Master of Arts Thesis

For points of compromise between privacy and surveillance, a proposition of a rational system design for surveillance drone policing

MA Interaction Design Communication 15-16
London College of Communication
University of the Arts London

Youngjoon Kim
KIM14435747

5,024 Words

Contents

0.0 Introduction

> "I grew up with the understanding that the world I lived in was one where people enjoyed a sort of freedom to communicate with each other in privacy, without it being monitored, without it being measured or analyzed or sort of judged by these shadowy figures or systems, any time they mention anything that travels across public lines."
> - Edward Snowden

In early June 2013, top secret information was leaked by Edward Snowden, an American computer professional who worked at the Central Intelligence Agency (CIA), to the press through The Guardian. The US National Security Agency (NSA) had been collecting personal information, such as the telephone records, text messages, and e-mails, of more than tens of millions of Americans (BBC, 2014). By revealing the news, hostility towards the US government and the governments of various countries all over the world was aroused. A large number of people have been raising their voice to stop monitoring people to preserve privacy as a fundamental human right.

With the computer-based monitoring surveillance system, we are living in a massive "Big Brother" aviary. Monitored with camera surveillance technology, we are losing the right to be freed to be alone. Approximately 5.9 million closed-circuit television (CCTV) cameras in the UK have been installed, according to research by The British Security Industry Association (BBC, 2013). In the United States, up to 30 million CCTV cameras have been deployed, and these are shooting footage for four billion hours a week (Vlahos, 2009). All of us are being surveilled. There is nowhere we can hide.

The advocates of the camera surveillance believe that the system keeps us from the unexpected dangers such as brutal terrors and crimes. However, even though there are numerous CCTV cameras almost everywhere, in recent years, more frequently, many nations are suffering from cruel terrors and crimes by terrorists and extremists such as ISIS, Islamic State of Iraq and al-Sham, around the world. According to List of Islamic Terror: 2016 (The Religion of Peace, 2016), from 1st January to 16th July 2016, for just seven months, terror attacks have killed 11,774

personnel and injured 14,303 in 1274 times, which is an enormous number. In fact, media reports dealt with problems as to the lack of security after the November 2015 Paris attacks, such as BBC's “Paris attacks: Security flaws and challenges highlighted” (Corera, 2015) and CNN's “How 'glaring' intelligence failures allowed a second bout of terror in Paris” (Robertson, 2015).

It, in this sense, is adequate to have the following questions. Is the extensive camera surveillance system efficient as the number of the camera? Is it more significant than our privacy? Do not they commit the abuse of power by depriving the right to have freedom?

As main subjects, there are three chapters composed of the issue from mass camera surveillance to the methods keeping privacy against the indiscriminate monitoring system. The first section will begin with an introduction of the current state of camera surveillance as well as advanced tracking systems such as the Unmanned Aerial Vehicle (UAV) called a Drone. After that, the phenomenon of anti-surveillance will be introduced.

From here, we will move to the research on the relationship between surveillance and privacy, taking a broad view but with design as the focus. In this chapter, the form of design regarding maintaining privacy against surveillance will be a central topic.

Based on the previous chapter, and after research and analysis of the structure required to protect privacy, a new system will be proposed. Moreover, with the on-going development of high technology, in practice, surveillance drone policing will be used, as the futuristic background speculated.

Firstly, let us look at the state in terms of the form of camera surveillance.

1.0 On-going camera surveillance

1.1 The effects of camera surveillance

With the ever-increasing use of surveillance technology such as closed-circuit televisions (CCTV), body-worn video, number plate recognition systems (ANPR), and drones, we are monitored by the system wherever we are (Weaver, 2015). The surveillance system officially existed for the citizen. However, intrinsically, on account of monitoring many and unspecified individuals, it becomes "mass surveillance," which means that the entire or a substantial segment of the population is monitored and tracked by the government or unspecific private organisations (Privacy International, nd). Mass surveillance platforms are premised on a primary purpose: to collect everything. Mine it, utilise it, extrapolate from it, investigate connections and patterns, and suspect thoughts or words.

In the name of security, in 2011, the Police Community Support Officers (PCSOs), estimated that 1.85 million camera machines were installed across Britain, and one camera was for 32 people (Lewis, 2011). After two years, in 2013, according to The British Security Industry Authority (BSIA), there were up to 5.9 million CCTVs in Britain, and the UK has a CCTV camera for every 11 people (Barrett, 2013). The number of CCTVs had been dramatically increased in a short period. In the US, there are about 30 million cameras deployed, and the cameras are monitoring our activities for 4 billion hours a week (Vlahos, 2009). According to a report 'Video Surveillance Market - Global Trends & Forecasts to 2013-2020', the global video surveillance market is anticipated to grow from 11.5 billion dollars in 2008 to 37.7 billion dollars in 2015 (Kille and Maximino, 2014). The investing amount has tripled in the last seven years.

A controversial question, with the current state, has consistently been addressed as to the 'efficiency' of the camera surveillance. Is the camera security system, as an ever-increasing investment, even reliable? Based on a quotation from a city spokesman in Chicago, the city had 22,000 cameras on its network in 2013, and since 2006, the video surveillance has solved 4,500 crimes. By contrast, in the meantime, in 2010, there were more than 150,000 brutal crimes reported, and in

the past six years, more than a million serious crimes have been estimated in the city. The surveillance cameras have statistically contributed to solving approximately 0.05 percent at best (Chicago Tribune, 2013). It means that based on the statistics, in Chicago, surveillance cameras rarely caught crime incidents. The number of cameras does not guarantee the prevention of every crime or terror around us, and the prejudice of being safe thanks to the cameras could additionally cause “fewer precautions” as well as “risk ignorance.”

1.2 The evolving Big Brother

As the only measure of capturing and amassing a moment of crime scenes, despite the relatively small effects of camera surveillance, we have depended on CCTVs as the foremost camera surveillance tool for our society. What is the most problematic aspect giving rise to the ineffectiveness of the system? Systemically, one of the most ineffective downsides is “static.” They cannot chase and track the risky scenes, and some blind spots still exist, although CCTVs are installed in as many places as possible. Even though in a bid to compensate the defect, police patrols are deployed, the number of patrols is not enough to cover every area.

Alternative measures have been set up, with the recognition of the limitation. The core value is ‘movable'. In the current state, the ‘body-worn video' also known as the ‘body-worn camera' that is usually put on the top-half of a police officer's uniform to record or gather video evidence, is one of the movable surveillance cameras (Shaw, 2016).

Furthermore, on the cutting edge of ‘movable' camera monitoring systems, the Unmanned Aerial Vehicle (UAV) has the possibility to complement the limitation. The UAV is commonly known as the ‘drone', an aircraft without a human pilot aboard (International Civil Aviation Organisation, 2011). In practice, police in Surrey, the UK, have constructed the largest drone squadron, using 250,000 pounds to acquire new drones to conduct policing. The police force in Surrey and Sussex has trained 38 members in how to manipulate UAVs, and they are planning to expand its fleet from one to five departures (Wired, 2016).

