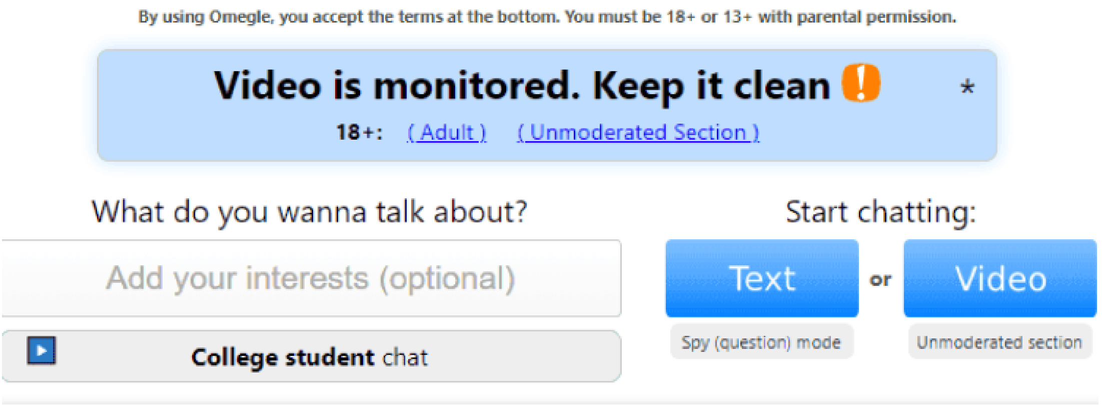
LSE Department of Law

Risk Management

lse.ac.uk/law
@LSELaw



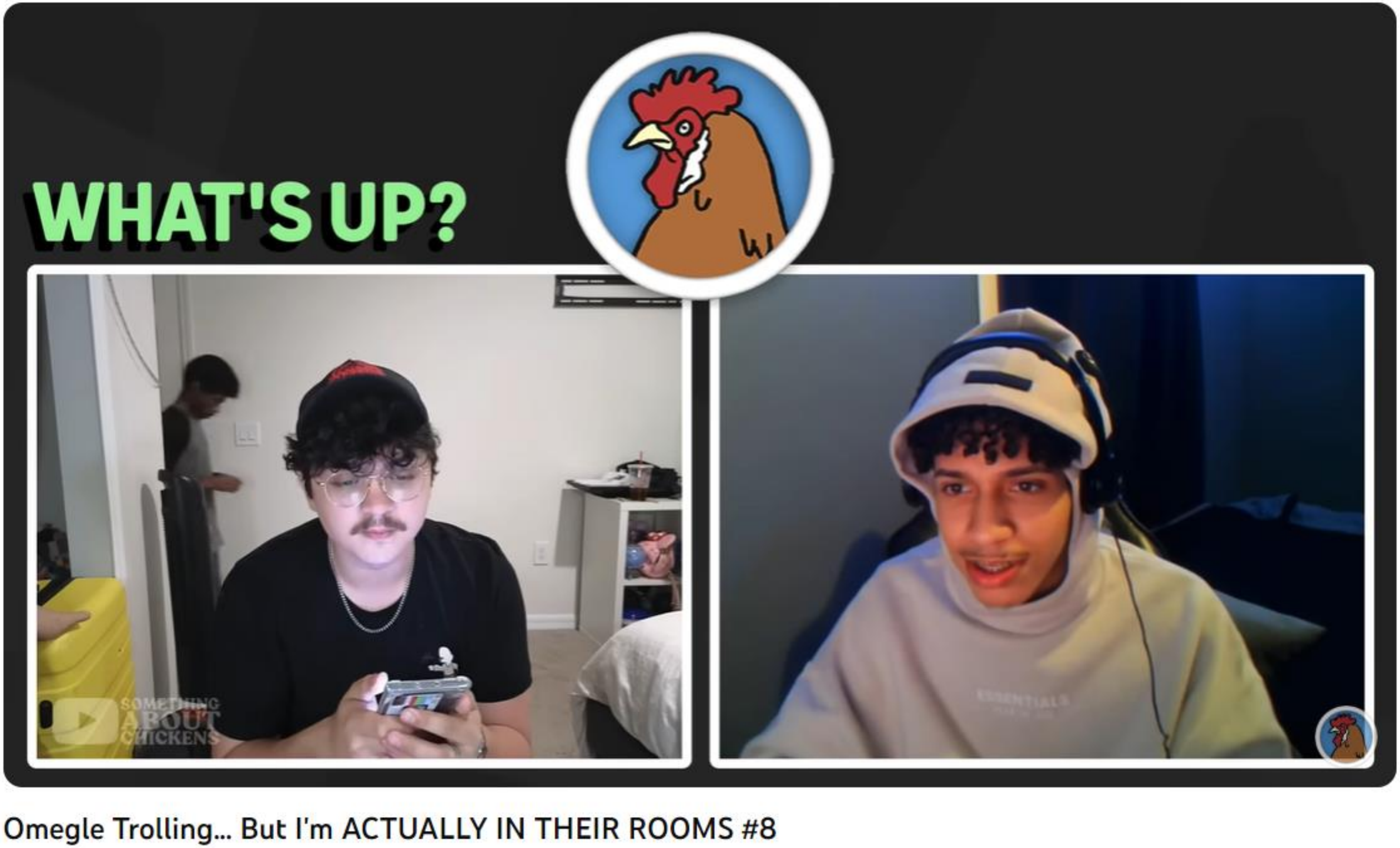
By using Omegle, you accept the terms at the bottom. You must be 18+ or 13+ with parental permission.

Video is monitored. Keep it clean !

What do you wanna talk about?

Start chatting:

- **Omegle** was one of the more popular video chat sites available online. It pairs random users identified as ‘You’ and ‘Stranger’ to chat online via ‘Text’, ‘Video’ or both.
- A user can also choose to add their interests, and Omegle will try to pair a user with someone who has similar interests. If not, you could meet anyone.
- Chats are anonymous unless the user states who they are. It’s free and no account sign up is required.



Omegle Trolling... But I'm ACTUALLY IN THEIR ROOMS #8

Is
@

Risks to children

- The DSA puts forward specific obligations for all online platforms “accessible to minors” (Article 28(1)).
- This obligation was included in the final text at the latest stage of the negotiations, as a “spin-off” of the prohibition of dark patterns proposed by the European Parliament.

Article 28(1)

“Providers of online platforms **accessible to** minors shall put in place **appropriate** and **proportionate** measures to ensure a high level of **privacy**, **safety**, and **security** of minors, on their service.”

LSE Department of Law

Article 28(1)

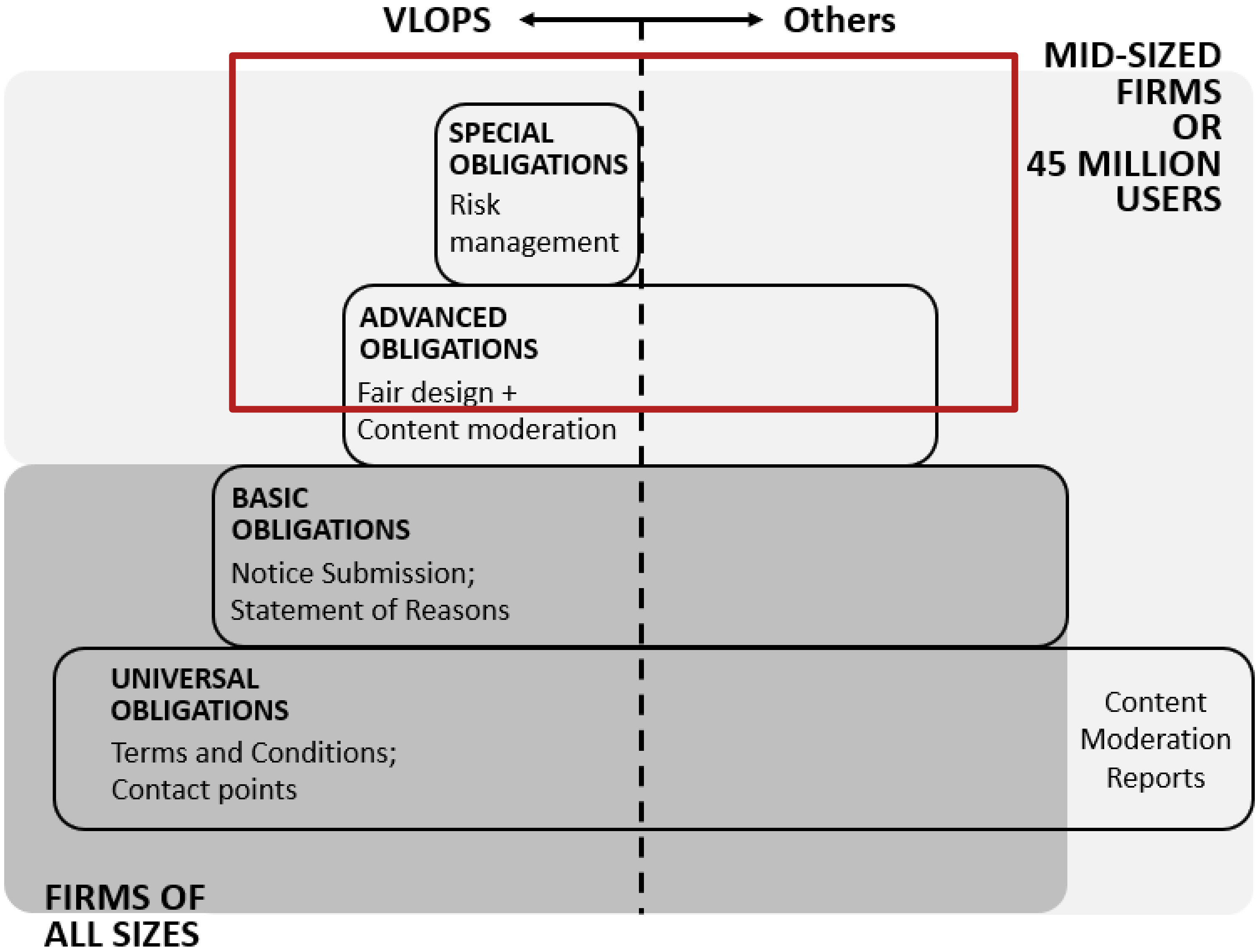
"Providers of online platforms **accessible to** minors shall put in place **appropriate** and **proportionate** measures to ensure a high level of **privacy**, **safety**, and **security** of minors, on their service."

Arguably:

only design-related interventions; not mini-Article 34; ex-ante measures, less related to content categories

Risk Management

Fair design practices		General risk management
Specific features	Specific issues	Anything
Advertising & Recommender systems (Art 26 & 27)	Children & consumer specific risks (Art 25, 28, 30 & 31)	Any other risks (Art 34)
Online platforms & mid-size +		VLOPs/VLOS Es: 45 mil +



VLOPS ← → Others

MID-SIZED FIRMS OR 45 MILLION USERS

SPECIAL OBLIGATIONS
Risk management

ADVANCED OBLIGATIONS
Fair design +
Content moderation

BASIC OBLIGATIONS
Notice Submission;
Statement of Reasons

UNIVERSAL OBLIGATIONS
Terms and Conditions;
Contact points

Content Moderation Reports

FIRMS OF ALL SIZES

Extras

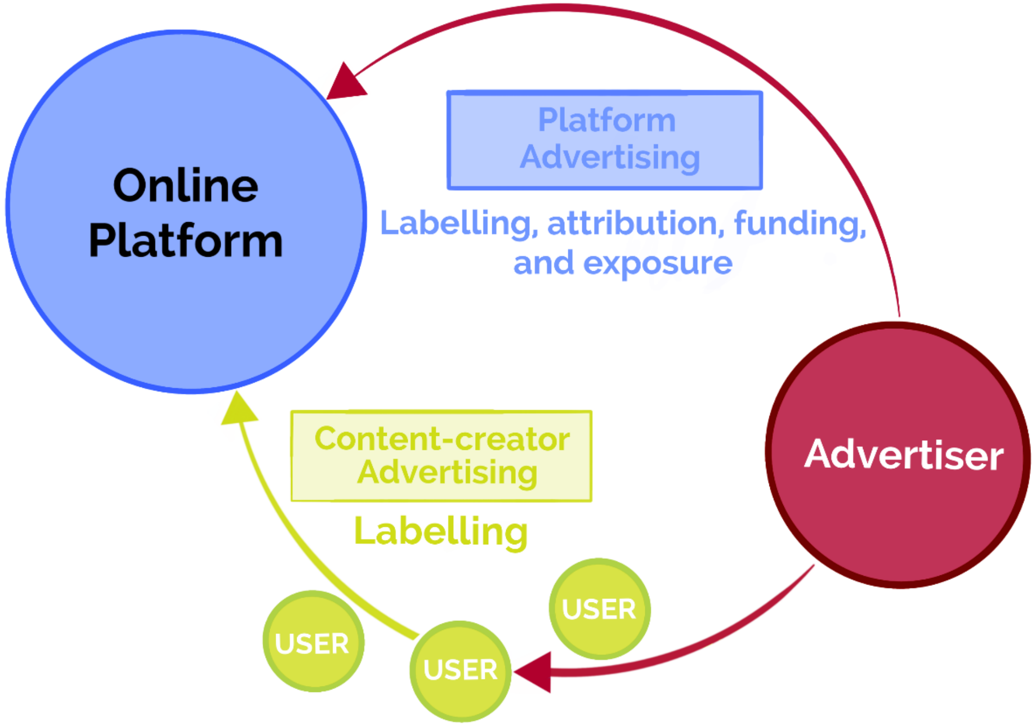
- General risk mitigation system (Art 34-37, 41)
- Opt-out in recommender systems (Art 38)
- Advertising archives (Art 39)
- Data Access (Art 40)
- Extra reporting obligations (Art 42)

Risk management

- Design & operate your services to minimise risks to others
  - The goal is not to eradicate, or entirely de-risk (plus, others have obligations too to avoid the risks)
- Pre-test features, re-test use & revise design or operations
  - C.f. move fast & break things
- OPs: mostly very specific measures (exception: child risks)
  - Unlike VLOPs: very open-ended

Advertising

- Obligation to properly disclose advertising (Article 26(1)&(2))
  - for users' advertising, only facilitate ("shall ensure [others] can identify")!
- Obligation to stop offering ads based on profiling of sensitive data (Article 26(3))

