

# Client Alert

---

27 June 2014

## Google Glass into Europe - A Small Step or a Giant Leap?

By Susan McLean and Ann Bevitt

Google Glass ("Glass") is the most high profile of the new wearable technologies that commentators predict will transform how we live and work.

Until now, the Android-powered glasses were only available in the U.S. However, as of this week, Glass has been launched in the UK. Now, if you are 18 years old, have a UK credit card and address and a spare £1,000, you can purchase your own Glass and see what the fuss is all about.

Google has stated that it selected the UK for its second market because "*[the UK] has a history of embracing technology, design and fashion and ... there's a resurgence happening in technology in the UK*". But perhaps it is also because the UK's data protection regulator, the Information Commissioner's Office (ICO), has a reputation for being one of the more pragmatic privacy regulators in Europe. Because, for all its exciting technological benefits, Glass raises some thorny legal issues, in particular in relation to privacy. In this alert we will address some of those key issues.

### WHAT IS GOOGLE GLASS?

As many readers will already be aware, Glass is a form of wearable technology that gives its users hands-free access to a variety of smartphone features by attaching a highly compact head-mounted display system to a pair of specially designed eyeglass frames. The display system connects to a smartphone via Bluetooth. Glass can run specialised Android apps known as "Glassware". In its current form, Glass can pull information from the web, take photographs, record videos, make and receive phone calls (via the Bluetooth smartphone connection), send messages via email or SMS, notify its user about messages and upcoming events, and provide navigation directions via GPS. Although Glass is still in the testing stage and boasts only a modest set of features, the prototype device has already caused quite a stir. In particular, it has some triggered significant privacy concerns.

### PRIVACY

In terms of privacy, Glass throws up a variety of issues. Due to its functionality, Glass is likely to process two types of data relating to individuals: (i) personal data and meta data relating to the wearer of the Glass ("Glass User") and (ii) personal data and meta data relating to any member of the general public who may be photographed or recorded by the Glass User ("Public"). In June 2013, a group of regulators and the Article 29 Working Party, wrote to Google inviting Google to enter into a dialogue over the privacy issues relating to Glass. The letter pointed out that the authorities have long emphasised the importance of privacy by design, but added that most of the authorities had not been approached by Google to discuss privacy issues in detail. In Google's response it stated that protecting the security and privacy of users was one of its top priorities. Google also identified various steps that it has taken to address privacy concerns, including a ban on facial-recognition Glassware.

# Client Alert

---

## PERSONAL DATA OF GLASS USER

As with any smartphone, Google will collect personal data and other meta-data relating to each Glass User. Google will need to comply with its obligations under the UK's Data Protection Act 1998 (DPA). A key element of such compliance will be putting in place an appropriate privacy policy for Glass Users. However, to date, Google has encountered some difficulties in this regard.

Indeed, in July 2013, the ICO wrote to Google confirming that Google's updated privacy policy raised serious questions about its compliance with the DPA. In particular, the ICO believed that the updated policy did not provide sufficient information to enable UK users of Google's services to understand how their data will be used across all of the company's products. It stated that Google must amend its privacy policy, and failure to take necessary action would leave the company open to the possibility of formal enforcement action.

Google has argued consistently that its privacy policy complies with EU data protection law. To date, no formal action has been taken by the UK, although Google has faced action elsewhere in Europe (e.g. in [Spain](#)).

## PERSONAL DATA OF PUBLIC

Glass Users who take photographs or video/audio footage of the Public in a recreational capacity will not be subject to the DPA because they can rely on the "domestic purposes" exemption. However, if Glass Users take photographs or footage for work purposes, their employers will need to ensure compliance with the DPA (see below).

Google states that Glass was designed with privacy in mind and argues that Glass poses no greater privacy risk to the Public than a smartphone with inbuilt camera. However, critics point out that taking a photograph or video/audio footage with a smartphone is very different from taking a photograph or video footage with a more discreet wearable device like Glass. Further, the Bluetooth connection between Glass and the Glass User's smartphone allows the possibility of real-time facial recognition, which raises a more detailed set of privacy concerns for the person identified (for example, his/her identity and location will be logged by the technology provider in the form of meta-data, whether he/she consents or not).

In response to these concerns, Google appears to be taking steps to implement changes to protect privacy. Google announced on June 3, 2013, that it would not allow applications with facial recognition on Glass. However, banning facial-recognition apps does not address the concern that people photographed or videoed by a Glass User, whether in a "zone of privacy" or in a public place in which there is no reasonable expectation of privacy, might not know what has happened. To deal with this point, Glass does limit a user's ability to take photos to cases where the Glass User either speaks an audible command or makes a visible swipe on the device's tactile sensor, and limits video recordings to 10 seconds in length without a Glass User holding on to the tactile sensor.