Aside from the research on the ‘autonomous' surveillance drone policing without

human manipulation, there was also an experiment that was conducted by the Swinburne University of Technology. Specifically, the drone can recognise and avoid collisions, and it can track objects based on GPS (Arceri and Munro, 2013). In 2015, the Superflux laboratory in London proceeded with a project called 'The Drone Aviary' that worked on investigating the social, political, and cultural potential of the drone technology in public space. Moreover, in this project, there was a part referred to by "Nightwatchman: The Surveillance Drone" as community policing. The team set up a scenario (Fig. 1).

> "A highly mobile data acquisition device used by everyone from local councils to law enforcement agencies. By securely connecting to a centralised database The Nightwatchman is able to amass and utilise huge amounts of location and subject specific information assisting in everything from documenting civil offences to detecting potential terror threats" (Jain, 2015).

Basically, in the scenario, the drone can collect and document various information to detect civil offenses and potential terror threats. Autonomous drone policing seems to be not far from the present.

1.3 Against indiscriminate and clandestine surveillance

Amidst the constant proliferation and development of camera monitoring systems, a controversial issue emerged. The issue is the "invasion of privacy." In fact, there have been mounting tensions between "security" and "privacy" for ages, and in 2013, the disclosure of a state secret through an influential news outlet triggered people´s antipathy against the mass surveillance system run by governments.

In June 2013, the Guardian newspaper reported that the NSA had been requiring and collecting all telephone records of Verizon customers, one of America's largest telecom companies, under a top-secret court order issued in April 2013 (Greenwald, 2013). Afterward, the Guardian revealed that the top classified information they got was from Edward Snowden, an ex-CIA systems analyst. Besides, he exposed that a British spy agency (GCHQ) collects and stores huge amounts of calls, emails, internet histories, social media posts, and web histories,

and they share them with the NSA (MacAskill, Borger, Hopkins, Davies and Ball, 2013). There are furthermore numerous exposures such as hacking Chinese networks, spying on EU internal computer networks, 38 embassies being under surveillance and seizing web traffic, and monitoring Latin America's phone calls (BBC, 2014). Mass surveillance has been conducted all over the world "indiscriminately" and "clandestinely."

There is no exception to camera monitoring system. Through the electronic eyes, they can watch every step, and they can track and collect our information indiscriminately and surreptitiously without any permission. Isabella Sankey, the director of policy at the campaign group Liberty, said,

> "Who cares if there is one camera or 10 on their street if that one camera is pointing into your living room" (Lewis, 2011).

Privacy should be protected from "public scrutiny." In 1890, Samuel Warren and Louis Brandeis, the United States jurists, defined privacy as "the right to be left alone" in "The Right to Privacy," a law review article. It is construed as the right of an individual to choose to be alone from interferences of others (Warren and Brandeis, 1890). In this sense, if there is no choice concerning not being watched from users using unidentified surveillance cameras, including the government, we have the right to raise our voice against the secret and indiscreet camera installations for unknowable purposes to keep the basic human right.

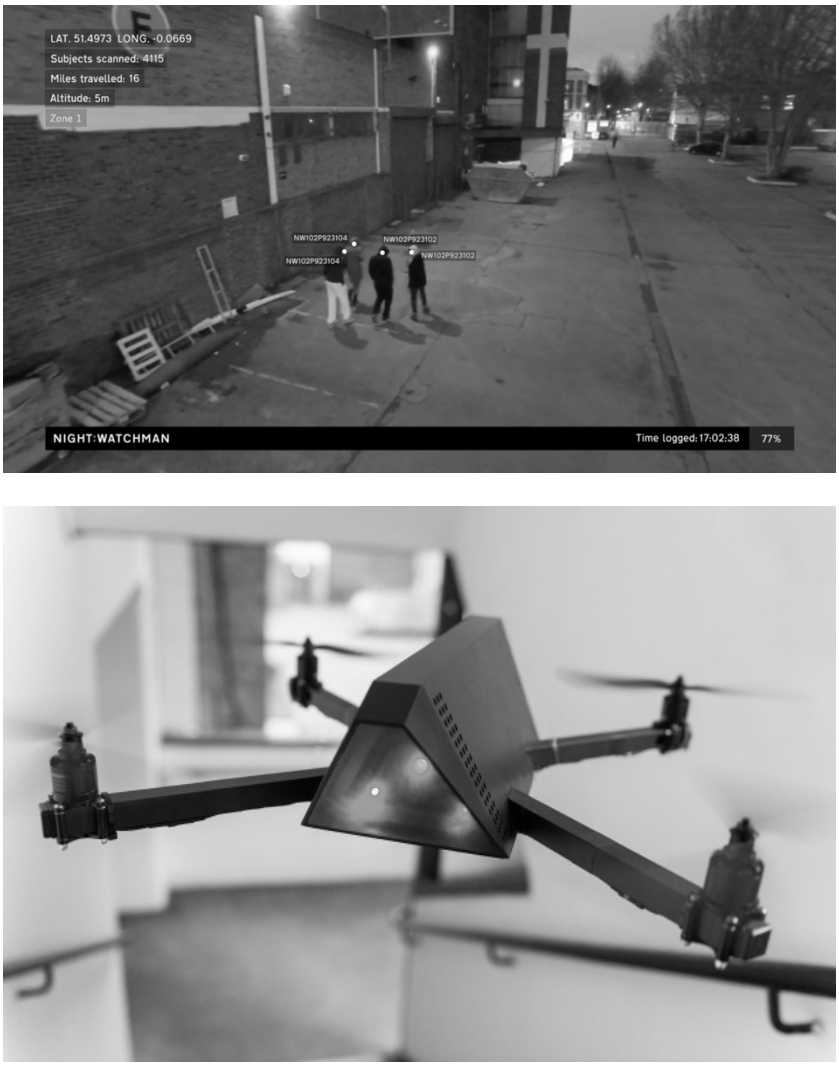

Fig. 1

A project called Nightwatchman: The Surveillance Drone was conducted by Superflux.

2.0 Privacy against the electronic eyes

2.1 The relationship between face and privacy

Through camera surveillance, we are exposed, and our personal data are exploited. How does the system recognise and identify us even if it can only watch people's appearance? In fact, there is no information such as name, date of birth, and residence inscribed on our faces. However, thanks to digital technology, by using a facial recognition programme, without any further information, the system can access people's personal data, whatever it wants to get.