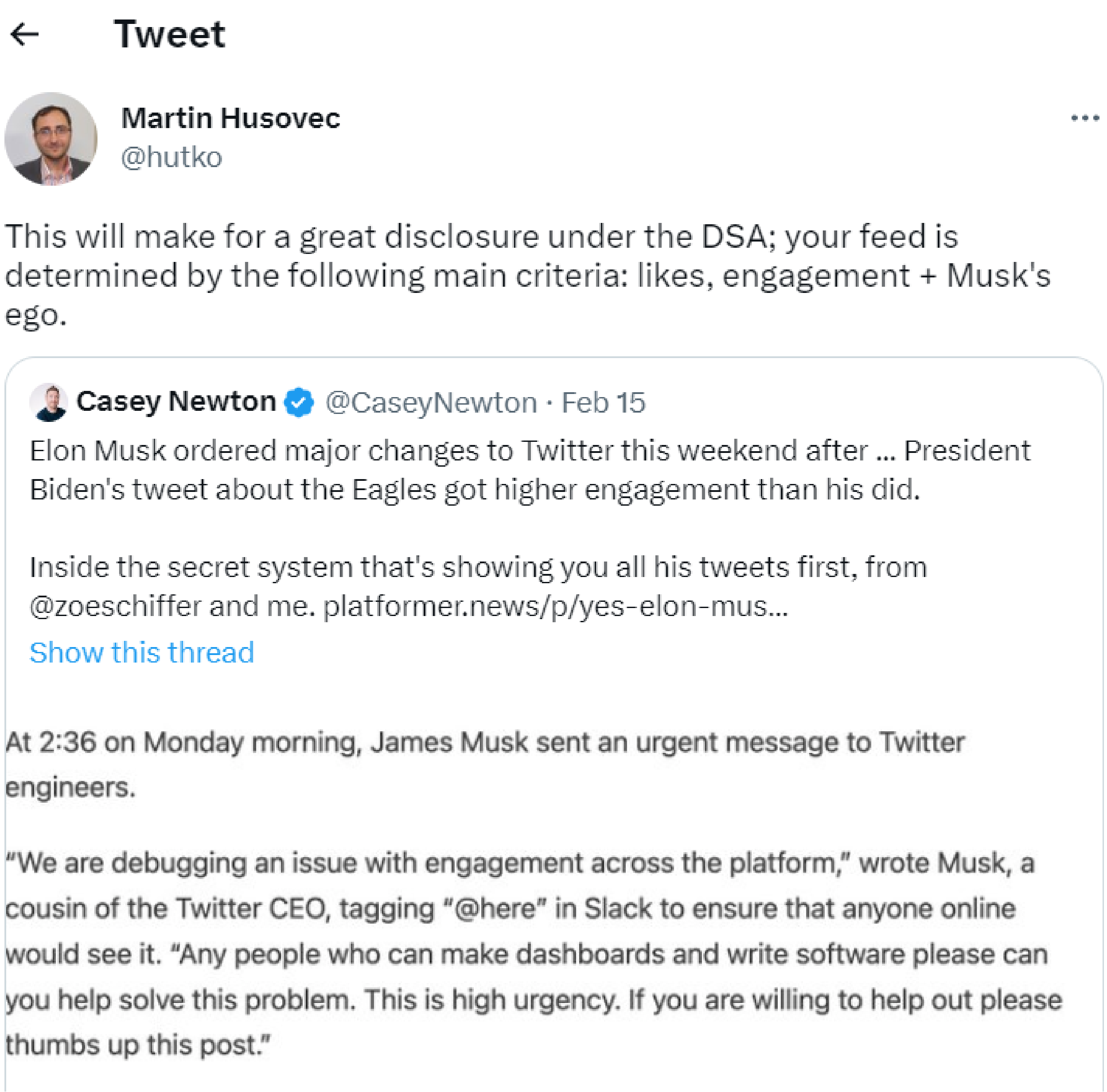

Online Platform
Platform Advertising
Labelling, attribution, funding, and exposure
Content-creator Advertising
Labelling
Advertiser
USER
USER
USER

Recommender systems

- The DSA only regulates what Cobbe and Singh call "open recommending".
  - Unlike "curated recommending", which recommends from within editorial content, such as on the website of media or streaming services, "open recommending", recommends from the pool of content which was not specifically vetted in any way.
- Open recommending operates on a much larger scale and with a wider pool of potential information to recommend.

RECSYS: Article 27

“Providers of online platforms that use recommender systems shall set out in their terms and conditions, in **plain** and **intelligible language**, the **main parameters** used in their recommender systems, as well as any **options** for the recipients of the service to modify or influence those main parameters.” = “explain **why** certain information is suggested”, at least: “(a) the criteria which are most significant in determining the information suggested to the recipient of the service; (b) the reasons for the relative importance of those parameters.”



Martin Husovec
@hutko

This will make for a great disclosure under the DSA; your feed is determined by the following main criteria: likes, engagement + Musk's ego.

Casey Newton @CaseyNewton · Feb 15

Elon Musk ordered major changes to Twitter this weekend after ... President Biden's tweet about the Eagles got higher engagement than his did.

Inside the secret system that's showing you all his tweets first, from @zoeschiffer and me. platformer.news/p/yes-elon-mus...

At 2:36 on Monday morning, James Musk sent an urgent message to Twitter engineers.

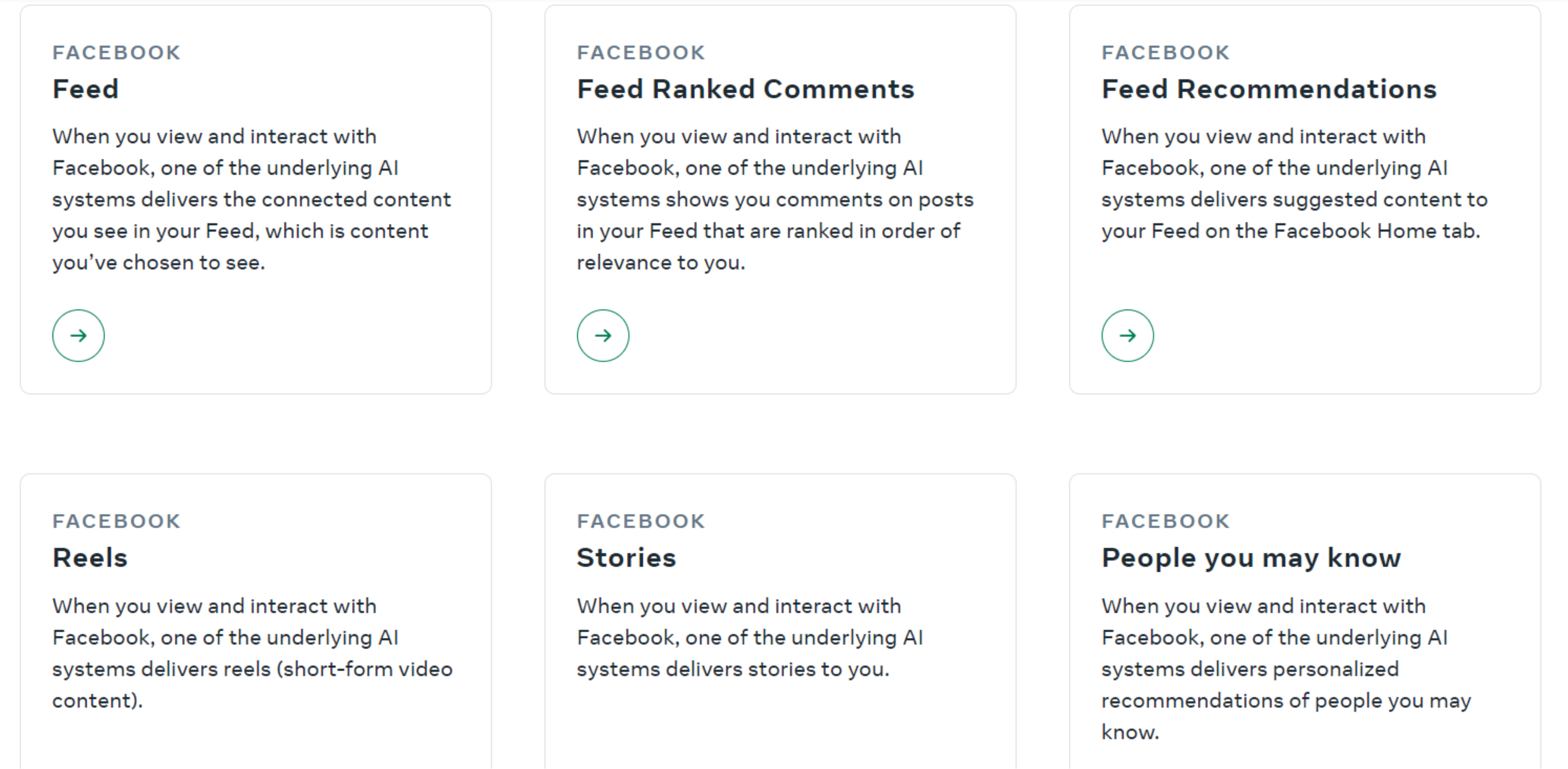
"We are debugging an issue with engagement across the platform," wrote Musk, a cousin of the Twitter CEO, tagging "@here" in Slack to ensure that anyone online would see it. "Any people who can make dashboards and write software please can you help solve this problem. This is high urgency. If you are willing to help out please thumbs up this post."

Article 38 (only VLOPs/VLOSEs)

"[VLOPs/VLOSEs] that use recommender systems shall provide at least one option for each of their recommender systems which is not based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679."

- Providers decide what opt-out they design
- Often different options make sense
  - e.g. on Facebook/Instagram: only chronological from friends/follows vs e.g., TikTok region-based

Given a wide range ..



FACEBOOK
Feed

When you view and interact with Facebook, one of the underlying AI systems delivers the connected content you see in your Feed, which is content you've chosen to see.

→

FACEBOOK
Feed Ranked Comments

When you view and interact with Facebook, one of the underlying AI systems shows you comments on posts in your Feed that are ranked in order of relevance to you.

→

FACEBOOK
Feed Recommendations

When you view and interact with Facebook, one of the underlying AI systems delivers suggested content to your Feed on the Facebook Home tab.

→

FACEBOOK
Reels

When you view and interact with Facebook, one of the underlying AI systems delivers reels (short-form video content).

FACEBOOK
Stories

When you view and interact with Facebook, one of the underlying AI systems delivers stories to you.

FACEBOOK
People you may know

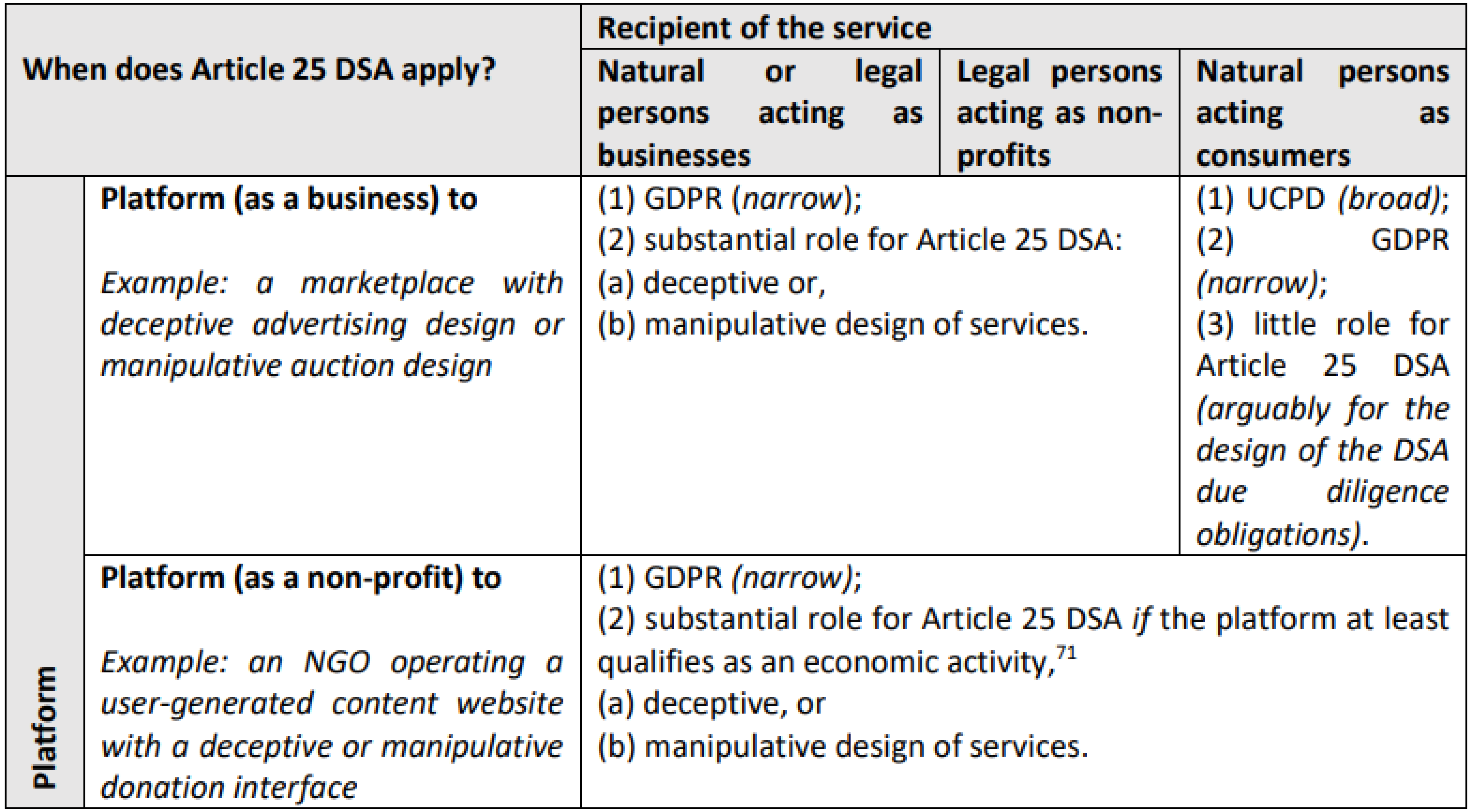
When you view and interact with Facebook, one of the underlying AI systems delivers personalized recommendations of people you may know.

