary substantially in their commitment to transparency of national security data access and related measures taken. *See, 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.

[22] 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.

[23] 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.

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 media reports.

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

C. The Recommendations should not prejudice the United States by overstating the impact of the judgment of the Court of Justice in *Schrems II* regarding FISA 702.

The proposed Recommendations incorrectly describe the *Schrems II* judgment as foreclosing data exporters from making any assessment of U.S. privacy protections relating to data access authorized by Section 702 of the Foreign Intelligence Surveillance Act (FISA 702). They assert (page 15) that "[t]he CJEU held . . . 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 FISA, 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 this excerpt, the proposed Recommendations prejudge an issue that the ECJ assigned data exporters the responsibility to assess in *Schrems II*. This guidance, if not amended, would pose a great and unfounded risk to transatlantic data flows by substituting the EDPB's expansive and unexplained interpretation of *Schrems II* for the assessment that the ECJ assigned to the data exporter. This guidance would leave companies transferring data from the EU to the United States no room to conclude that the many privacy safeguards in U.S. law and practice in place today relating to FISA 702 meet EU legal standards on data protection.

The ECJ in *Schrems II* did not undertake its own review of privacy protections in U.S. law relating to FISA 702 or assess whether they meet EU legal requirements. Indeed, the Court did not directly assess U.S. law at all—rather, the Court assessed only the description of U.S. law set out in Decision 2016/1250 (the "Privacy Shield Decision") issued by the Commission in 2016. The Court limited its review to the Commission's findings about U.S. law because it concluded that the Privacy Shield Decision was binding on the Irish Data Protection Commissioner, and that the questions the Irish High Court had referred to the ECJ "must therefore be regarded, in essence, as calling into question *the Commission's finding*, in the Privacy Shield Decision" about U.S. privacy protections "and, therefore, as calling into question the validity of that decision," so that "it should therefore be examined *whether the Privacy Shield Decision complies with the requirements* [of EU law]."[24] The Court in *Schrems II* thus did not make any ruling on U.S. law *per se.* The Court decided only whether the Commission's findings

[24] *Schrems II*, judgment §§ 156-61 (emphases supplied).

underlying Decision 2016/1250 established that privacy protections in U.S. law meet EU legal standards.[25]

By limiting its review to the information in, and assessing the validity of, only Decision 2016/1250, the Court undertook a task different from and far narrower than the task with which data exporters are now charged. For example, the Court's assessment of whether data collection authorized by FISA 702 meets the EU standard of "proportionality" was based not on an examination of the actual FISA 702 program elements, but instead on two quotations from a single recital in the Commission's discussion of FISA 702 in Decision 2016/1250.[26] In contrast, companies transferring data to the United States today may consider all current information about U.S. law and practice relating to FISA 702, including information not recorded by the Commission in Decision 2016/1250 and new developments that have occurred since 2016.

On September 28, 2020, the U.S. government published a White Paper identifying relevant information for data exporters and importers to consider when making determinations about whether FISA 702 meets EU legal requirements, with a particular focus on those issues that appear to have concerned the Court of Justice in *Schrems II*.[27] Among other information, the White Paper identifies important safeguards, not recorded by the Commission in Decision 2016/1250, relating to how a U.S. federal court oversees the propriety of how specific individuals are targeted under FISA 702 to obtain foreign intelligence information.[28] The White Paper also provides information about additional safeguards relating to that judicial supervision of FISA 702 targeting that have been instituted since 2016, and about new statutory and procedural reforms limiting FISA 702 collection, all of which have been instituted since 2016. The White Paper provides an up-to-date discussion of privacy safeguards relating to FISA 702, as well as citations to source documents providing additional relevant information. The U.S. Government continues, including since 2016, to publish previously classified court opinions that describe in detail the level of supervision by, and the redress available from, U.S. courts over intelligence activities conducted under the authority of FISA 702.

Companies transferring data from the EU to the United States are responsible for considering not only the limited conclusion made by the Court of Justice in *Schrems II* when invalidating Decision 2016/1250, but also these additional sources of information. The *Schrems II* decision makes clear that an assessment of "all the circumstances of the transfer of personal

---

[25] *Id.* §§ 201, 203(5) (ruling Decision 2016/1250 invalid).