Elke Oberg, a marketing manager in Cognitec Systems, which leads the industry, briefly spoke in terms of the working process of facial recognition system (Consumer Reports, 2016):

> "Essentially, what is being looked at is a landscape of the face. … Facial recognition software takes various measurements of each face and turns these into a string of numbers. Then, it's just a matter of comparing one string of numbers with another. The higher the similarity score, the more likely it is that you're looking at the same person."

In the system, the file that is produced after identification is called "faceprint," and it is used for various purposes, such as recognising shoplifters or criminals, verifying identities in systemically important national institutes, or simply for events. In fact, regardless of the aims of using facial recognition systems, if our faces were exposed, whether through videos and images, the system knows who we are as and has a 97.35% accuracy in doing so (Consumer Reports, 2016).

Where did the high accuracy come from? In summer 2014, Facebook released a research paper named "DeepFace," which is a facial recognition research project at the company. "DeepFace" is a profoundly advanced system which can analyse millions of images, and by using the face matching system, our personal information is investigated easily. It surpassed previous face detection software, such as the Next Generation Identification (NGI) run by Federal Bureau of

Investigation (FBI). Compared to NGI, the program has less accuracy than Facebook at approximately 85% (Brandom, 2014).

What exactly does this mean? In terms of obtaining personal data without any permission, it is no longer done at the national level. It is highly accessible for everyone, and it can be used surreptitiously everywhere. The face becomes, therefore, a significant issue regarding privacy. The exposure of our face is the equivalent meaning to informing people of who we are.

2.2 A typical form hiding face to keep privacy in digital era

In regard to the relationship between face and privacy, a noticeable form to hide faces to retain privacy for freedom is discovered. It appears in the form of 'The Spirit of Resistance', an anonymous group of internet-based international activist and hacktivist entities having countless members who choose to protect their identities from the world It has conducted a wide range of activities for the past few years since 2003. The group hacks into organisation networks, corporations, and even nations, and they knock down the server or bring core information against them, suppressing facts or taking away the right to know through the internet. More interestingly, the group has been using the Guy Fawkes mask as their symbolic identity, embodying demonstrating their commitment for everyone regarding guaranteeing the freedom of the right to know without any secret (Fig. 2) (Kelly, 2012).

In the real world, when people protest, the mask is used for the purpose of concealing the identity and protecting the face of members from camera surveillance. Use of the mask began in earnest when they protested against the Church of Scientology in 2008. They protested against the Church of Scientology in response to their action of pulling a video from the internet of Tom Cruise discussing Scientology as it was regarded as an abuse of power on the internet. At that time, the protesters were encouraged to hide their faces as a way of face protection from photographing anti-Scientology protesters by Church members. After the protest, the Guy Fawkes mask became a typical form for the purpose of hiding faces at a wide range of spots of demonstration (Forrester, 2008). In terms of the protest aimed at the Church of Scientology, Gabriella Coleman, an assistant

professor at New York University's department of media, culture, and communication, explained the meaning of the mask (Bilton, 2011).

> "Anonymous knew if they were going to meet in a visibly public space for the first time, they needed to conceal their identity. They inevitably chose the 'V for Vendetta' mask to do this."

The typical protection against the camera surveillance shows that for the right to get freedom, concealing faces is one of the most significant factors to be free from dangerous situations watched, captured, and identified by image records.

2.3 Cases of face protection appeared as forms of design

In design practice, the cases of face protection in the matter of privacy can be subdivided into two major forms focusing on space and body, respectively. Under the same purpose for keeping privacy in the public space, two types have two distinct "directions of the design process."

When it comes to the spatial design for face protection, it has been centrally emerging in an area of furniture design. When designers pondered a product aiming at how to keep privacy on the functional aspect, most of the designers who worked on the design focusing on privacy commonly had a tendency to come up with "an independent space added a function being able to hide faces," which can comfortably settle down by blocking disturbances. In fact, they believed that hiding faces from surroundings is enough to keep privacy.

A design product 'Privacy Chair' belonged to 'Dining Together Matters' as to a furniture design collection by Paula O'Connor is a representative. The overhead enclosure on chair solely covers a person's face (Fig. 3). Regardless of the exposure of other parts of the body, in the theory of the designer, in the public area, a person's privacy by only using face partition can be protected from others. There is another instance called the 'Privacy Desk' that comes with an immersive shell that provides privacy in any environment designed by Sophie Kirkpatrick (Fig. 4). The basic principle of the desk is the same as the 'Privacy Chair'. By hiding faces, the users of the desk can get their privacy without any disturbances. Besides, more

practically, a Japanese restaurant ‘Ichiran' convincingly demonstrates the importance of face protection by offering a face partition as one of the main reasons for being popular (Fig. 5).

In the meantime, the another form focusing on bodies is interpreted as ‘uninfluenced design by space'. Regardless of the space where people are, the form of privacy directly aims at cameras. The core value is how to ‘camouflage' faces to thwart facial recognition systems. Adam Harvey, a New York-based designer who worked on a system called CV Dazzle to prevent computer systems from recognising faces, said (Fig. 6) (Sunday Review, 2013),

> “My project, CV Dazzle, explores how fashion can be used as camouflage from face-detection technology, … Since facial-recognition algorithms rely on the identification and spatial relationship of key facial features, like symmetry and tonal contours, one can block detection by creating an anti-face.”

The project is one of the typical examples of technology used against the massive face detection technology. Two forms of design centering on “space” and “body” are symbolic in solving a specific issue in the matter of privacy in design practice.

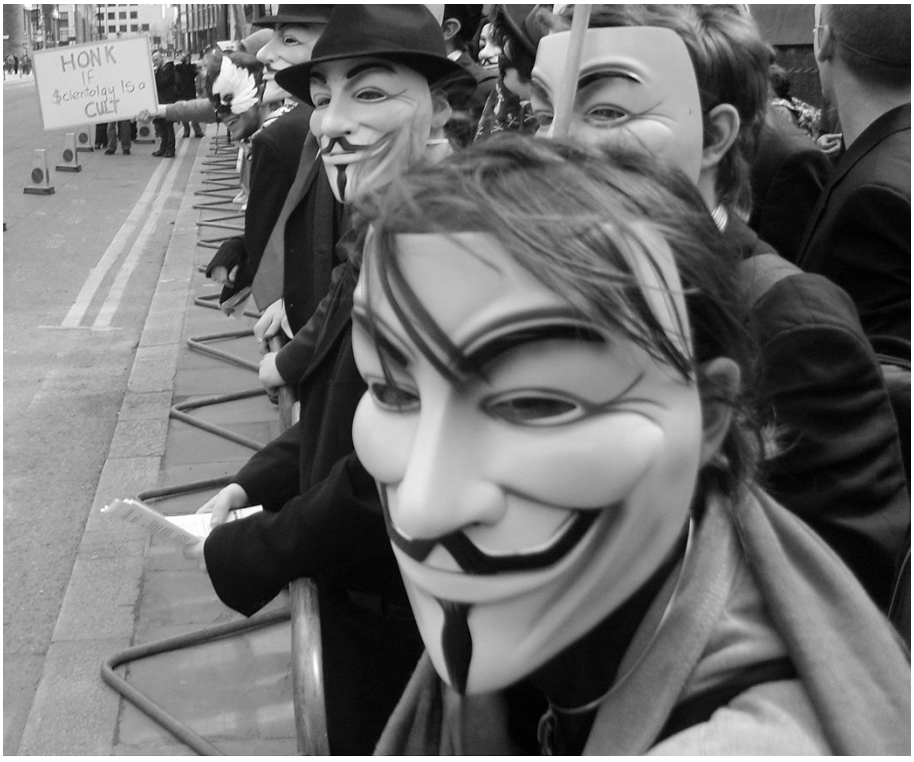

Fig. 2

Members of the group Anonymous wearing Guy Fawkes masks at a protest against the Church of Scientology in London, 2008.

