Slippery arguments: how the EDPB's positions on smart glasses could affect smartphones and more

by Peter Craddock

The smart glasses debate has brought to the fore reactionary views that have been prevalent throughout history, at least since the portable camera was invented. In my previous deep dive *("Blinded by the LED: smart glasses, GDPR, and the illusion of hardware indicators")*, I highlighted the fact that the same arguments being made today about covert surveillance through smart glasses were made in 1890, after the launch of the Kodak portable camera, and that similar arguments were also made more recently regarding drone photography, camera phones, portable cassette recorders and more.

The European Data Protection Board's Statement 1/2026 of the EDPB on smart glasses is nothing different.

For instance, the following passage is a description of audio recording functions on portable recording devices since the days of cassette players, and also describes recording apps that ship by default on smartphones: *"Unlike many other recording devices, they allow a near invisible or hidden collection, storage, and other forms of processing of personal data […] Therefore, they can facilitate the non-authorised recording of data subjects. In addition, some […] may have advanced microphones, which can record background conversations to which the user is not participating"*[1].

Similarly: *"Even if the device could be identifiable as [a recording device], individuals may still oppose being filmed or recorded, including because they are uncomfortable with the possibility of this taking place. This could also result in a subtle social effect, where individuals alter their behaviour, suppress spontaneity, and conform to social norms perceived to be more socially acceptable due to their perceived threat of unvetted surveillance"*[2]. This fear of surveillance has been voiced since 1890 and is hardly new to smart glasses.

Just because the fear is old, does not mean it is wholly unfounded or entirely without merit. As argued in my previous piece, the real issue is **misuse of technology, not the existence of the technology itself**.

Yet the EDPB's framing of smart glasses as particularly problematic – just like the statements of the Dutch DPA and Hamburg DPA beforehand – is the actual problem. They make smart glasses appear unlawful based on oversimplifications, without properly explaining how their reasoning should be specific to smart glasses.

Table of contents:

I. Oversimplifications get us nowhere 2

II. GDPR and legal obligations applicable to users 4

II.1. GDPR (in)applicability, household exemption, and private use in public spaces 5

II.2. Inapplicability of the GDPR to the user can limit its applicability to the provider too 6

II.3. Does public sharing introduce a risk of indirect application of the GDPR? 7

[1] EDPB Smart Glasses Statement, para. 7.

[2] EDPB Smart Glasses Statement, para. 8.

II.4. Where the GDPR applies: limited impact on users 7
II.5. Smart glasses? Smartphones? Digital recorders? Drones? Same GDPR framework 8
II.6. What about joint controllership between the user and the provider? 9
II.7. AI training as provider-only processing, not provider & user joint controllership 10
III. Other relevant legal frameworks for users 12
III.1. Image rights, or the right of personal portrayal 12
III.2. Criminal law restrictions 13
A) Voyeurism 13
B) Covert recording 14
C) Harassment and stalking 14
D) Troubles à l'ordre public 14
IV. Sharing and publication as real trigger, and "ask before sharing" 14
V. What about facial recognition? Or social acceptability? 16
VI. Conclusion and policy recommendations 17

I. Oversimplifications get us nowhere

"Filming of others is almost always prohibited", said the Dutch DPA (in the title of its article, no less), because *"[p]eople should be able to walk the streets freely without having to worry that someone is filming them without their knowledge and then sharing the footage or posting it online"*. It is strange that such a statement made it to publication, more than 20 years after social media usage became widespread. Moreover, recording and publication are different actions and follow different rules (and which are sometimes carried out through different devices), and they are carried out at a user's direction.

The Hamburg DPA's 53-page report may seem at first glance like a more serious analysis, the actual legal analysis is more limited and makes a number of assumptions about identifiability – without which the GDPR is inapplicable. (For instance, it states that *"The human voice is personal data"* – without even explaining the circumstances in which a voice recording makes an individual identifiable and from whose perspective, despite identifiability being a core condition for information to constitute "personal data" under data protection rules.)

As for the EDPB's "statement" itself, it is first worth asking oneself what the statement actually means.

The EDPB's core task – to *"ensure the consistent application of [the GDPR]"* – is described as taking various forms, including by *"examin[ing], on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of [the GDPR] and issu[ing] guidelines, recommendations and best practices in order to encourage consistent application of [the GDPR]"*[3].

This "statement" does little to foster consistent application of the GDPR across recording technologies. In the past, the EDPB has used statements to make comments on legislative initiatives or geopolitical developments.

[3] Art. 70(1)(e) GDPR.

One such statement was the Helsinki Statement on enhanced clarity, support and engagement (2 July 2025), in which it wrote the following:

> *"Across its efforts, the EDPB will strengthen its dialogue with stakeholders, holding proactive and early engagement to identify specific areas where further support and clarification is required, and providing the opportunity for stakeholders to flag possible inconsistencies and give feedback. The EDPB will publicly report on the main outcomes of public consultations."*

Yet based on what I have heard from a range of relevant stakeholders (from producers, technology companies, consultancy and academia), the statement on smart glasses does not appear to have involved any "proactive and early engagement", let alone a "dialogue with stakeholders". There was moreover no public consultation or any event organised by the EDPB to obtain feedback. Such a dialogue would have been critical, considering what the EDPB writes in that statement:

- The concerns raised in the quotes highlighted are not specific to smart glasses, and so their appearance in a statement *on smart glasses* specifically raises eyebrows. The statement does not explain how those criticisms are objectively different compared to those relating to other recording technologies, or why the legal implications should be different.

