P. BUZÁS, B. RÉVÉSZ

Péter Buzás, Balázs Révész*

DRONES AND THE PROTECTION OF PRIVACY WITHIN THE JURISPRUDENCE OF THE SUPREME COURT OF THE UNITED STATES

In the far distance a helicopter skimmed down
between the roofs, hovered for an instant like a bluebottle,
and darted away again with a curving flight. It was the police
patrol, snooping into people's windows.
/George Orwell: 1984/

Introduction

The use of unmanned aerial systems (UAS),[1] similarly to other modern surveillance technologies, may significantly affect the private life of the citizens by facilitating the collection of vast amount of information for law enforcement authorities. Some people are willing to sacrifice their privacy in order to live in a safer world expecting a positive trade-off between privacy and security.[2] Others have expressed concern regarding the application of the above-mentioned technologies.

Critics highlighted the negative impacts of the use of drones on privacy, taking into account the threats of surveillance in general. Furthermore, as these technologies became more advanced and at the same time publicly more available, concerns have been raised that the principles protecting privacy developed by the Supreme Court of the United States (SCOTUS) may not be efficiently applied regarding the use of UASs. Notwithstanding the lack of a judgment concerning drones, there is a solid case-law the collection of information by law enforcement authorities that shapes the protection of privacy in the U.S. These principles, constitutional tests and precedents may be rendered inapplicable in the future by the use of UASs by the authorities.

This article aims to provide an overview on the case-law of the SCOTUS concerning the right to privacy, and the applicability of the principles developed by the court in relation with the use of UASs by the authorities. Chapter 1 examines the impact of the use of drones on private life and the so-called panoptic effect. Chapter 2 analyzes the two primary arguments developed in the case-law of the SCOTUS on privacy: the property- and the privacy based approaches. Chapter 3 and 4 scrutinizes the aerial surveillance, and the decisions regarding the use of modern technology cases in accordance with the two main characteristics of drones. The article concludes that the approaches currently used by the SCOTUS do not protect the privacy of citizens. Therefore, as a solution, it draws the attention to the measures that may provide protection against unlawful use of drones by authorities: the need for a new approach applied by the courts, and to the importance of legislative actions in this rapidly developing field.

1. The Impact of the Use of Drones on Private Life

Today hundreds of "civilian" application of UASs are known.[3] One of the most rapidly developing field is the use of drones for law enforcement purposes. These systems may be equipped with technologies capable of collecting, recording, transmitting or processing information.[4] Furthermore, the technology facilitates the surveillance of one or more people, for instance the possible suspects of a crime.[5] These characteristics may serve the purposes of

* ***Péter Buzás*** *JD is currently the head of Unit of Freedom of Information at the National Authority for Data Protection and Freedom of Information. His professional expertise covers various aspects of the information rights. He has been a lecturer at ELTE Institute of Postgraduate Legal Studies since 2014. He teaches several courses on data protection, data security, and freedom of information. He is currently enrolled with his Ph.D. studies. His field of interest is the intersection of human rights and bioethics within the jurisprudence of the ECtHR. Mr. Buzás is the author of several academic articles and presentations on bioethics and human rights, data protection, and freedom of information.*

Balázs Révész *JD is currently the head of Department of Audit and Freedom of Information at the National Authority for Data Protection and Freedom of Information. He has been a lecturer at various institution, such as the National University of Public Service and at ELTE Institute of Postgraduate Legal Studies. He teaches several courses on data protection and freedom of information. He is currently enrolled with his Ph.D. studies. His field of interest is the data protection and freedom of information concerning the elections from a comparative perspective. Mr. Révész is the author of several academic articles and presentations on data protection and freedom of information.*

prevention or detection of and fight against crime.[6] Therefore, law enforcement authorities more frequently apply UASs throughout their operations.[7] On the other hand, these systems considerably extend the power of the state over the everyday life of citizens. The technological component of UASs implies the possibility for serious interference with the individual's private life.[8] The moving platform only amplifies this impact.