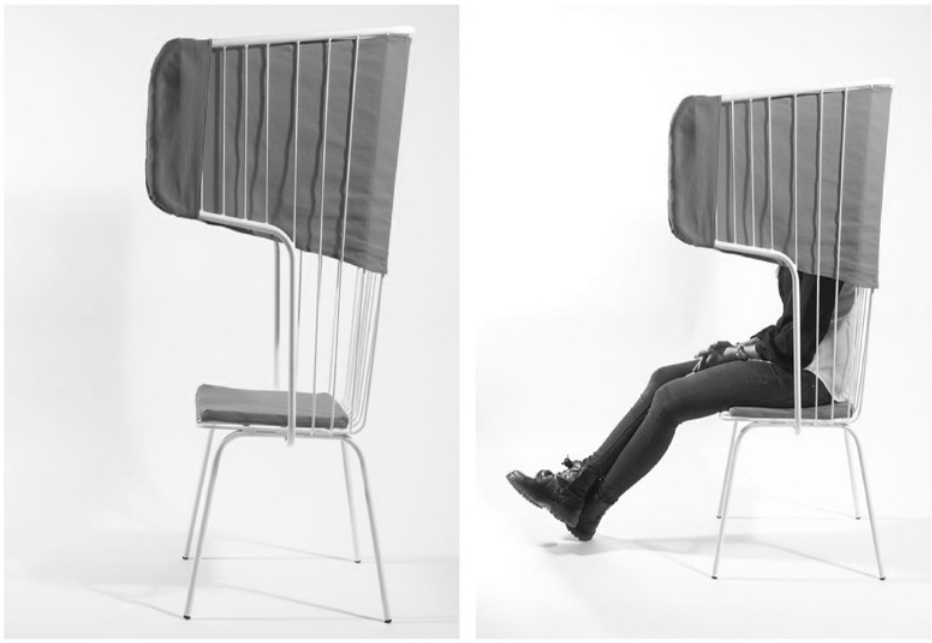

Fig. 3

The design and overhead enclosure limits the user's view,
encouraging conversation and interaction between individuals through an overhead enclosure.

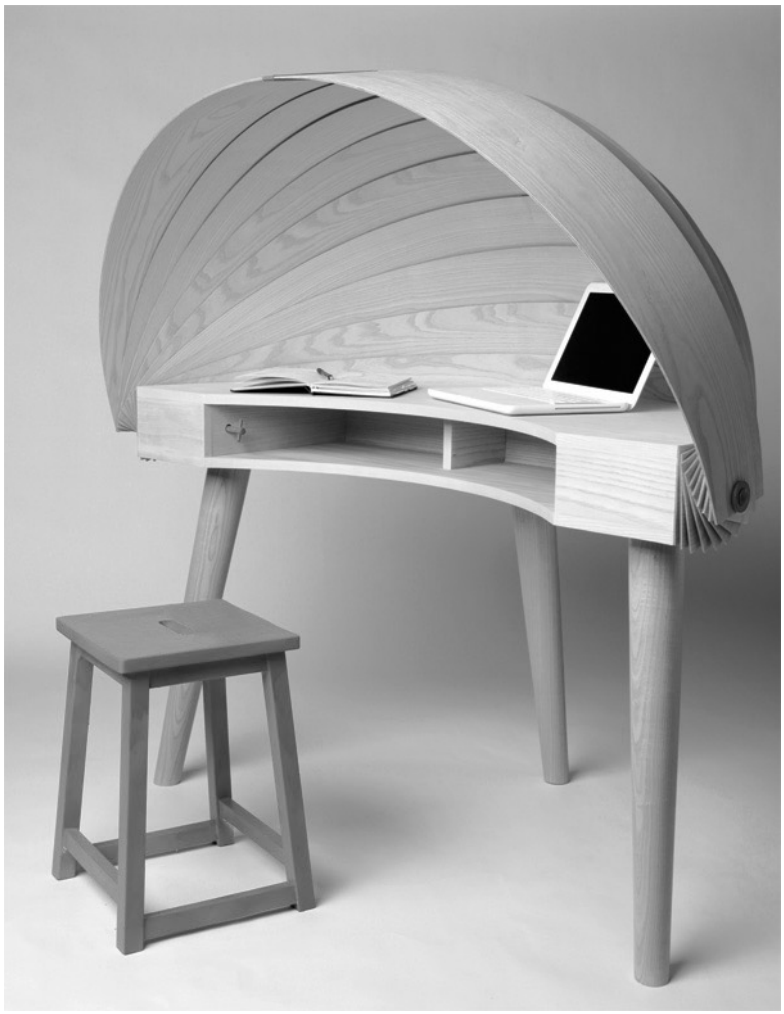

Fig. 4

Pull it up when you want to shut out the world and concentrate on the task as hand.

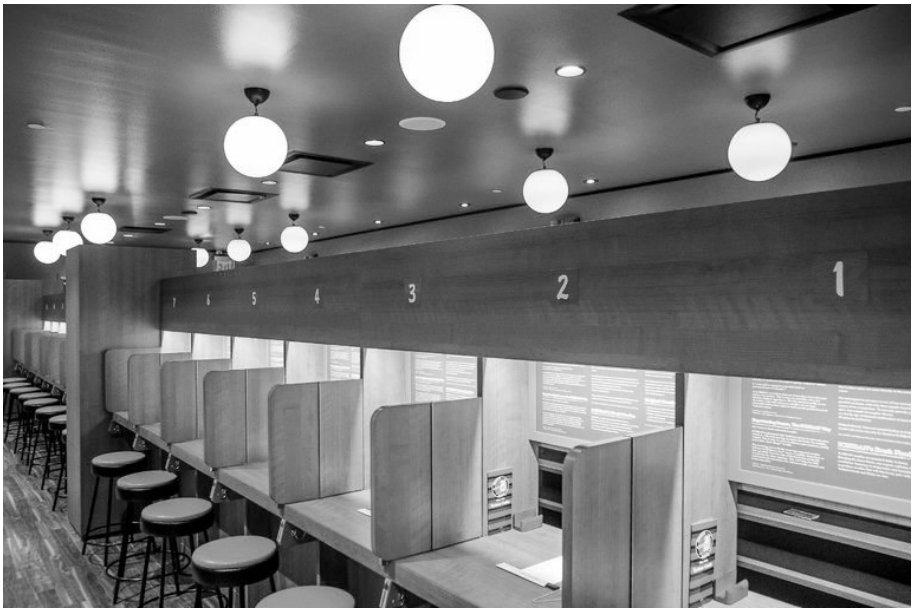

Fig. 5

Individual booths of Ichiran Ramen in Bushwick, Brooklyn.