- The statement assumes that all information is personal data, without even bringing up the question of identifiability. Yet (i) the use of optical sensors in smart glasses to assist in navigation (which is nevertheless mentioned) is not at all the same as filming for the purposes of publication in terms of the potential for identification, and (ii) identifiability depends on the person or entity being examined (as recent case law has shown). Failing to even acknowledge the identifiability issue is unfortunate.

- The EDPB states that providers/producers can be "independent or joint controllers" notably when "the provider of the AI functionalities of the smart glasses processes personal data in order to provide the user with an answer about its surroundings, for example by analysing an image from the glasses' camera feed in which other persons appear" – without examining (i) identifiability, (ii) which images are actually those that enable the AI functionalities to work (and whether they are different from the users' recordings), (iii) why that provider should not be viewed as a processor for the user, (iv) which (if any) purposes and means could be viewed as "jointly" determined for AI functionality and (v) how obligations should be met. Instead, it just leaves open questions as to whether compliance is even possible. Moreover, participation in one operation cannot make an actor controller of an earlier or a later one, because **joint controllership is confined to the stage of joint determination**. *[see further on what exactly can be covered by joint controllership – and what cannot]*

In other words, by using assumptions (i.e. shortcuts in legal reasoning), the EDPB's statement is **misleading** and **risks creating more legal uncertainty, not less**.

After all, where is the difference truly between video/audio capturing on smartphones today and smart glasses? And if the focus is surreptitious filming, which concerns arise specifically in relation to smart glasses and how do they objectively differ from other devices with cameras (smartphones, nanny cams, dashcams, drones, etc.)? Shouldn't cameras and audio recording capabilities of smartphones be banned to limit the risk of such privacy incursions?

Yet the recording capabilities of smartphones and other devices are widely known, and even immortalised in high-profile films (see e.g. *The Devil Wears Prada 2* [recording of a restructuring plan],

Knives Out [confession over a live call with a detective]). *[Regarding identifiability: in all of those cases, those examining the recording knew the subjects – who were therefore identified from their perspective.]*

Given the EDPB's task of ensuring a "consistent" application of the GDPR, it should therefore ensure that its positions do not create inconsistencies between (i) the way in which existing technologies are used and such use is permitted and (ii) the way in which they wish to regulate new technologies triggering similar questions. **Where there are similarities, the legal assessment should be similar. Only the objective factual differences can potentially lead to objective differences in legal assessment.**

In this context, perhaps the user is the one whose compliance is worth examining more carefully, to look at how smartphone and audio recording capability use can be reconciled with the GDPR and other laws – and then to look at how smart glasses differ. If the law in general (GDPR or otherwise) already regulates users' behaviour and tackles misuse, perhaps there is no need to foresee anything different for smart glasses.

II. GDPR and legal obligations applicable to users

Smart glasses, just like smartphones, pocket recording devices etc, are **dual-use devices**, not covert surveillance equipment. While some data protection authorities have claimed – beyond the scope of their own competence – that they are covert surveillance equipment, no authority with that topic within its remit appears to have claimed that to be the case, quite the opposite.

[For a more detailed analysis of the question, including how I reached this conclusion and a look at a specific German law on the issue, read "Blinded by the LED: smart glasses, GDPR, and the illusion of hardware indicators".]

This means that **distribution & sale restrictions applicable to covert surveillance equipment do not apply to smart glasses**. But just because covert use isn't the intent, does not remove the *possibility* of someone attempting to use them in that manner – and this is where **user responsibility** comes into play.

The same observation can be made in relation to the fear mentioned by the Dutch DPA: "*[p]eople should be able to walk the streets freely without having to worry that someone is filming them without their knowledge and then sharing the footage or posting it online*". To date, it does not appear that any provider of smart glasses is going around filming people in the EU without their knowledge and then sharing the footage or posting it online – that's possible *user* behaviour, not *provider* behaviour, so **user responsibility** must play a role again.

In this context, the most relevant legal question appears to be **what obligations apply today to users of smart glasses** (and similar devices). Calls for bans or rules on the restriction of use first have to look at the existing legal framework before attempting to create new rules. As it turns out, **there are quite a few rules that apply already**.

But first, let us look at one big topic: does the GDPR always apply to users/wearers taking photos or films in public spaces?

II.1. GDPR (in)applicability, household exemption, and private use in public spaces

As discussed in my previous analysis, users (i.e. the wearers) of smart glasses **act as controllers** where they **determine the purposes and means of processing**. This follows from the judgments of the Court of Justice of the European Union (CJEU) in *Lindqvist*[4] and *Ryneš*[5], both of which are based on the premise (not challenged by the CJEU) that natural persons, i.e. private individuals, may themselves be subject to data protection obligations when processing personal data relating to others.

The practical implications for smart glasses are that where a user chooses to use them for their own purposes and in doing so triggers the processing of information relating to an identified or identifiable natural person (= "I'm going to take a picture of Jack", "let's film Alice jumping around", "I'm activating the live transcription feature for what Gabby is saying"), the user can be required to comply with the GDPR **unless** the household exemption applies.