[26] *Id.* §§ 179-80 (quoting Commission findings in recital 109 of Decision 2016/1250 as basis for reviewing FISA 702 data access).

[27] U.S. Department of Commerce, Department of Justice, and Office of Director of National Intelligence, Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after *Schrems II* (Sept. 28, 2020), at link.

[28] *Id.* at 6-11. *Cf.* EDPB, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures § 40 (10 Nov. 2020) ("The ECtHR specifies that while prior (judicial) authorization of surveillance measures is an important safeguard against arbitrariness, regard must also be given to the actual operation of the system of interception, including the checks and balances on the exercise of power, and the existence or absence of actual abuse").

data" is appropriate.[29] Accordingly, we submit that the description in the Recommendations of the impact of the *Schrems II* judgment on transfers to the United States in light of FISA 702 should be removed. Instead, the Recommendations should clarify that the Court's conclusion was only that the Commission's record underlying Decision 2016/1250 did not establish that privacy protections in U.S. law relating to FISA 702 meet EU legal standards, and that data exporters may consider *all current and available* information regarding U.S. privacy protections relating to intelligence access to data under FISA 702 and any other legal authorities.

D. The Recommendations should follow the "specific circumstances" standard adopted by the Commission in its draft Decision on SCCs.

In paragraph 20 of its draft Decision on SCCs, published for public comment on November 12, the Commission adopted a holistic approach that allows data exporters to consider the totality of the specific circumstances surrounding the transfer of personal data, including "the content and duration of the contract, the nature of the data transferred, the type of recipient, the purpose of the processing and 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), the laws of the third country of destination relevant in light of the circumstances of the transfer and any additional safeguards (including technical and organisational measures applied during transmission and to the processing of the personal data in the country of destination)." The Commission's approach does not establish a definite hierarchy among the relevant factors which should be taken into account, thus allowing flexibility for data exporters to consider factors that in some circumstances might preclude transfer, but in other contexts might be compensated for by the presence of additional factors.

In contrast with the Commission's approach, the proposed Recommendations appear to establish a clearer hierarchy among certain factors and do not seem to allow companies to take account of the full range of potentially relevant factors. For example, at paragraph 42 the proposed Recommendations suggest that the likelihood of public authorities' need to access a company's data is merely a "subjective" factor that should not be taken into account and the assessment should be based only on so-called "objective" factors, most prominently an analysis of a third country's legislation. The Commission's draft Decision, on the other hand, allows companies to assess whether certain types of data, such as employee data, are in fact at risk of being accessed by government authorities. Such an assessment is not, as the proposed Recommendations suggest, merely "subjective" but may be based both on the nature of third country legislation and objective historical evidence regarding past data access requests by government authorities, both of which may indicate that these types of data are not at risk of being accessed by government authorities.

Similarly, at the top of page 15 the proposed Recommendations suggest that if third country legislation does not meet the "essential equivalence" standard then only technical measures can overcome its deficiencies. Again, the Commission's draft Decision calls for a more flexible approach in which organizational measures and an analysis of the specific circumstances, including the nature of the data, could provide a basis for the continued transfer

[29] *Schrems II*, judgment §§ 112, 113, 121.

of personal data. Likewise, use cases 6 and 7 both reflect an unnecessarily rigid approach that ignores the possibility that an objective assessment of the nature of the data and past records of government access requests may justify a conclusion that certain types of data, covered by these scenarios, are not at risk of being accessed by public authorities.

We encourage the EDPB to adopt the Commission's more flexible, pragmatic approach directing companies to take into account the range of specific circumstances relating to the underlying transfers. In particular, we encourage the EDPB to clarify, as discussed in our recent comments to the Commission,[30] 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. As explained in part II.B of these comments, it is only necessary for companies 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, 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 concrete impacts a transfer of personal data will have on individual privacy, as opposed to engaging in a speculative exercise about theoretical possibilities.

