EUROPEAN DATA PROTECTION SUPERVISOR

Technology report No 1

Smart glasses and data protection

***

This technology report on smart glasses and data protection aims at clarifying the state of play of smart glasses in the market, official positions on related privacy and data protection issues and future developments.

***

Brussels, January 2019

Postal address: rue Wiertz 60 - B-1047 Brussels

Offices: rue Montoyer 30 - B-1000 Brussels

E-mail: edps@edps.eu.int Website: http://www.edps.europa.eu

Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

Contents

Executive summary

Smart glasses are wearable computers with a mobile Internet connection that are worn like glasses or that are mounted on regular glasses. They allow to display information in the user's view field and to capture information from the physical world using e.g. camera, microphone and GPS receiver for augmented-reality (AR) applications.

The initial release of *Google*'s smart glass gained significant attention worldwide and increased the popularity of those devices. While the target audience has been initially the business sector (e.g. logistics, training simulations, etc.) with unit prices of about EUR 1500, recently competitors such as *Snap Inc.* address a wider and younger audience with cheaper models for about EUR 150.

While smart glasses may be very useful tools in many fields of application (technical maintenance, education, construction, etc.), their use has been discussed controversially because they also are considered to yield a high potential to undermine the privacy of individuals, especially where not properly privacy-friendly designed. The data protection impact of recording videos of persons in public places has already been discussed in the context of CCTV and dashcams. The sensors may record environmental information including video streams of the users' view field, audio recordings and localisation data. Furthermore, smart glasses may allow their users to process invisible personal data of others, such as device identifiers, that devices emit regularly in form of Wi-Fi or Bluetooth radio signals. These data may not only contain personal data of the users, but also of individuals in their proximity (non-users). Applications of the smart glasses may process recorded data locally or remotely by third parties after an automated transfer via the Internet. Especially when smart glasses are used in densely populated public areas, existing safeguards to inform data subjects by means of acoustic or visual indicators (LEDs) are not efficient. Smart glasses may also leak personal data of their users to their environment. Depending on the smart glass design, non-users may also watch the smart glass display, which may contain personal data such as private mails, pictures, etc. Like any other Internet connected device, smart glasses may suffer from security loopholes than can be actively exploited to steal data or run unauthorised software.

While smart glasses play so far only a marginal role in everyday life, experts estimate an important potential to increase productivity in the professional sector thanks to AR and the smart glasses initiatives of Facebook, Apple and Amazon will lead to an increasing adoption in the consumer market. Technological improvements in facial or voice recognition and battery life may allow for novel use cases of smart glasses in many sectors. For instance, in the law enforcement field, reports revealed in early 2018 that police officers employ smart glasses to match individuals (in crowds) against a database of criminal suspects using facial recognition. In this dynamic field, data protection authorities are challenged to keep pace with the rapid developments and provide guidelines. Indeed, many aspects have been covered already in the WP 29 Opinion on the Internet of Things.

With the GDPR, a harmonised set of principles and a system of tools have been provided, first and foremost for the controllers, processors and developers of smart glasses to assess and control their impact on data protection and privacy. At the current stage of the development, an urgent need for technology specific legislative initiatives does not appear to be justified. However, the development of smart glasses and similar connected recording devices underlines the need to establish a robust framework for privacy and electronic communications, as proposed with the ePrivacy Regulation.

1 Introduction

Smart glasses are wearable computers with a mobile Internet connection that are worn like glasses or that are mounted on regular glasses. They allow to display information in the user's view field and to capture information from the physical world using e.g. camera, microphone and GPS receiver, e.g. for augmented-reality (AR) applications[1]. As Internet-enabled devices, they can belong to the Internet of Things (IoT)[2].

Combining the vast potential capabilities of smart glasses such as AR, high resolution image projection, and 3D images live manipulation and their decreasing price, these products could soon become part of many people's lives. As an example, they may be used in manufacturing[3] and other engineering tasks.

The technology has raised concern due to its vast potential to harm individuals' data protection rights: non-authorized recording of data subjects' actions and activities both for the device users and for others in their view, incorporation of facial or voice recognition systems and the collection and storage of users' metadata are all examples of how these devices may affect the rights of individuals.

This report explores implications of smart glasses for privacy and data protection, the state of play of the main smart glass manufacturers, and provides an outline on its use and possible future developments.

This report does not consider psychological and social effects caused by the perceived or real difference of power in situations where individuals equipped with smart glasses encounter others without such devices.

2 Smart glass technology

Smart glasses provide their users with information and services relevant for their contexts and useful for their tasks.

While early models can perform basic tasks, such as serving as a front end display for a remote system, modern smart glasses are effectively wearable computers which can run self-contained mobile applications. Some models are equipped with a hands-free system that allows an operation via natural language voice commands, while others use touch buttons.

To identify security and privacy issues, a thorough analysis of the building components of the smart glasses is necessary. Essentially, the smart glasses (shown in Figure 1) are mobile wearable computers equipped with an embedded processor for executing codes and processing data, sensors for a diversity of applications, wireless connectivity, and a built-in Heads-Up-Display (HUD). Often, they are configured and managed through a smartphone, e.g. via Bluetooth connectivity.