Risks to consumers* (deceit & manipulation)

- A general obligation on online platforms to design their "online interfaces" fairly: "[P] shall not design, organise or operate their online interfaces in a way that **deceives** or **manipulates** the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make **free and informed decisions**.
- An interface is defined as "any software, including a website or a part thereof, and applications, including mobile applications" (Art 3(m)).
- Thus, any surface of a digital service that interacts with users is effectively covered (c.f. discussion about backend design)

But for VLOPs/VLOSEs:

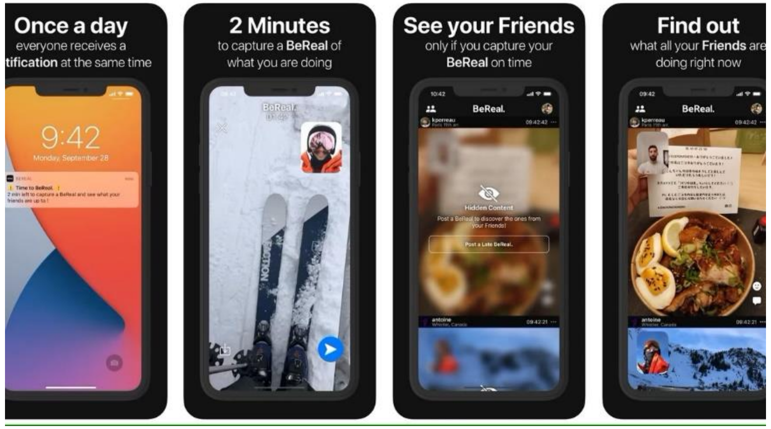
- It is part of general risk management?
  - “design”
  - “use” for users’ DPs

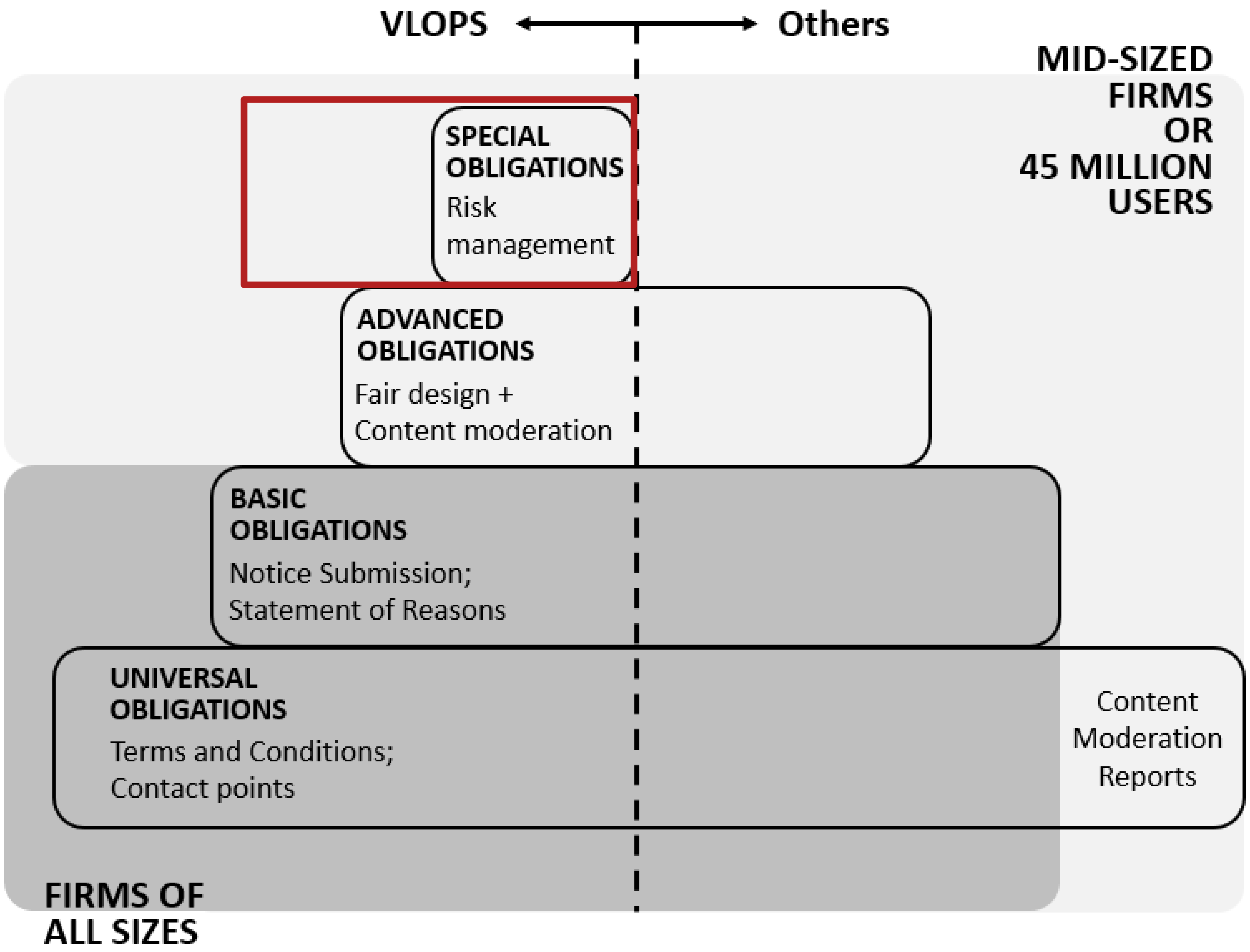


When does Article 25 DSA apply?		Recipient of the service		
		Natural or legal persons acting as businesses	Legal persons acting as non-profits	Natural persons acting as consumers
Platform	**Platform (as a business) to** *Example: a marketplace with deceptive advertising design or manipulative auction design*	(1) GDPR (*narrow*); (2) substantial role for Article 25 DSA: (a) deceptive or, (b) manipulative design of services.		(1) UCPD *(broad)*; (2) GDPR *(narrow)*; (3) little role for Article 25 DSA *(arguably for the design of the DSA due diligence obligations)*.
	Platform (as a non-profit) to *Example: an NGO operating a user-generated content website with a deceptive or manipulative donation interface*	(1) GDPR (*narrow*); (2) substantial role for Article 25 DSA *if* the platform at least qualifies as an economic activity,[71] (a) deceptive, or (b) manipulative design of services.		

Other product features: an example

- BeReal & risks created by peer pressure & tracking of daily activity and its sharing
- Unless risks are specific to children or deceptive/aggressive design, no obligation on the side of non-VLOPs to mitigate other risks.
- **Once they grow big**, then special VLOP obligations make all risks relevant.





VLOPS ⟷ Others

MID-SIZED FIRMS OR 45 MILLION USERS

SPECIAL OBLIGATIONS
Risk management

ADVANCED OBLIGATIONS
Fair design +
Content moderation

BASIC OBLIGATIONS
Notice Submission;
Statement of Reasons

UNIVERSAL OBLIGATIONS
Terms and Conditions;
Contact points

Content Moderation Reports

FIRMS OF ALL SIZES

Marketplaces

- Amazon
- Booking
- Google Shopping
- AliExpress

- Vinted
- Airbnb
- Roblox
- eBay
- Local

VLOP

45+ mil. users

Mid-sized

50+ FTE or 10+ mil EUR

Small Platforms

else

Social media

- Facebook
- Instagram
- Twitter
- TikTok
- LinkedIn
- Snapchat

- Tumbler
- Reddit
- BeReal
- Mastodon instances

VLOP

45+ mil. users

Mid-sized

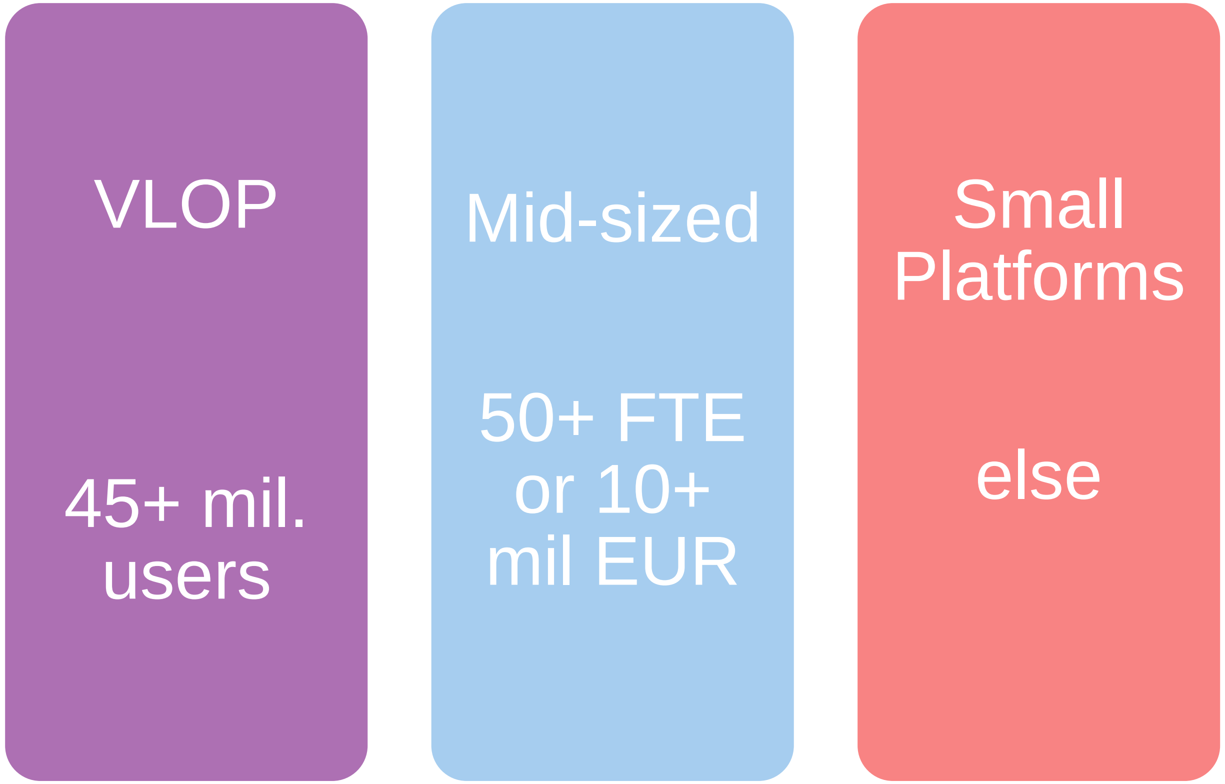
50+ FTE or 10+ mil EUR

Small Platforms

else

Content sharing services

- YouTube
- Instagram
- Pinterest
- Porn sites?
- Dailymotion
- OnlyFans
- Github
- Twitch



VLOP

45+ mil. users

Mid-sized

50+ FTE or 10+ mil EUR

Small Platforms

else

Search engines

- Google
- Bing

- Seznam
- DuckDuckGo
- Yahoo

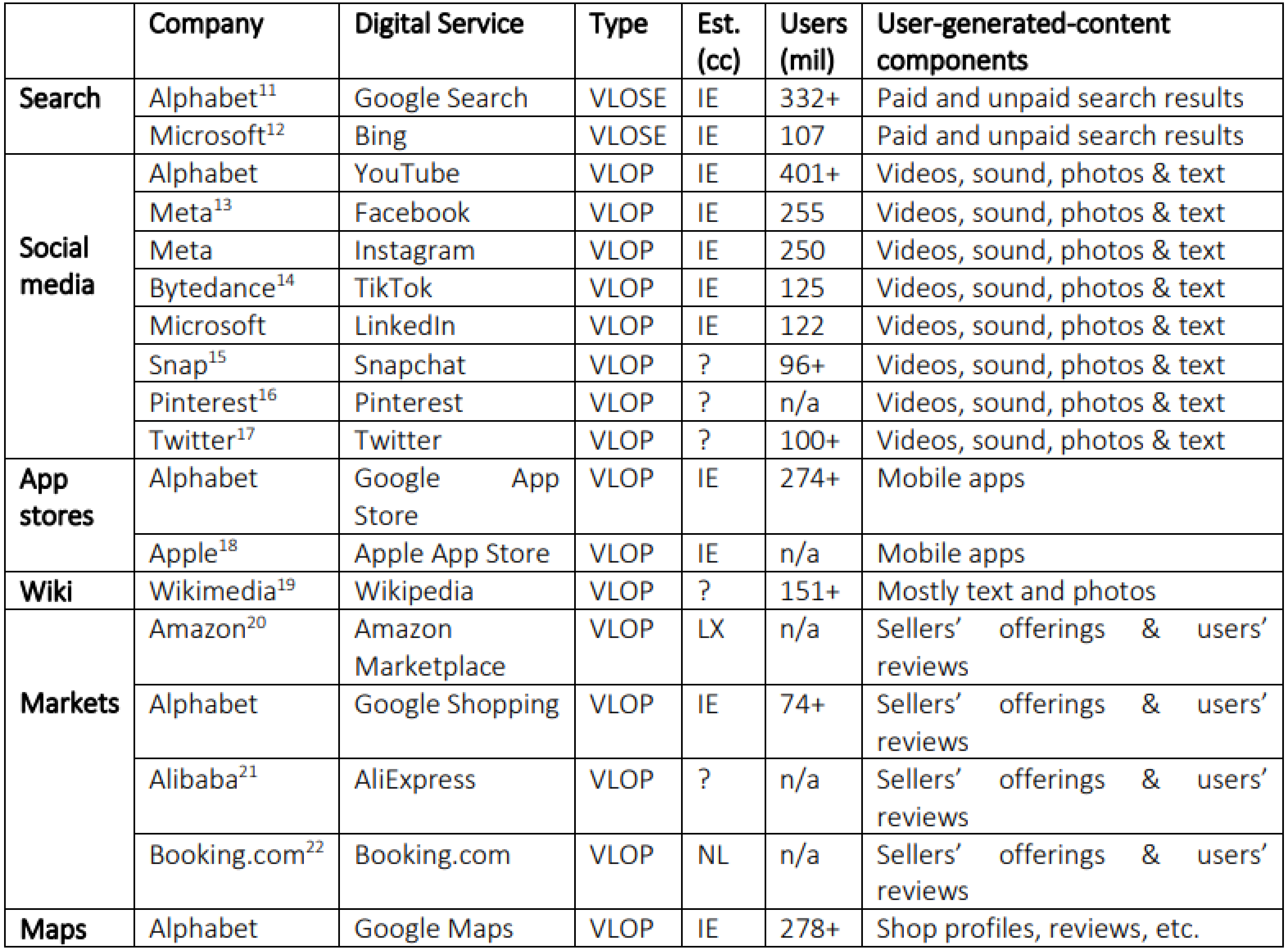
VLOSE

45+ mil. users

Small Search

else

VLOP



	Company	Digital Service	Type	Est. (cc)	Users (mil)	User-generated-content components
Search	Alphabet[11]	Google Search	VLOSE	IE	332+	Paid and unpaid search results
	Microsoft[12]	Bing	VLOSE	IE	107	Paid and unpaid search results
Social media	Alphabet	YouTube	VLOP	IE	401+	Videos, sound, photos & text
	Meta[13]	Facebook	VLOP	IE	255	Videos, sound, photos & text
	Meta	Instagram	VLOP	IE	250	Videos, sound, photos & text
	Bytedance[14]	TikTok	VLOP	IE	125	Videos, sound, photos & text
	Microsoft	LinkedIn	VLOP	IE	122	Videos, sound, photos & text
	Snap[15]	Snapchat	VLOP	?	96+	Videos, sound, photos & text
	Pinterest[16]	Pinterest	VLOP	?	n/a	Videos, sound, photos & text
	Twitter[17]	Twitter	VLOP	?	100+	Videos, sound, photos & text
App stores	Alphabet	Google App Store	VLOP	IE	274+	Mobile apps
	Apple[18]	Apple App Store	VLOP	IE	n/a	Mobile apps
Wiki	Wikimedia[19]	Wikipedia	VLOP	?	151+	Mostly text and photos
Markets	Amazon[20]	Amazon Marketplace	VLOP	LX	n/a	Sellers' offerings & users' reviews
	Alphabet	Google Shopping	VLOP	IE	74+	Sellers' offerings & users' reviews
	Alibaba[21]	AliExpress	VLOP	?	n/a	Sellers' offerings & users' reviews
	Booking.com[22]	Booking.com	VLOP	NL	n/a	Sellers' offerings & users' reviews
Maps	Alphabet	Google Maps	VLOP	IE	278+	Shop profiles, reviews, etc.

