



PRIVATE CCTV LIABILITY UNDER BIOMETRIC DATA PROTECTION RULES

Muhammad Faisal Hilmi Gunawan

Fakultas Hukum, Universitas Airlangga, Indonesia

Email muhammad.faisal.hilmi-2019@fh.unair.ac.id

Abstract:

The penetration of technology that is increasingly developing has a lot of impact on human life. Increasing technology also results in the rapid development of home security equipment, especially Closed-Circuit Television cameras (hereinafter mentioned as CCTV). The right to privacy, to which everyone is entitled to personal self-protection. Doctrinal legal research is a crucial aspect in recognizing various societal problems. Doctrinal research combines a systematic analysis of the provisions of legislation and the legal principles contained in it or derived from it, but also the logical and rational order of legal propositions and principles. Doctrinal legal research methods involve the analysis of legal propositions or legal concepts on which the main study is based. Case base approach demands the researcher to understand the reasons that used by the judges or another adjudicator until it reaches the final decision. Most personal data protection laws around the world distinguish between regular personal data and biometric data. At the beginning, Article 4 paragraph (1) of EU GDPR regular personal data commonly define on the laws as a set of data that able to identify a natural person either from electronic or non-electronic devices. Under the data protection laws regime especially GDPR, UK Data Protection Law and Indonesia Data Protection Law, mitigation during a data protection failure involving household CCTV systems typically involves taking immediate steps to minimize the impact of the breach. Furthermore, stated in the Fairhurst v Woodard case homeowner could be held liable for failure to protect the personal data if they use camera on the outside boundary of their house and they could face hefty fine and/or tools removal. Finally, this writing contributes to undergoing discourse on cyber law field especially in data protection law and provide insights for academicians, practitioner, and society.

Keywords: CCTV, Data Protection, Private Liability

Introduction

The penetration of technology that is increasingly developing has a lot of impact in human life. The increasingly advanced technology also results in the rapid development of home security equipment, especially Closed-Circuit Television cameras (hereinafter mentioned as CCTV) (Rawat, Deb, & Upadhyay, 2021). Homeowners use CCTV cameras as a tool to monitor activities inside and outside the home (Dahmen,

Thomas, Cook, & Wang, 2017). For example, homeowners usually install CCTV cameras to monitor pets or monitor flammable objects in the house. As the number of crimes that occur in residential areas increases, homeowners are taking steps to secure their homes by installing CCTV surveillance cameras (Wright, Glasbeek, & van der Meulen, 2015).

The right to privacy, to which everyone is entitled to personal self- protection. This right is guaranteed in the 1945 NRI Constitution and also In general, this right speaks of the right of an individual to be free from all forms of intervention and intrusion in all his lifelines including his personal data (Kettley, 2021). The use of CCTV cameras and other surveillance devices can result in being disrupted and even the loss of one's privacy rights. Therefore, a clear and concrete reason is needed to use it. Because the use of these tools can result in disruption or even loss of privacy rights of an individual, the installation of this tool must be done with caution and also pay attention to the efficiency of its use. So, it is important for homeowners before installing CCTV cameras to pay attention to the privacy rights of others, especially their closest neighbours (Kettley, 2021).

In addition, several CCTV cameras able to capture biometric data. Biometric data is defined as a personal data that results from specific technical processing related to physical, psychological, or behavioural characteristics of a natural person (Fairhurst, Li, & Da Costa-Abreu, 2017). Furthermore, biometric data also mentioned as a tool which attempts to identify specific user through unique characteristics. Nowadays, most households' CCTVs are equipped with biometric data identifiers such as facial recognition and motion detector. Thus, the usage of this kind of CCTV will set another obligation as biometric data considered as a special personal data on several data protection regulations especially on the UK Personal Data Protection Act 2018 and Indonesia Personal Data Protection Law no 27/2022.

Failure in the protection of personal data is a failure in a security breach that leads to the destruction, loss, alteration, unauthorized or unauthorized disclosure of, or access to, personal data (Di Martino et al., 2019). This is something that the controller and/or processor of personal data can avoid. Therefore, the installation of CCTV must be carefully considered by homeowners. In addition, it is also necessary to consider the coverage area that will be covered by CCTV cameras as well as whether the camera will record far outside the home area as installing CCTV outside the home's courtyard or capturing areas outside the courtyard will result in fulfilling the obligation under the data protection law.

Indonesia has also passed a personal data protection law which can serve as a guideline for household CCTV users in using the tool (Makarim, 2021). Therefore, the status of household CCTV users became controller of personal data after the law was passed. A household CCTV user becomes a person who determines the purpose and is in control of the processing of personal data and is obliged to have the basis for processing personal data. Therefore, with this status, household CCTV users are obliged to protect personal data from unauthorized processing.