The three main risks concerning privacy are the continuity, invisibility and the mass nature of surveillance. Firstly, the surveillance via these systems may be continuous. Between certain technical boundaries, drones may be operated for longer periods of time without interruption. Secondly, the surveillance by drones may be invisible since there is little or no chance for the individual to detect them.[9] Thirdly, the UASs may carry out mass surveillance. The technological and movement capabilities of these systems provide for the collection, recording and processing of information concerning masses of people.[10]

The three main risks culminate in the so-called "panoptic effect".[11] Due to fear of sanctions or other negative consequences, the individual under surveillance is more likely to obey the rules. However, this effect is independent from the actual surveillance hence even the slightest possibility may affect the person's behavior. Furthermore, the panoptic effect adversely affects human creativity and autonomy. The individual under surveillance is more likely to behave in accordance with actual or presumed expectations. According to Daniel J. Solove: "Surveillance is a different kind of privacy problem than disclosure, imposing a different type of injury to a different set of practices. Surveillance differs from disclosure because it can impinge upon practices without revealing any secrets. Being watched can destroy a person's peace of mind, increase her self-consciousness and uneasiness to a debilitating degree, and can inhibit her daily activities".[12]

2. Basic Approaches reading the Protection of Privacy

Since the use of drones for law enforcement purposes threatens the privacy of individuals, the question arises that how could the constitutional system of the U.S. limit the application of such technologies. What constitutional principles apply to these activities of the authorities? Would these principles provide sufficient protection for citizens?

The Constitution of the U.S. does not contain a provision of the citizens' right to privacy.[13] However, the Fourth Amendment states that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized".[14] Originally, this provision recognized the principle of sanctity of property that protected against unreasonable searches and seizures on behalf of the government.[15] However, the Fourth Amendment has subsequently been used by SCOTUS to protect the private life of the citizens in general, e.g. against any kind of unwanted interference of the authorities.[16] It may then be concluded that currently this provision serves as the strongest constitutional limit regarding the use of drones for law enforcement purposes.[17]

Considering the relevant case-law, there are two different approaches developed by the courts concerning the Fourth Amendment. The first and historically the older one focuses on the protection of the individuals' property.[18] According to this line of judicial reasoning, the basis of constitutional protection is the property and all adjacent areas owned by the citizen. These premises are inviolable without due cause and the necessary judicial warrants. On the other hand, the starting point of the second argument is the reasonable expectation of the individual and the society concerning the boundaries of privacy. This approach thus emphasizes a rather subjective side of the protection outlined in the Fourth Amendment.

2.1. Property-based protection

The early jurisprudence of the SCOTUS based the decision a Fourth Amendment search had occurred on the common-law notion of trespass, and therefore on the protection of property.[19] The argument was first applied by the court in the case of Boyd v. United States in 1886.[20] In its judgment, the SCOTUS linked the constitutional protection of privacy to the property of the citizen by recognizing that the common law principle of the sanctity of property inspired the wording of the Fourth Amendment.[21] However, the most famous precedent in this respect is Olmstead v. United Sates.[22]

In Olmstead, the SCOTUS had to decide whether the wiretapping of telephone cables outside the apartment of the defendant shall be considered as search under the Fourth Amendment. In its judgment of 1928 – with a narrow majority – the court found that the surveillance had not infringed the rights of the defendant. According to the majority, the activities of the authorities had not been aimed at material objects, such as the person, his home or his documents. Human speech – similarly to naked eyesight – is immaterial therefore it may not serve as the basis of constitutional protection.[23] The second line of reasoning focused on the physical trespass argument. The court found in this respect that no unlawful search had occurred, since "the wiretaps were not a physical intrusion into a constitutionally protected area".[24]

It is obvious, that the application of the traditional, property-based approach to the use of drones provides no efficient safeguards to privacy of the individual.[25] The basis of the technology is its maneuverability and movement in airspace, therefore it would not "cross" the borders of private property. In the absence of physical trespass however, no Fourth Amendment search occurs regarding the use of UASs.[26]

2.2. Privacy-based protection

Although Olmstead did not receive favorable reactions from the public, it was the precedent for almost four decades.[27] In the late 1960s, as developments in the field of surveillance technologies raised more privacy concerns, the courts realized the insufficiency of the property-based protection of privacy. Therefore, a new approach emerged in the jurisprudence that focused on the individual's subjective and society's objective expectations of privacy instead of the physical trespass into one's property. The key judgment in this respect is the Katz v. United States.[28]