Risk management

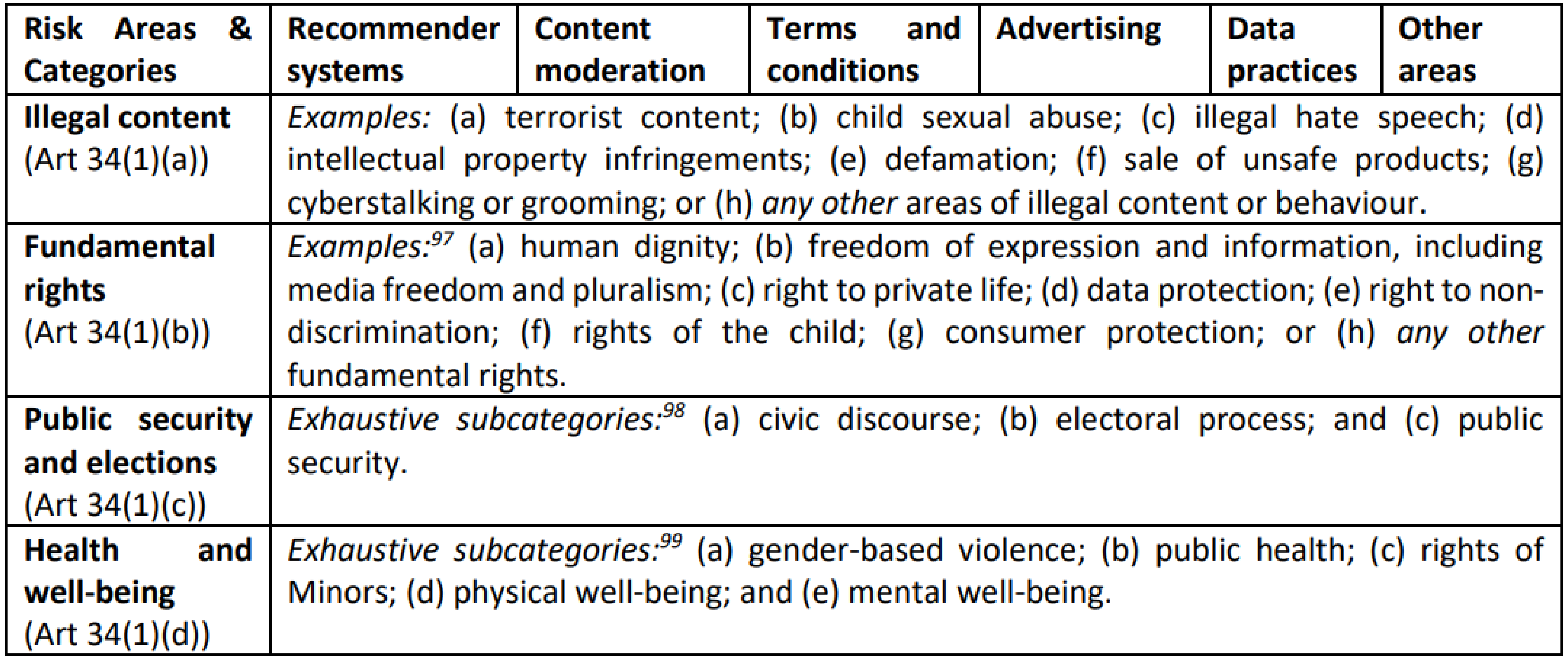
Risk Mitigation rules

- Article 33 – designation
- Article 34 – risk assessment
- Article 35 – risk mitigation
- Article 37 – audits
- Article 42(4) – transparency

VLOP’s risk management: Article 34(1)

Providers of very large online platforms and of very large online search engines shall diligently identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services. This risk assessment shall be specific to their services and proportionate to the systemic risks, taking into consideration their severity and probability, and **shall include** the following systemic risks: (..)

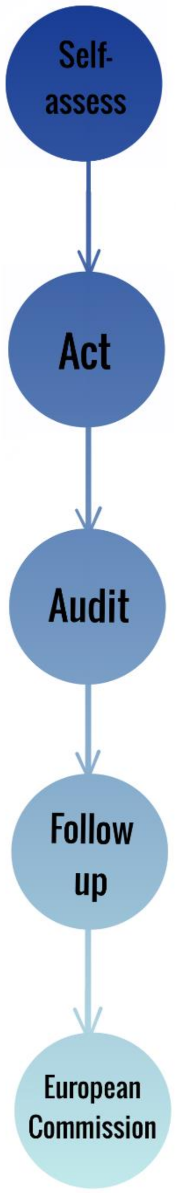
VLOP’s risk mitigation



Risk Areas & Categories	Recommender systems	Content moderation	Terms and conditions	Advertising	Data practices	Other areas
Illegal content (Art 34(1)(a))	*Examples:* (a) terrorist content; (b) child sexual abuse; (c) illegal hate speech; (d) intellectual property infringements; (e) defamation; (f) sale of unsafe products; (g) cyberstalking or grooming; or (h) *any other* areas of illegal content or behaviour.					
Fundamental rights (Art 34(1)(b))	*Examples:*[97] (a) human dignity; (b) freedom of expression and information, including media freedom and pluralism; (c) right to private life; (d) data protection; (e) right to non-discrimination; (f) rights of the child; (g) consumer protection; or (h) *any other* fundamental rights.					
Public security and elections (Art 34(1)(c))	*Exhaustive subcategories:*[98] (a) civic discourse; (b) electoral process; and (c) public security.					
Health and well-being (Art 34(1)(d))	*Exhaustive subcategories:*[99] (a) gender-based violence; (b) public health; (c) rights of Minors; (d) physical well-being; and (e) mental well-being.					

Risk Management Dialogue

- Regulatory dialogue put in place due to the opacity of the ecosystem & information asymmetry
- The regulator has no clear idea of risks, or contributing factors, and is in dark about solutions
- Forces providers to think about this, let themselves be reviewed by others (auditors, researchers, field NGOs), and then the regulator forms an opinion