In general, this means that the GDPR obligations apply to the user if using functionalities **directed towards identified or identifiable individuals** when in a public setting or with the intent of going beyond the user's private sphere.

Filming friends singing joyfully on the train? **The household exemption can also apply**, as long as you do not capture footage of any bystanders who might be **identifiable** from your perspective.

This observation stems not only from the *Ryneš* judgment but also from its combination with other case law of the CJEU. In *Ryneš*, it stated that the key criterion was whether a processing activity was *"directed outwards from the private setting of the person"*:

> *"To the extent that video surveillance […] covers, even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, it cannot be regarded as an activity which is a purely 'personal or household' activity"*[6]

The words "private setting" do not necessarily mean "within the confines of a home" but rather a private sphere that moves with the individual in his or her relationship with his known entourage. Limiting it to "within the confines of a home/private space" would limit it further than previous case law of the CJEU, which stated that:

> *"the [household] exception must be interpreted as relating only to activities which are carried out in the course of private or family life of individuals"*[7]

In other words, the household exemption applies to what an individual does in his/her house, on the street when with his/her family, etc., **as long as it stays within a private setting**. If the individual shares the photos online with an indeterminate number of people, that ceases to be within the user's private setting – but share it only with family, and the private setting can remain intact.

---

[4] CJEU, 6 November 2003, *Lindqvist*, C-101/01, EU:C:2003:596.

[5] CJEU, 11 December 2014, *František Ryneš*, C-212/13, EU:C:2014:2428.

[6] *Ryneš*, para. 33.

[7] CJEU, 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, EU:C:2008:727, para. 44.

Beyond family, are friends covered too? The use of the words "personal or household" can make it unclear, but the EDPB considers friends to be covered too[8].

If a bystander passes by or is included by chance in the resulting media asset (footage, photograph etc.), **the question of identifiability kicks in**. This is because if a bystander is not "identifiable" from the user's perspective, **there is no "personal data"** (= information relating to an identified or identifiable natural person), and therefore no processing of personal data *tout court*. The household exemption – processing of personal data "in the course of a purely personal or household activity" – is therefore irrelevant, as there simply isn't any personal data to start with.

If the bystander is identifiable (e.g. a famous person, someone the user knows from a magazine, a social event, etc.), then the GDPR can indeed apply – but its impact will then be limited.

II.2. Inapplicability of the GDPR to the user can limit its applicability to the provider too

The interesting thing about the inapplicability of the GDPR to the user's processing of potentially personal data is that it can also limit its applicability to the provider:

- Inapplicability due to non-identifiability: if a bystander is not identifiable from the user's perspective *and* from the provider's perspective, then the GDPR is inapplicable;

- Inapplicability due to household exemption in combination with non-identifiability: if the user takes a picture of individuals who are identifiable from the user's perspective **but** not from the provider's perspective, any processing of that picture by the provider on the user's behalf **cannot** be subject to the GDPR as long as the household exemption applies.

[Why "cannot be subject to the GDPR"? If the individual is not identifiable from the provider's perspective, that information is not "personal data" from the provider's perspective and the GDPR does not apply. If the household exemption applies, the GDPR does not apply from the user's perspective either – rendering even the "controller-processor" obligations under Art. 28 GDPR inapplicable. Therefore, the identifiable nature from the user's perspective does not make the information "personal data" from the provider's perspective as controller either.]

This does not affect the provider's own processing of **user-**related personal data, but it shows that the **bystander** part of processing is inherently tied to identifiability – and in practice, the bystander is most likely not readily identifiable by the provider, meaning that bystander data processing follows the user's GDPR (in)applicability. And despite what some regulators might think, processing for AI training does not magically transform bystander data into personal data, such that the same rules apply even where the provider's use of data for AI training purposes includes bystander data.

[For more on the issue of incidental processing / bystander data processing, read my analysis "Incidental processing and GDPR: from bystanders to spontaneous notes, do data protection rules apply?".]

[8] See Statement 1/2026 of the EDPB on smart glasses, as well as EDPB Guidelines 3/2019 on processing of personal data through video devices.

II.3. Does public sharing introduce a risk of indirect application of the GDPR?

The *Scania* and *SRB* judgments revealed the possibility of information becoming personal data depending on the recipient's identification capabilities. The idea is that if (i) information is **not** personal data from a particular person's perspective but (ii) that person shares the information with someone else who **does** have means of identification, then the information can be "indirectly" personal data for the sender.

This in practice requires foreseeability, though, as in both *Scania*[9] and *SRB*[10] it was foreseeable for the person making such information available to the third party that the third party would have such means of identification.

This does not mean that publishing a media asset online **necessarily** makes the GDPR apply, but it **increases the likelihood of that media asset reaching someone with means of identification**. This is because this foreseeability does not mean "hypothetical possibility" but requires a form of awareness: the sender **knows or ought to have known** that the recipient would have means of identification at its disposal.

For instance, a selfie with a bystander walking by in the background might theoretically be publicly accessible to billions of human beings through online publication, but it does not mean that it is foreseeable that the bystander in a picture or people who know that bystander will actually see it **and** likely recognise the bystander from the picture.

