Improving Google glass security and privacy by changing the physical and software structure

Seyedmostafa Safavi [1]*, Zarina Shukur [2]

[1,2.] Unit of Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia,43600 Bangi, Malaysia; E-Mails: Safavi@takhosting.info

Abstract: Following the exciting first reactions, Google Glass has encountered seriously criticism, due to the perceived threats to security and privacy. Cyber security is one of the most serious threats, both to private users and business enterprises. At present, Google Glass makes it easy for cyber hackers to gain access to our personal data, banking and credit card details, passwords or personal identification numbers. After conducting literature review and simple questionnaire survey in which 35 Glass owners and 30 privacy managers from the US took part, we analyzed the collected data to point out the weakness of the device. The response rate visibly showed problem of user privacy in design of product (16.7% satisfaction on design to protect privacy). Based on these analyses, we proposed 6 essential improvements to Glass security and privacy by redesigning the features that currently pose a threat to privacy of Google Glass users and other party involved. We can thus view Google Glass as an opportunity to draw attention to modern privacy concepts. It is likely that, given that the risks associated with Google Glass are being widely discussed, the threats have been around for much longer.
[Seyedmostafa Safavi, Zarina Shukur. **Improving Google glass security and privacy by changing the physical and software structure.** *Life Sci J* 2014;11(5):109-117]. (ISSN:1097-8135). http://www.lifesciencesite.com. 15

Keywords: Improve Google Glass; Wearable Technology; User Authentication; Physical Security; Governmental Security; Firewall; Privacy; Crime; Improvement

1. Introduction

While the Federal Trade Commission (FTC) demands that the user privacy and security are ensured(Safavi et al. 2013), according to the work presented in the public seminar on the Internet of Things (Atzori, Iera, & Morabito, 2010), the industry seems to be focused on ensuring that Internet communication is integrated in all their products, from smart devices and mobile phones, to sensing elements in houses, motorcars, and automobiles (Lohr, 2013). According to Cisco, it is estimated that, by 2020, thirty-seven billion intelligent devices will be communicating to each other (Dave Evans, 2013). Hence, we are quickly approaching the stage where everybody and everything will be connected through the net (Thierer, 2013).

At present, technology is already available (Kopetz, 2011) to assist with remote supervising and screening (Jiang, Liu, & Yang, 2004) of wearable computing devices like Google Glass (Rodríguez-Martín, Pérez-López, Samà, Cabestany, & Català, 2013) and auto capturing and tracking devices, as well as sensor material (Gobioff, Ghemawat, & Leung, 2003). Google Glass is essentially a wearable display utilizing the phone screen technology with an inbuilt powerful camera. The screen comes with automatic face detection and eye tracking technique, which may assist when walking by providing directions, as well as be used to record video film. Presently, only a small selection of developers and users can purchase Glass for $1500, and the full release is expected by end of year 2014.

1.1 Positive Points on Wearing Google Glass

Wearable devices, such as watches, eyewear, belts and rings, have been very popular among technology enthusiasts, as they are easy to use, leaving the hands free. Thus, it is possible to perform multiple tasks simultaneously while using the device. The most important points of using Glass for owner as well as 3rd parties are:

- **Wearable Computing:** Wearable electronic devices, especially Google Glass, may enable the users to utilize the sensors in an inappropriate way. Moreover, integrating this part of science into our everyday urban lives would irrevocably change our perception of the world, and infringe on our privacy, whereby we would have very few means of protecting our personal identity (Wu et al., 2012). Already, mobile technologies have allowed others, even complete strangers, to invade our private lives.
- **Protected Device:** The wearable device is worn on the user's face, allowing him/her to utilize it while performing other tasks. The most important aspect of Google Glass is its ease of use, as in difficult situations, such as war coverage, the wearer can simply look in the direction he/she wants to record. If the person needs to take cover or change position, he/she does not have to stop the recording. This is the main advantage of currently available wearable computing devices.

- **Advertising and Glass:** The popularity, and thus profitability, of such devices is very easy to envisage. For example, advertisers might tap into the technology to access information on user's purchasing habits, personal interests, and much more. Subsequently, they can use this information to advertise related products, thus enticing the consumers to purchase their merchandize (Shaikh et al., 2010), (Modares, Moravejosharieh, & Salleh, 2013).

1.2 Glass Vulnerability

At present, Google Glass does not have a secure enough PIN system or authentication in place. Skilled hackers have found out that this technology has a "root" characteristic, which may be accessed by connecting it to a personal computer or a laptop computer and passing certain programming commands to it. Based on these shortcomings, in this work, we have divided Google Glass vulnerabilities into two sections. In the first part, we describe how Glass may be met with a harsh reaction from the society, while in the second part, we elaborate on the experience using the Glass, revealing how it may infringe on the owner's safety and privacy.