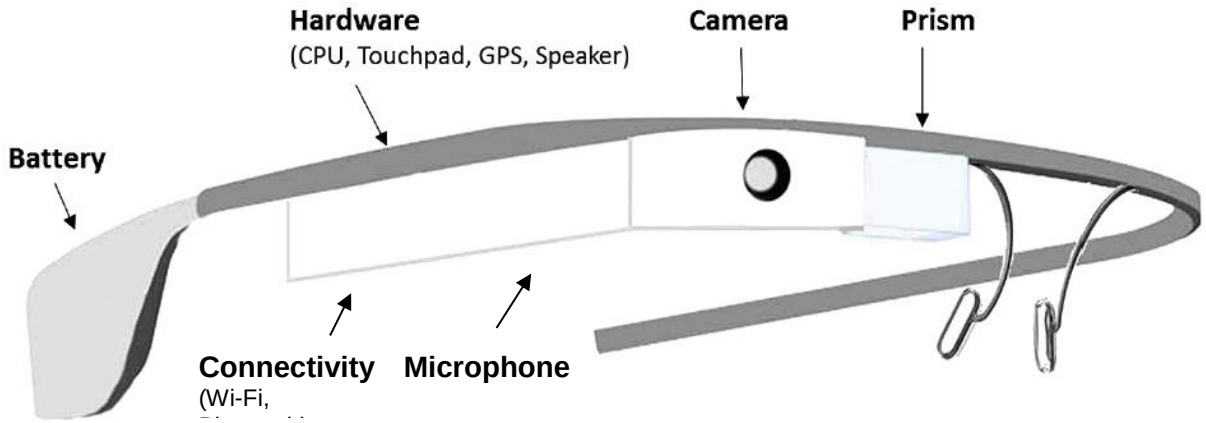

Figure 1. Smart Glass Hardware Components (Source: See endnote 2, license Creative Commons CC-BY)

The key components of smart glasses are as follows:

1. a CPU (Central Processing Unit) similar to what is being used in modern smartphones;
2. a GPS receiver for geo-localisation
3. inertial sensors such as accelerometer, gyroscope and compass to measure spatial movements and orientation;
4. speaker and microphone for audio input and output;
5. HUD for visual feedback;
6. camera for capturing pictures and record videos;
7. Wi-Fi and Bluetooth for wireless connectivity.

A central component of smart glasses is the HUD shown in Figure 2, which enables AR by projecting an image on a see-through display. It allows to overlay digital information on the view field of the user.

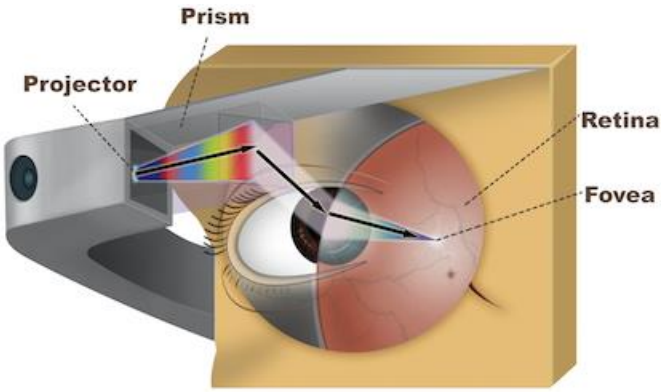

Figure 2. Smart Glass Heads-Up Display

3 Privacy concerns

Following the appearance of Google's smart glasses model *Google Glass* (see Section 6.1) in 2012, international data protection experts and authorities tried to assess how Google had considered privacy principles. Even though *Google Glass* was not the first wearable device with video and audio recording capabilities, the popularity and power of Google made its device very popular. Also, although smart glasses capabilities were not completely new (video recorders have already been available in the market in extremely compact forms), the combination of functionalities and the market approach made *Google Glass* triggered an intensive discussion of the privacy implications of these new kind of wearable devices.

In response, European[4] data protection authorities formally asked Google to address privacy concerns regarding *Google Glass*[5]. Google answered that privacy issues had been taken into consideration in the design phase (*privacy-by-design*). For example, sounds and blinking-lights would notify individuals in the user's proximity (non-users) that actions like recording a video or an audio track were performed by the *Google Glass*' user. Facial recognition features were not embedded in the software[6].

However, even if these measures might have made the device more *privacy-friendly*, security risks of smart glasses could also affect the privacy of the users and other persons within the range of action of the device (see Section 4.).

One of the main concerns regarding smart glasses is their capacity to record video and audio in such a discreet way that the people being recorded are not aware of it. Currently, the recording time of smart glasses is technically limited to a short time period of about one hour, but we could envisage future technology improvements that allow for near interruption-free recording. Data protection issues may arise whenever individuals within visual range are recorded, as this may happen without their knowledge, the recordings may be used for further data processing e.g. submitted to third parties in a cloud computing environment. Such situations may occur when recorded data is shared through social networks.