If sharing information online, does the sharing person **know**, or **ought he/she to have known**, that a recipient would have means of identification? This is not necessarily so. In practice, this will often require an additional step, i.e. **notification by the (until then possibly unknown) recipient that he/she is capable of (re)identifying the natural person**. When that happens, the information becomes personal data from the sharing person's perspective too and the GDPR starts to apply. Yet prior to such notification, that possibility of reidentification was likely merely hypothetical and not actually foreseeable.

II.4. Where the GDPR applies: limited impact on users

Where the GDPR applies, the range of controller obligations applies to users. Yet that does not mean that users should fear becoming controllers from a GDPR perspective.

The first important reminder is that if a person is not identifiable from the user's perspective, **that person is not a data subject**, and so none of the GDPR obligations apply to the user as controller in relation to that person. This does not mean that there is a need to examine photos with a magnifying glass, or pause every frame of a film to check if someone happens to be identifiable, but rather a need to at least glance at the photo/film before sharing it.

Next, many key GDPR obligations are reasonable and easily complied with by users as controllers, as long as they apply a touch of common sense.

[9] CJEU, 9 November 2023, *Scania*, C-319/22, EU:C:2023:837, para. 49.

[10] *SRB*, paras. 84-85.

For instance:

1. Data minimisation and purpose limitation (Art. 5(1) GDPR): as long as users do not start reusing media assets in different contexts (e.g. for production of a movie; making company posters with images) or linking the media asset to other data (e.g. "here's Peter at 12:15 on the Monday at the baker; I saw him again the supermarket the next day"), these principles are typically workable for consumers *[+ more on AI training hereunder].*

2. Data subject request management: with the GDPR applicable, the user has to comply with data subject rights (access and erasure being the most relevant ones, together with objection or consent withdrawal depending on the legal ground – see below). "Please delete my photo" is fairly easy for users to achieve.

3. Legal grounds (Art. 6 GDPR): as a controller, a user has to be able to justify the legal ground for the processing. Consent or legitimate interest are prime candidates (consent notably because of the interaction with the right of personal portrayal / image rights, though the latter doesn't require *GDPR-compliant* consent). Both remain available as long as the interference with the person's rights remains proportionate.

4. Transparency (Art. 13/14 GDPR): reaching out individually to the (identifiable) data subjects in the photo/film helps tackle this concern, but is it required?

- The EDPB has confirmed in its Guidelines 3/2019 on video devices the position set out by the Article 29 Working Party (WP29) in its Transparency Guidelines, namely that *"Article 13 applies to the scenario where the data is collected from the data subject. This includes personal data that […] a data controller collects from a data subject by observation (e.g. using automated data capturing devices or data capturing software such as cameras, network equipment, Wi-Fi tracking, RFID or other types of sensors)".*

- In that context, the "disproportionate effort" exception under Art. 14 would in theory not be applicable.

- As a result, the obligation to inform data subjects about the processing of their personal data may seem like a significant hurdle (no one is walking around with a privacy notice on their forehead), but if they are identifiable for the user, it usually implies that the user has *some* way of contacting them. If that is not the case (e.g. a celebrity), other factors may come into play and mitigate the risk of a finding of non-compliance.

Again: **non-identifiable natural persons are not "data subjects"** from the user's perspective, which reduces the impact of the application of the GDPR.

I will be looking at legal grounds, transparency and AI training at different stages hereunder, but this shows that GDPR compliance by individuals does not require a significant compliance exercise – and common sense helps a lot.

II.5. Smart glasses? Smartphones? Digital recorders? Drones? Same GDPR framework

An important thing to notice is that **the above is not in any way specific to smart glasses**. This is because the GDPR regulates **processing of personal data**, not specific technologies.

The elements mentioned above regarding bystander identification and the household exemption remain valid irrespective of the type of device used, and it is just as possible to be walking around with an unnoticed camcorder as it is with smart glasses.

A week ago, while walking to a meeting in Brussels, I saw a man in business attire walking towards a busy junction, in the middle of other pedestrians, and it was only as we were crossing one another that I noticed he was holding a camcorder in front of his chest and filming everything as he walked by. I did not notice it at first when I assume I entered his picture frame. Does the GDPR apply to his footage? Possibly not, because it is probably not foreseeable that someone to whom he shows the footage will be capable of reidentifying me.

On the audio front, smartphones possess strong audio recording capabilities, and dedicated hardware exists as well (portable recording devices). The same reasoning applies to them too.

This brings us back to the EDPB's statement on smart glasses. As indicated earlier, the statement highlights a range of concerns regarding recording capabilities, yet does not appear to offer any objective reason for which those concerns might not exist in relation to other devices that have long been in use yet never questioned by the EDPB.

Objective factual assessments can justify different legal assessments – yet in the absence thereof, calling out the risks inherent to smart glasses without indicating that those risks exist equally in relation to existing devices with widespread adoption undercuts the point the EDPB is trying to make.

II.6. What about joint controllership between the user and the provider?

Some might counter the above by claiming that joint controllership makes this irrelevant, i.e. that even if the user is a controller, the provider must necessarily be a joint controller with the user.

Yet this type of reasoning is based on an overexpansive approach to joint controllership that would render **any** form of service into joint controllership – which in turn would render the notion irrelevant because it then applies all the time to everything.