Self-assess

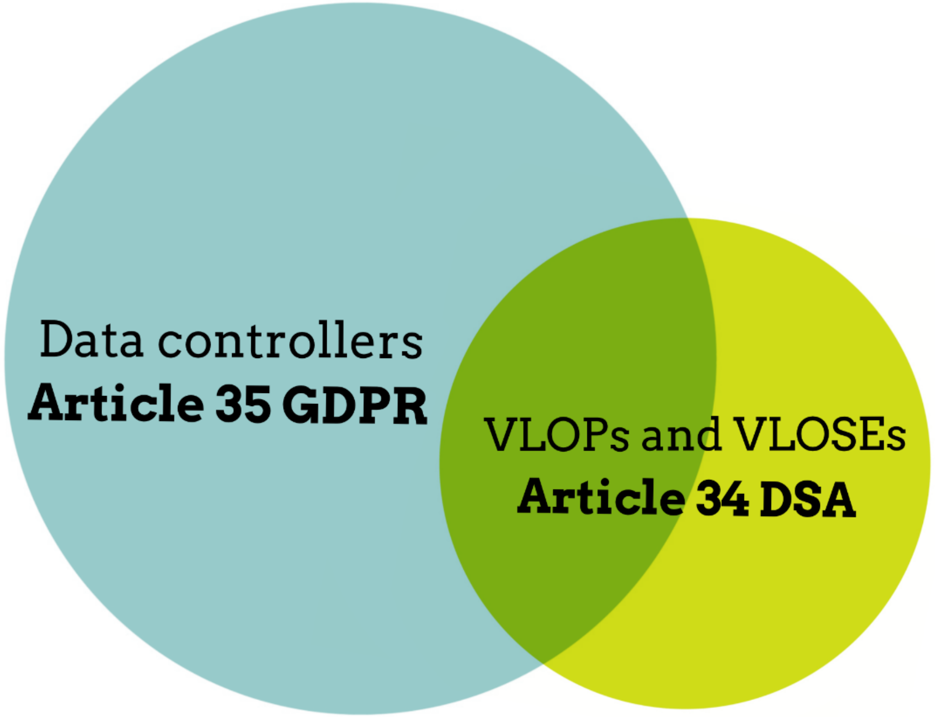
Act

Audit

Follow up

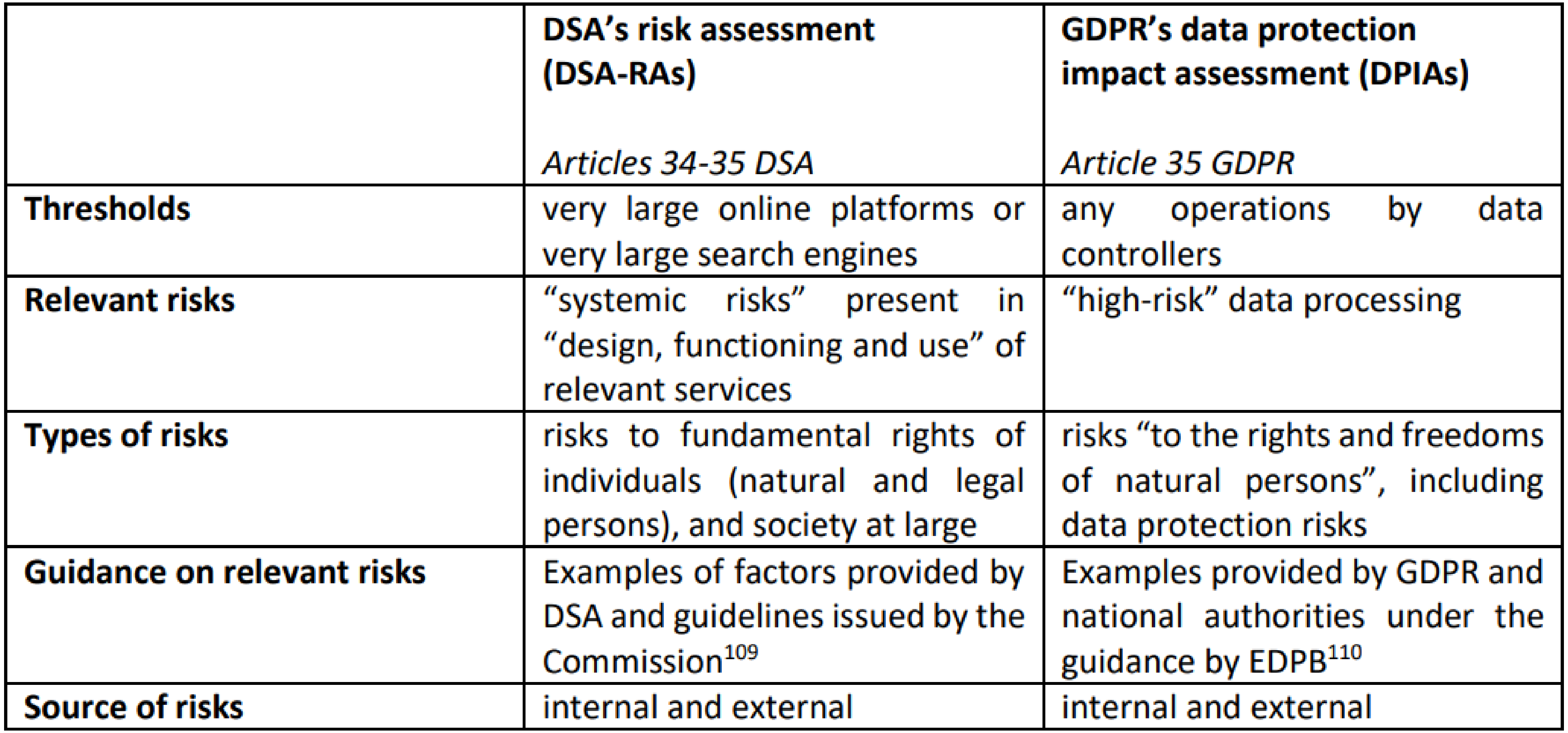
European Commission

DPIAs vs DSA-RAs


Data controllers
Article 35 GDPR

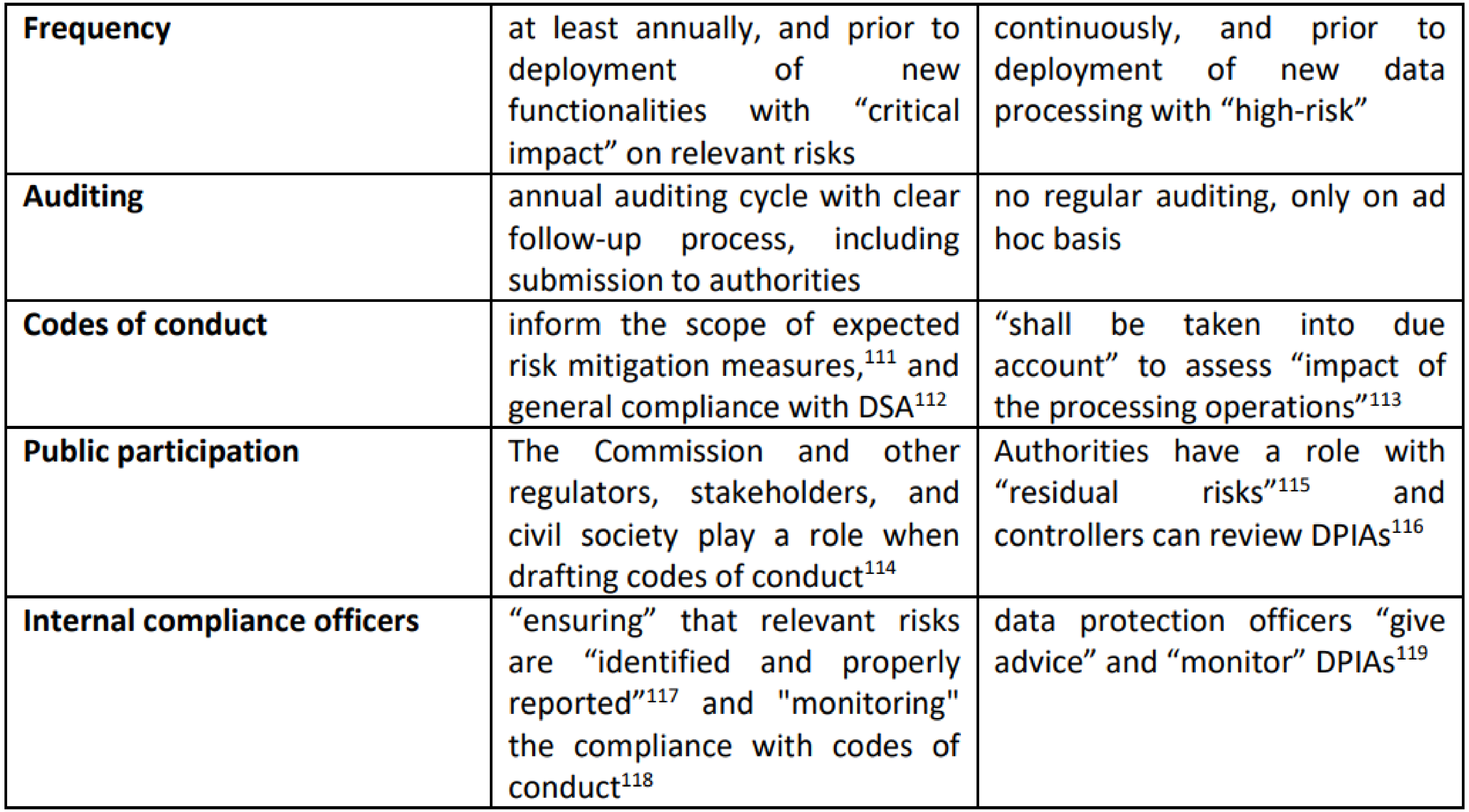
VLOPs and VLOSEs
Article 34 DSA

DPIAs vs DSA-RAs



	DSA's risk assessment (DSA-RAs) *Articles 34-35 DSA*	**GDPR's data protection impact assessment (DPIAs)** *Article 35 GDPR*
Thresholds	very large online platforms or very large search engines	any operations by data controllers
Relevant risks	"systemic risks" present in "design, functioning and use" of relevant services	"high-risk" data processing
Types of risks	risks to fundamental rights of individuals (natural and legal persons), and society at large	risks "to the rights and freedoms of natural persons", including data protection risks
Guidance on relevant risks	Examples of factors provided by DSA and guidelines issued by the Commission[109]	Examples provided by GDPR and national authorities under the guidance by EDPB[110]
Source of risks	internal and external	internal and external

DPIAs vs DSA-RAs

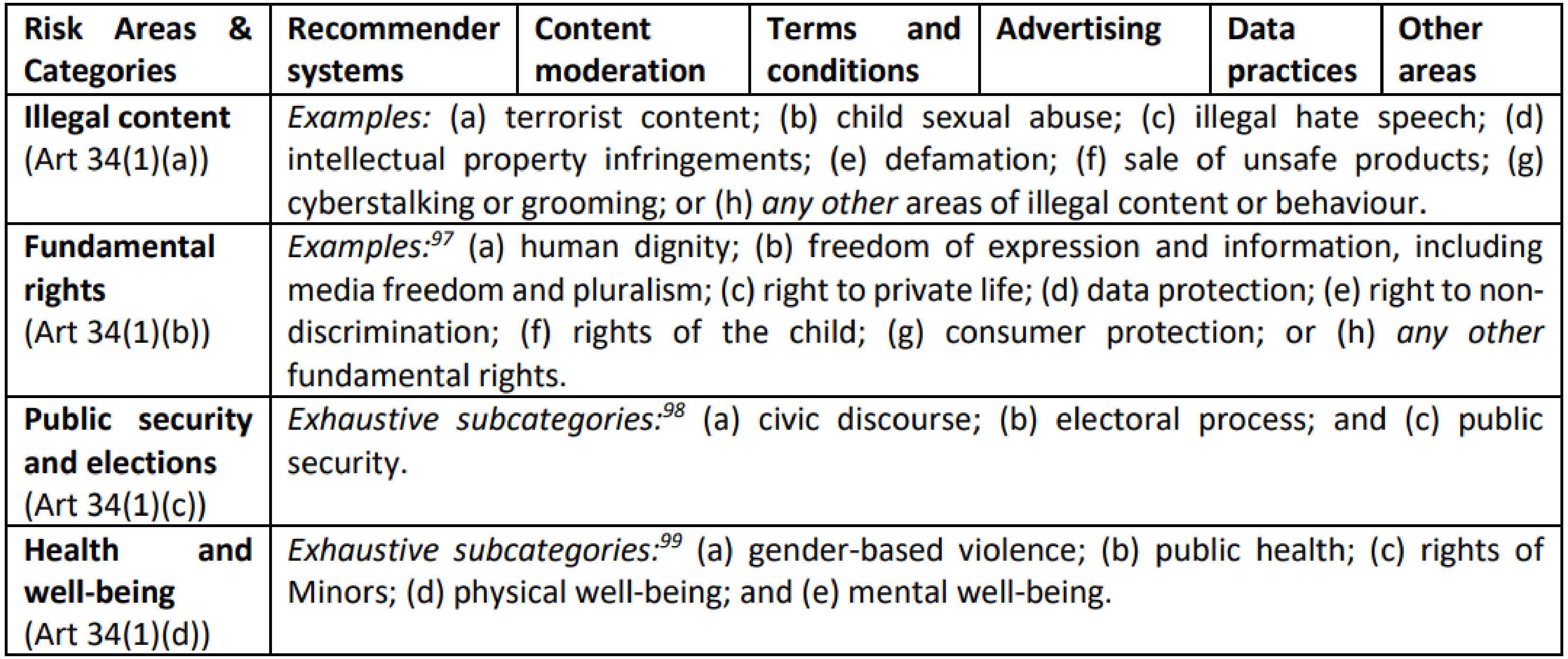


Frequency	at least annually, and prior to deployment of new functionalities with "critical impact" on relevant risks	continuously, and prior to deployment of new data processing with "high-risk"
Auditing	annual auditing cycle with clear follow-up process, including submission to authorities	no regular auditing, only on ad hoc basis
Codes of conduct	inform the scope of expected risk mitigation measures,[111] and general compliance with DSA[112]	"shall be taken into due account" to assess "impact of the processing operations"[113]
Public participation	The Commission and other regulators, stakeholders, and civil society play a role when drafting codes of conduct[114]	Authorities have a role with "residual risks"[115] and controllers can review DPIAs[116]
Internal compliance officers	"ensuring" that relevant risks are "identified and properly reported"[117] and "monitoring" the compliance with codes of conduct[118]	data protection officers "give advice" and "monitor" DPIAs[119]

Risks

- Hate speech & social media
- Fake products & online marketplaces
- Disinformation & encyclopaedias
- Self-harm content & social media
- Sexual violence & rental-marketplace services
- Fraud & app stores

VLOP’s risk mitigation



Risk Areas & Categories	**Recommender systems**	**Content moderation**	**Terms and conditions**	**Advertising**	**Data practices**	**Other areas**
Illegal content (Art 34(1)(a))	*Examples:* (a) terrorist content; (b) child sexual abuse; (c) illegal hate speech; (d) intellectual property infringements; (e) defamation; (f) sale of unsafe products; (g) cyberstalking or grooming; or (h) *any other* areas of illegal content or behaviour.					
Fundamental rights (Art 34(1)(b))	*Examples:*[97] (a) human dignity; (b) freedom of expression and information, including media freedom and pluralism; (c) right to private life; (d) data protection; (e) right to non-discrimination; (f) rights of the child; (g) consumer protection; or (h) *any other* fundamental rights.					
Public security and elections (Art 34(1)(c))	*Exhaustive subcategories:*[98] (a) civic discourse; (b) electoral process; and (c) public security.					
Health and well-being (Art 34(1)(d))	*Exhaustive subcategories:*[99] (a) gender-based violence; (b) public health; (c) rights of Minors; (d) physical well-being; and (e) mental well-being.					

Risks 1

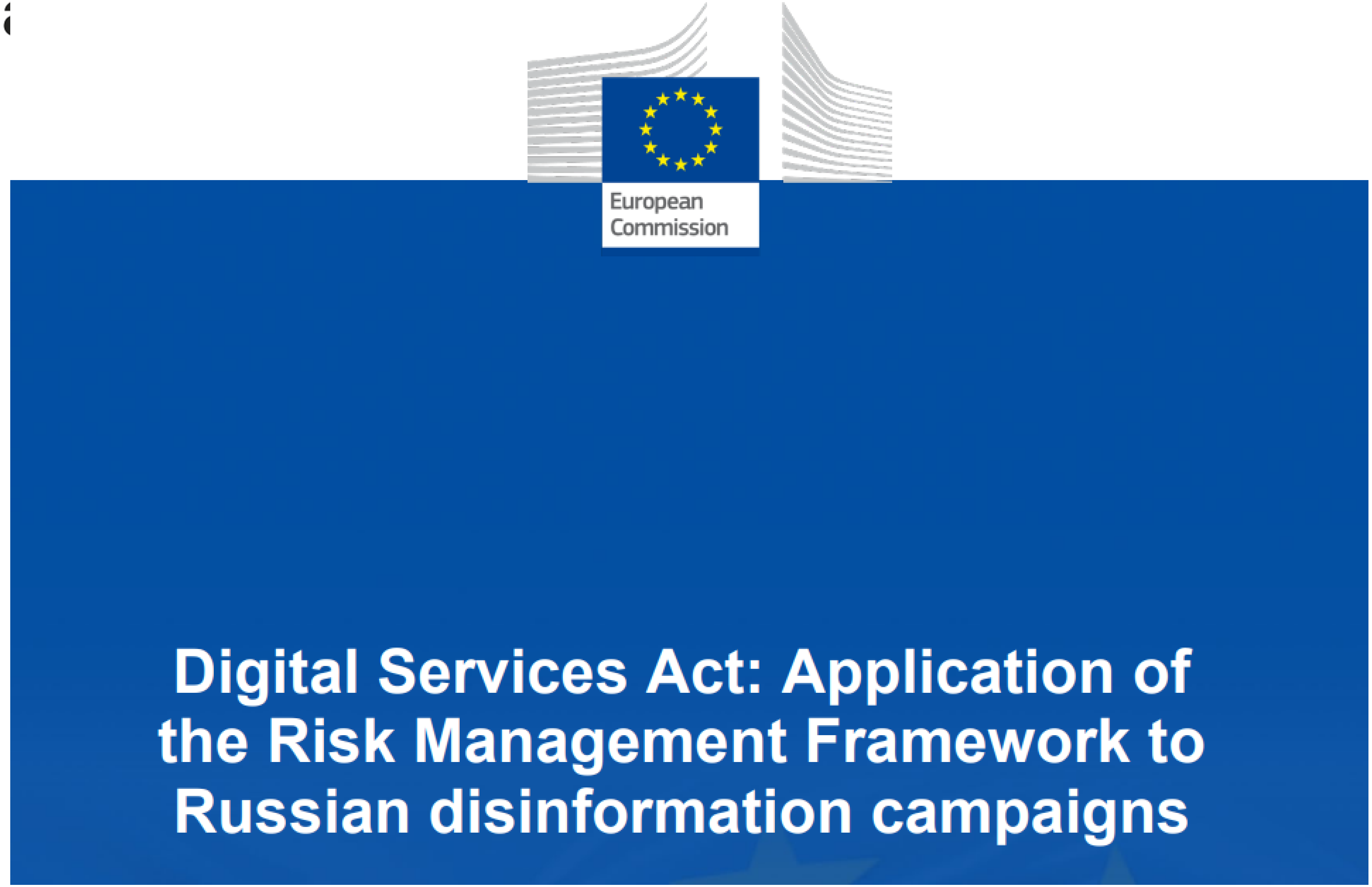
- Hate speech & social media (= Article 34(1)(**a**))
- Fake products & marketplaces (= Article 34(1)(a))
- Sexual violence & rental-marketplaces (= Article 34(1)(**a,d**))
- Fraud & app stores (= Article 34(1)(a))
- Disinformation & encyclopedias (= Article 34(1)(**c**))
- Self-harm content & social media (= Article 34(1)(**b**,**d**))

Risks 2

- Safety of journalists & social media (=Article 34(1)(**a,b,c,d**)
- Over-blocking & social media (=Article 34(1)(**b,c**)
- Stalking & platforms (=Article 34(1)(**a,b,d**)
- Consumer fraud & maps (=Article 34(1)(**a,b,d**)
  - See this nice paper.