- Privacy issues for 3rd party: The main issue associated with the usage of Google Glass pertaining to 3rd party is that this person may inadvertently be identified/recorded by the device. As the device can be easily programmed to recognize the faces and record the footage containing video and voice recording, the implications to those around the wearer are obvious. (Bialas, 2011) At present, there is no mechanism that can safeguard those recorded by the Glass (shown in Figure 1).
- Privacy issues for Governments: The ease with which the information can be recorded and transmitted by the Glass may threaten national security (as shown in Figure 1), as antisocial factors will be able to instantly share sensitive or restricted data in order to conduct illegal activities, or gain access to restricted data pertaining to all governmental organizations. On the other hand, governments may use the device to spy on others, whereby the role of such individuals changes from that of a passive participant in an abstract recollection, to that of a first-person participant. It is thus possible that such technology would create a state of Uberveillance (Michael & Clarke, 2012).
- Privacy issues for the device owner: As shown in Figure 1, Google Glass owners presently face four privacy concerns described below (Preibusch, 2013). Firstly, the device user may be unknowingly recording data that may have serious implications. For example, one of the applications built into the Google Glass can track the wearer's progress while exercising. Thus, while such information may have practical and beneficial value when shared with the doctor, if accessed by insurance company, it could affect the owner's insurance premium. Secondly, one of the main envisaged usages of Google Glass and similar gadgets is recording video of the wearer's surroundings, and thus others within the scene. This brings many questions regarding the appropriateness of such technology, as it infringes on privacy of those that are involuntarily included in the footage. Thirdly, Google Glass tracks the owner's eye movements and uses retinal recognition to authorize the smart device to gather data without asking for explicit permission. However, changes in the size of the pupil can be used to infer someone's affinity toward a product or another person. For instance, these changes can be used to detect the products the wearer is most attracted to and later use this information in advertising. Since the wearer is not conscious of these involuntary reactions of his/her body, Glass can, without the owner's consent, transmit this data to a third party. Thus, rather than serving the owner, the device can actually benefit others (Keith, Thompson, Hale, Lowry, & Greer, 2013). Fourthly, it is likely that the Glass owner will not always be diligent in switching off the gadget while typing the ATM PIN numbers, passwords, reading bills, and registering tax information. This information can thus become readily accessible to hackers, who will use Glass to record the personal data of its owner for future misuse.

1.3 Some supported cases on Glass privacy vulnerabilities

To highlight the privacy treats associated with wearable devices, such as Glass, we are presenting several cases that were reported at the time of Glass release. For example, Michael DiGiovanni created Winky—an application that enables the Google Glass owner to shoot a photo via Glass camera with a wink of an eye (Google Glass, 2013). Therefore, this is a clear violation in the new edition of Glass, despite the Google announcement that the Company will not allow any changes to the way they envisaged photo or video capture.

In addition, it is currently possible to use QR code to force the gadget to use malicious wireless local area network access point or a Bluetooth connection (Hacking the Internet of Things for Good, 2013). However, this error in the configuration was discovered by Lookout Security, which informed Google and the issue was resolved in a timely

manner. Still, we should be aware that not all issues are easily detectable, and many that are cannot be quickly addressed by updating the underlying code. Glass privacy vulnerability is further exemplified by Chris Barrett (a movie maker), who was recording fireworks party in Wildwood, N.J., and accidentally recorded an arrest (The first arrest filmed on Google Glass, 2013). While this feature may be beneficial to the authorities, it also raises concern regarding the role of citizens in upholding the law.

