



Privacy Interest Vis a Vis National Security Interest in the Regulation of Video Surveillance Services: Lesson Learned from Indonesia

Brian Amy Prastyo

Universitas Indonesia

Sulistyanto Widagdo

Universitas Indonesia

Abstract

The integration of video surveillance system with artificial intelligence makes the system able to perform automated analysis and automated decision making. Thus the use of video surveillance system has raised the issues of privacy protection. That leads to the question whether the regulation for the business of video surveillance system should be controlled by the government. By applying normative legal approach, the authors found out that in Indonesia the arrangement of video surveillance system services is divided into several business classifications. Furthermore it is suggested that the regulation for the business of video surveillance system should balance the interests of the protection of privacy and the safeguarding of national security.

Keywords: video surveillance systems, cctv, privacy, national security, cyber law

Introduction

Competition among business operators of video surveillance systems has made this service business grow rapidly. Now video surveillance systems can be used to perform automatic identification systems by matching biometric data, automatic detection or tracking of objects, detecting an activity automatically, until the results of machine analysis can make automatic decisions, and many other advanced capabilities.

The increasing use of video surveillance systems makes the question of how a person can have privacy in public if every movement can be observed by others, this will also make people start to worry or worry that what they do will be misinterpreted or cause negative consequences. In addition to privacy issues, video surveillance systems are susceptible to security problems due to weak security systems such as the breach of video surveillance system security that will occur abuse, one example such as law enforcement or state affairs that can be breached by terrorists or enemies, instead will become "double vision" which is a weapon for yourself.

Therefore, the debate always arises, especially between those who need the use of a video surveillance system with individuals, communities and activists who defend human rights (especially privacy rights here). The results of the search of the author in several previous studies indicate that efforts to formulate the legality of the use of video surveillance systems aim to balance the interests between users, organizers, and those affected by video surveillance systems. (Gras: 2004, de Vries & van der Burgt: 2005, Rajpoot & Jensen: 2015). Gras believes that regulation is the key to providing solutions to balance the interests of the parties in the implementation of a video surveillance system. (Gras: 2004) However, it has not elaborated further to what extent regulations related to business licensing affect the business of video surveillance services and are able to balance national security interests with the interests of privacy protection.

The author examines the rules regarding business licensing in Indonesia to assess which approaches of interest tend to be prioritized in Indonesia. By learning from Indonesia's experience, the authors recommend that video surveillance services businesses need to be supervised by an independent body.

Methods

The authors collect rules in Indonesia related to business licensing of video surveillance services. The rules are grouped into 3 (three) classifications, namely business licensing rules issued by the ministry of commerce, rules for the implementation of electronic systems issued by the ministry of communication and information, and rules related to the duties and functions of the state police. These rules are then analyzed qualitatively using a conceptual approach.

The concept of surveillance itself is not something new. Staples, Foucault and Lyon have each proposed definitions of the term surveillance. Staples defines it as "the act of keeping a close watch on people." (Staples: 1997) While Foucault defines it as a "micro-technique of discipline that targets and treats the body as an object to be watched, assessed and manipulated." (Mathiesen: 1997) Lyon, which views surveillance with a view to monitoring everyday life, defines surveillance as a "collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data has been garnered." (Lyon: 2001) The definition of Lyon provides an overview, both direct and indirect surveillance, utilizing electronic technology and depending on information from each individual. Object focus is more personal and not only the body but information collected.

Results

In Indonesia there are 3 (three) business classifications that are included in the video surveillance system services business. First, trade in video surveillance systems, not just hardware or equipment, but also software. In this classification related regulations, there is within the scope of authority of the Ministry of Trade authority, but not limited to Law Number 7 of 2014 concerning Trade and other regulations that are level or below, such as the provisions of trade permits, namely Trading Business Licenses (SIUP), Figures Importer Identity (API), Customs Registration Number (NIK), as well as standardization and certification of video surveillance systems.

Second, the electronic system administration service business, in this classification related regulations, is within the scope of the authority of the Ministry of Communication and Information Technology, with regulations such as but not limited to Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, as well as other regulations at the level or below, such as provisions for registration of electronic system providers for those who oversee public servants, need to have governance policies, operating procedures, security systems from security attacks, audit mechanisms that are carried out periodically against the Electronic System which can be carried out independently (self assessment) and then apply the management system security information standards such as SNI ISO / IEC 27001 and other standards.

Third, the provider of the security system, which is the business operator that provides services to carry out operational activities of video surveillance systems. In Indonesia, it is referred to as the Security Services Business Entity (BUJP) which is within the scope of the authority of the Indonesian National Police, with regulations such as but not limited to KAPOLRI No Pol Regulation: 17 of 2006 concerning Guidance for Guidance for Security Services Enterprises, as well as other regulations of the same level. In addition to that it is also necessary to promulgate the provision of a service business license for the application of security equipment, a certificate as an association of an Indonesian security services business entity, implementing a security management system standard, and making an audit report on its business activities.

The constellation of laws and regulations shows that Indonesia has not constructed a balanced regulation between the interests of protecting privacy and national security interests. The absence of specific licensing arrangements related to the marketing and installation of video surveillance has resulted in the product trading business becoming very widespread in Indonesia. However, these conditions appear to be out of control, because there are no rules that show that there are government agencies in Indonesia that routinely evaluate the benefits and side effects of the business. Until now there is no government agency in Indonesia

that provides information to the public about how safe the data obtained from the operation of camera surveillance is and what actions have been taken against its abuse. This indicates that the main parties benefiting from the conditions of trading in video surveillance services are the perpetrators of service businesses only. While the benefits of improving the quality of privacy protection are not visible.