Likely to compartmentalise

- Inevitable that risks must be divided into parts
- E.g. risks to objectives (financial s.) > RTO aggregated
  - E.g. financial crime / consumer understanding, etc.
- Potentially: Art 34(1)(a)-(d) + stakeholders + risk profile
  - Depends also on the scope (“systemic” vs “mitigation”)
- Tricky: over-blocking risks (FoE)



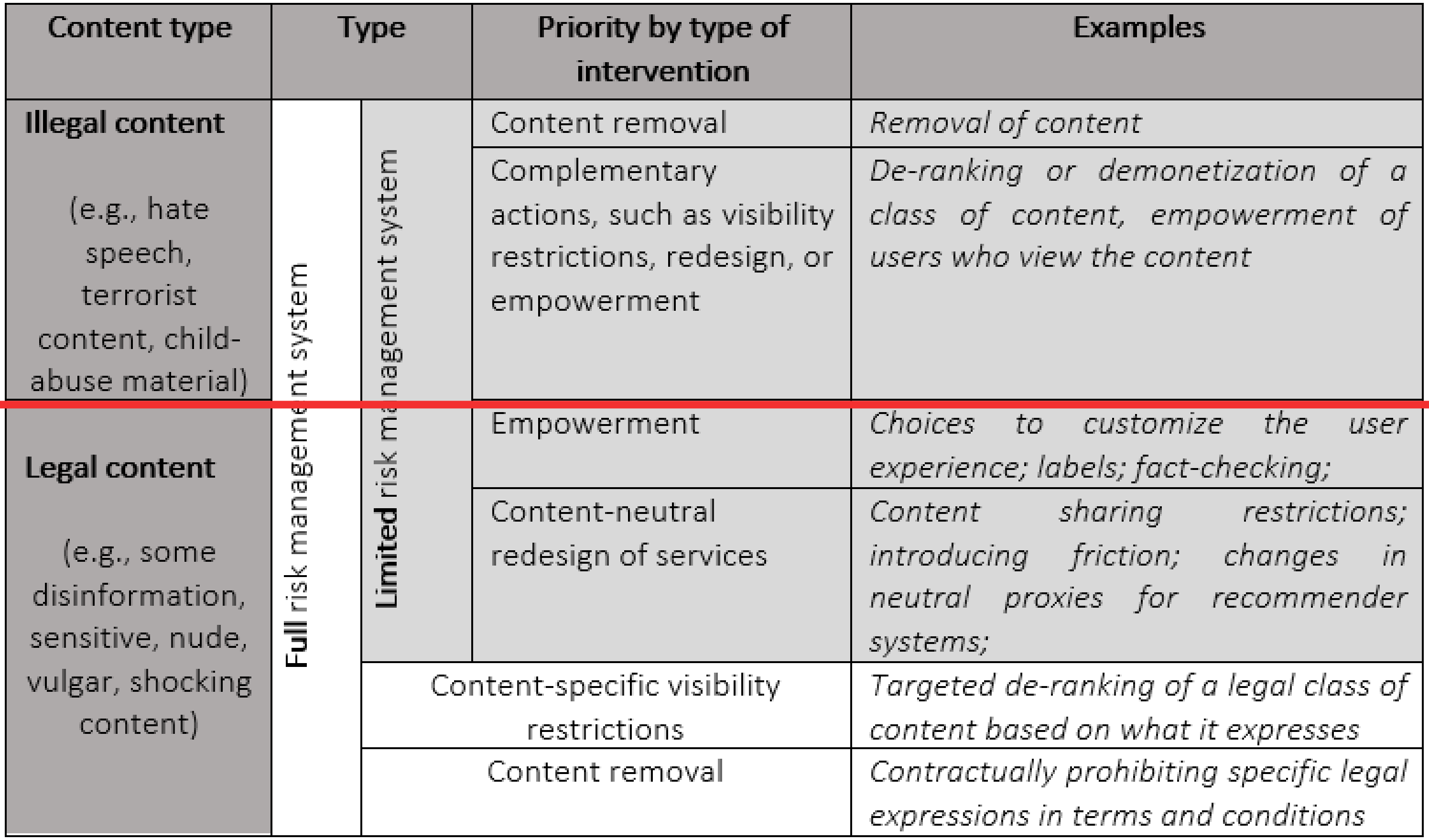
European Commission

Digital Services Act: Application of the Risk Management Framework to Russian disinformation campaigns

Risk analysis vs mitigation

- Analysis is very broad (legal + illegal)
  - “diligently identify, analyse and assess **any** systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services”
- Mitigation is more limited (depends)
  - “shall put in place reasonable, **proportionate** and effective mitigation measures, tailored to the specific systemic risks identified pursuant to Article 34, with particular consideration to the impacts of such measures on fundamental rights”

Risk Mitigation Measures



Content type	Type		Priority by type of intervention	Examples
Illegal content (e.g., hate speech, terrorist content, child-abuse material)	**Full** risk management system	**Limited** risk management system	Content removal	*Removal of content*
			Complementary actions, such as visibility restrictions, redesign, or empowerment	*De-ranking or demonetization of a class of content, empowerment of users who view the content*
Legal content (e.g., some disinformation, sensitive, nude, vulgar, shocking content)			Empowerment	*Choices to customize the user experience; labels; fact-checking;*
			Content-neutral redesign of services	*Content sharing restrictions; introducing friction; changes in neutral proxies for recommender systems;*
			Content-specific visibility restrictions	*Targeted de-ranking of a legal class of content based on what it expresses*
			Content removal	*Contractually prohibiting specific legal expressions in terms and conditions*

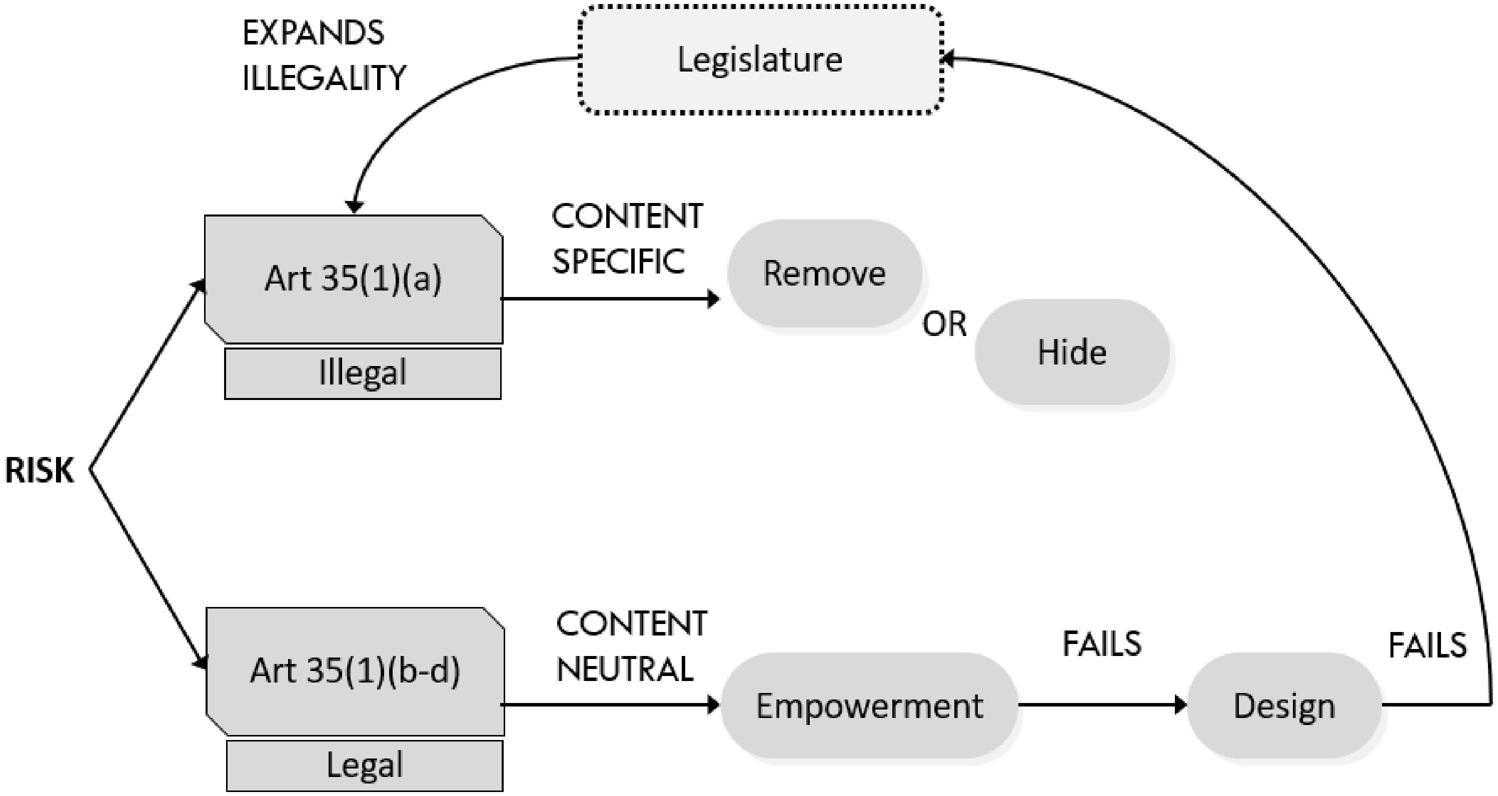
Categorisation will IMO matter

- For counter-measures: Article 34(1)(**a**) allows the most because the legislatures banned the content/practice
- If a **risk is not made illegal**, the regulator has some limited space to ask for measures due to rule of law.
  - In some cases, Ps are happy to go beyond illegal = e.g., spam
  - In other cases, this can be controversial = e.g. self-harm, disinfo
  - Or be against the business model = toxicity of over-use

A restriction “prescribed by the law”?

- Could Article 34 serve as a basis for an obligation to prohibit a class of content for everyone?
  - E.g., prohibit all information about a diet that harms people
  - IMO: no, unless there is a specific legislation
  - E.g., de-rank all information with pro-Kremlin narratives
  - IMO: no, unless there is a specific legislation
  - BUT: content-neutral: super-users; authentication; interface;

Risk Mitigation Measures



EXPANDS ILLEGALITY

Legislature

Art 35(1)(a)

Illegal

CONTENT SPECIFIC

Remove

OR

Hide

RISK

Art 35(1)(b-d)

Legal

CONTENT NEUTRAL

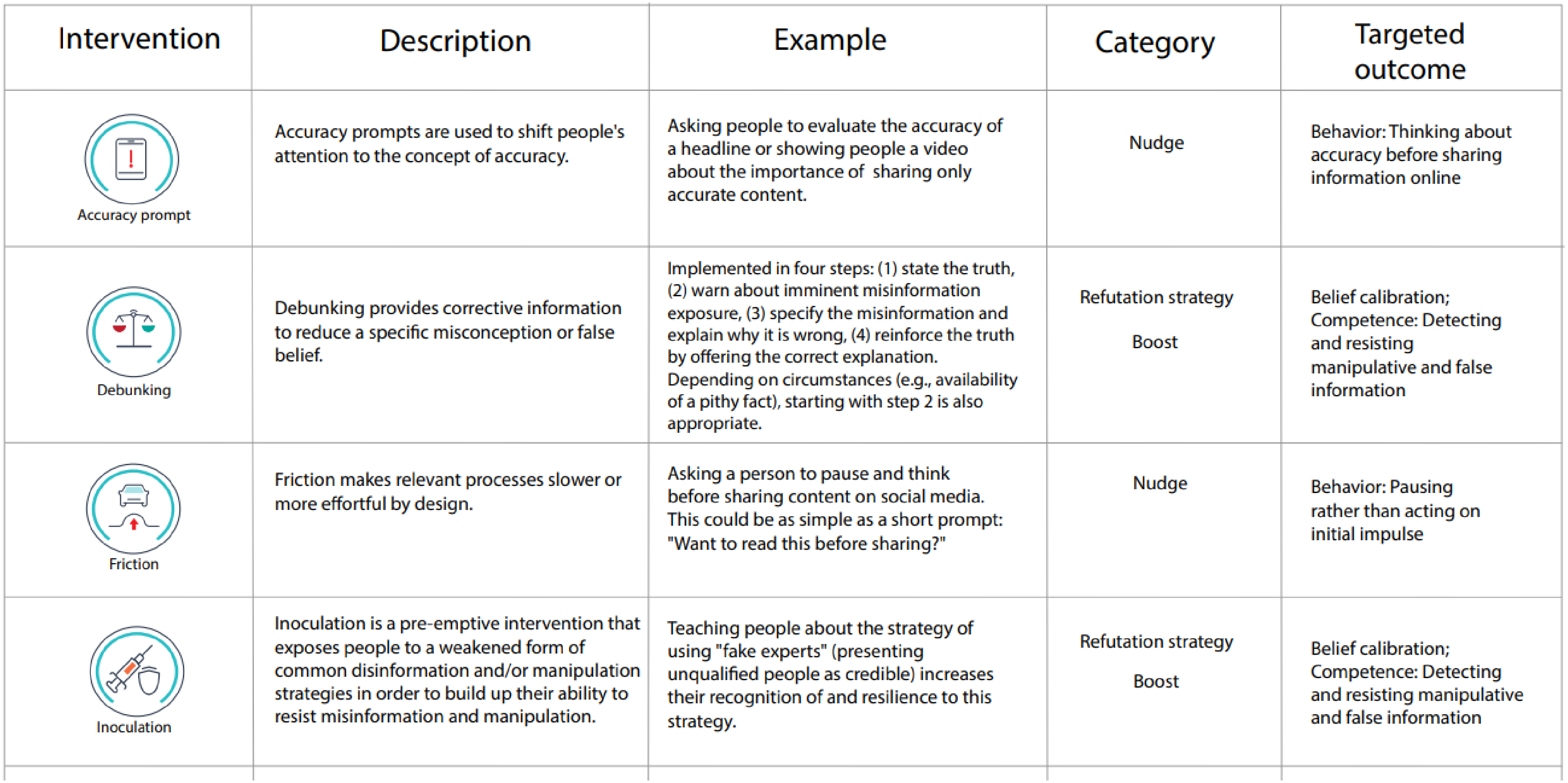
Empowerment

FAILS

Design

FAILS

Disinformation toolkit (Kozyreva et all (2022))



Intervention	Description	Example	Category	Targeted outcome
Accuracy prompt	Accuracy prompts are used to shift people's attention to the concept of accuracy.	Asking people to evaluate the accuracy of a headline or showing people a video about the importance of sharing only accurate content.	Nudge	Behavior: Thinking about accuracy before sharing information online
Debunking	Debunking provides corrective information to reduce a specific misconception or false belief.	Implemented in four steps: (1) state the truth, (2) warn about imminent misinformation exposure, (3) specify the misinformation and explain why it is wrong, (4) reinforce the truth by offering the correct explanation. Depending on circumstances (e.g., availability of a pithy fact), starting with step 2 is also appropriate.	Refutation strategy Boost	Belief calibration; Competence: Detecting and resisting manipulative and false information
Friction	Friction makes relevant processes slower or more effortful by design.	Asking a person to pause and think before sharing content on social media. This could be as simple as a short prompt: "Want to read this before sharing?"	Nudge	Behavior: Pausing rather than acting on initial impulse
Inoculation	Inoculation is a pre-emptive intervention that exposes people to a weakened form of common disinformation and/or manipulation strategies in order to build up their ability to resist misinformation and manipulation.	Teaching people about the strategy of using "fake experts" (presenting unqualified people as credible) increases their recognition of and resilience to this strategy.	Refutation strategy Boost	Belief calibration; Competence: Detecting and resisting manipulative and false information

Risk mitigation vs P’s rule-making power

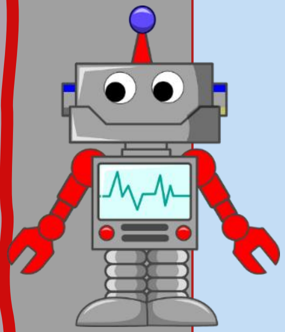
- Article 14(4) is one limit: grossly disproportionate
- Article 34 could be another: but IMO only if it can invoke legislation as a statutory basis for an action
    - Beyond illegality mandate, cannot rewrite illegality
    - But demarcation with conduct prohibitions (e.g., age-gating de facto prohibits the display of content X for children)
- P’s can go beyond but cannot be forced by COM

Counter-risk: Over-blocking

- Blocking lawful content due to fears of liability
- Ps can decide to contractually constrain the platform
- Over-blocking is about unintentional collateral effects due to low investment in technology, staff or processes
  - Use of copyright filters and their accuracy
  - Use of child abuse filters and their accuracy

LSE Department of Law

For instance: DSA vs Article 17 CDSMD = audits!