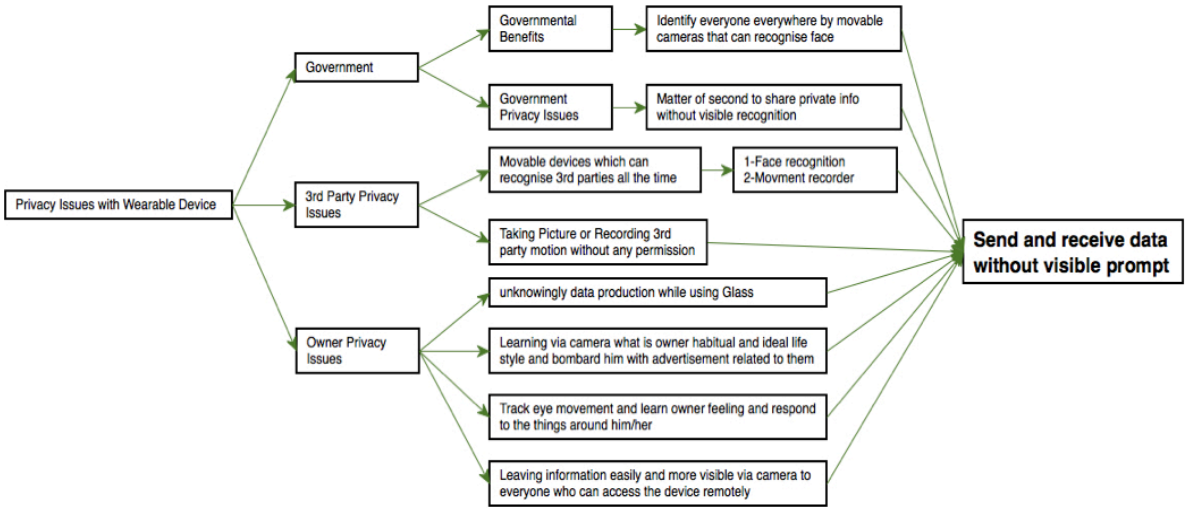


Figure 1: Privacy Issues with Wearable Devices

Tech profession considers that Barrett has registered first arrest caught on Google Glass with help of device camera designed to take short movies. This movie may indicate that Glass from Google can elevate the citizen journalism to the next stage because the glass is far less visible than a hand-held camera and may go unnoticed by the casual observers.

2. Glass Privacy Issues

One of the main concerns regarding Google Glass is that the device is capable of recording pictures and videos that may erode our security and privacy. Google designers have tried to answer to these concerns by making Glass small screen visible while trying to work with it. For instance, to take a picture or record a video with Google Glass, the users currently need to give voice command or tap the Glass. However, hackers are testifying that it is possible to re-engineer Google Glass to operate in the way it was not intended (HENN, 2013). It is thus evident that the potential for misuse of this and similar devices in tremendous, calling for further examination of the role of privacy in the digital age (Arun, Rajeesh, & Thampi, 2013).

2.1 Fighting Glass in Different Countries

As Google Glass is still in the testing and developing phase, its use has been outlawed in some countries around the world. In April 2013, letter, co-signed by ten privacy and information commissioners (from Israel, Canada, Mexico, Australia, New Zealand, Switzerland and European committee) (OAIC, 2013), raised eight questions related to privacy precautions in Google Glass. They asked about Glass and data gathering, the way Google was planning to use the information, and required more data on the Glass features, such as facial recognition.

The Congressman Joe Barton asked Google to release more data on the role of Glass within the Google privacy act and standards.

However, Google failed to fully address all the questions raised, in particular that pertaining to ensuring privacy of those in the vicinity of the Glass wearer. Barton stressed that Google must ensure that all individuals should have a right to secure their privacy.

In the response issued by Google, the CEO Eric Schmidt has dismissed the privacy concerns as insignificant and antiquated. According to Dwyer, “While the only bloodline of the existence of company is to sell data, we shouldn’t expect any priority to privacy of users” (Dwyer, 2011).

2.2 Google Response

In response to the issues related to the potential security breaches associated with Google Glass, Google initially announced that it would not allow facial recognition applications on Google Glass until “strong privacy protections” were in place (Co., G. Project Glass, 2013).

In the second stage, we envisage that Google will recall the devices issued to the first group of users, allowing them to replace them with the new versions, so that any physical vulnerabilities associated with prior releases will be eliminated via the device exchange (Co., G. Google Glass, 2013). In addition, Google announced that one of the top Company's priorities is ensuring that privacy of the users is protected. In that respect, they designed Google Glass so that the only way the owner can record using the device is by initiating the process using a sound or a tap, which is easily detectable by those around him/her.

Finally, Google assured the public that the product will only be released to the market if no issues remain after it has been properly tested, in particular the features most likely to affect mobile privacy and security.

For example, Google newly decided not to permit facial recognition applications for Google Glass because of the privacy implications. This is a good example of technology having to retract its goals due to the legal and societal implications.

3. Comparison of existing Glass with our suggested prototype

After conducting simple questionnaire survey in which 35 Glass owners and 30 privacy managers responded to 25 questions, quantitative data were drawn from it administered in United State of America. The survey consists of 25 privacy questions. The data analysis of the survey guided the development of the new proposed model that can cover main privacy issues with physical and software structure of the existing Google Glass. We analyzed the collected data, which allowed us to create a new framework for Google Glass privacy protection, thus bringing a number of improvements to the current Glass version.

Table 1 presents the comparison of the new prototype with the current Google Glass, as described in section 3 of this paper.