In Katz, the SCOTUS had to decide whether the wiretapping of a public telephone booth shall be considered as search under the Fourth Amendment. The court signaling the shift in its approach stated that constitutionality of the operation of the authorities shall be based on the expectations of the individual concerned: the Fourth Amendment protects the people not places.[29] According to the majority, the protection does not apply to activities that are made purposely public by the individual, even in his or her home or office. On the other hand, private activities carried out even in a publicly accessible area be subjected to constitutional protection.[30] The court thus focused on the intent of the defendant at the moment of entering the telephone booth and closing its doors. Recognizing the role of the telephone in modern society and telecommunications, it found that the defendant used the telephone booth under the presumption that his conversation in it remains private.[31] Consequently the police had violated his rights under the Fourth Amendment when it used wiretapping technologies.[32]

The arguments of the SCOTUS in Katz introduced the new, privacy-based approach to the jurisprudence. However, the majority decision did not provide clear-cut guidelines for the courts. The so-called Katz test has been derived from Justice Harlan's famous concurring opinion. The test has two basic prongs considering the constitutionality of any privacy intrusion. Firstly, the court shall examine whether the individual concerned has an actual expectation for the respect for his or her privacy.[33] Secondly, whether this expectation was considered reasonable by society.[34] The activities of the authorities will only be lawful in the case they comply with both the individual's subjective and society's objective expectations concerning privacy.[35]

The application of the Katz test to the use of UASs by authorities would have a slightly different outcome as the property-based approach. The subjective prong of the test would usually be met concerning areas where the individual has a reasonable expectation of privacy, for instance, the home, the curtilage, or any similar area.[36] However, the protection only applies when the individual took the necessary measures, such as the building of a fence, to protect the area against unwanted intrusion or trespass. Areas like open fields does not fall under the Fourth Amendment.[37] Even if the use of drones falls under the subjective prong of the Katz test, fulfilling the requirement of the objective prong would be more difficult. In case the constitutionally protected area become visible for external viewers, the subsequent collection of evidences is usually considered lawful by the courts. Due to their physical and technological capacities, UASs may gather information through ways that used to be considered impossible. For instance, through a little hole in a wall, or via thermal sensors. These capabilities may render the constitutional protection insufficient.[38]

3. Aerial Surveillance Trilogy[39]

Taking into account the technological capabilities of UASs, both the traditional property-based approach and the Katz test provide insufficient protection to privacy. The maneuverability and the application of modern technologies are factors that may render the constitutional principles inapplicable for surveillance carried out by drones. Thereafter, the jurisprudence of the SCOTUS concerning aerial surveillance and information gathering via the use of modern technologies shall also be examined.

Considering the constitutionality of aerial surveillance of the home, there three pivotal precedents in the relevant jurisprudence. In these cases, the court extended the application of the Katz test to situations in which the authorities used aircrafts in order to gather information and evidence concerning suspect of possible crimes. The decisive factors regarding the constitutionality of the complained activities were the technology used for surveillance (method) and the vantage point of the person carrying out surveillance (position of the aircraft).

In the case of California v. Ciraolo, the SCOTUS had to decide on the lawfulness of surveillance by the naked eye, from an airplane flying at an altitude of 1000 feet above the property of the Ciraolo. In 1986, the court found that the defendant had had a reasonable expectation of privacy concerning all activities carried out in his backyard surrounded by a fence, even in respect of the possession of illegal plants grown therein, therefore the case fell under the subjective prong of Katz test. On the other hand, the majority noted that police surveillance had been carried out from the publicly navigable airspace, at the altitude used by civilian aircrafts as well, hence all evidence had been gathered without physical trespass of the property. Furthermore, society had not recognized the defendant's expectation of privacy as reasonably since anyone travelling at the same altitude could have observed the criminal activities taking place in the property of Ciraolo.[40] The surveillance complained therefore had not met the objective requirement of the Katz test.[41]

In Dow Chemical Co. v. United States[42] the SCOTUS examined whether surveillance of an industrial area from 1200, 3000 and 12000 feet using a standard aerial mapping camera, constitutes search under the Fourth Amendment.[43] It found that the area owned by the company shall be considered as open field to which the constitutional protection had not been extended.[44] Finally, the court briefly dealt with the issue of the technology and noted that the camera used by the authorities had been available for the public. According to the SCOTUS, surveillance via commercial technologies did not violate the right to privacy of the citizens.[45]