Smart glasses could be used by services in charge of security and safety. In principle, there is nothing to suggest that such services could not use smart glasses in a well-defined and thoroughly restricted manner and in full compliance with fundamental rights, including the rights to privacy and to data protection. Law enforcement services, e.g. police officers, could use smart glasses to record interactions with the public, to identify individuals in crowds using facial recognition, to scan vehicle license plates, to live stream video to a control room, and to process biometric information of e.g. wounded or unconscious subjects. According to reports in early 2018[7], Chinese police officers have piloted smart glasses to match individuals in visual range in a crowd against a remote database of criminal suspects using facial recognition[8]. Collecting recordings from public areas, smart glasses can constitute a tool of mass surveillance. As an alternative option to smart glasses, law enforcement officers are increasingly equipped with body cameras[9], which provide the same recording functions as smart glasses but not the same output functions.

Manufacturers have to respect their accountability to data protection and privacy, and consider these rights when designing devices. Legislators must consider necessity and proportionality when they discuss legislative initiatives aiming at the use of connected devices for law enforcement and security purposes.

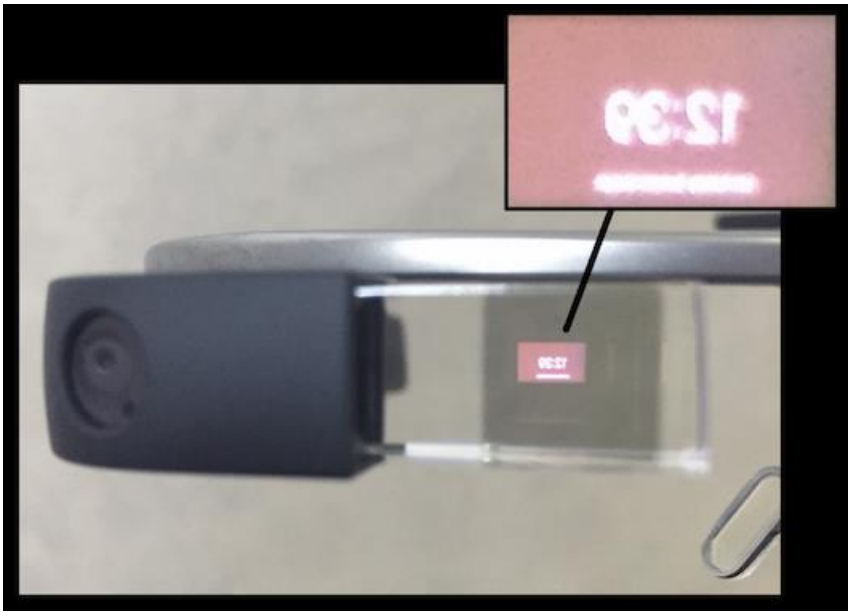

Figure 3. Smart Glass See through Display

Users of smart glasses may also create a certain risk to their own privacy and personal data[10], when the technical features of the device make it possible for persons close by to observe their interaction with the smart glasses. In Figure 3, we see a significant display design limitation that reduces the privacy of the user. A transparent screen is the essence of providing augmented reality. However, this allows other people in close proximity to see the user's display as well, which may show confidential information, e.g. pictures or private messages.

With a large variety of interconnected IoT devices, personal data such as activity and health profiles can be collected in an increasing number of situations of everyday life. Sensors of IoT devices allow to collect information that goes beyond direct user inputs and encompasses information on the device environment from which personal data may be interfered indirectly without their knowledge and consent.

Most of the **privacy considerations** on IoT devices are also applicable for smart glasses:

- lack of data control by users and especially by non-users: impossibility to consent and to be informed properly, mainly for non-users
- inferences derived from data and repurposing
- intrusive analysis of behaviour and profiling
- limitations on the possibility to remain anonymous for the user
- lack of anonymity due to the high identifiability of the information being processed, e.g. facial pictures, videos, sound recordings or even the possibility of the devices themselves to identify the individuals under their reach using face and voice recognition and Wi-Fi- and Bluetooth signals; and
- the processing of special categories of data, which requires special safeguards
- the security risks attached to mass market products: it is not clear how smart glasses manufacturers will balance the implementation of confidentiality, integrity and availability measures at all levels of processing with the need to optimize the use of computational resources and energy by objects and sensors.

Also, most of the **data protection recommendations** for IoT devices are pertinent here:

- apply data minimization, e.g. not collecting location data unless really needed;
- perform a data protection impact assessment;
- embed data protection by design and by default in the development process;
- provide appropriate information to users and non-users, develop new and creative ways to inform and enquire the consent from non-users;
- specific user control before publication on social networks; and
- security and vulnerabilities notifications and security updates;

A more detailed review of the data protection aspects of IoT/wearable devices is given in the Article 29 Data Protection Working Party Opinion 8/2014 on the Recent Developments on the Internet of Things adopted on 16 September 2014[11].