As explained in my piece "Blinded by the LED: smart glasses, GDPR, and the illusion of hardware indicators":

> *"if a user instigates the processing (by the [provider]) of personal data of others in support of the service to the user (for instance, cloud uploads of videos for backup purposes, live transcription or translation), the processing is at least primarily for purposes determined by the user. The result is that the user must be deemed as controller and the [provider] as processor, except to the extent that the personal data in question is also processed separately for other purposes by the [provider].*
>
> *The fact that the [provider] has envisaged that the product could be used for various purposes does not make it a joint controller for the user's own processing as holding otherwise would risk transforming a large range of service providers that merely facilitate processing into joint controllers. For example, a cloud hosting provider designs a hosting service with a view to helping customers achieve certain processing activities; should a user select that provider, it uses the provider's hosting service for its own purposes, not for purposes that converge with those of the provider. The same reasoning applies to smart glasses: the [provider] designs the product with a view to helping users achieve certain processing activities, and a user selecting that [provider]'s smart glasses uses their processing capabilities for its own purposes."*

Other examples than cloud hosting with a link to images include image hosting and photo library backups (where clearly the provider has anticipated and facilitated processing of photos), e-mail providers (who clearly envisage that there will be processing of content likely to be shared by e-mail, including images), videoconferencing (where clearly the provider anticipates the processing of facial features through the processing of images) and more.

Designing a service is not enough to make a provider joint controller for everything that the user as controller does with the data, and the reverse is also true: merely triggering a service by using it is not enough to make the user a joint controller of what the provider then does with the resulting data.

This leads me to an important note: in the case of smart glasses, just as with a smartphone, **photos and videos taken by the user appear to stay on the device until the user him- or herself shares or uploads them**.

AI functionality is **separate** – just as any AI functionality on smartphones (such as Google's well-known "Google Lens" feature), a smart glasses AI assistant captures the frame needed to answer or to provide functionality. This is separate from the user's own process of collecting and transmitting media assets.

These are therefore independent operations, each with its own purpose and its own decision-maker, and not operations for which both are joint controllers. Joint controllership requires joint determination of purposes and means of the same operation. Supplying a device capable of supporting that operation (= provider), and then separately triggering that operation by use of that capability (= user/wearer) are two separate things.

II.7. AI training as provider-only processing, not provider & user joint controllership

AI training then occupies an interesting space, also because of various misconceptions about it.

First, it is worth pointing out that so far there does not appear to be much (or even any) evidence that the photos or films specifically collected by users for their own purposes while using smart glasses are used for AI training purposes. This appears to be the working assumption of many authorities, yet with video and photography this makes little sense in terms of efficiency and cost, with metadata (e.g. data about the context, the way in which the user interacted with the device or its output, etc.) being a more compelling source of teachings. It would be good to see what evidence authorities rely upon to make this assumption.

For instance, a spokesperson for Meta, one of the technology providers in the smart glasses market, recently put it in the following terms in an interview with the Irish broadcaster RTE:

> *"If you take a photo on your glasses, it remains on your device. It goes to nobody, nowhere else" […] "If you were to ask the AI a question, like 'what plant is this?', then it has to take a photo to know what you're asking about and analyse that. That photo could then be used to keep training the model."*[11]

[11] RTÉ, Brian O'Donovan, "Meta defends AI smart glasses amid criticism", 23 October 2026.

[Given that the EDPB's statement does not appear to reflect this particular perspective, this perhaps shows again the importance of actual stakeholder involvement.]

Next, one should avoid assuming that the user somehow influences and determines the purposes and (essential) means of AI training processing:

- While the user's choice to e.g. wear the smart glasses does enable the generation of data that could be eligible for training, the user does not influence its purpose. Only the provider decides the training purposes and means, and which information to process for AI training purposes. The user only benefits indirectly from such processing by virtue of the fact that it will help improve the product *for all users* (including the user).

- The user has no motive, no "own purposes", for the AI training processing, while the CJEU stressed that influence is not enough – it needs to be coupled with "own purposes" (*"a natural or legal person who exerts influence over the processing of personal data, **for his own purposes**, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a [joint] controller"* – emphasis mine[12]).

In other words, although the user provides the initial trigger enabling the generation of information *(it yet to be seen whether that is actually personal data)* that could potentially be used for AI training purposes (by using specific AI capabilities through the smart glasses, similarly to activating specific AI functions on a smartphone), the user's "contribution" (if any) to AI training processing stops there.

Instead: (i) the wearer decides whether, when and what to record; (ii) the provider alone decides whether and how AI features work. Those are different operations (not even successive ones), with different purposes, different decision-makers. They even concern different data (different images). There can therefore not be any joint control for those (distinct) processing activities.

Finally, it is again worth stressing that not all data being processed for AI training purposes is "personal data" from the provider's perspective, for the reasons set out in sections 2.1-2.3 above *(and that is without counting on whether any additional anonymisation techniques are used by the provider in the framework of that training process).*

This all contributes to the finding that **if there is personal data within the corpus for AI training, the provider is most likely a sole controller** in relation to that processing.

Should the user be able to prevent such training on the basis of personal data that relates to him/her? Two considerations are key:

- To the extent that any personal data is involved, AI training is likely to be based on the legal ground of **legitimate interests** (more specifically, usually the legitimate interest of the provider in ensuring that its models/systems perform as intended, are safe and continue to be improved). This leads to the availability of the **right to object** for the data subject, i.e. the right for a data subject to invoke "grounds relating to his or her particular situation" to prevent that processing of his/her personal data from continuing (Art. 21(1) GDPR).

