E. Applying the Findings to the Illustrative Scenarios and Gaps Identified

Scenario 1:

Provider X operates an online platform XYXYX as a website on which users can freely upload audiovisual content generated by them. The content made available is exclusively of a pornographic nature, which is the focus of the platform's design and description. The platform offers the content in a categorised manner, includes search functions and makes recommendations for specific content to users entering the platform. The text content of the website is entirely in the language of EU Member State B including for the majority of the titles and descriptions of the videos, which are created by the users when uploading the content. Before users accessing the platform XYXYX can watch a video for the first time, they are asked to confirm that they are at least 18 years old by clicking the button "OK" following the text box indicating this question; there are no further measures foreseen for age verification or limitation of access to any of the content made available on XYXYX. The imprint of the website lists company X as provider of the website, which has its registered office in EU Member State A. In EU Member State B the website is available under the top-level domain of ".b" (XYXYX.b).

The service described in scenario 1 will likely fulfil the conditions to be qualified as a video-sharing platform service according to Art. 1(1)(aa) AVMSD, which is a service where the principal purpose of the service (or of a dissociable section thereof or an essential functionality of the service) is devoted to providing (programmes,) user-generated videos(, or both,) to the general public, for which the video-sharing platform provider does not have editorial responsibility, in order to (inform,) entertain (or educate), by means of electronic communications networks within the meaning of point (a) of Art. 2 of Directive 2002/21/EC and the organisation of which is determined by the video-sharing platform provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing. As the offer mainly consists of user-generated videos and the provider organises these videos by categorising them and providing search functions and recommendations, these requirements are fulfilled without difficulty.

According to Art. 28b(1)(a) in conjunction with Art. 6a(1) AVMSD, Member States shall ensure that VSP providers under their jurisdiction take appropriate measures to protect minors from programmes, user-generated videos and audiovisual commercial communications which may impair their physical, mental or moral development. As such potentially appropriate measures, Art. 28b(3) (f) AVMSD mentions, inter alia, establishing and operating age verification systems for users. This means that both Member State A and B must have obligations in place in their national law obliging VSPs to appropriately protect minors in a comparable way. Nonetheless, the appropriateness of the exact measures to be taken and how these measures have to be applied depends to a certain extent on the national implementation and the respective monitoring efforts. It could well be that Member State A adopted the wording of the AVMSD in its national legislation and leaves the assessment of the appropriateness of the measures to be taken in the first instance to the (VSP) providers. This approach in actual fact was chosen by most Member States in the transposition of the latest revision of the AVMSD. Member State B, on the other hand, could have made it mandatory in its national legislation to have specific, effective age verification mechanisms in place, which possibly even state that any lack of applying such systems may amount to an offence.

Member State B does not have jurisdiction in the present case, because according to Art. 28a(1) AVMSD this lies with the Member State on whose territory the service is established. According to the imprint of the website this is State A. It is irrelevant for the determination of jurisdiction that the offer is obviously directed exclusively or mainly at users in Member State B, if there is such an establishment in another EU Member State. Therefore, Member State B would in principle be prevented from taking action based on its national law against the website or the VSP provider because of the country-of-origin principle. This would also apply if the service disseminating the content would have editorial control over the videos and fulfil the requirements of Art. 1(1)(a)(i) in combination with Art. 1(1)(g) AVMSD to be qualified as on-demand audiovisual media service. If it were responding to the content of an audiovisual media service provider, Member State B would have resort to the derogation procedure of Art. 3(2) AVMSD if the conditions of the procedure are respected. No such procedure exists in case of VSPs. However, B could attempt to request mutual assistance from A.

Art. 30a(3) AVMSD provides a mechanism for mutual assistance, but it applies only if audiovisual media services are concerned and is closely connected to possible derogation decisions. It does not extend to VSP matters.