In the 1989 case of Florida v. Riley the court examined whether surveillance of "the interior of a partially covered greenhouse in a residential backyard from the vantage point of a helicopter located 400 feet above the greenhouse" constitutes search under the Fourth Amendment.[46] While it found that the defendant had had an expectation of privacy concerning the interior of the greenhouse, this expectation had not been recognized by society as objectively reasonable.[47] The SCOTUS took into account that the helicopter used by the court had been flying in accordance with FAA regulations at the time of the case.[48] Since anyone travelling at an altitude of 400 feet could have surveilled the illegal activities of the defendant through partially covered roof of the greenhouse, the activities of the authorities had not violated to the Fourth Amendment.[49]

Since the operation of UASs is very similar to that of the fixed-wing aircrafts – airplanes or helicopters –, principles applied in the so-called Aerial Surveillance Trilogy shall also be taken into account regarding the use of drones for gathering of information by the authorities. Firstly, any surveillance carried out from a lawful vantage point, e.g. an altitude considered legal by the FAA, does not violate the rights of the citizens. Observance from an aircraft flying in the navigable airspace is constitutional, unless it endangers the health or life of the individuals.[50] Secondly, difference shall be made between naked eye surveillance and surveillance via the use of modern technologies. Information collected by naked eye and by commercial technologies is usually deemed lawful. On the other hand, the application of technologies that extends the information gathering capabilities of the person beyond naked eye, or technologies not available for the public may be considered the infringement of the right to privacy.

4. Modern Technologies and the Protection of Privacy

It may be concluded from the jurisprudence concerning aerial surveillance that the technological component rather than the maneuverability may be the decisive factor of the use of UASs for collection of information. Modern technologies not only facilitate surveillance but extend the capabilities of authorities beyond everyday observations. As a consequence, it is necessary to analyze the relevant case-law of the SCOTUS concerning the used of advanced intelligence technologies.[51]

In United States v. Knotts the court had to decide on the constitutionality of a tracking device attached to barrels containing chemicals used for drug production, for the purposes of surveilling the movement of the defendant in public areas, such as roads.[52] The SCOTUS found that the outcome of the applied technology had been similar to the naked eye surveillance and following of the defendant by authority personnel.[53] Furthermore, it took into account that the tracking device had not transmitted signals from within constitutionally protected areas.[54] As a consequence, the court stated that the defendant could not have a reasonable expectation of privacy whilst travelling on public roads hence a Fourth amendment search had not occurred.[55] However, it also noted that unlimited and continuous surveillance may infringe upon the right to privacy.[56]

In the similar case of United States v. Karo, the SCOTUS found that the use of a tracking device violated the Fourth Amendment rights of the defendant.[57] In its judgment, the court found that the authorities could not observe the movement of the barrels containing chemicals used for drug production via the naked eye. Instead, they had fallowed the signals transmitted by the device. However, the technology had been operation from within the home of the defendant, a constitutionally protected area.[58] Consequently, the SCOTUS considered the activities of the authorities to be a Fourth Amendment search.[59]

In Kyllo v. United States the SCOTUS examined whether the use of a thermal-imaging device to detect heat signatures within a private home was unconstitutional.[60] The court faced for the first time in its jurisprudence the problem of surveillance of a constitutionally protected area with a technology that does not imply physical intrusion into the observed area.[61] To this end, it decided to apply both the property-based approach for the protection of privacy and the Katz test. Utilizing these arguments, the SCOTUS found that the use of any technology that enables the collection of information that would have been unobtainable without physical intrusion into a constitutionally protected area, violated the Fourth Amendment.[62] However, the applicability of this new principle was limited by the court to technologies that are not in "general public use".[63] According to the majority, since the thermal-imaging device applied in the case of Kyllo had not been available for the general public, the authorities had violated the right to privacy of the defendant.