Indonesia has laws on intelligence that gives the intelligence agency immense authority to collect data. However the rule of law in Indonesia can be said not to make it possible for the public to know the extent of the intelligence agency's ability to collect data from the results of operating camera surveillance and how much data it has collected. Therefore, these conditions actually increasingly make privacy protection increasingly neglected, because the public cannot evaluate the performance of intelligence in preventing abuse of data collection results from camera surveillance.

Based on these findings, a rule that forms a supervisory body is needed. This Supervisory Board needs to make a Guidelines for Video Surveillance System, which contains guidelines on the installation, use and implementation of video surveillance systems, such as how to use a video surveillance system so as not to cause privacy violations and how to manage data or information from the results of the surveillance of video surveillance systems for users of video surveillance systems. There is also a need for a list of standards for video surveillance systems that can be followed by the organizer. In addition, it is also necessary to require certification from providers of video surveillance systems. The certification shows that the providers of video surveillance systems have operated and run their businesses in the implementation of video surveillance systems in accordance with existing provisions, adhering to existing standards, and avoiding the existence of misuse and violation of data or personal information contained in the system he made or in the operation of the video surveillance system. This certification can be given by a third party who has the authority and competence provided by the state in this case the government to assess the video surveillance system held by the organizer in accordance with all existing legal provisions and does not violate the privacy of other parties.

In addition, it can be added to the registration of permits in each installation of the use of a video surveillance system to the Superintendent who can delegate the authority to grant the permit to the local government to facilitate the public in registering permits in areas that will be installed by video surveillance systems and make it easier for Supervisors to supervise.

* We gratefully acknowledge financial support from Universitas Indonesia through PITTA program.

References

- Boulanin, Vincent. (2012). Defence and Security Industry: Which Security Industry are You Speaking About? IRSEM. Paris Papers N°6
- Costin, Andre. (2016). Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations, TrustED '16 Proceedings of the 6th International Workshop on Trustworthy Embedded Devices, 45-54. doi: 10.1145/2995289.2995290
- James Vincent, Artificial Intelligence is going to supercharge surveillance, <https://www.theverge.com/2018/1/23/16907238/artificial-intelligence-surveillance-cameras-security> accessed on 13 February 2018
- Liss, C. (2014). Security Sector Reform in Southeast Asia: The Role of Private Security Providers. In: Heiduk F. (eds) Security Sector Reform in Southeast Asia. Critical Studies of the Asia Pacific Series. Palgrave Macmillan, London. doi: 10.1057/9781137365491_7
- Lyon, David. (2001). Surveillance Society: Monitoring Everyday Life, Philadelphia: Open University Press.
- Mahmood Rajpoot, Q., & Jensen, C. D. (2015). Video Surveillance: Privacy Issues and Legal Compliance. In V. Kumar, & J. Svensson (Eds.), Promoting Social Change and Democracy through Information Technology IGI global. doi: 10.4018/978-1-4666-8502-4.ch004
- Marianne L. Gras. (2004). The Legal Regulation of CCTV in Europe. Surveillance & Society, The Politics of CCTV in Europe and Beyond. (2) 2/3, 216-229. doi: 10.24908/ss.v2i2/3.3375
- Marti, Carlos. (2011). A Survey of the European Security Market. Economics of Security Working Paper 43. Berlin: Economics of Security
- Marx, Gary T. (2002). What's New About the "New Surveillance"? Classifying for Change and Continuity. Surveillance & Society, 1 (1): Launch Issue, 8-29. doi: 10.24908/ss.v1i1.3391
- Marx, Gary T. (2015). Surveillance Studies. In International Encyclopedia of the Social & Behavioral Science (2ns ed.) edited by James Wright, 23:733-741. Oxford: Elsevier.
- Mathiesen, Thomas. (1997). The Viewer Society: Michael Foucault's 'Panopticon' Revisited, Theoretical Criminology, 1 (2), 215-234. doi: 10.1177/1362480697001002003
- Miller, Kevin. (2014). Total Surveillance, Big Data, and Predictive Crime Technology: Privacy's Perfect Storm, Journal of Technology Law & Policy, 19:105-146
- Nord, G. Daryl, Tipton F. McCubbins, Jaretta Horn Nord. (2006). E-Monitoring in the Workplace: Privacy, Legislation, and Surveillance Software. Communications of the ACM, 49 (8), 72-77 doi: 10.1145/1145287.1145290
- Nouwt, J.; de Vries, B.R.; van der Burgt, D. (2005). In S. Nouwt, B. R. de Vries, & C. Prins (Eds.), Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy, Information Technology & Law Series; No. 7, 114-137



- Richards, A. & Smith, H., (2007). Addressing The Role Of Private Security Companies Within Security Sector Reform Programmes. Saferworld, London.
- Slobogin, Christopher. (2002) Public Privacy: Camera Surveillance of Public Places and The Right to Anonymity. Mississippi Law Journal, Vol. 72, 213-315. doi: 10.2139/ssrn.364600
- Staples, W. G. (1997). The Culture of Surveillance: Discipline and Social Control in the United States, New York: St. Martin's Press.