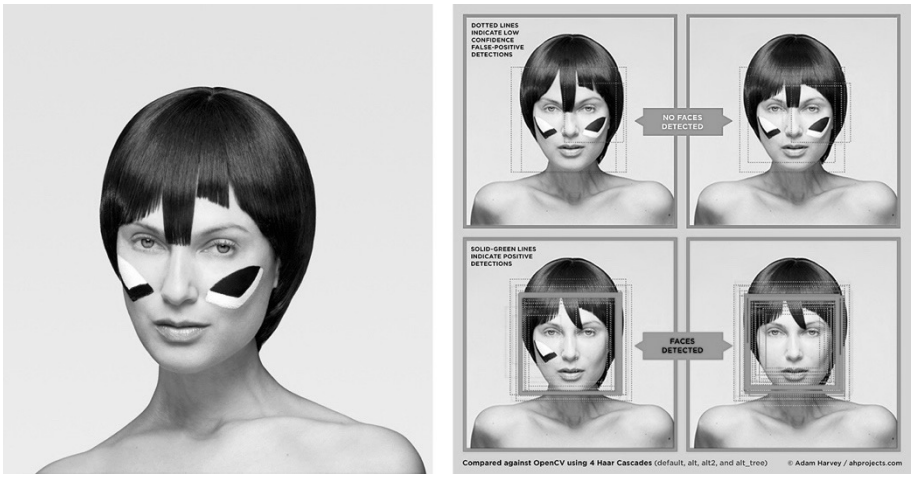

Fig. 6

Camouflage from Computer Vision.

3.0 A protection system for visual anonymity

3.1 Visual anonymity provided by the system itself

The drawbacks of being exposed online have been made all too clear in high-risk circumstances over the past few years. The Burmese military junta and the Iranian government trawled online images of citizens or activists who appear in videos of anti-regime demonstrations to target them. Apart from these highly dangerous situations, there is also the exposure to various threat factors in invading privacy (Gregory, 2016). It is called the importance of "visual anonymity," which refers to the importance of "image protection" among recognisable. In this issue, several systems have had endeavours to adopt self-censorship to avoid revealing faces online. According to WITNESS' Cameras Everywhere, the international human rights organisation (YouTube, 2012),

> "No video-sharing site or hardware manufacturer currently offers users the option to blur faces or protect identity."

In this regard, YouTube, an online video-sharing platform, started a new service in 2012 offering an option to blur faces in videos to protect privacy. This is because when people film and post footage related to the risks of human rights, it is important to protect oneself and others in such videos (YouTube, 2012). Besides, from 2016, the company is launching a new advanced feature. Any objects can be blurred, even as the blurred images move immediately in videos for more people suffering from the indiscriminately and confidentially exposed faces (Fig. 7) (YouTube, 2016).

With the evolving map services, Google has been offering a service called Google Maps since 2005. In 2007, the map added a tool called 'Google Street View' that can see the map as street panoramic view images. In terms of privacy concerns capturing the world, including people, John Hanke, director of Google Earth and Google Maps, in an interview at the Where 2.0 conference, said,

> "The technology uses a computer algorithm to scour Google's image

database for faces, then blurs them."

When they were gathering pictures of public areas for the map service, the project was capturing faces, license plates, and other sensitive information. In the process, for the purpose of protection for 'visual anonymity', the company launched a challengeable system automatically detecting and blurring faces (Fig. 8). By using the automatic system, it succeeded in sufficiently blurring up to 89 percent of faces in the self-evaluation sampled from Google Street View imagery (Frome, Cheung, Abdulkader, Zennaro, Wu, Bissacco, Adam, Neven and Vincent, 2009). They recognised the importance of 'image records management' and 'face protection', and they redeemed themselves of the drawbacks of being recognised online.

In fact, the systems, 'YouTube' and 'Google Street View', have been conducting the protection of visual anonymity, which is different from the forms of design mentioned in the Chapter 2.2 (Active part in hiding face in digital era) and 2.3 (Typical design forms of face protection) due to the responsibility 'themselves' to complement the services with privacy matters and not as the forms of 'resistance'.

3.2 Challenges to overcome the limitation of face protection system

Services that blur faces, offered by several services, such as YouTube and Google Street View, have endeavoured to overcome the shortcomings of the undiscriminating online exposure of faces for the last few years. Nevertheless, these systems are imperfect. Google has suffered from unexpectedly exposed face images recorded by moving cameras. Since the launch of Google Street View, numerous people have sought and indiscriminately shared those images on the Internet without any permission.

In fact, in 2011, Google acquired a facial recognition software company called PittPatt and participated in a project, under Carnegie Mellon University, that developed facial recognition technology based on a wide range of algorithms that can match people's face on photos and videos after shooting the images (Rao, 2011). However, there are numerous misses. It is still far from perfect.

In 2009, for instance, in Google Street View, a Canadian woman, Maria Pia Grillo,

suffered from the invasion of “visual anonymity” while she was sitting outside. Google captured an exposed part of her breast in front of her house. According to the court paper (17), she was shocked and embarrassed because when she checked her house using Google Street View, she discovered an image of her exposed cleavage. Years later, in 2014, the court ruled on the legitimacy of suing for the unloading of an inappropriate image without her approval, and Google must pay her compensation (Roberts, 2014). This case showed the “imperfection” of the systems blurring faces even though these aim to defend privacy.

In the case of YouTube, a bigger drawback than that of Google was involved. The street view service at least automatically applies the blurring system to faces, and offers the street view online. By contrast, even if YouTube offers the blurring system to every user, not everyone will actively use the tool. It is entirely up to the user's decision, which means that it is not working enough.

What is the fundamental problem with the errors in terms of blurring faces? Besides, even though the systems perfectly protect faces, a problem has still existed. In conclusion, these are strongly related to the ‘sequence of working process'. Google and YouTube had undoubtedly endeavoured to hide faces ‘after shooting'. In fact, most digitalised systems, however, potentially cause unexpected errors and failures of result derivation since the step-by-step processes are managed ‘in the intervals'. Captured original images without face protection are retrieved from the storages, and then, by using facial recognition systems or by users in person, those face images are covered with blurs. In the process between capturing and blurring images, is it possible to perfectly conduct face protection with plenty of pictures? It is impossible with 100 percent accuracy.