Table1: Comparison of the existing Glass with the proposed improved prototype

Privacy Sector	**Google Glass**	**Suggested Prototype**
User Authentication	None	Improved
Locking Mechanism	None	Improved
Notification	Available (kind of notification)	Improved
Physical Security	None	Improved
Governmental Security	None	Improved
Firewall	None	Improved

4. Proposed Privacy Protection in Google Glass

Following the analysis of the data provided by the first Glass owners, we are proposing an improved prototype Glass that can protect the privacy and enhance the device, allowing it to reach a much broader market. In addition, our approach can address the issues related to the Glass vulnerability we have previously identified, by adopting the solutions described below:

I. User Authentication: We are suggesting that Google Glass should introduce a type of auto-protect system, which brings identification functionality for Glass user (e.g., PIN authentication process, or some system based on bio-metrics, including an eye focus to open the lock, a retinal scan, voice scan, and so on)

II. Locking Approach: The Glass should incorporate auto cover, so that the user can use voice command (for example, OK GLASS LOCK / OK GLASS UNLOCK) to close it, shown in Figure 4, to ensure security of the Glass user.

III. Notification Approach: The response rate to the privacy questionnaire visibly showed problem of user privacy in design of Google Glass (16.7% satisfaction on design to protect privacy). We are suggesting modifying the Glass look features (as shown in Figure 2), whereby the notification that the device is turned ON is displayed for 5 seconds after shooting picture or a video. In Figure 3, we can see the proposed solution, whereby LED is positioned next to the camera, notifying the others that the camera has been used. In Figure 4, we demonstrate the functionality similar to that offered by Smartphone, whereby LED and Flash are combined, in addition to the 5-second safe zone that ensures privacy of passersby.

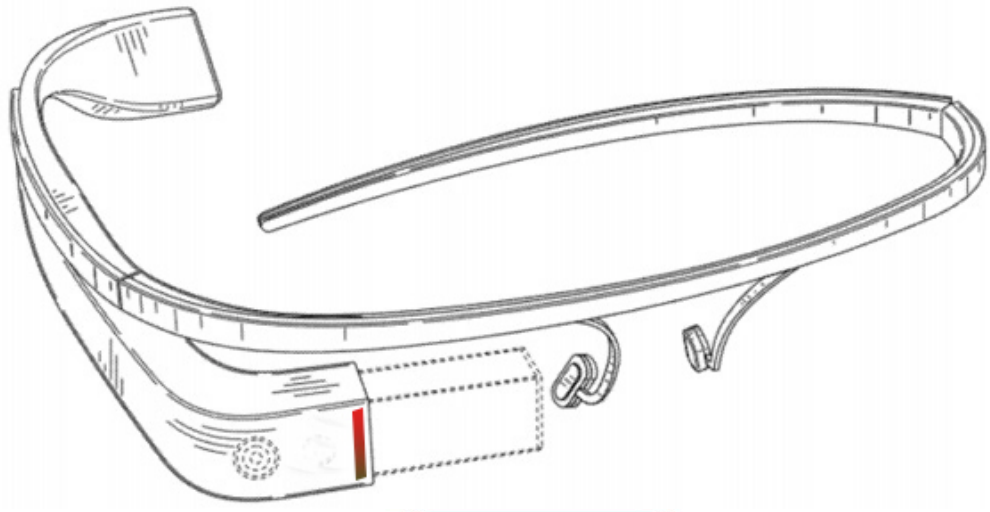
IV. Physical Security Approach: Because the Glass is something very personal, if the device is stolen, it would be useful if Google allowed the owners to use the MAC address to track the device (Zendehdel & Paim, 2013). In addition, we can improve the Glass access control and Media access control to the device by covering the physical security adjustment.

V. Governmental Security Approach: As shown in Figure 1, governmental issues are very realistic and, in order to mitigate these security breaches associated with the device, we are proposing that Google design and develop sensors that would prohibit usage of Glass devices in specific areas. It may also be feasible to allow only specific organizations to purchase the device for use in high-security situations. On the other hand, if we combine the cover prototype with this sensor, it may automatically close the cover, thus prohibiting recording. This functionality could also be achieved online, whereby an administrator could monitor

device usage and switch off any that are in prohibited zones.

VI. Firewall Approach: The Glass should incorporate a firewall system that would protect the owner from any unauthorized use. In such cases, it could, for example, close the camera cover, as well as notify the owner. This could be accomplished by device vibration, which would be a suitable and timely notification mechanism. Similarly, the device usage could be verified by checking the log file online by Google support team.