In addition, the recent case that happened in the United Kingdom which involved a personal biometric data was the breach of BioStar 2 fingerprint system. In this case, Suprema, the company which responsible to this incident was linked BioStar 2 system to another access control system which is AEOS. This system is used by 5,700

organisations in 83 countries, including governments, banks, and the UK Metropolitan police. Furthermore, the data includes detailed personal information of employees and unencrypted usernames and passwords, giving hackers access to user accounts and permissions at facilities using BioStar 2.

In addition, the UK also passed the Data Protection Act in 2018 as a comprehensive personal data regulatory statute (Alexander, 2019; Prasad M & Menon C, 2020). The law also places household CCTV users as natural persons who determine the purposes and means of processing personal data. The UK through its personal data protection regulatory agency, the Information Commission's Office. The agency has also made guidelines related to the use of household CCTV and the rights of the data subjects recorded in it. The UK also set up a special surveillance camera commission called the Surveillance Camera Commissioner to oversee surveillance cameras with a wider scope.

Based on the description above, it is interesting to write an article with the title "Private Cctv Liability Under Biometric Data Protection Rules".

Method

Doctrinal legal research is a crucial aspect in recognizing various societal problems. In addition, the study focuses on coherence and cohesion. This research involves searching for general principles, is logically consistent, and is built from research through specific examples. Thus, doctrinal research combines a systematic analysis of the provisions of legislation and the legal principles contained in it or derived from it, but also the logical and rational order of legal propositions and principles. So, this study use doctrinal research.

Results and Discussion

Household liability on CCTV Cameras Data Protection Failure

Under the data protection laws regime especially GDPR, UK Data Protection Law and Indonesia Data Protection Law, mitigation during a data protection failure involving household CCTV systems typically involves taking immediate steps to minimize the impact of the breach and prevent further unauthorised access or data compromise. Here are some key mitigation measures to consider:

Identify and Isolate the Breach

Typically, the primary concerns with video surveillance systems pertain to privacy matters due to clear and understandable reasons (Elmaghraby & Losavio, 2014). The privacy implications of VSSs are particularly significant given the recent disclosures on worldwide surveillance initiatives, with a specific focus on video surveillance scandals.

Fairhurst V Woodard Case: One of Influential Court Decisions on Domestic Surveillance

Dr Mary Fairhurst (hereinafter referred as claimant) who owns a property at 83 Cromwell Avenue, Thame, Oxfordshire. She was filing a claim against her neighbour, Mr. Jon Woodard (hereinafter referred as defendant) who lives in s 87 Cromwell Avenue. In the car park, The Claimant owns two parking spaces located immediately

behind the rear garden boundary fence of No 83. The Defendant owns one parking space immediately behind the rear garden boundary fence of No 87 and rented the adjacent space from the owners of 89 Cromwell Avenue since November 2019.

On the shed of the boundary fence, the defendant installed a floodlight and sensor and video and audio surveillance camera with an integrated motion sensitive spotlight which pointed in the direction of the car park. Moreover, he also installed a combined doorbell and video and audio surveillance system pointing towards the Cromwall Avenue. On Number 85's gable end wall, he also installed the "Driveway Camera, pointing down the driveway towards the car park.

The claimant case is summarised as nuisance, breach of privacy which subject to UK Data Protection Act 2018 and course of conduct to harass someone under Protection from Harassment Act 1997.

In the other hand, in his witness testimony, the Defendant stated that he began investigating how to set up a security camera to monitor his car only in February and March 2019, not in 2018, and that as part of that process, he reached out to the Information Commissioner's office via the web page to learn about what he needed to carry out before installing such a camera. His evidence that he asked the ICO if he could register to be a data controller but was told he couldn't because No 87 was a domestic dwelling is extremely surprising advice from the ICO, as it is patently incorrect and is as incorrect under the DPA 2018 as it was under its predecessor legislation.

Both claimant and defendant have a somewhat perfect neighbourly relationship. The defendant also installed flood lightning on the shed to provide nighttime lightning to his garage. Moreover, after the defendant moved back post renovation in 2018, he bought a ring doorbell and shed camera on 9 April 2019.

Moreover, the driveway camera the Driveway Camera was a dummy camera and not operational, his position on this has changed. The judge does not accept the evidence that he was telephoned by Ms Vantuykom's partner from Ms Vantuykom's phone in a panic, but he originally thought it was Ms Vantuykom and reported it to the Claimant as such. That seems to be highly improbable, and he tripped himself up in cross-examination when he confirmed that he was a very old family friend of Ms Vantuykom

The Ring Doorbell is also manufactured by Ring. It too is a high definition (1080 HD) motion-activated video security cameras with a wide-angle lens, infrared night vision, built-in microphone and speakers, two-way audio facility and a 110-decibel alarm. Like the Ring Spotlight Cams, its sends motion-activated alerts in the form of a 30 second video clip, and can also be used to provide video and audio feeds on demand at the push of a button on the app. The manufacturer's information discloses that it has a wider field of view than the Ring Spotlight Cams, at 155 degrees horizontal.