This means that Member State B could not rely on a specific procedure enshrined in law but could still make a request to Member State A asking to ensure that X operates the website in compliance with Art. 28b AVMSD. Because of a lack of procedures for VSP constellations in the current AVMSD, this was a focus area for the MoU that ERGA Members agreed on. In section 2.1.3. there are details on how the regulatory authorities want to provide each other mutual assistance, also concerning matters related to protection of minors and in connection with VSPs (see point 2.1.3.4. (c) and (f)). For VSP-related matters there is even a dedicated section in the MoU which addresses cooperation between the regulatory authorities to achieve a compliance of VSPs on a "macro level"; so rather than regarding individual items that have not been dealt with appropriately by a provider, it aims at the more general problems that may occur (point 2.2.1.1. (d)). It could be easily argued that offering a VSP service focusing on pornographic content without any age verification instrument besides a question to the user about whether they are of age and the consequential open availability of the pornographic content is a 'macro' issue. In cross-border cases where the matter created by a non-domestic VSP is of special relevance for a targeted state, another section of the MoU lays down how ERGA members can submit requests for cooperation and how other regulatory authorities should react to them (point 2.2.1.3.5). These procedures are promising in that they carefully describe adequate steps which could also help in the case of B and A. However, and this is not only obvious from the legal nature of the Memorandum but also explicitly acknowledged by the parties to it, the MoU is not legally binding and no legal obligations arise out of it. This means that if A has not reacted so far to the way provider X has rolled out its service – possibly because the regulatory authority is not of the opinion that it is problematic – then it may well be that a mutual assistance or cooperation request would not be responded to and there would not be a (direct) measure that the national regulatory authority of B would have against that.

Although in this case it would seem that there cannot be two different opinions on the inappropriateness of age verification tools that only request clicking an "OK" button confirming a supposed age of 18 or more, especially as pornography in Art. 6a(1) AVMSD is mentioned as one of the categories that are most harmful for minors and therefore require the strictest measures (which is repeated for VSPs in Art. 28b(3) sentence 4 AVMSD), the procedures currently applicable are purely voluntary. Obviously, in a case such as scenario 1, where a Member State would not act on a mutual

assistance request, it can be doubted that Member State A would be acting in accordance with the 'effet utile' principle of EU law, as the Directive's application in practice in that Member State (even if based on the national transposition) would not be reaching the goals of the Directive. However, it would only be the Commission that could initiate an infringement proceeding ultimately bringing A to the CJEU.

If it were not such a clear-cut case of content endangering minors, e.g. if it was only nudity or simple depictions of violence that would be available on the service of X, the regulatory authority of B might not even see a need to act. The same could be the case if there are age verification instruments foreseen which B for providers under its own jurisdiction would hold to be inappropriate but at the same time not completely ineffective. If B would decide to act itself because of the situation being a grave risk, the regulatory authority would have to rely on X's cooperation. If X cannot even be reached – it is possibly not identifiable via the imprint and additional searches – or simply does not react to any requests, restrictive measures against the accessibility of the website in B could only be addressed to domestic providers of other services, such as internet access providers, for blocking the website. These measures would depend on the framework of derogation measures under the ECD (Art. 3(4)(a)(i)), but they would also depend on fulfilling the proportionality requirement in light of the measure being addressed against another provider than the content provider, and they would have to complete the procedural steps foreseen if B would not resort to the urgency procedure. Even if such a measure leads to a successful blocking of access to the website for users in B – as long as they do not use, e.g., VPN or other tools to imitate a different geolocation with which they access the content –, the problem is that the measure will be directed against the URL as it stands when the investigation is completed, here: "www.XYXYX.b". If X as the provider changes its domain, here for example to "www.XYXYX.ba", the validity of the original measure does not extend to it and – at least the way the law stands now – a new procedure would have to be initiated.