Figure 2: Showing Notification line for 5 seconds during and after taking picture or video with Glass



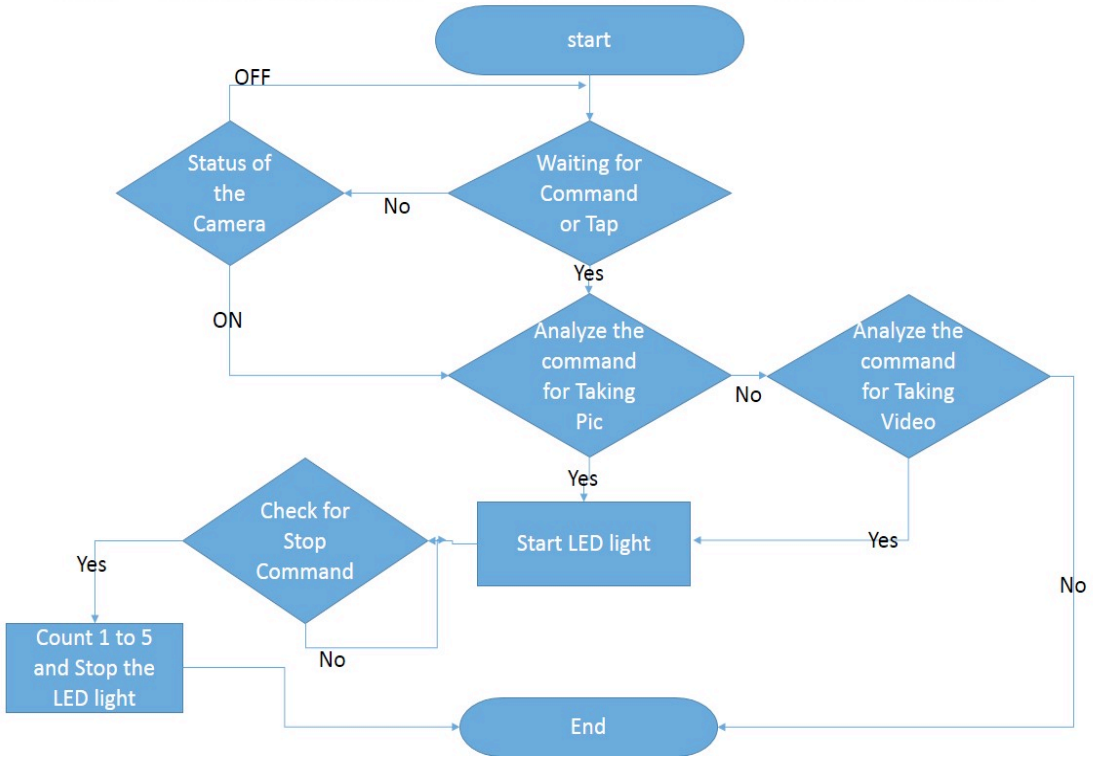
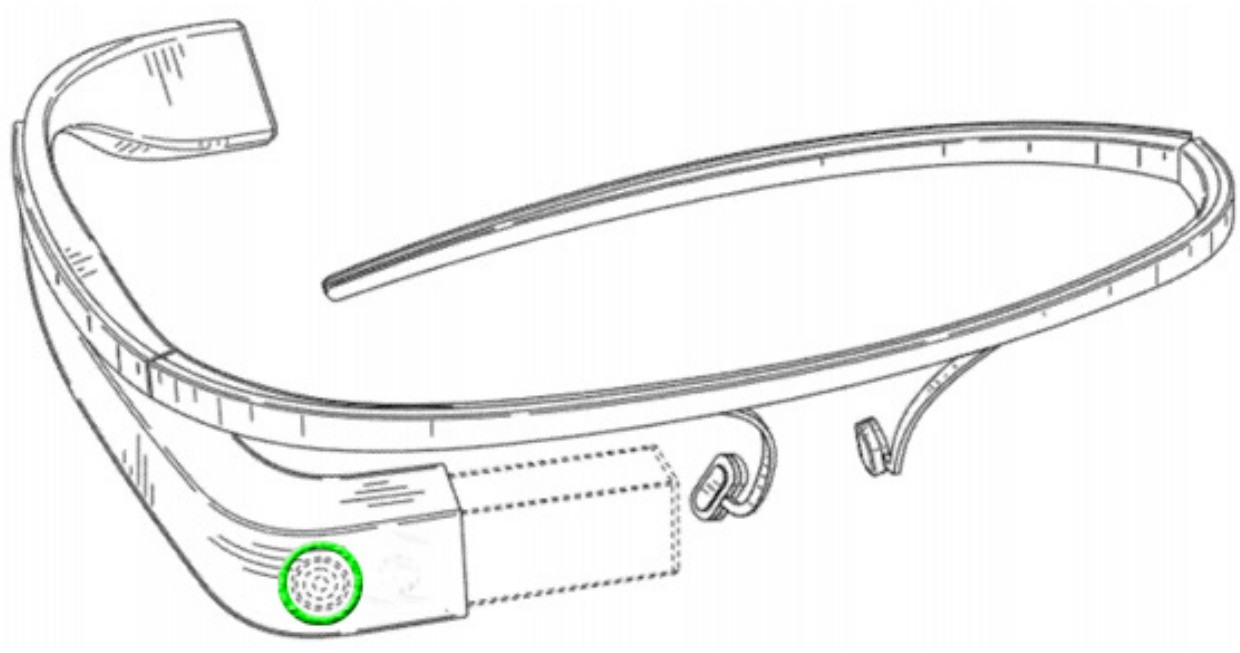