Let us look back at the case of ‘CV Dazzle', which was a design project to hide faces from surveillance cameras specifically mentioned in the last paragraph of Chapter 2.3. Since the practitioners camouflaged themselves on their faces ‘in real time', it was a perfect way to protect faces against cameras without exception. There is no another process after being monitored. It can be a reference to a combined system of detecting and blurring faces at the same time. Besides, in the middle of working process, before the process, blurring faces, original images that faces are already exposed still exist. It is possible to be exposed, or someone can access those images intentionally. For perfection, in this sense, conducting ‘facial

recognition' and ‘hiding faces' simultaneously is suggested as a key process for the guarantee of ‘visual anonymity'.

3.3 Points of compromise for a rational design system of surveillance drone policing

Before suggesting the real-time face protection installed to surveillance cameras, a monitoring environment is expected. With on-going development of technology, the UK is setting up a drone troop to use drones as flying patrols instead of the existing CCTV, and there is a plan to expand it from one to five departments (Wired, 2016). Surveillance drone policing has become real in daily lives. People will suffer from the monstrous flying eyes more than the present, and it is highly possible to lose the opportunities being able to resist the increasing pressure of the brutality. For the surveillance drone policing era, a rational system is suggested in order to compromise points to alleviate the tensions between ‘privacy for human rights' and ‘surveillance for security'.

There were a number of experimental projects for hiding faces by blurring or pixelating faces in real time. What if real-time face protection system is installed on drone's eyes? It would be points of compromise to mitigate the tensions between privacy and surveillance against indiscriminate and confidential camera surveillance by drone policing (Fig. 9). Could it become an appropriate suggestion ‘from irrational to rational monitoring system' for the public in preparation for drone's surveillance eyes?

From the other perspective, through facial recognition algorithms in real time, we can prevent high-risk hazards by recognising, monitoring, and tracking ex-convicts, criminals, and terrorists by taking away the fundamental right of face protection from them (Fig. 10).

In 2014, a movie series ‘Black Mirror' was televised. Among the series, in the special ‘White Christmas,' an impressive system was shown. It is referred to a ‘blocking and marking ex-convicts' system being able to check in the last scene of the movie. In the last scene, the whole body of an ex-convict is pixelated in red, and he is physically blocked from another human permanently (Fig. 11) (Cinnamon, 2015). The system can make dangerous people pixelated with red

colour as a warning sign in real time. The sci-fi movie provides a vision to mark offenders in real time. In the opposite method, for criminals, without face protection, what if their faces are exposed? It deprives offenders of the basic human right being protected with blurred faces as their responsibility for the crimes.

In the surveillance drone policing era expected, from the research and questions, the three key points such as ‘face protection' in ‘real time' ‘without protection for offenders' are anticipated as worth points of compromise against mass surveillance.

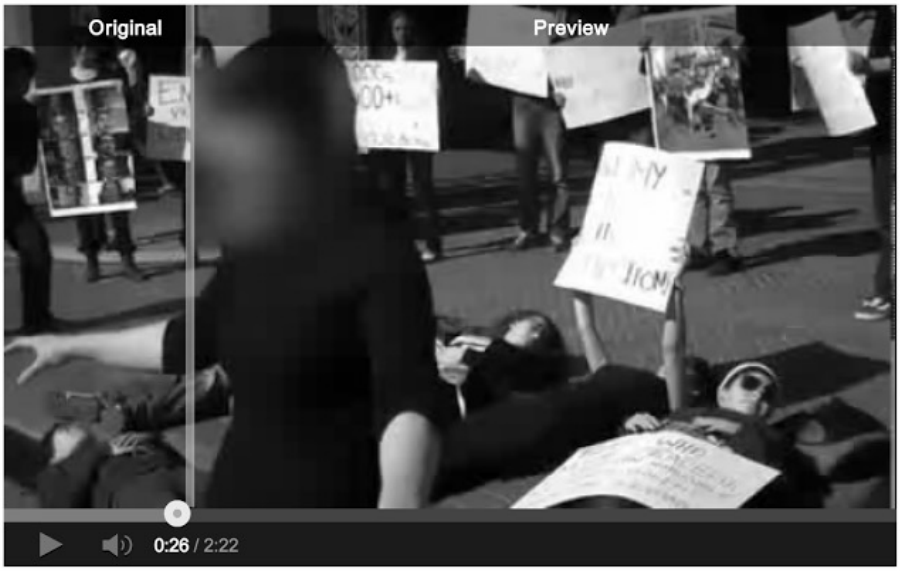

Fig. 7

Face blurring when footage requires anonymity in YouTube.

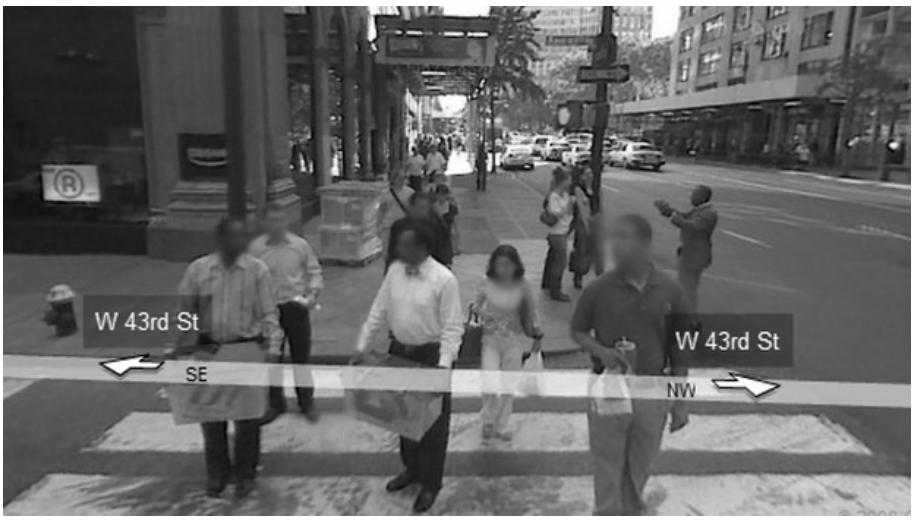

Fig. 8

Blurring faces in Google Street View.