4 Security concerns

Hacking smart glasses is feasible[12]. In 2013 and 2014, hackers demonstrated that it is possible to replace the operating system in *Google Glass* devices and to deactivate the sound and light notifications installed by Google to inform non-users on the use of the recording functionalities. A facial detection system[13,] was also developed.

Researchers made proposals[14] for changing the physical and software structure of *Google Glass*, to improve its security and privacy. Redesigning features that currently pose threats to the security and privacy of smart glass users and other people include: *User Authentication, Locking Mechanism, Notification, Physical Security, Governmental Security, and Firewall*. However, it is generally difficult or even impossible to proof the absence of features, such as undercover recording and a backdoor for third parties, or an unnoticed security loophole.

Accountability and trust are building blocks for network and information security. Moreover, security threats can be easily related to the operating system. Since Android is a popular operating system used for smart glasses, the same threats to Android security for smartphones apply. Vulnerabilities discovered in the past allowed for attacks that make the device partially or fully unusable, or enable an attacker to spy or steal user's data. Other threats include existing Android malwares or viruses that can infect the device through malicious applications.

Smart glasses can also be exploited to threaten the security of their users. As many applications on such devices provide an immersive experience, malicious applications may deceive users about the real world. For example, thieves could put together a plan of users' houses if they come into possession of smart glasses data recorded at home[15].

Besides the specific security risks of smart glasses, they also suffer from all security issues common for IoT/wearable devices. With usually few resources such as computing power and battery supply, certain security solutions, e.g. encryption, are difficult to implement or need specific schemas. Also, as for any IoT device, consumer guarantee and lifecycle management is complex due to the, mainly, personal use of those devices. Mobile devices have further a higher risk to get lost. A more detailed review of the security aspects of IoT/wearable devices can be found in the Article 29 Data Protection Working Party Opinion previously mentioned[11].

5 Business case

Google Glass has effectively disappeared from the consumer market, and no similar device has achieved a comparable level of attention or distribution. Nevertheless, research and development efforts have continued, and new products have been announced to be in preparation, targeting mainly professional markets.

The main use of smart glasses is expected in professional applications with AR as the main *business case*. AR is claimed to be able to optimize effectiveness, productivity and safety of employees and other actors. Providing for AR, smart glasses are beneficial in several fields and activities, such as health-care or transportation.

For instance, by using AR, air carriers are training jet engine technicians through a self-contained application, thus being able to minimize the expenses of having on-the-spot sessions. Also, it is expanding its role in the logistics sector in order-picking processes.

Smart glasses enable field experts or factory workers to work faster, more focused and hands-free[16]. Industries claim that smart glasses increase the efficiency, quality and safety of their manufacturing programs.

Smart glasses may be used to support technicians inspecting fire detection installations in especially complex installations. They can also guide technicians with remote expertise.

According to *Gartner*, the impact on field service may amount to USD 1 M per year in the next three to five years thanks to '*diagnosing and fixing problems more quickly and without needing to bring additional experts to remote sites*'[17].

In 2015, ABI Research[18] estimated that approximately 90% of smart glasses would be sold to police, military, security, warehouse, and bar code scanning operations.

Smart glasses are already in use in law enforcement in several countries[19].

- *The New York City Police Department trialled Google Glass and other smart glasses in 2014[20].*
- *China's police officers piloted in 2017 smart sunglasses with built-in facial recognition to recognize criminals in crowds[21].*
- *Abu Dhabi[22] police plans to begin using smart glasses to catch criminals, identify missing people, and scan license plates on vehicles.*

New developments, like Spectacles by Snap (see Section 6.3) may re-launch smart glasses as a mass-consumption item oriented towards a personal use (consumer wearables), mainly for recording personal events[23] without the possibility to interact with information or enrich *reality* with an additional information layer.

In the following figure we present the categories of the application of smart wearable devices in general.