Figure 3: Showing LED notification that can stay on for 5 seconds after taking picture or video with Glass



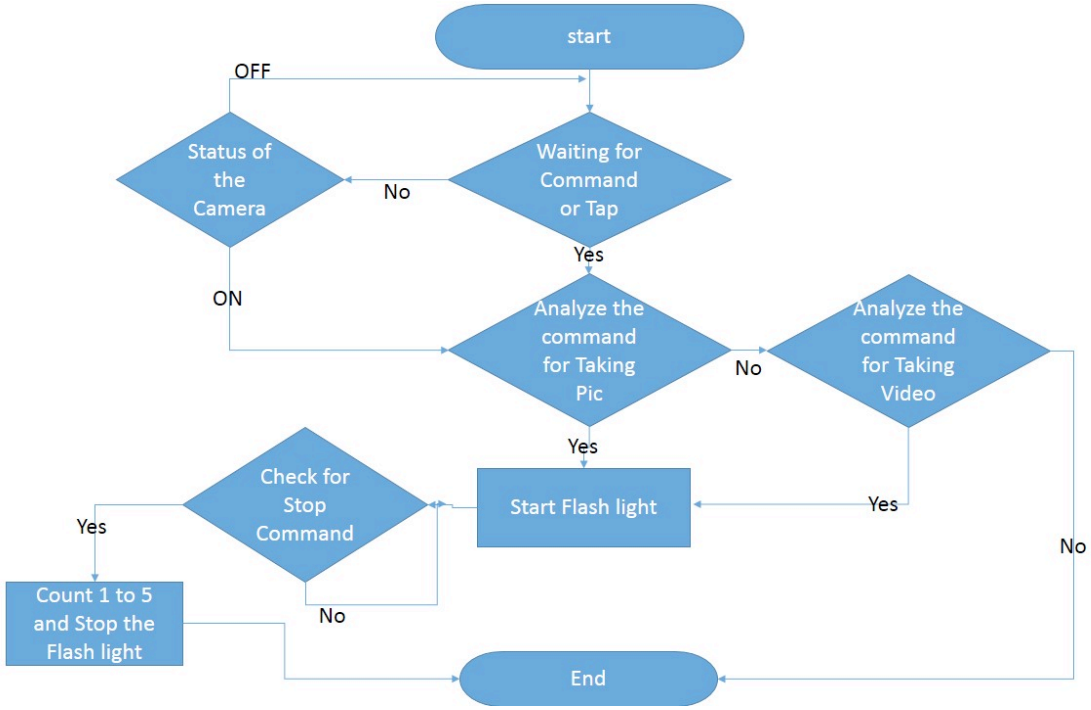
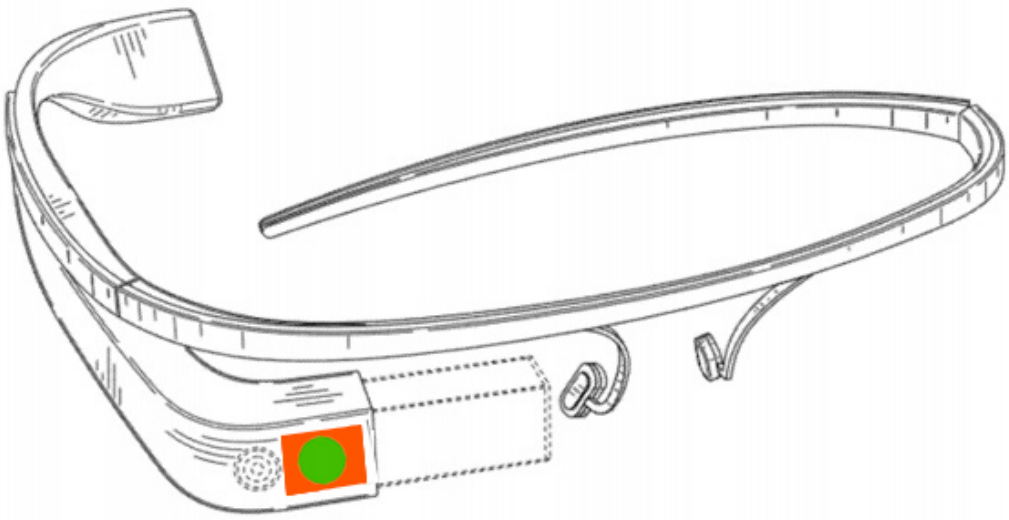
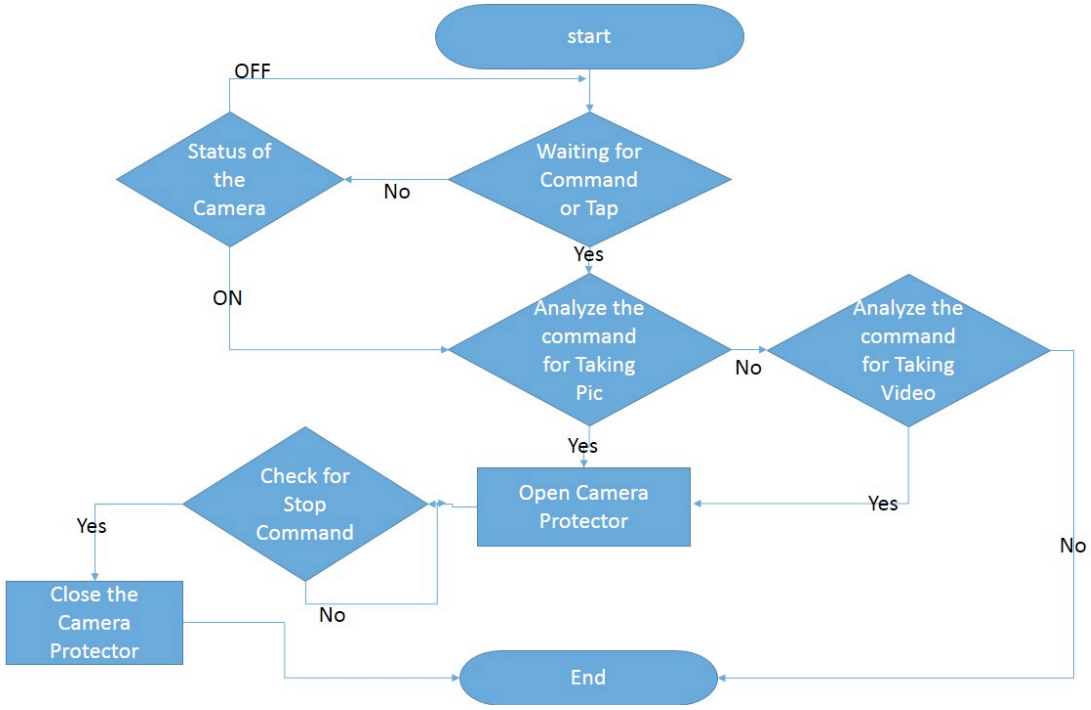