- The right to object is not, however, an absolute right. If "**compelling legitimate grounds**" exist that override the data subject's interests, rights and freedoms, the processing can continue

[12] CJEU, 10 July 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, para. 68.

(Art. 21(1) GDPR). Such compelling legitimate grounds are for instance often invoked if there is an objection to parts of AI training or other processes that relate to security, fraud prevention and detection, or the prevention of unlawful or questionable behaviour (e.g. learning both about good uses and bad uses of technology).

III. Other relevant legal frameworks for users

The GDPR is just one type of legislation that can be relevant to the operation of smart glasses. Others are equally applicable, but also with a limited impact in practice for legitimate uses.

III.1. Image rights, or the right of personal portrayal

Many Member States recognise image rights, also known as the right of personal portrayal, and which protect individuals against the unauthorised use, dissemination or exploitation of certain aspects of their physical identity.

While the precise scope of these rights differs between jurisdictions, they generally seek to safeguard an individual's control over the use of their image; in an era of deep-fakes, the scope of personality rights has become even more of a societal issue, with discussions ongoing about whether these rights also cover likeness (to the sound of one's voice or to one's physical appearance).

These rights vary slightly in their labelling and scope from one Member State to the next. The *droit à l'image* in France, *droit à l'image / recht op afbeelding* in Belgium, *Recht am eigenen Bild* in Germany and *portretrecht* in the Netherlands all share a same objective: giving individuals a degree of control over the capturing of their likeness, as well as publication and exploitation thereof.

As the Belgian version puts it, the principle is that *"Neither the author, nor the owner of a portrait, nor any other possessor or holder of a portrait, shall have the right to reproduce it or communicate it to the public without the consent of the person depicted or their successors in title for a period of twenty years from the date of their death"* (Article XI.174 of the Belgian Code of Economic Law – French / Dutch).

An important exception to this rule typically concerns persons appearing incidentally in the photo – i.e. not the focus. See for example section 23 of the German *KunstUrhG (Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie)*, which states in its paragraph 2 that no consent is required for the dissemination of "images in which the persons appear only as an accessory next to a landscape or other location" – i.e. incidental appearances. Other exceptions to the authorisation or consent requirement often include public figures in the exercise of their public role, newsworthy events and more.

Put differently, if a person is recognisable yet not a public figure, and is not appearing merely incidentally, that person retains control over how he or she is presented, portrayed and exploited in public or commercial contexts.

Applied to smart glasses, a user of smart glasses who records and subsequently disseminates footage of identifiable individuals may face not only obligations under data protection law, but also claims based on image rights, personality rights or related civil law doctrines. Just as with any dissemination of footage of identifiable individuals taken through other means, from smartphones to camcorders.

III.2. Criminal law restrictions

Many of the behaviours most frequently cited by critics of smart glasses are already explicitly prohibited under criminal law provisions across EU Member States, raising the question as to why these concerns are even relevant as an argument against the use of smart glasses. After all, one does not assume that every user of smartphones, camcorders or portable recording devices is committing criminal offences – yet the potential also exists.

Indeed, the categories of (mis)conduct examined hereunder (voyeurism, covert recording, stalking, harassment and the unlawful dissemination of intimate or private imagery) are criminal offences **irrespective of the type of device used**.

So before looking at whether smart glasses should be subject to specific rules, it is important to refresh one's memory: these rules exist and prohibit certain kinds of behaviour in any event. Not every use of smart glasses runs afoul of such rules, quite the opposite – in the same manner as not every use of binoculars, dashcams, nanny-cams, smartphones etc. is unlawful.

A) Voyeurism

Many EU Member States prohibit or restrict non-consensual recording in locations where individuals hold a reasonable expectation of privacy.

For instance, Article 226-1 of the French *Code pénal* prohibits the capture, recording or transmission of the image of a person situated in a private place without consent. Article 226-2 of that same criminal code extends liability to the keeping, dissemination or use of such recordings. In Spain, Section 197.7 of the *Código Penal* (as amended by the *Ley Orgánica* 1/2015) provides for a similar rule.

Similarly, Section 201a of the German *Strafgesetzbuch* (StGB) criminalises certain forms of unauthorised image capture that infringe an individual's highly personal sphere of life, while additional offences may arise in relation to recordings of intimate content.

Where the recording covers situations in which the subject is unclothed or engaged in sexual activity, this is even more frequently a criminal offence. For instance, Article 135 of the new Belgian Criminal Code (French / Dutch) prohibits voyeurism of such a nature, and its Article 136 prohibits the dissemination of content of a sexual nature (i.e. naked or engaged in an explicit sexual activity) without the agreement of the person. Similarly, Article 226-2-1 of the French *Code pénal* specifically criminalises the unauthorised transmission of speech or images of a sexual nature.

With such provisions, the fact that a recording device has a particular form factor (wearable, handheld, etc.) does not alter that assessment. The decisive factor remains the conduct of the user and the context in which the recording takes place.

In this context, the key question is not whether problematic use is regulated *(it is)*, but whether the existing framework is sufficient – and sufficiently enforced. Anecdotal evidence suggests that the enforcement part may be the part that lags the most (along with often insufficient awareness that voyeurism can be a criminal offence and that victims can file a complaint with law enforcement authorities).