A "controller" of personal data is defined in Article 4 of the UK GDPR as a natural or legal person... which alone or jointly with others determines the purposes and means of the processing of personal data as in the case, the claimant does not clearly mention the purpose of the audio recording collection. Thus, the processing of personal data is not lawful unless it is necessary for one of the specified purposes (Zuiderveen Borgesius, 2015).

Section 167 of the DPA provides the court with jurisdiction to grant injunctive relief if it is satisfied that there has been an infringement of the data subject's rights under the data protection legislation in contravention of that legislation and may make an order for the purposes of securing compliance with such legislation. That can be an order requiring a data controller to take specified steps, or refrain from taking specified steps and to put a timetable in place for compliance (Calder, 2021).

The Claimant seeks damages for the harassment and data protection breaches and the judge have found and injunctive relief relating to the removal of the Shed Camera, the Removal of the Ring Doorbell and preventing the reinstallation of the Driveway Camera.

At the end, the court awarded the Claimant's claims in harassment and breach of the DPA 2018 succeed and defendant's ring doorbell must be removed. Furthermore, this case became remarkable as Judge stated that video data collection just lawful and declare that audio collection is unlawful (Rowden & Wallace, 2018). As many homeowners does not aware to the potential issues that might be arise especially from personal data protection law compliance, special consideration should be given to the audio recording aspect of smart video equipment, as it has the potential to significantly infringe upon privacy. This might potentially result in a violation of the General Data Protection Regulation (GDPR), even if the utilisation of video capture can be deemed justifiable (Gumzej & Dragicevic, 2019; Sharma, 2019).

Rights of Data Subject When a Domestic CCTV Get Breached

If an individual's personal information is unlawfully accessed through a domestic CCTV system that includes biometric data, the person responsible for controlling the equipment may be held liable according to data protection regulations. Furthermore, according to the UK PDPA, a controller may be held accountable for failing to adhere to data protection legislation. Furthermore, individuals have the ability to exercise many rights under the UK PDPA.

In addition, if the compromised data are sensitive data (in casu biometric data) data subject are entitled to notification without undue delay as controller are in the best position to determine which channels of communication are most suitable for notifying individuals of a security incident, especially if those individuals frequently engage with their customers. Nonetheless, it goes without saying that a controller should exercise caution when utilising a compromised contact channel, as this channel could also be exploited by assailants posing as the controller.

Homeowner Private Liability on Biometric CCTV Data Breach

Installing a biometric CCTV camera as a domestic surveillance tool possess many risks, so, in majority of the data protection laws around the world, installing domestic CCTV requires checks and even privacy impact assessment as it categorised as an intrusive surveillance media. Thus, in the case of protection failure, homeowner could be held liable under the law.

In addition, CCTV installation must be satisfying data minimisation principle, storage limitations, lawfulness, fairness, and transparency principles. Along with that, on the case of *Fairhurst v Woodard*, the claimant argued that the Cameras collected such personal data, that the transmission to the Defendant's phone or computer or other

device, the retention of any such images or sound on such a device and their onward transmission to others.

As the defendant, acquired data beyond the borders of his property, primarily via the Driveway Camera but additionally through the other Cameras, implies that he must show the Court that such data processing is permissible.

Domestic CCTV Dispute Settlement

Having a CCTV dispute with your neighbour is an exquisite matter as it deals with privacy concerns, legal actions, and property rights. Moreover, this kind of dispute will lead to deterioration of neighbourly relations. Here are some things to consider when resolving a CCTV dispute with your neighbour.

1. Open Communication:

Initiate an open and respectful dialogue with your neighbour. Both parties shall show their good faith to communicate and settle the dispute. This includes listening actively and explain our perspective to understand each other.

2. Review Local Regulations:

Familiarize yourself with local laws, ordinances, and regulations governing the use of surveillance cameras. Ensure that your installation complies with these rules.

3. Offer Compromises:

If feasible, propose compromises to address your neighbour's concerns. This may include adjusting the camera's positioning, altering its field of view, or setting specific times for recording.

4. Use Privacy Features:

If your CCTV system offers privacy features, such as motion detection zones or the ability to schedule recording times, consider using these to minimize intrusions on your neighbour's privacy.

5. Seek Mediation:

If direct communication does not lead to a resolution, consider engaging a neutral third-party mediator. Mediation can help facilitate a constructive conversation and find common ground.