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,[31] 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 FISA 702, the form of compulsory process of concern to the Court of Justice in *Schrems II*. For those companies not receiving FISA 702 orders, there is no need to conduct an assessment of U.S. privacy protections relating to FISA 702 under EU standards. 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 EDPB 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 EDPB 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 U.S. intelligence agencies, the possibility

[30] Comments from the U.S. government on Proposed SCC Decisions at 8-9 (10 Dec. 2020), at link.

[31] *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.

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 EDPB should make this clear.

E. Provisions in the proposed Recommendations calling for data encryption that, if widely adopted, is likely to have serious adverse impacts on public safety and national security in the United States, Europe and other countries around the world should be reconsidered.

Encryption plays a crucial role in protecting such important interests as personal data privacy, intellectual property, trade secrets, and cyber security. Certain kinds of encryption, however, make it very difficult if not impossible for law enforcement and intelligence agencies to obtain information needed to protect public safety and national security. Balancing these two competing and important considerations is difficult. Here, the proposed Recommendations would, for the first time of which we are aware, in effect require companies to implement encryption that would effectively block all government access to personal data if they wish to transfer the data to countries whose laws have not been assessed as meeting EU data protection standards. For example, the proposed Recommendations state (paragraph 44) that if the data importer falls under FISA 702, which authorizes compulsory access to data held by certain U.S. companies for foreign intelligence purposes, "transfer tools may only be relied upon for such transfer if additional supplementary technical measures make access to the data transferred impossible or ineffective." And the Recommendations repeatedly suggest (paragraphs 36, 37, 39, 44, 48-50; Annex 2, paragraphs 84-85) the use of end-to-end encryption as an effective technical supplementary measure to achieve this result, and does not identify any other available supplementary measures, leaving end to end encryption as the only available tool for such transfers.

If widely adopted by companies, this recommendation to employ end-to-end encryption would have profound negative impacts on Member State governments and other rights-respecting countries by broadly denying lawful access to electronic data that is important for protecting public safety and national security. The proposed Recommendations are substantially overbroad insofar as they foreclose *all* government access to data transferred from the EU to the destination country, not just access under laws that are the subject of concern. In other words, this approach could foreclose not only access under laws that are deemed inadequate under EU standards, but also access pursuant to laws that the EDPB and all concerned would agree provide appropriate data protection and privacy protections that meet or exceed EU standards. Thus, for example, ordinary criminal search warrants issued by federal judges in the United States based on a high "probable cause" standard could be blocked by the encryption required by the proposed Recommendations. This would have serious and needless adverse effects on public safety and security.

If put into place, the Recommendation would leave the U.S. government unable to execute EU Member States mutual legal assistance (MLA) requests for data located in the United States that they consider necessary for criminal investigations. Nor could the U.S. government facilitate emergency requests from EU Member States for disclosure of electronic data where there is an imminent threat to life, as the United States currently does without requiring any MLA request. The data may not be available. We expect that much of the encrypted data would

also be unavailable within Europe, depending on how the companies configure their networks in response to the EDPB's Recommendations. Some could choose to apply end-to-end encryption to data and data transfers regardless of their location, and certainly data that EU Member States may seek for their investigations may be located only outside Europe but encrypted and thus unavailable as a result of the proposed Recommendations.

The proposed Recommendations are in this respect in tension with recent positions taken by the EU, as well as other statements made by governmental leaders from around the world, on the issue of lawful access. For example, late last year, in the context of combating sexual abuse of children, the Council of the EU urged "industry to ensure lawful access for law enforcement and other competent authorities to digital evidence, . . . without prohibiting or weakening encryption and in full respect of privacy and fair trial guarantees consistent with applicable law."[32] The Council recently adopted a further resolution that proposes a better balance between privacy through encryption and the ability of competent authorities to lawfully access relevant, encrypted data.[33] In that resolution, while the Council recognized and supported the development and use of strong encryption, it also emphasized that it is "essential to preserve the powers of competent authorities in the area of security and criminal justice through lawful access to carry out their tasks, as prescribed and authorized by law."[34] The concerns of the EU have been echoed by other government leaders around the world.[35]