The recent judgment in United States v. Jones may be considered the most important since Katz.[64] In the case, the SCOTUS examined whether a surveillance by a global positioning device attached to the defendant's vehicle for 28 days violated the Fourth Amendment.[65] The authorities had obtained a warrant legalizing the surveillance for 10 days, however they only attached the tracking device to the vehicle on the 11th day, and subsequently collected more than 2000 pages of information.[66] In its judgment, the court returned to the property-based approach and found that the attachment of the global positioning device to the vehicle constituted physical trespass into the defendant's property.[67] Since the warrant had already been expired at the time of the application of the device, the right to privacy of the defendant had been violated by the authorities.[68] Notwithstanding the use of a rather originalist argument in the judgment, Justice Scalia writing for the majority emphasized that the Katz test had not been overturned, its application is only complemented by the property-based protection of privacy.[69]

Considering the constitutionality of the technological aspects of the use of drones, two main factors shall be examined. Firstly, whether the UASs applied for surveillance is a technology in general public use. In this respect, devices used for recreational or sport purposes meet this requirement.[70] However, there had been occasions where law enforcement authorities operated a UASs developed primarily for combat situations that is obviously been available for the public.[71] One may conclude that drones in general are available for the public on the market due the

commercialization of recreational devices but does this mean that all kinds of UASs fall under the requirement developed in Kyllo? And even if the drone itself is used in general public, the information processing technology equipped on it may not be considered as such. For instance, the most developed optical, infrared, thermal or other sensors capable of collecting information from a constitutionally protected area without physical intrusion may not be obtained from the commercial market, thus surveillance applying these devices would be contrary to the Fourth Amendment. But for how long? Everyday new technologies are introduced into the daily lives of individuals. The time for the commercialization of new inventions has shortened significantly in the past few decades. The pacing of development may render the above mentioned principles ineffective tomorrow and hence the protection of privacy built on them insufficient.

Conclusion

The SCOTUS has not yet dealt with a case concerning the use of drones by authorities in order to gather evidence or collect other information regarding an individual. As to the current jurisprudence, it may be concluded that there are very few limitations concerning the application of UASs. Approaches applied by the court take into account facts that are already superseded by the drones solely because of their technological characteristics. The current constitutional framework therefore may not provide sufficient protection for the protection of privacy of the individual.

As a solution, some academics have emphasized the need for the development of a new privacy test applied by the SCOTUS in its jurisprudence.[72] The authors argue that the basis of the new approach would be the so-called "mosaic theory" found in two separate opinions in Jones. This theory introduces a kind of holistic approach towards surveillance that focuses on the constitutionality of the activities of the authorities in general instead of every single activity. This way the level of protection of privacy may be significantly raised.[73] Another argument focuses on the efficient legal regulation in this field.[74] They emphasize that the enacted laws may provide for a more efficient protection of unwanted intrusions of privacy. Either way, it is obvious that the use of UASs by the authorities demand urgent answers from both the judiciary and the legislators in order to protect the rights of the individuals.

---

[1] See FAA Modernization and Reform Act of 2012, Pub. L-. No. 112-95. § 331(9).

[2] See for instance Daniel J. Solove: Nothing to Hide – The False Tradeoff between Privacy and Security. Yale University Press, New Haven, 2011.

[3] Towards a European Strategy for the Development of Civil Applications of Remotely Piloted Aircraft Systems (RPAS) (SWD(2012) 259 final). Available at: https://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2013438%202012%20INIT

[4] Jonathan Olivito: Beyond the Fourth Amendment: Limiting Drone Surveillance through the Constitutional Right to Informational Privacy, Ohio State Law Journal, 74(2014)/4. p. 677.

[5] Brendan Gogarty: Unmanned Vehicles, Surveillance Saturation and Prison of the Mind, Journal of Law, Information and Science, 21(2011–2012)/2, p. 181.

[6] Sean Sullivan: Domestic Drone Use and the Mosaic Theory (December 3, 2012). UNM School of Law Research Paper No. 2013-02. Available at SSRN: https://ssrn.com/abstract=2212398 or http://dx.doi.org/10.2139/ssrn.2212398

[7] See Olivito, op. cit., p. 678.

[8] Margot E. Kaminski: Drone Federalism: Civilian Drones and the Things They Carry, California Law Review Circuit, 2013/4, p. 72.