Scenario 1 therefore shows that even in such an obvious case of need for enforcement there are challenges that cannot be resolved satisfactorily with certainty under the current framework. And this does not even address possible consistency issues with the jurisdiction of the DSC under the future DSA with regard to the obligations of online platforms to protect minors.

Scenario 2:

Broadcaster C is based in State D, which is located outside of Europe. It is directly financed by State D, and it is openly communicated that D has the power to take editorial decisions over the programme of C. C does not have any other subsidiaries or offices within or outside of the EU. C broadcasts in its linear offer a daily programme dealing with current medical and health issues. In several of these programmes, persons declared as medical experts for the field spoke repeatedly about findings that Corona vaccinations cause serious damage to health. This is done without reference to any scientific evidence. They further spread the theory that governments of EU Member States are aiming to reduce population numbers by mandating the use of the vaccinations. Senior management staff of C have publicly declared that government representatives of State D decided on the content of these programmes and selected the 'experts' to be invited. The linear offer of C is broadcast both via satellite operated by a provider in a EU Member State and via a live stream on the internet, which runs on C's own servers. In both ways the offer is available in EU Member State E and the programmes in question have corresponding subtitles in the national language of E. As a result of those broadcasts there has been considerable unrest among the population of E, and a considerable decline in the vaccination rate in the population could be observed compared to the situation before the programmes were broadcast.

Scenario 2 is about an audiovisual media service that distributes its programmes within the EU but is located outside of it. On first view it is evident that it is a linear audiovisual media service and could therefore, in principle, be within the scope of the AVMSD. Irrespective of the question of whether or not there is a legal competence to deal with such providers by EU Member State E, there is a difficulty to have access to provider C for example to request information on the financing or structure. It is not of immediate relevance that the programme of C is directed at citizens in the EU and namely Member State E through the subtitles in the national language of E, as the AVMSD does not follow the market location but the country-of-origin principle in order to determine jurisdiction. According to Art. 2(1) AVMSD, Member States (only) have to ensure that providers under their jurisdiction comply with the AVMSD. C clearly does not have an establishment in any of the EU Member States as it does not have any other subsidiaries or offices but the base in D. Therefore in principle each Member State in which the content is available – due to the satellite dissem-

ination likely all of the EU Member States – is competent to deal with the service. However, this changes if a jurisdiction is deemed to be determined due to one of the technical criteria as mentioned in Art. 3(4) AVMSD. The provider of the satellite service which is located in the EU is not a sufficient link between service provider C and the single market to create jurisdiction due to the technical criterion. However, it is likely (and in the case of the actually relevant satellite service providers currently operating in the EU typically the case) that such a provider either will be offering its clients uplinks, which are also within the State where it is established or another EU Member State, or will be using satellite capacities, which are appertained to the Member State where it is established. In either way it is sufficient to create jurisdiction.

However, such jurisdiction results only for the satellite transmission of the programme, so questions related to this are in the scope of application of the AVMSD. For the transmission of exactly the same content and in parallel to it via an internet stream, however, there is no such jurisdiction of a Member State, so that for this dissemination the legal framework of the AVMSD does not apply.

For the internet stream, under the current framework it is only the legal rules besides the AVMSD that are relevant. On first glance, relevance of the DSA could be considered as content dissemination is concerned. However, C distributes its own content via its own servers, so there is no intermediary involved between C and the availability of the online stream on the internet. An intermediary service only comes into play between the end user/viewer and his or her access to the internet from where he or she can then visit the livestream of C. The ECD and derogation procedures allowing to deviate from the internal market principle are not applicable here either, as the provider of the potentially illegal content is not established in any of the EU Member States.