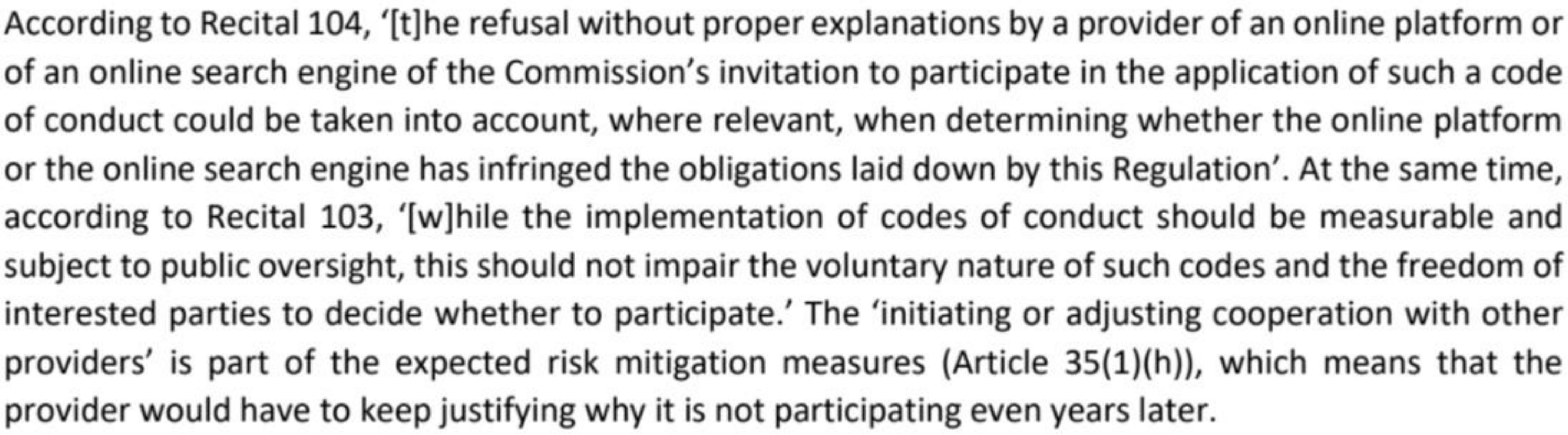


Level 1	Level 2	Level 3	Level 4	
Notification by RHs (Art 16 DSA)	Assessment and decision (Art 17 DSA)	Internal contestation by users (Art 20 DSA)	External contestation by users (Art 21 DSA)	Transparency
Submission of reference data by RHs (Art 17(4)(b))	Automated assessment and decision (Art 17(4)(b))	DSA implements CDSMD (Art 20 DSA)	DSA implements CDSMD (Art 21 DSA)	DSA implements

Codes of Conduct

- Not binding directly (EC cannot find incompliance)
- But participation is quasi-obligatory
- Content creates prima facie evidence of best practices
- DSA Officers have to monitor compliance
- Part of auditing

Codes of Conduct



According to Recital 104, '[t]he refusal without proper explanations by a provider of an online platform or of an online search engine of the Commission's invitation to participate in the application of such a code of conduct could be taken into account, where relevant, when determining whether the online platform or the online search engine has infringed the obligations laid down by this Regulation'. At the same time, according to Recital 103, '[w]hile the implementation of codes of conduct should be measurable and subject to public oversight, this should not impair the voluntary nature of such codes and the freedom of interested parties to decide whether to participate.' The 'initiating or adjusting cooperation with other providers' is part of the expected risk mitigation measures (Article 35(1)(h)), which means that the provider would have to keep justifying why it is not participating even years later.

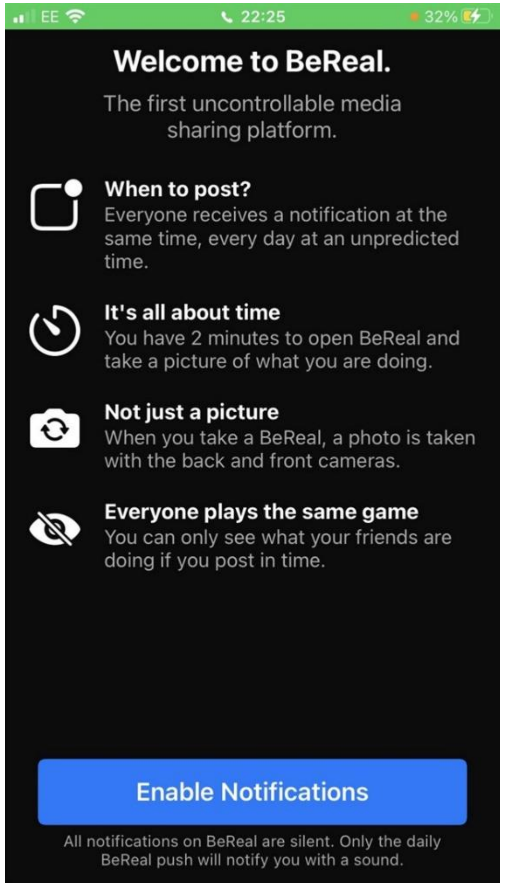
LSE Department of Law

Risk allocation in the ecosystem

- What *precautions* do we expect from the platforms?
  - IF we expect that they solve everything, it invites carelessness
  - DSA cannot eradicate the risks
- What *precautions* do we expect from victims, and their guardians?
  - Need to avoid moral hazard
- What *precautions* do we expect from others?
  - Civil society, authorities, schools, friends, etc.

Peer-pressure & children

- Can providers be tasked to entirely solve the problem of peer pressure among children?
- How much responsibility is left with parents, and others?



Welcome to BeReal.

The first uncontrollable media sharing platform.

When to post?
Everyone receives a notification at the same time, every day at an unpredicted time.

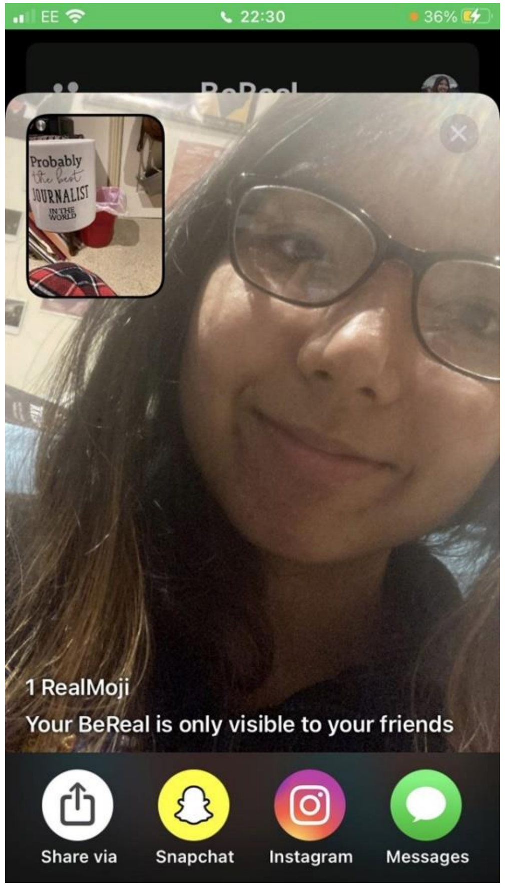
It's all about time
You have 2 minutes to open BeReal and take a picture of what you are doing.

Not just a picture
When you take a BeReal, a photo is taken with the back and front cameras.

Everyone plays the same game
You can only see what your friends are doing if you post in time.

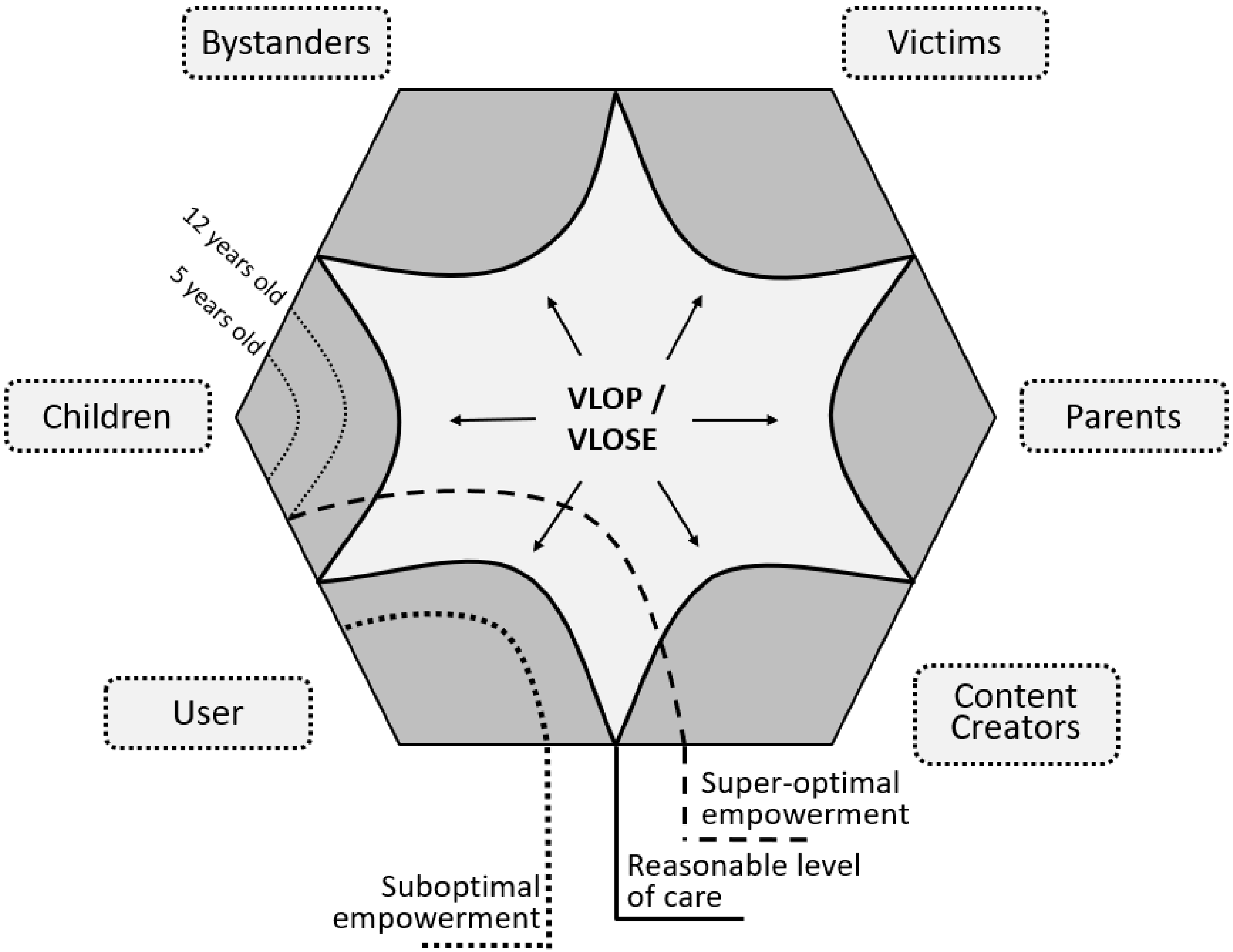
Enable Notifications

All notifications on BeReal are silent. Only the daily BeReal push will notify you with a sound.

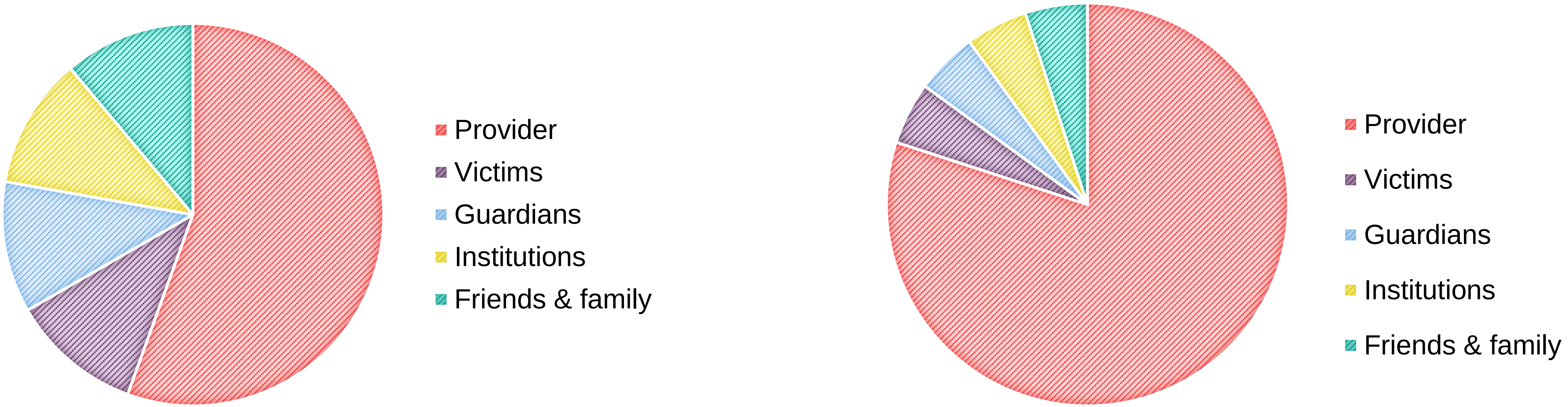


Your BeReal is only visible to your friends

DRAFT


Bystanders
Victims
12 years old
5 years old
Children
VLOP /
VLOSE
Parents
User
Content
Creators
Super-optimal
empowerment
Reasonable level
of care
Suboptimal
empowerment

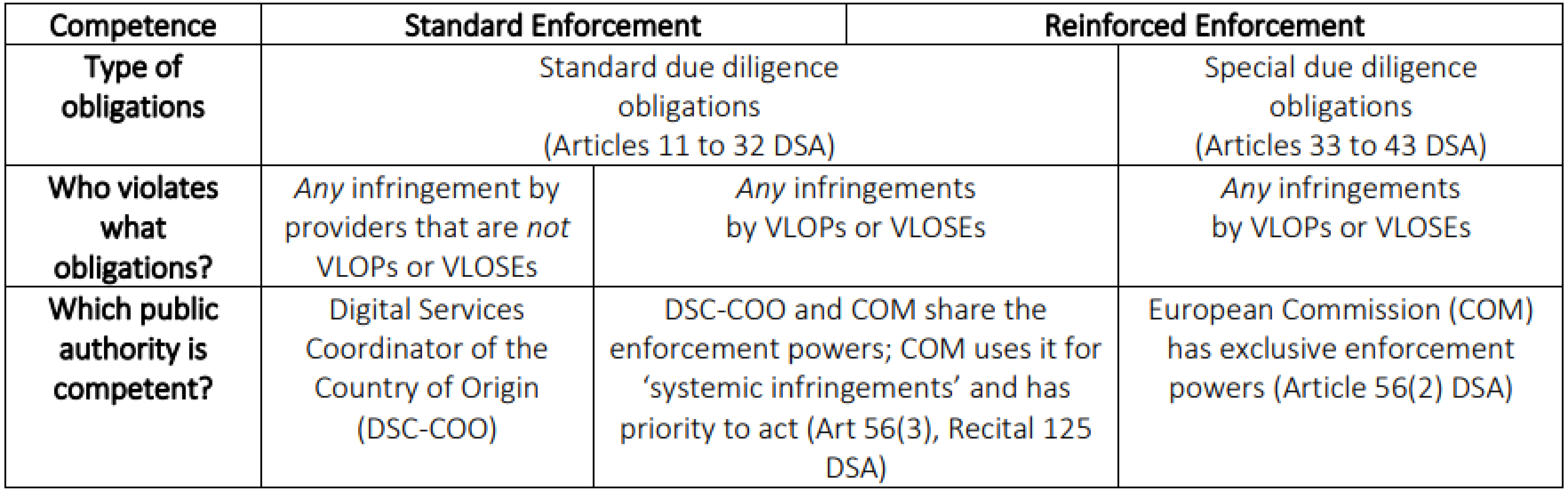
Risk allocation (Over-protective vs Protective)



Enforcement

Department of
Law

Who enforces?