Accordingly, as it is with smartphones today, we expect that the use of Glass in public spaces will need to be regulated via a combination of: (i) social norms; and (ii) rules enforced by the businesses operating in those spaces. Indeed, in the U.S., various establishments (including restaurants, bars, cinemas and casinos) have, to date, banned the device from their premises and it has been reported that certain UK cinemas, gyms and cafes

# Client Alert

---

are planning to implement rules about the wearing of Glass in their establishments. Google has itself published a guide for Glass users entitled "*How not to be a Glasshole*".

## GLASS IN THE WORKPLACE: KEY ISSUES FOR COMPANIES

For some time commentators have identified a variety of potential uses for Glass in the workplace. The benefit of having access to information on a hands-free basis could be hugely advantageous to a variety of workers, including medical professionals and fire officers. There are also clear advantages for certain professionals, such as police officers and security guards, to be able to make contemporaneous recordings whilst on duty. But with Virgin Atlantic Upper Class staff recently conducting a trial use of Glass, its potential application in the workplace is far broader than you might initially anticipate.

Indeed, earlier this month Google launched the first round of its 'Glass at Work' programme, which is intended to encourage the development of Glassware in the form of enterprise applications. Its first partners include the provider of content for live broadcasts and context-aware applications for the sports, entertainment, building/security and medical industries; a provider of museum guides; and the provider of apps for the energy, manufacturing and health care sectors.

Any company implementing Glass at Work will need to ensure that it complies with its obligations under the DPA, in terms of the processing of personal data relating to both employees and third parties. Note that although there is currently no specific guidance from the ICO on Glass (or any wearable tech, generally), there is some (currently draft) guidance which affects "body worn video cameras". This guidance is in the form of a revised CCTV code of practice which was launched by the ICO for consultation at the end of May 2014 ("Code"). The consultation concludes on 1 July 2014. This guidance is not directly on point, but offers some high level direction.

Despite the absence of specific guidance from the ICO or any regulator, there are key issues that any organization should take into consideration in light of the new wearable technologies that are proliferating:

- Ensure data protection compliance:
  - carry out a privacy impact assessment to ascertain whether use of Glass is justified, necessary and proportionate, as opposed to less privacy-intrusive alternatives;
  - take a "privacy by design" approach. If Glass is identified as the most appropriate equipment for your purposes, ensure that its use is restricted so that it does no more than is necessary for its specified purpose;
  - establish who has responsibility for the control of information, e.g. deciding what is recorded, how the information should be used and to whom it may be disclosed;
  - ensure that appropriate privacy notices are provided to individuals who may be recorded;
  - avoid using Glass to record audio, as this is unlikely to be justified;
  - delete information as soon as it is no longer required;

# Client Alert

---

- where any personal data collected via Glass is to be shared with third parties, ensure that appropriate contractual arrangements are put in place; and
- regularly review whether use of Glass continues to be justified.
- Make all necessary adjustments to contractual documentation to take account of the use of Glass, including the collection of personal data and meta-data via the device.
- Put in place policies which make clear when and where Glass can be worn and which prohibit covert recording, and carry out all necessary training on these. For example, as with smartphones, there may be some particularly sensitive buildings or locations where Glass is not permitted.
- Put in place appropriate technical security measures to protect the personal data and other sensitive information collected via Glass.
- Have in place appropriate procedures to wipe Glass if stolen or lost.
- Monitor use of Glass by employees and ensure that all Glass are returned prior to employees leaving the company.
- Take steps to ensure that confidential information and intellectual property is not compromised as a result of the use of Glass in the workplace.

## CONCLUSION

The market for wearable tech has grown significantly in the last few months, and all the signs are indicating that it is going to keep on growing. Glass is just the next step in this market which now also boasts smart-watches, rings, brooches and other wearable devices. Google is testing the waters in the UK and, despite the significant concerns referred to above, it seems very likely that this “small step” from the U.S. to the UK is going to lead to a “giant leap” in the spread and take-up of wearable technology.

## Contact:

**Susan McLean**

+44 (0)20 7920 4045

[smclean@mofo.com](mailto:smclean@mofo.com)

**Ann Bevitt**

+44 (0)20 7920 4041

[abevitt@mofo.com](mailto:abevitt@mofo.com)

# Client Alert

---

## **About Morrison & Foerster:**

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's* A-List for 10 straight years, and *Fortune* named us one of the “100 Best Companies to Work For.” Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at [www.mofo.com](http://www.mofo.com).

*Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.*