The scenario poses the additional difficulty of the substantive rules applicable. Currently, there are no explicit rules in EU law on the topic at issue here with the content of C, primarily disinformation as it is possibly a campaign with the intention to destabilise, and with state-controlled content in the service. Therefore, the relevant legal framework including on whether and how reactions to C are possible depend on the law of Member State E. It could be imagined that E has passed specific laws dealing with disinformation or expecting certain editorial standards in news items of a linear programme, such as independence and accuracy. There could also be rules in criminal law. If media law would, e.g., require certain conditions

for a licence for broadcasting before a linear programme is allowed to be disseminated on the territory of E, the illegality in case of C's service would also become relevant for the DSA, if it would be otherwise applicable, when intermediaries are addressed that are involved in transmission of that broadcast and ordered to block access.

For the satellite transmission of C's service, the next hurdle in the AVMSD is that it must be questioned whether the substantive rules address this type of content disseminated. Although the effect as described in this scenario certainly can be harmful, currently the AVMSD neither prohibits disinformation as such nor establishes a requirement of independence for audiovisual offerings from state interference. In addition, there are no general obligations for audiovisual media service providers to comply with journalistic standards such as truth or impartiality of reporting. Any such rules would depend on whether they are existent in the Member State of jurisdiction or – if E would want to trigger a derogation procedure – in Member State E. If the Member State of jurisdiction would not have any specific rules for this situation, there would not be a fallback clause in the AVMSD qualifying the content as illegal under the Directive. Art. 6(1) AVMSD, for example, only covers the prohibition of "incitement" to hatred or violence, but mere spreading of disinformation as such does not necessarily come with a negative targeting of a specific group of persons, because in the scenario the programmes imply that it is the governments of the EU Member States that have a secret plan in mind.

A possible justification to take measures against dissemination in E, however, can be found in the derogation mechanism under Art. 3(2) AVMSD. In that regard, services prejudicing or presenting a serious and grave risk of prejudice to public health can be reacted to with restrictive measures if the derogation procedure is completed. Maybe the risk presented by the service would even qualify for a derogation under Art. 3(3) AVMSD due to the reaction of the people, as it may constitute a serious and grave risk of prejudice to public security. However, in both cases a multistep procedure as described in detail above would have to be completed by the Member State E firstly, although the threat by the service is very current and at a high level. Only if it would be a derogation procedure under Art. 3(3) AVMSD, the Member State could act in the urgent procedure laid down in Art. 3(5) AVMSD within a month of alleged infringement taking place (here some of those medical programmes) by taking restrictive measures without awaiting the outcome of the regular derogation procedure. But even then a compatibility of the measures would retrospectively have to be

reviewed by the Commission. Another issue with the restrictive measures that E could take is that they directly only concern means which it can enforce on its own territory, for example advising cable networks not to pick up and retransmit the satellite signal of C's service. The dissemination of the satellite signal as such and the reception possibility for viewers in E via a satellite dish is not affected by a restrictive measure in E, as a supplementary action based on the law of the Member State with jurisdiction would be necessary (but is not mandated by the AVMSD) in addressing the satellite provider.

This scenario shows that law enforcement in case of providers not regularly established in an EU Member State strongly depends on the means of dissemination, although from the perspective of the recipients and their interests protected by fundamental rights this should not be relevant. It is further evident that speedily reactions by regulatory authorities are not the norm even if the situation at hand is of high urgency. Finally, the consequence of successful derogation procedures under AVMSD is still limited.

Scenario 3:

Provider F operates a social media platform on which users can network with each other and share content in various forms (text, images, audio, video, combinations thereof) with each other and with the general public. The website on which the platform is operated is accessible in all Member States of the EU, but under different top-level domains. F has its headquarters in state G which is located outside Europe. It operates a European branch in EU Member State H, in the offices of which the design of the offer is decided in a binding manner for the offer as it is put on the market in the EU area under all the top-level domains which are available in the EU Member States, namely those with a country-specific top-level domain. User I, who registered himself as user on the platform with a valid email address under a pseudonym, shares a video which is publicly available and not only to registered users of the platform. In the video he can be seen masked and armed with a rifle and calls in an electronically distorted voice for an attack on the head of government of State J, which is an EU Member State. The real name or even place of residence of the user are not made known on the platform. The video in question is shared multiple times by other users and subsequently spreads widely over the whole network across different EU Member States.