6. Legal Advice:

Consult with a legal professional to understand your rights and responsibilities concerning the CCTV camera. They can provide guidance on how to proceed within the bounds of the law.

7. Document Agreements:

If you and your neighbour reach an agreement on changes to the camera setup or its usage, document the agreed-upon terms in writing. Both parties should sign the agreement for clarity and future reference.

8. Install Warning Signs:

Place visible warning signs indicating the presence of CCTV cameras on your property. This can help address privacy concerns and inform individuals that they are being recorded.

9. Consider Removal or Relocation:

If the dispute remains unresolved and your neighbour's concerns are valid, consider whether relocating or removing the CCTV camera is a viable option.

10. Legal Recourse:

As a last resort, if all attempts at resolution fail, consult with an attorney to explore potential legal actions or defences based on local privacy and property laws.

Remember that maintaining a good relationship with your neighbour is often more valuable than the surveillance footage your camera captures (Lyon, 2018). Prioritize open communication and compromise to find a solution that respects both your security needs and your neighbour's privacy concerns.

Conclusion

In conclusion, this writing has delved into the realm of data protection law. Throughout the analysis of doctrinal legal research and analysing relevant cases, statutes, academic journals, government, or data protection authorities' guidelines, and relevant web article, we have found several important issues to highlight.

Install CCTV only in necessary areas and avoid monitoring private areas such as bedrooms or other personal spaces. Ensure that the CCTV is not directed towards neighboring homes or irrelevant public areas.

This research highlighted the importance of awareness of the data controller to ensure every data they possess is satisfying data protection principles and stressing on the building of privacy awareness by both data subjects and data controller. Moreover, this research is contributing to the understanding of private liability on biometric CCTV in the realm of legal concept and offering reference to enhance privacy awareness in the society. Finally, this writing contributes to undergoing discourse on cyber law field especially in data protection law and provide insights for academician, practitioner, and society.

Bibliography

- Alexander, Christopher Bret. (2019). The general data protection regulation and California consumer privacy act: The economic impact and future of data privacy regulations. *Loy. Consumer L. Rev.*, 32, 199.
- Calder, Alan. (2021). The EU data protection code of conduct for cloud service providers: a guide to compliance.
- Dahmen, Jessamyn, Thomas, Brian L., Cook, Diane J., & Wang, Xiaobo. (2017). Activity learning as a foundation for security monitoring in smart homes. *Sensors*, 17(4), 737.
- Di Martino, Mariano, Robyns, Pieter, Weyts, Winnie, Quax, Peter, Lamotte, Wim, & Andries, Ken. (2019). Personal Information Leakage by Abusing the {GDPR}'Right of Access'. Fifteenth Symposium on Usable Privacy

- and Security (SOUPS 2019), 371–385.
- Elmaghraby, Adel S., & Losavio, Michael M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research*, 5(4), 491–497.
- Fairhurst, Michael, Li, Cheng, & Da Costa-Abreu, Márjory. (2017). Predictive biometrics: a review and analysis of predicting personal characteristics from biometric data. *IET Biometrics*, 6(6), 369–378.
- Gumzej, Nina, & Dragicevic, Drazen. (2019). Video Surveillance in the Workplace under the Croatian Act on Implementation of the General Data Protection Regulation. *Zbornik PFZ*, 69, 327.
- Kettley, Sarah. (2021). Lifelines. *Airea: Arts and Interdisciplinary Research*, (3), 35–51.
- Lyon, David. (2018). *The culture of surveillance: Watching as a way of life*. John Wiley & Sons.
- Makarim, Edmon. (2021). Privacy and personal data protection in indonesia: the hybrid paradigm of the subjective and objective approach. *Data Protection Around the World: Privacy Laws in Action*, 127–164.
- Prasad M, Deva, & Menon C, Suchithra. (2020). The Personal Data Protection Bill, 2018: India's regulatory journey towards a comprehensive data protection law. *International Journal of Law and Information Technology*, 28(1), 1–19.
- Rawat, Abhishek, Deb, Dipankar, & Upadhyay, Jatin. (2021). *Recent Trends In Peripheral Security Systems*. Springer.
- Rowden, Emma, & Wallace, Anne. (2018). Remote judging: The impact of video links on the image and the role of the judge. *International Journal of Law in Context*, 14(4), 504–524.
- Sharma, Sanjay. (2019). *Data privacy and GDPR handbook*. John Wiley & Sons.
- Wright, Jordana, Glasbeek, Amanda, & van der Meulen, Emily. (2015). Securing the home: Gender, CCTV and the hybridized space of apartment buildings. *Theoretical Criminology*, 19(1), 95–111.
- Zuiderveen Borgesius, Frederik J. (2015). Personal data processing for behavioural targeting: which legal basis? *International Data Privacy Law*,

5(3), 163–176.