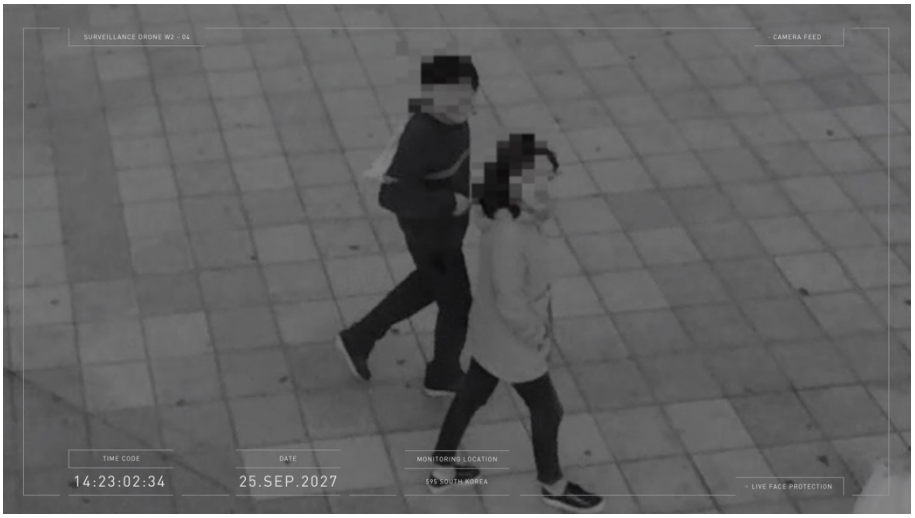

Fig. 9

Jay Youngjoon Kim. Documentary Film of a project called 'Points of Compromise' in London College of Communication Postgraduate Shows 2016.

Fig. 10

Jay Youngjoon Kim. Documentary Film of a project called 'Points of Compromise' in London College of Communication Postgraduate Shows 2016.

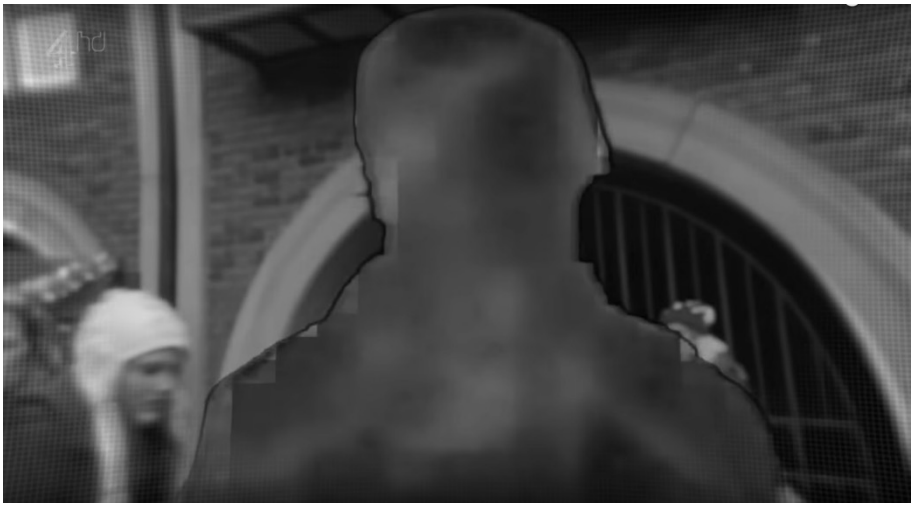

Fig. 11

The Last Scene of White Christmas, Black Mirror.

4.0 Conclusion

There is no high and low priority between privacy and surveillance. The issue is frequently fluctuated depending on issues. However, based on reliable data, camera monitoring systems are inefficient considering the number of the electronic eyes, and the case in Chicago demonstrated it regarding the contribution to solving crimes at less than 1 percent at best (Chicago Tribune, 2013). Therefore, are the surveillance cameras useless? We can hardly say that it is unusable as a failure since there have been no proper alternative systems. However, the emerging drone policing is notable. Surveillance drone policing expected as a replaceable tool has shed light on the drawbacks of the existing camera surveillance. In fact, drone patrols are expected enough as a suitable tool that can overcome the problems such as ‘the spatial limitation of camera deployment' and ‘static position'.

Based on evolving drones, assuming we are living in surveillance drone policing, it means that the monitoring eyes will be stronger, more powerful, and more uncontrollable than the present. Proper points of Compromise are needed to be proposed, with a rational system design for surveillance drone policing, prior to the full-scale beginning of the flying eyes system. Besides, the points of compromise should be implemented, within the system, itself, and not from an outside form of resistances because, at least, it is an essential endeavour to protect the public at the national level and not the individual level.

What are the points of middle ground between privacy and surveillance? It is highly related to ‘visual anonymity' called ‘face protection'. In the digital era, the face is our identity, and with the facial recognition system, there is no place to hide. If cameras expose faces as video-based materials, more than 90 percent of the population is recognised, exposing their identities and personal information to whoever wants to get them. In this regard, the priority to protect privacy is keeping ‘visual anonymity', especially the ‘faces'. What if the face protection system applies to drone surveillance cameras? There is a possibility of irrational or rational monitoring systems for the public. It is for every citizen. On the contrary, for offenders, they lose the basic right to keep their visual anonymity for the purpose of safety and security. Face protection will represent a criterion of human rights. The suggested rational design system will be a worthy attempt in reaching a

compromise on the issue of privacy and surveillance in the drone policing era.

List of Illustrations

https://youtube.googleblog.com/2012/07/face-blurring-when-footage-requires.html [Accessed 21 November. 2016].

Fig. 8

Blurring faces in Google Street View. Available at: https://www.cnet.com/news/google-begins-blurring-faces-in-street-view/ [Accessed 21 November. 2016].

Fig. 9

Youngjoon Kim. Documentary Film of a project called 'Points of Compromise' in London College of Communication Postgraduate Shows 2016.

Fig. 10

Youngjoon Kim. Documentary Film of a project called 'Points of Compromise' in London College of Communication Postgraduate Shows 2016.

Fig. 11

The Last Scene of White Christmas, Black Mirror, Netflix.

Bibliography

Arceri, D. and Munro, J. (2013). *Autonomous Surveillance Drone*. [video]. Available at: https://www.youtube.com/watch?v=rK2KWHq1pCQ [Accessed 3 October. 2016].

Barrett, D. (2013). *One surveillance camera for every 11 people in Britain, says CCTV survey*. The Telegraph, [online] Available at: http://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html [Accessed 7 November. 2016].

BBC News. (20134). *5.9 million CCTV cameras in UK*. BBC News, [online] Available at: http://www.bbc.co.uk/newsround/23279409 [Accessed 2 November. 2016].

BBC News. (2014). *Edward Snowden: Leaks that exposed US spy programme*. BBC News, [online] Available at: http://www.bbc.com/news/world-us-canada-23123964 [Accessed 1 October. 2016].

Bilton, J. (2011). *Masked Protesters Aid Time Warner's Bottom Line*. The New York Times, [online] Available at: http://www.nytimes.com/2011/08/29/technology/masked-anonymous-protesters-aid-time-warners-profits.html?_r=0 [Accessed 10 November. 2016].