In scenario 3, unlike in the other two scenarios, the question already arises as to whether the offering is covered by one of the provider definitions in the AVMSD. The user (I) is most probably not a provider of an audiovisual media service in the sense of the AVMSD (Art. 1(1)(a)), as the sharing of that video seems more incidental and not part of a recurring and editorial activity offered for commercial purposes as a service, e.g. resembling a news channel of a linear service or a catalogue of programmes of a non-linear service. In addition, if Member State J wanted to take action against user I – for example as part of a criminal investigation –, the initial problem would be that user I is not identifiable directly; hence procedures would have to be initiated to find out, e.g. from the platform provider F via the valid email address (although without a proper name), who user I is. Without going into detail here as this is beyond the scope of the analysis in this study, a potential order to provide information about the user I addressed to the intermediary F as foreseen in the procedure under Art. 10 DSA could apply. It is noteworthy that the setup under that provision, which also includes information flows via the DSCs, is complex, and it will have to be seen how efficiently this works in practice.

More interesting in our context is that a possible action by Member State J against F with the aim of removing the content could be considered. Potentially the service of F could qualify as VSP under the AVMSD, which, as stated in Recital 5, can include social media services if "the provision of programmes and user-generated videos constitutes an essential functionality of that service". This criterion of essential functionality as mentioned in the definition of VSPs was included to open further the scope of application of the AVMSD by not requiring that the main or a dissociable part of a service has the purpose of providing programmes or user-generated videos, but that it can be enough if there is the functionality of sharing videos and this is an essential functionality of the service. In order to give some direction, the Commission issued Guidelines on this criterion, as Recital 5 authorised (but did not mandate) the Commission to do. However, these non-binding Guidelines still leave it to the legislative framework of the Member State having jurisdiction to decide whether or not a specific service qualifies as VSP because of the essentiality of the function. Typically this decision will depend on a classification by the regulatory authority. In the present case, the social media platform is made up of sharing possibilities for all kinds of data, not only user videos, so the determination is at least not obvious, even though possible.

If there is a possibility that the service of F is a VSP, the jurisdiction determination is based on Art. 28a(2) to (4) AVMSD. In particular it is to be assessed differently than would be the case for an audiovisual media service according to Art. 2(3), for which the establishment and place of programme-relevant decisions is decisive. Art. 28a AVMSD foresees a cascade of criteria which allow to assume a "fictitious" establishment for VSP providers that are not established in an EU Member State but have connections to the Single Market through a presence in at least a Member State. According to Recital 44, the legislators deemed it to be appropriate to ensure that the same rules apply to VSP providers which are not established in a Member State and to those that are actually established in one of them, to make sure that the aims of protecting minors and the general public set out in the AVMSD can be reached. Therefore a parent undertaking or a subsidiary established in a Member State or where those providers are part of a group and another undertaking of that group are established in a Member State is sufficient to constitute an establishment of the part of the undertaking actually providing the VSP. F is established outside of the EU in G, but it operates a subsidiary branch in H – whereby it is not relevant which activity is provided by that branch, rather whether it is the place of

first activity in case there would be more than the one branch in H within the EU. In the scenario Art. 28a(2)(a) AVMSD would create jurisdiction for H because F would be regarded to be established there. If F is such a VSP under jurisdiction of H, the content of user I would likely violate Art. 6(1)(b) AVMSD and H would have to make sure that F has taken appropriate measures according to Art. 28b(3) AVMSD and, if not, take supervisory action.

This scenario shows the complexity of establishing what type of service under which jurisdiction is involved in the dissemination of illegal content by its users and what reach possible reaction measures have. Especially the multiplication of content in short periods of time, as described in this scenario, makes effective enforcement more difficult if it happens retroactively.