Figure 4: Showing Camera Protector that can cover the camera lens to stop the recording, as well as protecting its surface from any kind of damage





5.0 Conclusion

In this paper, we have improved security enhancement for Google Glass with the help of privacy related questionnaire responded by 35 Glass owners and 30 privacy managers, and result analysis from response rate to the privacy questionnaire visibly showed privacy issues in design of Google Glass and that is equal to 16.7% satisfaction on existing design of the device, and suggested to redesign in 6 privacy sectors to make this product more privacy acceptable in technological as well as political situations.

Improving our way of life by developing applications that can improve our communication as well as help with common everyday tasks is the goal behind every novel technology. However, while we cannot deny the utility of these innovations, many electronic applications and devices are gathering information about us, whether we are aware of it or not. While we have already given permission for our data being recorded, stored and used for various purposes, we must make every effort to prevent the misuse of private and sensitive information.

Presently, Google cannot reassure its users that their information is safe. Moreover, even if the Company takes every measure to make its products and applications safe and secure, it is likely that cyber criminals would eventually identify a way to breach security systems in place. That is the price we have to pay for the immense advancements in technology we have witnessed over the past few decades. Historically, potentially unsafe products were granted entry to the market, as although automobiles, guns, petrol, computing devices and so on, can potentially harm, their utility surpasses the associated risks. While the focus of this paper was Google Glass, the findings reported here are applicable to any device that can be potentially misused to infringe on the privacy of others. Thus, the entire wearable computing device sector must be mandated by law to incorporate design features that would prohibit such usage.

Policymakers should make sure that the rules governing the security are in place, rather than simply limiting Internet development and usage. It is better to let creation carry on, and address real damages as they develop.

Acknowledgements:

This research was supported by The National University of Malaysia (UKM) grant ERGS/1/2013/ICT04/UKM/01/1. We are very thankful to anonymous reviewers for their comments, reply and suggestions for Google Glass survey, which helps and improve the future researchers.