Brandom, R. (2014). *Why Facebook is beating the FBI at facial recognition*. The Verge, [online] Available at: http://www.theverge.com/2014/7/7/5878069/why-facebook-is-beating-the-fbi-at-facial-recognition [Accessed 9 November. 2016].

Chicago Tribune. (2013). *How helpful are surveillance cameras?*. Chicago Tribune, [online] Available at: http://articles.chicagotribune.com/2013-05-06/opinion/chi-how-useful-are-surveillance-cameras-20130506_1_cameras-boston-marathon-serious-crimes [Accessed 7 November. 2016].

Cinnamon, L. (2015). *Black Mirror: White Christmas is A Christmas Carol where everybody pays and nobody changes*. Lynn Cinnamon, [online] Available at: http://lynncinnamon.com/2015/12/black-mirror-white-christmas-special-and-the-horrors-of-extra-time/ [Accessed 3 October. 2016].

Consumer Reports. (2016). *How Facial Recognition Works: The Ghost in the Camera*. Consumer Reports, [online] Available at: http://www.consumerreports.org/privacy/how-facial-recognition-works-the-ghost-in-the-camera/ [Accessed 9 November. 2016].

Corera, G. (2016). *Paris attacks: Security flaws and challenges highlighted*. BBC, [online] Available at: http://www.bbc.com/news/world-europe-34853376 [Accessed 22 September. 2016].

Forrester, J. (2008). *Dozens of masked protesters blast Scientology church*. Boston.com, [online] Available at: http://archive.boston.com/news/local/articles/2008/02/11/dozens_of_masked_protesters_blast_scientology_church/ [Accessed 10 November. 2016].

Frome, A., Cheung, G., Abdulkader, A., Zennaro, M., Wu, B., Bissacco, A., Adam, H., Neven, H. and Vincent, L. (2009). *Large-scale Privacy Protection in Google Street View*. In: IEEE International Conference on Computer Vision. [online] Google, p. 1. Available at: http://static.googleusercontent.com/media/research.google.com/ko//pubs/archive/35481.pdf [Accessed 14 November. 2016].

Greenwald, G. (2013). *NSA collecting phone records of millions of Verizon customers daily*. The Guardian, [online] Available at: http://www.zdnet.com/article/tracking-terrorists-with-iomniscient/ [Accessed 1 October. 2016].

Gregory, S. (2016). *It's Far Too Hard to Anonymize Video–We Have to Do Better*. Wired, [online] Available at: https://www.wired.com/2016/02/visual-anonymity [Accessed 13 November. 2016].

Jain, A. (2015). *The Drone Aviary*. Superflux, [online] Available at: http://www.superflux.in/blog/the-drone-aviary [Accessed 3 October. 2016].

Kelly, B. (2012). *Investing in a Centralized Cybersecurity Infrastructure: Why 'Hacktivism' can and should influence cybersecurity reform*. Boston University Law Review. 92 (5): 1663–1710. Retrieved May 2, 2013.

Lewis, P. (2011). *You're being watched: there's one CCTV camera for every 32 people in UK*. The Guardian, [online] Available at: https://www.theguardian.com/uk/2011/mar/02/cctv-

cameras-watching-surveillance [Accessed 7 November. 2016].

MacAskill, E., Borger, J., Hopkins, N., Davies, N. and Ball, J. (2013). *GCHQ taps fibre-optic cables for secret access to world's communications*. The Guardian, [online] Available at: https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa [Accessed 1 October. 2016].

Mento. (2014). *Ultima IV: Quest of the Avatar*. Giant Bomb, [online] Available at: http://www.giantbomb.com/ultima-iv-quest-of-the-avatar/3030-14381/ [Accessed 12 November. 2016].

Privacy International. (nd). *Mass Surveillance: What is mass surveillance?*. Privacy International, [online] Available at: https://www.privacyinternational.org/node/52 [Accessed 1 October. 2016].

Rao, L. (2015). *Google Acquires Facial Recognition Software Company PittPatt*. Tech Crunch, [online] Available at: https://techcrunch.com/2011/07/22/google-acquires-facial-recognition-software-company-pittpatt/ [Accessed 21 November. 2016].

Roberts, J. (2014). *Google must pay Canadian woman $2,250 for showing her cleavage in Street View*. Gigaom, [online] Available at: https://gigaom.com/2014/10/29/google-must-pay-canadian-woman-2250-for-showing-her-cleavage-in-street-view/ [Accessed 14 November. 2016].

Robertson, N. (2016). *How 'glaring' intelligence failures allowed a second bout of terror in Paris*. CNN, [online] Available at: http://edition.cnn.com/2015/11/18/europe/paris-terror-attacks-intelligence-failures-robertson/ [Accessed 22 September. 2016].

Shaw, D. (2016). *Police body cameras 'cut complaints against officers'*. BBC News, [online] Available at: http://www.bbc.co.uk/news/uk-37502136 [Accessed 8 November. 2016].

Sunday Review. (2013). *Face to Anti-Face*. The New York Times, [online] Available at: http://www.nytimes.com/interactive/2013/12/14/opinion/sunday/20121215_ANTIFACE_OPART.html?_r=0 [Accessed 13 November. 2016].

TheReligionofPeace. (2016). *List of Islamic Terror: 2016. List of Islamic Terror Attacks*,

[online] Available at: https://www.thereligionofpeace.com/terror-2016.htm [Accessed 22 September. 2016].

Vlahos, J. (2009). *Surveillance Society: New High-Tech Cameras Are Watching You*. Popular Mechanics, [online] Available at: http://www.popularmechanics.com/military/a2398/4236865/ [Accessed 2 November. 2016].

Warren, S. and Brandeis, L. (1890). *The Right to Privacy*. Harvard Law Review, No.5.

Weaver, M. (2015). *UK public must wake up to risks of CCTV, says surveillance commissioner*. The Guardian, [online] Available at: https://www.theguardian.com/world/2015/jan/06/tony-porter-surveillance-commissioner-risk-cctv-public-transparent [Accessed 3 November. 2016].

Wired. (2016). *Surrey now has the UK's 'largest' police drone project*. Wired, [online] Available at: http://www.wired.co.uk/article/surrey-police-uk-largest-drone-trial [Accessed 8 November. 2016].

YouTube. (2012). *Face blurring: when footage requires anonymity*. YouTube, [online] Available at: https://youtube.googleblog.com/2012/07/face-blurring-when-footage-requires.html [Accessed 13 November. 2016].

YouTube. (2016). *Blur moving objects in your video with the new Custom blurring tool on YouTube*. YouTube, [online] Available at: https://youtube-creators.googleblog.com/2016/02/blur-moving-objects-in-your-video-with.html [Accessed 13 November. 2016].