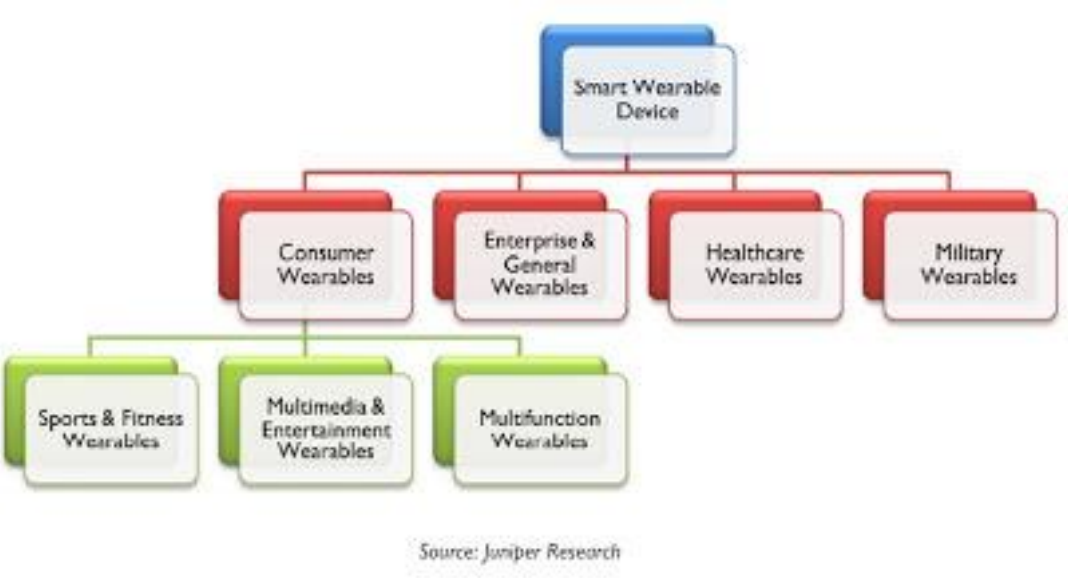

Figure 4: Categories

6 Past and recent developments

6.1 Google Project Glass

A very popular smart glasses device was produced by the Google Project Glass[24] whose product termed *Google Glass* was publicly announced in April 2012[25]. Google Glasses were equipped with different sensors like microphone, accelerometer, gyroscope, magnetometer, ambient light sensor, proximity sensor, touch pad and a HD camera.

Connected to the Internet, they allowed to access Google Search or Google Maps or to take videos and pictures. The user interacted with the device in two ways: via voice command or via a touchpad located on the side of the device. The experience was enhanced by the *MyGlass* website and mobile application, giving users a place to monitor the status of their device and to manage its settings.

Some specific applications were provided by third-party developers via APIs (application programming interfaces) and a dedicated framework. Several proofs of concept were proposed in healthcare. For instance in January 2014, a Melbourne[26] tech start-up created a breastfeeding application that allowed mothers to nurse their baby while viewing instructions about common breastfeeding issues (latching on, posture, etc.) or call a lactation specialist via a secure Google Hangout videoconference, thus being able to recognize the issue by means of the mother's camera on her smart glasses. As another example, virtually augmented surgery was carried out as part of a pilot programme utilizing software by the remote video software company Vipaar[27] to allow surgeons to communicate remotely with each other.

In October 2014, after several journalism and mass media applications were proposed, the European University Press published the first book to be read with Google Glass.

The privacy and data protection implications of this kind of devices received some attention by data protection authorities, for example, in 2014, the French Data Protection Commission (CNIL) released an issue of their "Cahier Innovation et Prospective" on the body as the new connected object ("le corps, nouvel objet connecté") which sees Google Glass as a symbol for a new wave of data collection devices[28].

After two stages of beta-testing (in early 2013 and in June 2014), Google interrupted the production for consumer market in January 2015. In late 2015, the design was reviewed and a new patent of an improved design was approved in November 2015 by the US Patent Office[29].

6.2 Current developments of smart glasses projects

Meanwhile, many competitors started developing their own version of smart glasses, with some common features and functionalities that will be hereby described. The market of smart glasses is currently expanding and may dramatically reshape the way people live and do business.

Firstly, most smart glasses are equipped with cameras and microphones to record video and pictures. Some models also incorporate GPS receivers. Interestingly, some companies incorporate cameras (and microphones) only upon explicit request by the customer in the pre-order stage.

Secondly, AR, the most common use case, is continuously improved to make the subject's interaction with reality more interactive and informative. Therefore, smart glass applications are developed to support for example voice dictation (*speech-to-text software*), motion tracking, and piloting drones.

A survey[30] demonstrated that most consumers perceive smart glasses as a combination of fashion and technology. The fear that smart glasses can threaten their privacy and data protection does not seem to significantly impact their adoption intention.

The recent trend in smart glasses design leads to models that are difficult to distinguish from ordinary glasses[31]. In consequence, personal data of non-users may be captured secretly and without effort – either with or without the intention of the actual user. In both cases, basic data protection principles such as confidentiality and the right to informative self-determination of non-users are at stake.

6.3 Spectacles by Snap

Spectacles[32] by the company *Snap* are targeted to young audiences, at a price lower than current or previous competitors. For example, the Google Glass project was in fact targeting a segment of customers with high purchase power, the device was priced at about 1,500 €, whereas Spectacles price below 200 € would make it more accessible to a wider and younger public, thus being potentially able to become a widely used mainstream product within the sector in the future.

On the day of the announcement, Snapchat declared that it was being rebranded as *Snap Inc.*, proving the high expectations, the company had in the new product[33].