Corresponding Author:
Seyedmostafa Safavi
Unit of Cyber Security,
Faculty of Information Science and Technology,
Universiti Kebangsaan Malaysia(UKM),43600
Bangi, Malaysia.
E-mail: Safavi@takhosting.info

References

1. Safavi, S., Shukur, Z., & Razali, R. (2013). Reviews on Cybercrime Affecting Portable Devices. Procedia Technology, 11, 650-657.
2. Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer Networks, 54(15), 2787–2805.
3. Zendehdel, M., & Paim, L. H. (2013). Predicting Consumer Attitude to Use On-line Shopping: Context of Malaysia. Life Science Journal, 10(2).
4. Bialas, A. (2011). Common Criteria Related Security Design Patterns for Intelligent Sensors—Knowledge Engineering-Based Implementation. Sensors, 11(8), 8085–8114.
5. Dave Evans. (2013). Thanks to IoE, the Next Decade Looks Positively "Nutty." Cisco Blog. Retrieved December 11, 2013, from http://blogs.cisco.com/ioe/thanks-to-ioe-the-next-decade-looks-positively-nutty.
6. Dwyer, C. (2011). Privacy in the age of Google and Facebook. Technology and Society Magazine, IEEE, 30(3), 58–63.
7. Gobioff, H., Ghemawat, S., & Leung, S.-T. (2003). The Google file system. ACM SIGOPS Operating Systems Review. doi:10.1145/1165389.945450.
8. Google Glass: what it's like to use, by the inventor of the 'Winky' photo app http://www.theguardian.com/technology/2013/may/13/google-glass-winky-mike-digiovanni (accessed Dec 30, 2013).
9. Hacking the Internet of Things for Good. https://blog.lookout.com/blog/2013/07/17/hacking-the-internet-of-things-for-good/ (accessed Dec 30, 2013).
10. The first arrest filmed on Google Glass http://news.cnet.com/8301-17852_3-57592559-71/the-first-arrest-filmed-on-google-glass/ (accessed Dec 30, 2013).
11. The Office of the Australian Information Commissioner (OAIC) http://www.oaic.gov.au/news-and-events/statements/privacy-statements/google-glass/(accessed Dec 31, 2013).
12. Co., G. Project Glass https://plus.google.com/u/0/+ProjectGlass/posts/fAe5vo4ZEcE (accessed Nov 23, 2013).
13. Co., G. Google Glass http://www.google.com/glass/terms/ (accessed Nov 23, 2013).
14. HENN, S. (2013). Clever Hacks Give Google Glass Many Unintended Powers. Retrieved December 14, 2013, from http://www.npr.org/blogs/alltechconsidered/2013/07/17/202725167/clever-hacks-give-google-glass-many-unintended-powers.
15. Jiang, L., Liu, D.-Y., & Yang, B. (2004). Smart home research. In Machine Learning and Cybernetics, 2004. Proceedings of 2004 International Conference on (Vol. 2, pp. 659–663). IEEE.
16. Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. International Journal of Human-Computer Studies, 71(12), 1163–1173.
17. Modares, H., Moravejosharieh, A., & Salleh, R. (2013). Secure Connection in Mobile IPv6. Life Science Journal, 10(2).

18. Kopetz, H. (2011). Internet of things. In Real-Time Systems (pp. 307–323). Springer.
19. Lohr, S. (2013). A Messenger for the Internet of Things. New York Times. Retrieved December 11, 2013, from http://bits.blogs.nytimes.com/2013/04/25/a-messenger-for-the-internet-of-things.
20. Michael, K., & Clarke, R. (2012). Location Privacy Under Dire Threat As Uberveillance Stalks The Streets. Precedent (Focus on Privacy/FOI), (108), 24–29.
21. Preibusch, S. (2013). Guide to measuring privacy concern: review of survey and observational instruments. International Journal of Human-Computer Studies.
22. Rodríguez-Martín, D., Pérez-López, C., Samà, A., Cabestany, J., & Català, A. (2013). A wearable inertial measurement unit for long-term monitoring in the dependency care area. Sensors (Basel, Switzerland), 13(10), 14079–104. doi:10.3390/s131014079.
23. Shaikh, R. A., Jameel, H., d'Auriol, B. J., Lee, H., Lee, S., & Song, Y.-J. (2010). Achieving network level privacy in Wireless Sensor Networks. Sensors (Basel, Switzerland), 10(3), 1447–72. doi:10.3390/s100301447.
24. Arun, E., Rajeesh, J., & Thampi, R. K. (2013). Privacy Preserving Mobile Data Cloud With Sandboxing. Life Science Journal, 10(7s).
25. Thierer, A. (2013). Privacy and Security Implications of the Internet of Things. Available at SSRN 2273031.
26. Wu, H.-Y., Rubinstein, M., Shih, E., Guttag, J., Durand, F., & Freeman, W. (2012). Eulerian video magnification for revealing subtle changes in the world. ACM Transactions on Graphics (TOG), 31(4), 65.

3/5/2014