[9] Steven Friedland: The Difference between Invisible and Visible Surveillance in a Mass Surveillance World (February 7, 2014). Elon University Law Legal Studies Research Paper No. 2014-02. Available at SSRN: https://ssrn.com/abstract=2392489

[10] Ibid.

[11] Gogarty, op. cit., pp. 185–189.

[12] Daniel J. Solove: Conceptualizing Privacy, California Law Review, 90(2002)/4, p. 1130.

[13] Brandon Nagy: Why They Can Watch You: Assessing the Constitutionality of Warrantless Unmanned Aerial Surveillance by Law Enforcement, Berkeley Technology Law Journal, 29(2014)/1, p. 143.

[14] Available at: www.law.cornell.edu/constitution/fourth_amendment.

[15] See Entick 95 Eng. Rep. 807(Gr. Brit. 1765)).

[16] Sullivan, op. cit.

[17] Olivito, op. cit., p*,* 682.

[18] See Nagy, op. cit., p. 143–146.

[19] Nagy, op. cit., p. 143.

[20] Boyd v. United States, 116 U.S. 616, 626–627. (1886).

[21] See ibid. pp. 616, 628.

[22] Olmstead v. United States, 277 U.S. 438. (1928).

[23] *Andrew B.* Talai: Drones and Jones: The Fourth Amendment and Police Discretion in the Digital Age, California Law Review, 102(2014)/3, p. 753.

[24] Nagy, op. cit., p. 145.

[25] Thomas Bryan: State v. Bossart: Adapting the Fourth Amendment for a Future with Drones, Catholic University Law Review, 63(2014)/2, p. 488.

[26] Talai, op. cit., p. 761.

[27] Nagy, op. cit., p. 145.

[28] Katz v. United States, 389 U.S. 347. (1967).

[29] Nagy, op. cit., p. 147.

[30] Katz v. United States, 389 U.S. 351. (1967).

[31] Nagy, op. cit., p. 148.

[32] Talai, op. cit., p. 754.
[33] Michael L. Smith: Regulating Law Enforcement's Use of Drones: The Need For State Legislation, Harvard Journal on Legislation, 52(2015)/2, 436.
[34] Ibid.
[35] Nagy, op. cit., p. 148.
[36] Ibid., p. 157.
[37] Bryan, op. cit., p. 472.
[38] Talai, op. cit., p. 76.
[39] Olivito, op. cit., p. 683.
[40] Talai, op. cit., p. 763.
[41] Ibid.
[42] Dow Chemical Co. v. United States, 476 U.S. 227. (1986).
[43] Nagy, op. cit., p. 150.
[44] Ibid., pp. 150–151.
[45] Ibid.
[46] Florida v. Riley, 488 U.S. 445. (1989).
[47] Olivito. op. cit., p. 686.
[48] Smith, op. cit., p. 437.
[49] Nagy, op. cit., p. 153.
[50] Bryan, op. cit., p. 488.
[51] Sullivan, op. cit., p. 23.
[52] United States v. Knotts, 460 U.S. 276. (1983).
[53] Bryan, op. cit., p. 473.
[54] Ibid., p. 474.
[55] Sullivan, op. cit., pp. 13–14.
[56] Smith, op cit., p 441.
[57] United States v. Karo, 468 U.S. 705. (1984).
[58] Bryan, op. cit., p. 474.
[59] Ibid., p. 474.
[60] Kyllo v. United States, 533 U.S. 27. (2001).
[61] Nagy, op. cit., p. 160.
[62] Ibid., pp. 160–161.
[63] Olivito, op. cit., p 687.
[64] Bryan, op. cit., p. 478.
[65] United States v. Jones, 132 S. Ct. 945, 949. (2012).
[66] Sullivan, op. cit., p. 20.
[67] Nagy, op. cit., p. 163.
[68] The SCOTUS applied the property-based approach again in Florida v. Jardines, 569 U.S. (2013).
[69] Nagy, op. cit., p. 163.
[70] Bryan, op. cit., p. 490.
[71] State v. Brossart, No. 32-2011-CR-0049 (Dist. Ct. N.D. July 31, 2012).
[72] Talai, op.cit., pp. 778–780.
[73] Bryan, op. cit., p. 490.
[74] Smith, op. cit., pp. 448–453.