YouGov presented a survey on Snap's Spectacles on how intrusive smart glasses as Spectacles would be considered[34]:

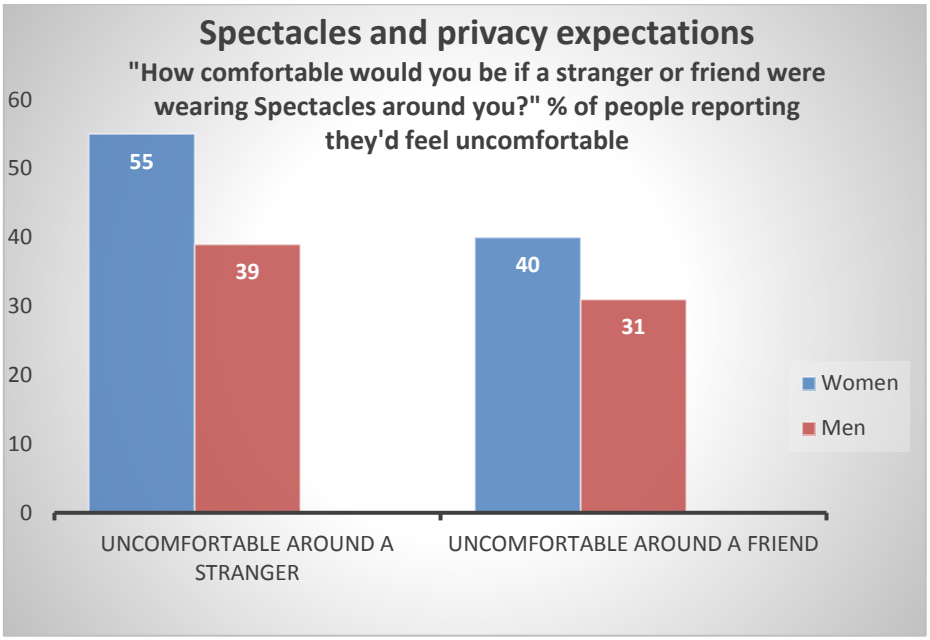

Figure 51: Perceived intrusiveness of Spectacles smart glasses

A second version of Spectacle[35] was launched in the USA in April and in Europe in May 2018. The new version aims to be even more convenient and fashionable.

6.4 Early-stage initiatives

Not surprisingly, other manufacturers are currently paying a closer look to the growth of the IoT, as well as to smart glasses in particular.

According to Bloomberg[36] and other media[37], *Apple Inc.* may be currently exploring the possibility to develop such a device, starting to engage with suppliers and stakeholders. In 2016, Microsoft started offering its product Hololens, but only aiming at developers.

Amazon wants to take on *Google Glass* and *Hololens*. Currently,[38] it is working on a pair of smart glasses powered by its artificial intelligence assistant *Alexa*. Amazon's smart glasses as announced won't feature a camera, helping to overcome privacy concerns.

Intel plans to release in 2018 AR smart glasses indistinguishable from ordinary glasses[39]. These smart glasses will be hands-free and they will rely on a mixture of voice controls, AI, head motions and lasers and will also not feature a camera.

Furthermore, *Facebook'*s Chief Executive Mark Zuckerberg, who recently stated[40] that smart glasses will be widely available within a decade, told Fortune[41] that its virtual reality company *Oculus* is indeed looking at opportunities to minimize customers' expenses for their future products.

7 Legal considerations

From the analysis of their technical features and the different use cases, it is evident that smart glasses can perform a number of operations on different types of data:

- recording audio and video material, or combined audio-visual,
- recording other sensor data such as location (e.g. via GPS or Wi-Fi), movement, orientation etc., independently or correlated with audio or video recordings,

- store such recordings in the memory of the glasses device, if appropriate after aggregation, compression or other methods to reduce the needed storage space,
- transmit the recorded data over a network to other computers,
- analyse the data to extract certain information elements on the glasses device, e.g. to identify objects in a visual context, or determine the device's position on a map,
- receive data from another computer, which could be related to the processing of data previously transmitted from the glasses device or selected by a different algorithm,
- feed data from local processing or received from elsewhere back to the user, through visual or audio output,
- erasing data on the device.

These building blocks allow the development of complex and powerful applications and systems. Not all scenarios include the processing of personal data, e.g. a glasses application may be developed to help a technician to identify the parts of a complex machine and assess their state of functioning, but a high number of scenarios are likely to concern the processing of personal data, either as their central function or in the context of other functions.

At the latest since the CJEU judgement in the *Ryneš* case on the use of a CCTV camera installed by an individual in a family home, it has been clear that the recording of images of individuals constitutes the processing of personal data[42].

Where the use of smart glasses includes the processing of personal data, they must be operated in compliance with the applicable law which includes the relevant data protection law (such as the general Data protection regulation – GDPR – in a European context). Depending on other characteristics of the glasses device or the services to which it is connected, also the ePrivacy legislation, legislation on terminal devices and radio equipment and other specific legislation may apply.

Since the introduction into the market and the subsequent withdrawal of *Google Glass*, the European Parliament and the Council have adopted the GDPR. The GDPR lays down principles for the fair and lawful processing of personal data, which include transparency, the requirement of a valid legal base for a processing operation, purpose limitation, data minimisation, limitation of data retention, data quality and security, rights of the data subjects and independent supervision. The GDPR clarifies the responsibilities of the controllers and processors and introduces the principle of accountability as an overarching obligation to strive for compliance not only with the letter of the law. It also provides concrete instruments and tools to achieve accountability, with a risk based approach implemented inter alia in data protection impact assessments (DPIA), data protection by design and by default, nomination of data protection officers as well as codes of conduct and certification.