B) Covert recording

I have covered the issue of covert recording devices, in particular through the example of Germany, in my previous piece "Blinded by the LED: smart glasses, GDPR, and the illusion of hardware indicators". As explained in there, the key item to look out for is whether a device is a "dual-use" device, i.e. a device that is intended to be used in other scenarios (such as smartphones, smart glasses and portable recording devices). – as dual-use devices are generally not subject to the restrictions on covert recording devices. Examples of actual covert recording devices (button cameras, spy cameras etc.) differ significantly from e.g. smart glasses for this reason.

C) Harassment and stalking

If any individual – with smart glasses or any other recording device – were to persistently record another person specifically, without the authorisation of that person, that could meet the conditions for harassment or stalking under national criminal law. Further dissemination of the footage is not typically a requirement in this context.

For instance, in Germany, Section 238 StGB criminalises repeated conduct directed at another person and significantly interfering with their way of life by e.g. repeatedly *"visit[ing] the physical vicinity of this person"* or *"distribut[ing] or mak[ing] available to the public an image of that person"*. French law emphasises harassment with an impact on physical or mental health (Article 222-33-2-2 *Code pénal*), Belgian law focusses on wilful and serious disturbance of tranquillity (Art. 237 of the Belgian Criminal Code – French / Dutch) and Spanish law penalises the act of *"insistently and repeatedly, and without being legitimately authorised,"* seeking the proximity of another (Section 172 *ter* of the *Código Penal*).

Once again: these provisions are technology-neutral and could easily apply to any actual harassment using any device, whether a smartphone, smart glasses, etc. – even analogue/film cameras are covered.

Moreover, recording is not even a requirement for there to be harassment. Binoculars or physical presence could suffice in certain cases.

D) Troubles à l'ordre public

One idea that was floated by some was that "troubles à l'ordre public" (i.e. public order harm) could be used to prevent certain uses of smart glasses. While the idea of this becoming a general rule and enabling a ban appears to be far-fetched, it is correct that if a particular natural person uses smart glasses – just in the same way as one could use a smartphone or even binoculars – in a manner that threatens public order (physical safety, public tranquillity, public health or public dignity), that use can be restricted.

IV. Sharing and publication as real trigger, and "ask before sharing"

All of the above highlights a common theme: **the law is already capable of covering misuse of any tool or technology**, and outside of situations of misuse, there are typically **consent or authorisation requirements** when it comes to the use of footage of an identifiable natural person beyond a private environment. The concerns generally highlighted by regulators are therefore already met in practice at legislative level, as users are required by law to respect certain boundaries.

It also illustrates the fact that the key concern many have with smart glasses is the **potential for sharing without transparency**.

But let us look at some of the key claims brought forward:

- "LEDs aren't visible enough from afar" is a poor argument, due to the fact that the resolution of smart glasses is already less than that of smartphones for actual user-activated camera or recording features – significantly decreasing or even removing the likelihood of identifiability.

- "LEDs are confusing" – this is an interesting one, but it only shows that LEDs are a crutch that ultimately should disappear. *[I have argued in my piece "Blinded by the LED: smart glasses, GDPR, and the illusion of hardware indicators" that LEDs are unhelpful from a GDPR transparency perspective.]*

- "Smart glasses allow *[insert tech provider name here]* to perform mass surveillance or capture masses of personal data": due to the fact that available documentation and statements by some providers shows that AI training material stems from lower resolution footage that is separate from user-requested photography and film, and that they are not geared towards faithful reproduction of likeness but rather pattern recognition of type of object etc., this argument appears to be based on technical misunderstandings.

The key claim that remains is this one:

- A wearer/user could misuse the recording capabilities of smart glasses to obtain footage of someone else without authorisation and either share it further or misuse it.

On misuse, the above sections – in particular that on criminal law – illustrate existing rules aimed precisely at tackling such misuse.

And what about sharing then?

As highlighted in the GDPR section above, case law of the CJEU *"does not mean that publishing a media asset online **necessarily** makes the GDPR apply, but it **increases the likelihood of that media asset reaching someone with means of identification**. This is because this foreseeability does not mean "hypothetical possibility" but requires a form of awareness: the sender **knows or ought to have known** that the recipient would have means of identification at its disposal."*

That identifiability issue is also central to image rights, due to the exception for individuals who are merely an accessory and not the focus of the media asset (footage, photograph, recording).

This leads me to the "**ask before sharing**" principle.

From a practical perspective, many legal risks associated with smart glasses, as well as any other device with recording capabilities, can be mitigated through a simple principle: **where an identifiable individual is the subject or focus of a media asset, users should consider obtaining that individual's approval before sharing that media asset with others**.

While the law foresees various exceptions depending on the precise context (e.g. journalistic, artistic, public interest), the principle of seeking permission before publication reflects the underlying objectives of data protection law, image rights and personality rights. It also aligns with existing social norms governing the responsible use of smartphones, cameras and social media.

Importantly, **this principle is not unique to smart glasses**. The same expectation already applies to many forms of digital content creation and online publication. The issue is therefore not the existence of a new technology but the responsible exercise of discretion by users when deciding whether to share content involving third parties.

V. What about facial recognition? Or social acceptability?

"Surely this cannot be all there is to smart glasses", some may say. The combination of AI and platforms with access to large datasets must necessarily mean that there is a risk of facial recognition and widespread surveillance, right? And smart glasses must clearly be unacceptable from a societal perspective, no?