We also believe encryption is unlikely to be a practical, realistic option for many companies as the effort to protect privacy would also mean that the companies themselves cannot access and use the encrypted data. This would frustrate the purpose of many data transfers. If the only available mechanism for the transfer of personal date between the United States and Europe is end to end encryption, we believe the result will be a significant restriction on U.S.-EU commerce as many, perhaps most, existing commercial relationships that involve the transfer of personal data will be prohibited, as end to end encryption is not commercial viable in many business contexts. The United States and the European Union enjoy a $7.1 trillion economic relationship—with $5.6 trillion in transatlantic trade annually. According to some estimates, nearly $450 billion of this trade involves digital services. In truth—given the ongoing digitization of virtually every industry sector and the fact that cross-border data flows between the U.S. and Europe are the highest in the world—far more of that overall $5.6 trillion in trade is

[32] Council of the European Union, *Council Conclusions on Combating the Sexual Abuse of Children*, 12862/19 (8 Oct. 2019), at link.

[33] Council of the European Union, *Council Resolution on Encryption—Security through Encryption and Security Despite Encryption*, 13084/1/20 (24 Nov. 2020), at link.

[34] *Id.*

[35] *See* Council of the EU, Press Release, *Joint EU-US Statement Following the EU-US Justice and Home Affairs Ministerial Meeting* (11 Dec. 2019), at link; U.S. Department of Justice, Press Release, *International Statement: End-to-End Encryption And Public Safety* (Oct. 11, 2020), at link. Gilles de Kerchove, the EU Counter-Terrorism Coordinator, welcomed the international statement on end-to-end encryption and public safety and noted that in "the fight against terrorism it is crucial that the law enforcement agencies have lawful access to encrypted messages when the legal requirements for such access are fulfilled." Council of the European Union, *Counter-Terrorism Coordinator, Current Reactions*, at link.

facilitated in some way by cross-border transfers of data. Requiring end to end encryption for all personal data transfers could significantly impair this relationship.

These concerns are not hypothetical or abstract. A government mandate to expand end-to-end encryption would create more lawless space for terrorists, child predators, drug traffickers, hackers, and the like to cause harm in the real world. For example, some social media and technology companies, such as Facebook, Google, and Microsoft, voluntarily scan their platforms for known child sexual abuse material. These images are then reported to the CyberTipline operated by the National Center for Missing and Exploited Children (NCMEC). In 2019, NCMEC received almost 17 million CyberTips, which identified a total of over 69 million files related to child sexual abuse. Although the CyberTipline is a mechanism for American companies to report online child exploitation, the majority of CyberTips (typically around 95% of reports received per year) are forwarded to law enforcement in foreign countries. In particular, in 2019 more than 3 million of the reports of child sexual abuse images and videos originated from an offender in the EU. In the first nine months of 2020, more than 52 million child sexual abuse files have been reported to NCMEC, and more than 2.3 million of these files involve an offender or a child victim in the EU.

A mandate for end-to-end encryption is likely to have an immediate, measurable, devastating impact on the volume of CyberTips sent to NCMEC. For example, if Facebook adopts end-to-end encryption for its Messenger service, upwards of 12 million CyberTips will disappear overnight. These CyberTips are valuable leads that result in the investigation and prosecution of child sex offenders, and the rescue and recovery of their victims. Thus, preserving the ability of social media and technology companies to monitor their own platforms is as important as preserving lawful access.

In view of these considerations, we submit that the sections of the proposed Recommendations that would in effect require exporters to use encryption of data that blocks all government access as a supplementary measure be removed.

III. Conclusion

In conclusion, we appreciate the opportunity to provide these comments and our views regarding data exporters' responsibility to assess privacy protections in the laws and practices of destination countries and, as necessary, identify and adopt supplementary measures. As we have in the past, we offer to meet with the EDPB to engage in direct and more detailed dialogue on these matters, to reduce these concerns. In view of the high stakes for data exporters and interested governments, we believe that such a dialogue is more essential than ever.