With these principles and this toolkit, it is first and foremost the controllers and to some extent processors that will have to assess the impact of any intended operation using smart glasses for the processing of personal data, whether a formal DPIA is legally required or not.

Supervisory authorities may be consulted in the assessment process. They would also have to take a position via the European Data Protection Board on any codes of conduct or certification schemes, in particular those of EU wide importance. Such initiatives by controllers or their associations, or investigations triggered by complaints or own initiative[43], or requests from the Commission may trigger the supervisory authorities to develop more specific guidance on certain applications of smart glasses.

The application of data protection principles to video recordings as such has been already the subject of case law concerning other technologies (e.g. dash cams, CCTV, facial recognition systems) and some of the principles from these cases can be applied to smart glasses and help to assess the conditions under which smart glasses could be legally used in the European Union.

More severe risks to privacy and data protection could derive from the use of smart glasses by law enforcement authorities, as experimented already in some third countries, e.g. China.

Smart glasses, like any device enabling facial recognition, have the potential to be a really useful crime fighting tool. However, the use of facial images, especially in public places, is very intrusive for individual freedoms, especially because images (and other biometric data) can be captured without the data subject being aware. In a democratic society, such difficult balances between public benefit and individual fundamental rights (privacy and data protection) must not be decided by the police, but by Parliament through informed debate and legislation[44].

In case they are asked to adopt legislation enabling law enforcement use of smart glasses, legislators at EU and national level should bear in mind the need to perform a necessity and proportionality test applying the criteria of the necessity toolkit[45] elaborated by EDPS.

As regards the use of smart glasses and similar devices in the private sector or in other administrative functions than in the area of justice and security, in principle the current legislation provides a robust framework. The enhancement of the capabilities and the expected massive rollout of sensor-equipped connected devices will, however, cause a significant increase of the amount and the sensitivity of personal data which becomes available in the devices and the networks that connect them. This development is another compelling reason to complete the adaptation of the EU's legal framework for the protection of privacy and personal data. First and foremost, this requires the rapid adoption of an ePrivacy Regulation with robust safeguards against uncontrolled use of privacy intrusive operations on networks and connected devices.

Another requirement for effective protection of the fundamental rights of individuals to the privacy and the protection of personal data is effective enforcement of the laws. It is important that the supervisory authorities are equipped with the necessary resources and expertise to effectively exercise their tasks in view of rapid and important developments.

8 Conclusion

Smart glasses are a particular class of IoT devices. In consequence, the processing of personal data and its transmission to the Internet yields similar data protection implications as already discussed in Article 29 Data Protection Working Party Opinion 8/2014. Data protection legislation (among others) is fully applicable and several privacy concerns have to be evaluated in their application and appropriate measures have to be applied in every different context.

However, due to the high number of sensors, and the fact that they are worn as ordinary glasses, smart glasses allow to record much more data from the physical world than others IoT devices. One can expect for the future that the number of sensors and the quality and quantity of captured data will further increase. Furthermore, technological improvements will contribute to apply near interruption-free use and less and less intrusive designs resembling ordinary glasses.

In order to assess their contribution to surveillance measures, an assessment should also take account of other technological developments which increase the availability of video recordings of persons in the public space, such as CCTV cameras, dash cams, but also the video recordings that drones and autonomous vehicles will take for their operation and to provide evidence in case of accidents.

At the current stage of the development, the completion of the revised data protection framework by the adoption of an **ePrivacy Regulation** with robust safeguards and full and effective application of existing **legislation**, first and foremost the **GDPR**, appears more important than launching new legislative initiatives which would address specific technologies.

---

[1] Philipp A. Rauschnabel, Alexander Brem, Bjoern S. Ivens, Who will buy smart glasses? Empirical results of two pre-market-entry studies on the role of personality in individual awareness and intended adoption of Google Glass wearables, In Computers in Human Behavior, Volume 49, 2015, Pages 635-647, ISSN 0747-5632, https://doi.org/10.1016/j.chb.2015.03.003.

[2] European Commission, Study "Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination", Final Report, p. 18, https://ec.europa.eu/digital-single-market/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination

[3] https://electrek.co/2018/12/11/tesla-google-glass-ar-factory-workers/

[4] Article 29 Working Party, Letter addressed to Google regarding Google Glass, a type of wearable computing in the form of glasses, 2013, https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130618_letter_to_google_glass_en.pdf.

[5] IWGDPT, Working Paper on Privacy and Wearable Computing Devices, 2014, https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2015/28042015_en_2.pdf .