Competence	Standard Enforcement	Reinforced Enforcement	
Type of obligations	Standard due diligence obligations (Articles 11 to 32 DSA)		Special due diligence obligations (Articles 33 to 43 DSA)
Who violates what obligations?	*Any* infringement by providers that are *not* VLOPs or VLOSEs	*Any* infringements by VLOPs or VLOSEs	*Any* infringements by VLOPs or VLOSEs
Which public authority is competent?	Digital Services Coordinator of the Country of Origin (DSC-COO)	DSC-COO and COM share the enforcement powers; COM uses it for 'systemic infringements' and has priority to act (Art 56(3), Recital 125 DSA)	European Commission (COM) has exclusive enforcement powers (Article 56(2) DSA)

COM: Examples

- TikTok’s inaction to protect users against manipulation by a foreign government (e.g, China) is an exclusive COM competence because it relies on a risk mitigation obligation
  - Special obligations
- TikTok’s failure to issue transparency reports can be within shared competence if systemic (COM & DSCs)
  - Standard due diligence obligations for Ops
  - For instance: affects more MS than one; or recurring.

COM

- Can act on its own initiative and has priority
- Article 66(2): “The Digital Services Coordinators shall, without undue delay after being informed of initiation of the proceedings, transmit to the Commission any information they hold about the infringement at stake. The initiation of proceedings pursuant to paragraph 1 of this Article by the Commission shall **relieve** the Digital Services Coordinator, or any competent authority where applicable, of its powers to supervise and enforce provided for in this Regulation pursuant to Article 56(4).”

DSC: Examples

- TikTok’s first-reported failure to issue an explanation to some journalists upon suspension of their accounts
- BUT: if re-curing, COM can step in (Article 56(3)); DSCs can even ask the COM to assess the matter (Article 65(2))
- Three DSCs can push the DSC of the establishment to review cases (Article 58(2)); if they fail, COM can step in within referral (Article 59) and ask DSC-EST to act.

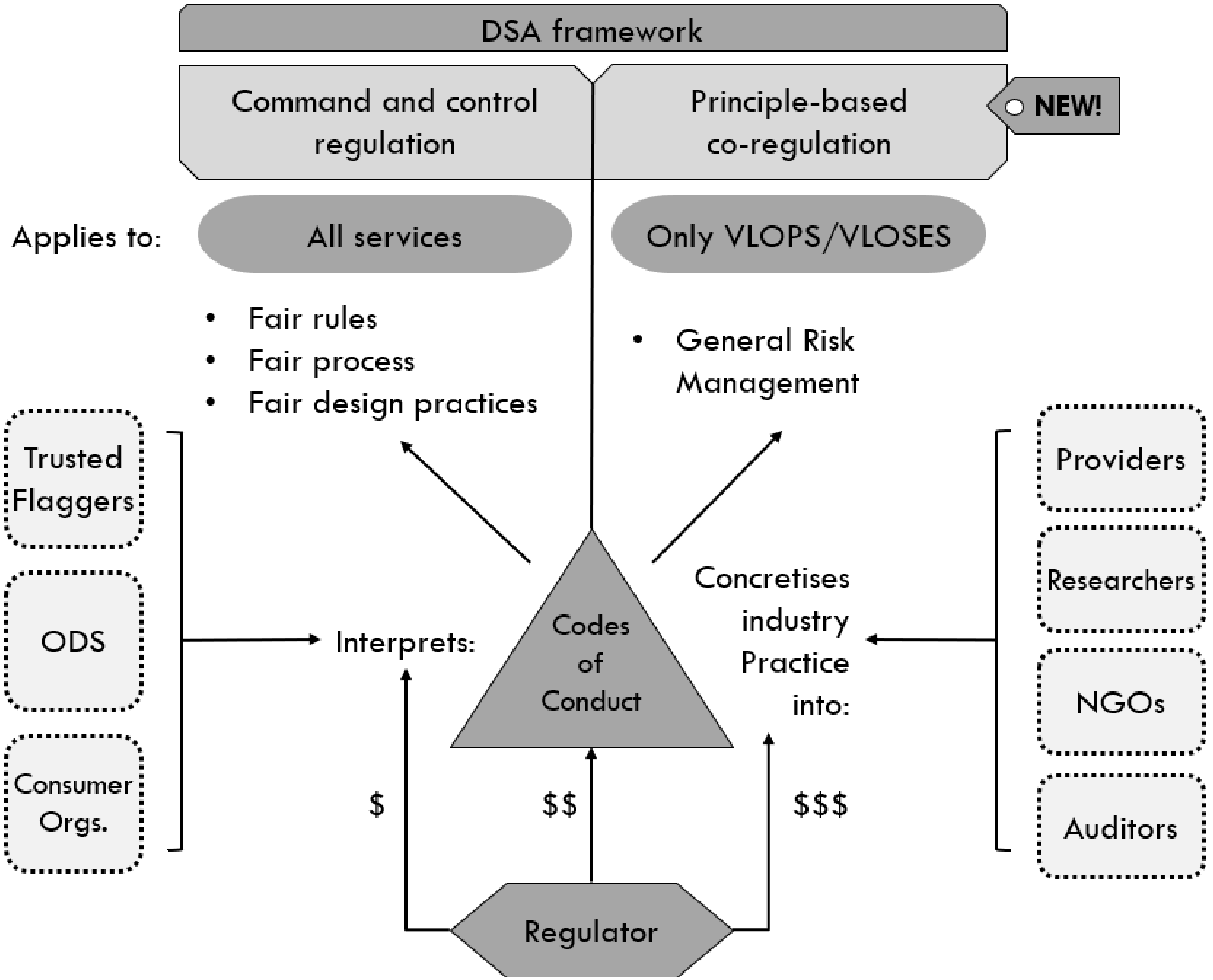
Systemic vs Non-systemic

Recital 125 explains Article 56(3): “On the other hand, the competent authorities in the Member State where the main establishment of a provider of very large online platform or of very large online search engine is located could be better placed to address individual infringements committed by those providers, that **do not raise any systemic or cross-border issues**. In the interest of efficiency, to avoid duplication and to ensure compliance with the principle of ne bis in idem, it should be for the Commission to assess whether it deems it appropriate to exercise those shared competences in a given case and, once it has initiated proceedings, Member States should no longer have the ability to do so.”

LSE Department of Law

DRAFT

- Cost of Enforcement
- Prescriptive vs Other rules



lse.ac.uk/law
@LSELaw

Private enforcement

- The DSA’s focus is on public enforcement.
- Its entire Chapter IV deals with enforcement by national public authorities and the European Commission.
- There is very little in the DSA about private enforcement by impacted companies and individuals. By private enforcement, we refer to legal means of privates to defend their rights or claim damages in courts when those rights are violated.

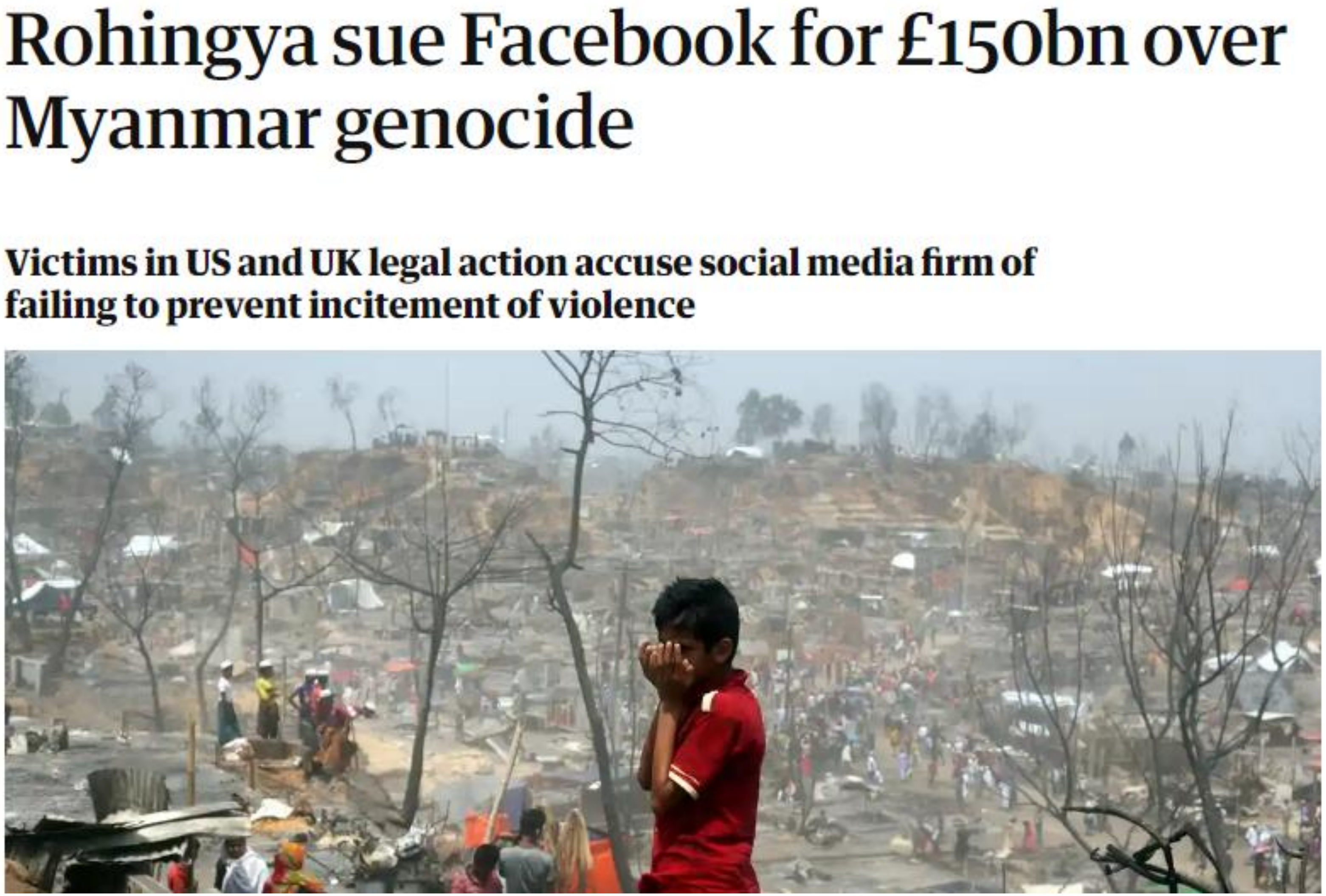
Does DSA (Chapter 3) create rights?

- The conferral of rights by the DSA?
- Argument PRO: often specificity of obligations & to whom they are owed; directly applicable
  - Article 86 speaks of “exercise the rights conferred by this Regulation”
  - Article 54 (“Recipients of the service shall have the right to seek, in accordance with Union and national law, compensation from providers of intermediary services, in respect of any damage or loss suffered due to an infringement by those providers of their obligations under this Regulation.”)
- Argument AGAINST: formulation of regulatory expectations for public enforcement = strong case for some obligations

My view (likely majority view)

- Most of the due diligence obligations are capable of conferring rights on individuals
  - Explanation, transparency, appeal, access to interfaces, etc.
- But some are of regulatory nature where no specific content is clear before the regulator gets involved
  - Risk mitigation under Article 34; maybe Article 28?
  - Only after the COM exercises its powers and concretises the content

Even if you can argue damages in the EU, still COM would have to conclude violation of the DSA first.



Rohingya sue Facebook for £150bn over Myanmar genocide

Victims in US and UK legal action accuse social media firm of failing to prevent incitement of violence

Some examples

- A failure to design fair content moderation rules (Article 14)
- A failure to issue a statement of reasons (Article 17)
- A failure to reinstate the content following a successful complaint (Article 20)
- A failure to suspend abusive notifiers or users (Article 23)
- A failure to issue reports concerning content moderation (Article 15)
- A failure to protect against dark patterns (Article 25)
- A failure to comply with advertising obligations (Article 26)
- A failure to allow traders to comply with their information obligations (Article 31)

LSE Department of Law

Main vehicle for enforcement: contracts

- Recipients (consumers, businesses) are usually in a contractual relationship with providers
  - Sometimes not: websites listed in search results; user of net;
- DSA informs the content of their mutual rights as mandatory law that cannot be contracted away
- Thus, contractual remedies can be used to enforce

LSE Department of Law

Example: Influencers

- Video-sharing platform and influencer are in a contractual relationship.
- The DSA's due process provision that regulates content moderation will modify the rights of content creators against rights termination, reinstatement, explanation, remedies to such decisions, and arrangements about the publicity of those decisions.
- For instance, an influencer whose content is demonetised can claim explanations, and have them reviewed internally by the company. If the provider fails to do so, the influencer can seek damages, and reinstatement of the content.

LSE Department of Law

Damages are not automatic (Art 54)

- Any violation of individual rights derived from the DSA will have to be reviewed against national law that grants such remedies.
- Very often, such laws will require the existence of damage, and a causal link, to trigger compensation. Mere violation is unlikely to be enough (e.g., transparency disclosures)
- Thus, a failure to comply with the DSA might violate the rights of several affected individuals at once, but not necessarily lead to an obligation of providers to compensate all or even most of them.

Injunctions

- Article 90 only mentions injunctions for consumer organisations
- How about individual injunctions?
  - No expressly provided
  - Arguably, implicitly required by the DSA too
    - They are less than damages
    - Effectiveness argument