If any organisation does decide to actually roll out facial recognition on smart glasses (and not merely have a theoretical capability thereof), there is once more existing legislation to deal with that:

- The AI Act explicitly prohibits *"the placing on the market, the putting into service for this specific purpose, or the use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage"* (Art. 5(1)(e) AI Act). While reports of putative facial recognition ideas do not meet these conditions, it shows already that certain misuses are unlawful.

- Any facial recognition system that does not meet those conditions would likely fall within the scope of the AI Act's "high-risk AI systems" classification – notably the concept of *"remote biometric identification systems"* defined in Article 3(41) and listed as a high-risk AI system under Annex III(1)(a) of the AI Act. This does not mean it is prohibited, but that it is subject to strict requirements and obligations.

- Plus, the GDPR itself continues to apply to facial recognition, notably its Article 9(1).

The theoretical possibility of a certain functionality does not mean that it is actually placed on the market, put into service or used. Instead, just as in the cases described above, **statutory interventions, bans and restrictions in use cannot be taken on the basis of assumptions**.

This may explain partly why some regulators have turned to another approach. Instead of seeking to restrict use through the law (after perhaps finding out that this cannot be done as easily as they had hoped – as the German example of covert surveillance legislation shows), they seem to have shifted to the notion of "**social acceptability**".

In February, the CNIL proposed to the European Data Protection Board to commission a study on social acceptability on smart glasses from a French sociologist – a few months after the CNIL itself had commissioned a survey on the topic. The CNIL appears to have played a significant role in the study as well, with the EDPB-commissioned study report stating the following:

> *"This research has been followed by the CNIL and more specifically its Digital Innovation Laboratory (LINC), with Vincent Toubiana* [note: Head of LINC, the CNIL's Digital Innovation Lab]*, Mehdi Arfaoui and Martin Bieri being the main correspondents. We thank them here for the proposal made in February 2026 to carry out this survey and for their support in carrying it out."*

That report commissioned and published by the EDPB (at EU level therefore) is the result of a survey *"among a diverse sample of **22 individuals**, divided between owners and users of connected glasses (N=7) and non-users (N=15) who share the common characteristic of having a more or less diffuse knowledge of these devices, without being owners of them"* (emphasis mine).

In the light of the limited number of interviewed individuals, the last words of the conclusion, namely that *"the collective resistance expressed by some non-users – who demand radical design constraints or the strict application of current or imagined consent rights – outlines a future political struggle"*, appear to be somewhat diluted.

More generally, it is worth wondering whether the EDPB was even right to commission such a study, given that its tasks are not to assess sociological questions but to ensure consistency in the GDPR's application (as discussed above).

In this context, it is unclear which conclusions, if any, can be drawn from the study, other than the fact that the EDPB wishes to bring social acceptability to the fore on the basis of a handful of interviews. Instead, it would have been far better to include a broader range (and larger number) of perspectives, ideally from across the EU. There are only limited references to the impact that smart glasses can have on the daily lives of individuals with visual impairments, no considerations on the actual technical working of smart glasses (and so the distinction between perceived and actual functioning). A more complete study could have been interesting from a policy perspective, but this study less so.

VI. Conclusion and policy recommendations

All of the above results in a few general observations:

1. The "**ask before sharing**" principle is the best means of compliance (and it tackles the real trigger for concerns regarding privacy).

2. Smart glasses are dual-use devices, not covert surveillance equipment.

3. The GDPR applies to users in certain circumstances, but many everyday uses fall outside of the scope of the GDPR, notably if a bystander is not identifiable.

4. Where the user is not subject to the GDPR, the provider's obligations regarding user-triggered processing are equally limited, with potential inapplicability as a result.

5. Publishing content online does not automatically transform content (photos etc.) into personal data and thus trigger the GDPR. The key question is whether the user knew or ought to have known that a recipient could identify the individual to whom the information relates.

6. Where the GDPR does apply, a user's obligations (data minimisation, responding to erasure requests, identifying a legal ground etc.) are manageable with common sense.

7. AI training is not based on the same images as those captured actively by users.

8. Misuse is already regulated under criminal law (re voyeurism, harassment, etc.), irrespective of the type of device.

9. The scope of image rights, or the right of personal portrayal, varies by jurisdiction, but generally requires authorisation or consent, unless a person is unidentifiable.

10. The key legal question is not which device is used but whether **the user conducts him- or herself in a manner that complies with the law and respects others' rights**.

In conclusion, **smart glasses do not require new laws**, and regulators would do well to assess the technical validity of assumptions before taking any positions specific to smart glasses. In particular, more awareness about the difference between user-taken recordings and AI-supporting recordings could lead to more accurate legal positions. Just like with smartphones, binoculars, drones, etc., the misuse by users of technology can give rise to sanctions, without providers being on the hook for the actions undertaken by users.

Ultimately, the best way to manage those risks for users is to apply the principle of "**ask before sharing**", but some work on awareness of what smart glasses *actually* do could help with the additional concern some have been raising, that of social acceptability. The relevance of that concept for legal reasoning, however, has yet to be shown, and it is my hope that the EDPB will use its authority and power (and budget) for in-depth legal analyses rather than for small-scale sociological surveys