[6] https://www.priv.gc.ca/en/opc-news/news-and-announcements/2013/let_130627_google/

[7] http://www.bbc.com/news/world-asia-china-42973456,

[8] https://techcrunch.com/2018/02/08/chinese-police-are-getting-smart-glasses/

[9] e.g. US Library of Congress, Global Legal Monitor, 1 July 2017, Germany: Bodycams for Federal Police Officers, http://www.loc.gov/law/foreign-news/article/germany-bodycams-for-federal-police-officers/

[10] J. Hong, "Considering privacy issues in the context of Google glass." Communications of the ACM, ACM, vol.56, no.11, pp.10-11, November 2013.

[11] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

[12] A deep analysis of hacking techniques and bugs is provided extensively in http://www.saurik.com/id/16

[13] http://www.npr.org/sections/alltechconsidered/2013/07/17/202725167/clever-hacks-give-google-glass-many-unintended-powers

[14] S. Safavi, Z. Shukur. "Improving Google glass security and privacy by changing the physical and software structure," Life Science Journal, vol.11, no.5, pp.109-117, 2014.

[15] https://www.vs.inf.ethz.ch/edu/FS2014/UCS/reports/MaricaBertarini_SmartGlass_report.pdf

[16] https://proceedix.com/devices/smart-glasses?gclid=EAIaIQobChMIqLHwo4vZ1gIVqbftCh3aKwLMEAMYASAAEgJBE_D_BwE

[17] http://www.gartner.com/newsroom/id/2618415

[18] https://www.rrmediagroup.com/News/NewsDetails/NewsID/11654

[19] While plans were reported for the Brazilian police to use smart glasses at international sports events in Rio de Janeiro in 2014 and 2016, there is no indication if these plans were ever implemented.

[20] Brandon Carte, USA TODAY, Feb 17, 2014, Police departments have their eye on Google Glass, https://eu.usatoday.com/story/tech/2014/02/12/us-police-consider-google-glass/5341597/

[21] Jon Russell, TechCrunch, 8 February 2018, Chinese police are using smart glasses to identify potential suspects, https://techcrunch.com/2018/02/08/chinese-police-are-getting-smart-glasses/?guccounter=1

[22] https://www.khaleejtimes.com/news/crime/soon-smart-glasses-to-catch-criminals-wanted-vehicles-

[23] The network TV program Black Mirror explored possible effects of recording and reviewing personal perceptions with technological means in its episode The Entire History of You, http://www.theneuroethicsblog.com/2017/08/the-neuroethics-blog-series-on-black_8.html

[24] Goldman, David (April 4, 2012). "Google unveils 'Project Glass' virtual-reality glasses". Money. CNN. Retrieved April 4, 2012. https://money.cnn.com/2012/04/04/technology/google-project-glass/

[25] http://www.forbes.com/sites/greatspeculations/2012/04/05/google-glass-sound-as-crazy-as-smartphones-and-tablets-once-did/#4ceacbf35b74

[26] https://www.smallworldsocial.com/wp-content/uploads/SWS-Breastfeeding-Press-Release.pdf

[27] http://www.uab.edu/news/latest/item/3896-uab-does-virtual-surgery-with-vipaar-and-google-glass

[28] Cahiers IP, Innovation et prospective, No. 2, CNIL 2014, p. 19, https://www.cnil.fr/sites/default/files/typo/document/CNIL_CAHIERS_IP2_WEB.pdf

[29] https://www.dezeen.com/2015/11/30/google-patent-bendy-google-glass-style-device-wearable-technology/

[30] http://www.philipprauschnabel.com/wp-content/uploads/2016/04/Result-for-respondents_download.pdf

[31] https://www.wired.com/2016/01/carl-zeiss-smart-glasses/

[32] https://www.spectacles.com/

[33] http://www.theverge.com/2016/9/23/13039184/snapchat-spectacles-price-release-date-snap-inc
[34] https://today.yougov.com/news/2016/09/28/snapchat-spectacles-privacy-problem/
[35] https://techcrunch.com/2018/04/26/snapchat-spectacles-2/?guccounter=1
[36] https://www.bloomberg.com/news/articles/2016-11-14/apple-said-to-explore-smart-glass-in-deeper-wearables-push
[37] http://uk.businessinsider.com/apple-is-working-on-smart-glasses-2016-11?r=US&IR=T
[38] http://www.mirror.co.uk/tech/amazon-working-pair-google-glass-11207169
[39] https://www.techradar.com/news/intel-vaunt
[40] http://www.dailymail.co.uk/sciencetech/article-3536408/The-bots-coming-Mark-Zuckerberg-shows-Facebook-s-smart-AI-assistants-says-smart-augmented-reality-sunglasses-available-decade.html
[41] http://fortune.com/2016/10/06/facebook-virtual-reality-headset-invest/
[42] CJEU Judgement of 11 December 2014 in case C‑212/13 *František Ryneš v Úřad pro ochranu osobních údajů*, ECLI:EU:C:2014:2428.
[43] http://www.teinteresa.es/tecno/Entrevistas-Google-Glass_0_881912492.html
[44] https://www.gov.uk/government/news/metropolitan-polices-use-of-facial-recognition-technology-at-the-notting-hill-carnival-2017
[45] https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf