Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study☆

*Uri Volovelsky**

Striks Law School, College of Management, Israel

Keywords:
Unmanned aerial vehicles
Drones
Israel
Privacy
Data
United States
Europe
Federal Aviation Administration
FAA Modernization and Reform Act
Safety

ABSTRACT

In recent years we have witnessed a growing demand for the use of Unmanned Aerial Vehicles ("**UAVs**") in civilian contexts. Government authorities (such as law enforcement agencies), corporations and private individuals have identified the advantages inherent in the use of UAVs. At the same time, corporations marketing and manufacturing UAVs for civilian purposes, and the industries that support these manufacturers, have identified the enormous economic potential which may be derived from the sale and maintenance of UAVs (and the cameras and other equipment assembled into them). Hence, in the coming years, we will undoubtedly witness a rapid expansion of the civilian use of UAVs.

Given the assumption that the entry of UAVs into the civilian market is a certainty, what are the possible implications for the fundamental right to privacy, and does the issue of permits for civilian uses of UAVs indicate that privacy protection laws are now irrelevant? In answering these questions, the article deals with *five* problems. The *first* problem relates to the fact that, although it is a fundamental right, the right to privacy is vague; there is an essential difficulty in defining privacy and the situations in which it applies, including situations that involve the use of UAVs. The *second* problem focuses on finding a balance between the advantages inherent in the civilian use of UAVs and possible harm to the right to privacy and other fundamental rights such as freedom of expression. As the article will describe in detail, it is not possible to determine, *a priori*, whether the advantages of using UAVs outweigh their disadvantages, or vice versa. The *third* problem arises from the possibility of restricting the use of UAVs, either at the data collection stage, or, alternatively, at the stage at which the data is used. As shall be explained, this is a moral question, the answer to which varies from one legal system to another. The *fourth* problem concerns the choice of Israeli law as the basis for examining whether the law can provide suitable tools to deal with the risks involved in the use of UAVs. In this context, it should be noted that although Israel is considered a leading manufacturer of UAVs, Israeli law is unique, *inter alia*, in light of the fact that the Israeli legal system combines elements of both common law and continental law, and the fact that regulation of the use of UAVs in Israel is in its infancy. The *fifth* problem arises from the element of uncertainty. Given that the existing system of laws does not provide a sufficient response to a possible threat to

☆ Winner CLSR 'Best Academic Paper' Award at the 2013 IAITL 8th International Conference on Legal, Security and Privacy Issues in IT Law (LSPI), Bangkok, Thailand, 11–14 November 2013. The article is dedicated with all my heart to my loving parents for their ongoing love, support and advice and for educating me to be a better person, and to my mentor, Professor Tamar Gidron for her friendship, support and wise guidance.

* Striks Law School, College of Management, The College of Management Academic Studies (COMAS), 7 Yitzhak Rabin Blvd., Rishon LeZion, 7502501, Israel.
E-mail address: uri.volovelsky@gmail.com.

http://dx.doi.org/10.1016/j.clsr.2014.03.008

fundamental rights (in the instance discussed in the article, the threat which UAVs pose to the right to privacy), how should the legislature regulate the use of UAVs, without harming the delicate balance between the advantages and disadvantages inherent in their use.

The article focuses on Israel as a case study and also comprehensively examines the solutions to the problems described above, as adopted in the United States and Europe.

1. Introduction

Was it permissible for paparazzi to use an Unmanned Aerial Vehicle ("**UAV**")[1] to photograph Tina Turner's wedding?[2] Should Barbra Streisand have been allowed to suppress free speech protection when an incriminating picture was collected with the aid of a UAV?[3] By what criteria should we judge a person who flies a UAV near the window of a female resident living on the fourth floor of an apartment building?[4] Should UAVs be used for the purpose of monitoring class exams?[5] Bearing in mind the extensive use made by the United States administration of technological means for surveillance purposes, should the police or other governmental authorities be given permits to operate UAVs equipped with cameras, wiretapping equipment, and facial recognition software, for the purpose of policing and law enforcement?[6] If so, under what conditions should such use be permitted? Is it appropriate for commercial corporations, operating on the basis of profit considerations, to obtain a permit to operate UAVs equipped with cameras, knowing that the photographs and images will be sold to the highest bidder?[7] What importance should be given, from the point of view of the right to privacy, to a possible decision by Google to use photographic UAVs, as part of its *Google Street View* service?[8] Are there legal and/or technological means that would allow the preservation of anonymity when such UAVs are used? And, more broadly speaking, will the use of UAVs for civilian purposes (both by a country's legally constituted authorities and private entities) make privacy protection laws irrelevant?[9]

The questions presented above become even more meaningful if we take into account the fact that there is a growing worldwide trend to increase the number of permits issued for civilian uses of UAVs and at the same time they are becoming less expensive to purchase and operate.[10]

The aviation authorities in various countries are the regulatory authorities responsible for granting permits and regulating the operation of UAVs.[11] In the United States, the Federal Aviation Administration ("**FAA**") first authorized the use of UAVs in 1990[12] and since then has granted permits for the operation of approximately 1500 UAVs (of these, 327 permits are still active). These permits were issued to law enforcement agencies, such as the Department of Homeland

[1] A UAV, also known as Unmanned Aircraft System or a drone, is defined as: "A powered, aerial vehicle that does not carry a human operator, uses aerodynamic forces to provide vehicle lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry a lethal or nonlethal payload". Dept of Defense, Dictionary of Military and Associated Terms 494 (2001, amended, April 2010).

[2] Martin U. Müller & Andreas Ulrich, *Snapping Tina's Wedding: Paparazzi Turn to UAVs*, Spiegel Online Int'l (Aug. 1, 2013) http://www.spiegel.de/international/europe/paparazzi-use-UAVs-to-photograph-tina-turner-wedding-in-switzerland-a-914179.html. *See* also the discussion regarding the increased use of UAVs in *Australia in Renee Viellaris, Unmanned aircraft bought online being deployed to monitor private and public property*, Couriermail (Aug. 31, 2013) http://www.couriermail.com.au/news/queensland/unmanned-aircraft-bought-online-being-deployed-to-monitor-private-and-public-property/story-fnihsrf2-1226707858451.

[3] Admin, *Streisand Seeks Court Help to Remove Aerial Photographs*, Atlis Geomatics Down to Earth Information (Dec. 21, 2012) http://www.atlisgeo.com/2012/12/21/streisand-seeks-court-help-to-remove-aerial-photographs/. Kenneth Adelman, founder of the California Coastal Records Project, a scientific photographic database documenting the California coast was hit with a SLAPP suit from Barbara Streisand arguing that a picture taken by a UAV had invaded her privacy. The lawsuit was dismissed. For a comprehensive analysis of SLAPP suits *see* Tamar Gidron, *World Map of Libel Tourism and Defamation Law in Israel*, 15(2) Hamispat L. Rev. 385 (2010).

[4] Rebecca J. Rosen, *So This Is How It Begins: Guy Refuses to Stop UAV-Spying on Seattle Woman*, The Atlantic (May 13, 2013).

[5] Lee Moran, *Drones monitor test-taking students to catch cheating*, New York Daily News *(Jan. 13, 2014)* http://www.nydailynews.com/news/world/drones-monitor-test-taking-students-article-1.1577723.

[6] James Ball, Julian Borger & Glenn Greenwald, *Revealed: how US and UK spy agencies defeat internet privacy and security*. The Guardian (Sep. 6, 2013) http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

[7] Matthew Gryczan, *UAV Industry Set to Soar when FAA Gives Nod*, Crain's Detroit Business (July 7, 2013) http://www.crainsdetroit.com/article/20130707/NEWS/307079980/UAV-industry-set-to-soar-when-faa-gives-nod#.

[8] In Europe, Google is subject to strict conditions regarding the use of its *Street View* service. *See* Mark Hachman, *EU Asks Google for More Privacy in Street View*, PC Magazine (Feb. 26, 2010) http://www.pcmag.com/article2/0,2817,2360725,00.asp; In the United States, Google was subject to claims on the basis of breach of privacy. *See* Jonathan Stempel, *Google Loses Appeal in Street View Privacy Case*, Reuters (Sep. 10, 2013).

[9] Michael D. Birnhack, *Control and Consent: The Theoretical Basis of the Right to Privacy*, 11 Mishpat Umimshal – Law and Government in Israel 11 (2007).

[10] For example, the new pocket drone developed and market by Airdroids is equipped with a camera and operated through the operator's personal tablet; it is sold online for only USD 75. *See* also Damon Poeter, *Is That a Pocket Drone or Are You Just Happy to Spy on Me?* (Jan 10, 2014) PC Magazine http://www.pcmag.com/article2/0,2817,2429406,00.asp.

[11] For an analysis of the problems accompanying the regulation of the aviation authorities' use of UAVs for civilian purposes, *see* Part 4 below.

[12] Federal Aviation Administrartion officeal website http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=14153.

Security and the Federal Bureau of Investigation, as well as to local police stations and universities. There is no question that this number will rise in the near future.[13]

In 2012, the United States Congress passed the FAA Modernization and Reform Act ("**Modernization Act**").[14] Among its other key provisions, the Modernization Act allocates USD 11 billion to the FAA for the purpose of modernizing the air traffic control system. It is planned for United States airspace to be opened to the commercial use of UAVs by the year 2015. Recognizing that the regulation of UAVs requires multi-agency cooperation, the Unmanned Aircraft System (UAS) Comprehensive Plan was published,[15] providing for specific goals and objectives to be met by each Federal Agency. It is expected that as a result of the Modernization Act, approximately 30,000 UAVs will be flown in the United States national airspace by the year 2020.[16] The FAA has recently chosen six UAV research and test sites. These sites will be used by the FAA for the purpose of conducting research into the certification and operational requirements needed to safely integrate UAS into the United States national airspace.[17] In order to mitigate the concern that the testing of UAVs would infringe upon people's privacy, the FAA will impose privacy safeguards including, *inter alia*, the requirement that test-site operators maintain written records of the devices flown in their facilities and create a written plan as to how data collected by UAVs would be used.[18]

UAVs first entered the EU policy discussion in 2002,[19] and according to the European Commission's declared target, by the year 2028, civilian UAVs will be fully integrated into European airspace.[20] So far, in Europe, the European Aviation Safety Agency has granted approximately 400 permits,[21] and currently there are over 400 UAV development projects underway in twenty European countries.[22]

Although no official data is available, in Israel, the Israeli Civil Aviation Authority ("**CAA**") has granted an operating license to at least two companies that operate UAVs for commercial purposes, subject to *meeting safety and security constraints but without taking into consideration privacy implications*.[23]

Other matters which may influence (for better or worse) the formulation of rules applicable to the use of UAVs, are the commercial potential inherent in the UAV world market, estimated at USD 89.1 billion over the coming decade and the impact which the UAV industry will have on the job market.[24] Thus, it is not surprising that private hedge funds and institutional and private investors are increasing their interest in

[13] Richard M. Thompson II, UAVs in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses 3 (Congressional Research Service, Apr. 3, 2013) (hereinafter UAVs in Domestic Surveillance Operations).

[14] 2012, P.L. 112-95. 126 Stat. 11. Compare with the attempt to impose restrictions on the use of drones and government surveillance by Olympia (capital of Washington) State House. Lisa Baumann, *House Passes Drone, Government Surveillance Bills*, The Olympia (Feb. 17, 2014) http://www.theolympian.com/2014/02/17/2990592/house-passes-drone-government.html.

[15] Unmanned Aircraft System (UAS) Compressive Plan (Joint Planning and Development Office, September 2013) http://www.faa.gov/about/office_org/headquarters_offices/agi/reports/media/UAS_Comprehensive_Plan.pdf.

[16] Robert Johnson, *FAA: Look For 30,000 Drones To Fill American Skies By The End Of The Decade* Business Insider (Feb 8, 2012) http://www.businessinsider.com/robert-johnson-bi-30000-drones-by-2020-2012-2#ixzz2qSfn8Qf1. The FAA has recently chosen six UAV research and test sites. These sites will be used by the FAA to conduct research into the certification and operational requirements needed to safely integrate UAS into the United States national airspace.

[17] *See* Matthew L. Wald, *F.A.A. picks Diverse Sites to Carry Out Drone Tests*, The New York Times (Dec. 30, 2013) http://www.nytimes.com/2013/12/31/us/politics/us-names-domestic-test-sites-for-drone-aircraft.html?_r=0.

[18] Unmanned Aircraft System Test Site Program: A Rule by the Federal Aviation System Test Site Program (Federal Registar: The Daily Journal of the United States Goverment, Nov. 14, 2013) https://www.federalregister.gov/articles/2013/11/14/2013-27216/unmanned-aircraft-system-test-site-program; Alan Levin and David Mildenberg, *Drones to Take Flight at Six Test Sites Chosen by FAA*, Bloomberg Politics (Dec. 30, 2013) http://www.bloomberg.com/news/2013-12-30/drones-to-take-flight-at-six-test-sites-chosen-by-faa.html.

[19] For a complete and comprehensive description of UAVs in European airspace *see* Ben Hayes, Chris Jones & Eric Topfer, Eurodrones Inc. 10 (Transnational Institute and Statewatch, Feb., 2014) (hereinafter Eurodrones).

[20] *Id.*, at 14.

[21] Roadmap for the Integration of Civil Remotely-Piloted Aircraft System Into the European Aviation System 8 (European RPAS Steering Group, Annex II, 2013) (hereinafter Roadmap for the Integration of Civil Remotely-Piloted Aircraft System).

[22] Jeffrey *O'brien. Amazon Drones –The Sky's the Limit for MRO Spares*, MACMMS (Jan., 31 2014) http://www.maintenanceassistant.com/blog/amazon-drones-skies-limit-mro-spares/.

[23] Ministry of Transportation The Civil Aviation Authority, http://caa.gov.il/index.php?option=com_content&view=article&id=342&Itemid=239. *See* also the discussion in Part 5 below. The Civil Aviation Authority of Israel has authorized two companies, Steadicopter and Bladeworks, to operate UAVs in the civilian airspace of Israel (Dec. 24, 2013) http://www.israeldefense.com/?CategoryID=472&ArticleID=2656.

[24] According to a recent study, ordered by the "Association for Unmanned Vehicle System International", more than 70,000 new jobs will be created in the first three years following the integration of UAVs into the United States national airspace. Staff Writers, *UAV Industry Will create 70,000 Jobs Over Next 3 Years*, Space Daily (Mar. 13, 2013) http://www.spacedaily.com/reports/AUVSI_Study_Finds_Unmanned_Aircraft_Industry_Poised_to_Create_70000_New_Jobs_in_the_U_S__in_Three_Years_999.html. *See* also Towards a European Strategy for the Development of Civil Applications of Remotely Piolted Aircraft System (RPAS) (European Commission Working Document, Spet., 4 2012) http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT stating that: "In these times of economic downturn, Europe needs more than ever to identity and support, in the context of the Europe 2020 Strategy, opportunities to boost industrial competitiveness, promote entrepreneurship and to create new business in order to generate growth and jobs. The emerging technology of Remotely Piloted Aircraft Systems (RPAS) applied to the development of civil aerial applications (commercial, corporate or governmental non-military) can contribute to these objectives". *See* also Teal Group predicts Worldwide UAV Market Will Total $89 Billion in ITs 2013 UAV Market Profile and Forecast (Teal Group Corporation, June 17, 2013) http://tealgroup.com/index.php/about-teal-group-corporation/press-releases/94-2013-uav-press-release.

companies and startups involved in the design, development and marketing of UAVs for civilian purposes,[25] alongside hiring professional lobbyists to influence policymakers and regulators to adopt rules that will benefit UAV manufacturers and operators[26] as well as initiating public relations campaigns.[27] Subject to various limitations, countries have a clear incentive to allow civilian use of UAVs, if they wish to obtain a share in this growing market.[28]

We can identify three reasons why the Israeli experience is an interesting test case regarding the question whether privacy laws offer appropriate protection in light of the use of UAVs for civilian purposes. The first is the practical-economic reason. The State of Israel is considered the world's largest producer of UAVs for military and civilian purposes.[29] Israel's leading position is likely to allow it to influence the scope of information collected through UAVs, and thus the extent of infringement of the individual's privacy. The second reason touches on the fact that in Israel there is no public discourse on the use of UAVs in the civilian market, and the Israeli legislature has, so far, not yet made UAV operational permits dependent on criteria and/or requirements relating to privacy (as opposed to safety requirements). As will be explained below, this approach stands in contrast to that adopted in other countries, and to the public discourse in the United States and the European Union. It would be of extreme interest to examine whether Israeli law, particularly the Protection of Privacy Law ("**PPL**")[30] and existing legal rulings, appropriately protect an individual's privacy. The third and final reason relates to the unique characteristics of law in the State of Israel, which combines principles of common law and civil law.[31]

It is important to note that the use of UAVs for civilian purposes raises additional significant issues such as how to ensure that the use of UAVs would not endanger the safety of residents living in densely populated areas or interfere with the regular operation of commercial aircraft.[32] Although such issues deviate from the topic discussed in this article, it is important to emphasize that there is a close and direct connection between the safety of UAVs and the preservation of the right to privacy. At present, the FAA does not consider the use of UAVs to be safe; consequently, they are not permitted to fly in major urban skies where the United States National Airspace System operates the majority of its manned aircraft.[33] The inability to fly over heavily inhabited areas (for example, major cities) significantly interferes with the ability of UAVs to collect information on individuals located in those area; fewer flights, in turn, lessen potential infringements of individuals' right to privacy.[34]

Finally, there is a direct and clear connection between the design of *military UAVs* and the development of *military technologies* to be embedded within UAVs, on the one hand, and the issue as to whether and to what extent civilian UAVs affect individuals' right to privacy.[35] Governments, in control of taxpayer money, may decide to invest significant amounts of public funds in the development of military technologies without having to prove that such investments are economically beneficial. To illustrate the public sector's ability to invest significant funds in the development of UAV related technologies, it is helpful to consider the following data. At present, one-third of American warplanes are drones.[36] Technologies, such as facial recognition software and cameras assembled on UAVs that allow their operators to take

[25] *See*, for example, Philip Ross, *A Drone That Delivers Pizza? Investors Say Commercial Drones Show 'Much Potential'*, International Business Times (Nov. 2, 2013) http://www.ibtimes.com/drone-delivers-pizza-investors-say-commercial-drones-show-much-potential-1452902; Olga Kharif, *As Drones Evolve From Military to Civilian Uses, Ventures Capitalists Move In*, The Washington Post with Bloomberg (Nov. 1, 2013) http://www.washingtonpost.com/business/as-drones-evolve-from-military-to-civilian-uses-venture-capitalists-move-in/2013/10/31/592ca862-419e-11e3-8b74-d89d714ca4dd_story.html. According to the article, "Venture investors in the United States poured $40.9 million into drone-related start-ups in the first nine months of this year, more than double the amount for all of 2012".

[26] *See* Eurodrones, *supra* note 19, at 14. *See* also the publications of the UVS International (the international loby group representing the interests of drone manufactures)_http://uvs-international.org/.

[27] Jefferson Morley, *Drones' New Weapon: P.R.*, SALLON (May 22, 2012) http://www.salon.com/2012/05/22/drones_new_weapon_p_r/; Ryan Gallagher, *Surveillance drone industry plans PR effort to counter negative image*, The GuardIan (Feb. 2, 2012) http://www.theguardian.com/uk/2012/feb/02/surveillance-drone-industy-pr-effort.

[28] Unmanned Aircraft System: Measuring Progress and Addressing Potential Privacy Concerns Would Facilitate Integration into the National Airspace System 11 (United States Government Accountability Office, Sept. 2012) (hereinafter Unmanned Aircraft System: Measuring Progress and Addressing).

[29] Gili Cohen, *Israel is World's Largest Exporter of UAVs, Study Finds*, Haaretz (May 19, 2013) http://www.haaretz.com/news/diplomacy-defense/israel-is-world-s-largest-exporter-of-UAVs-study-finds.premium-1.524771 (Isr.). *See* Part 5 below.

[30] Protection of Privacy Law, 5741–1981, SH No. 1011 p. 128 (Isr.).

[31] For an enlightening review of the unique character of the Israeli legal system and the development of Israeli law from a system based on principles of civil law to one that combines civil and common law principles, *see* Tamar Gidron, Israel, *in* Mixed Jurisdictions Worldwide: The Third Legal Family 577 (Vernon V. Palmer ed., 2012).

[32] Other questions may involve the implications UAVs may have for defense, cyber and communications security, national airspace and general aviation.

[33] Also known as "Class B airspace". *Fact Sheet – Unmanned Aircraft Systems (UAS)*, Federal Aviation Administration (Jan. 6, 2014) http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=14153.

[34] Rancho Mirage, *California City to Vote on Banning Drones*, USA Today (April 4, 2013) http://www.usatoday.com/story/news/nation/2013/04/04/rancho-mirage-hobby-drones-ban/2052193/.

[35] Muhammed El-Hasan, *Economic Boon Could be on Horizon as Drones Evolve from Military to Civilian Uses*, Los Angeles Daily News (June 21, 2013) http://www.dailynews.com/general-news/20130622/economic-boon-could-be-on-horizon-as-drones-evolve-from-military-to-civilian-uses; Carol Kuruvilla, *Police Officers, archaeologists, and farmers are using high-tech drones for civilian purposes*, New York Daily News (Feb. 21, 2013) http://www.nydailynews.com/news/national/photos-high-tech-drones-find-non-war-civilian-article-1.1270332.

[36] Torie Bosch, *Drones Now Make Up Nearly one-Third of U.S. Military Aircraft*, Future Tense The Citizen's Guide to the Future (Jan, 9, 2012) http://www.slate.com/blogs/future_tense/2012/01/09/drones_make_up_one_third_of_u_s_military_aircraft_.html.

pictures from a high altitude, were initially developed for military purposes before being applied to civilian UAVs.[37] In a recent case in the United States, a video taken by a Predator UAV, a military aircraft usually armed with Hellfire missiles and deployed to monitor borders in countries such as Pakistan and Afghanistan, for the first time served as key evidence in the conviction of a suspect in a criminal trial.[38]

Part 2 of this article will discuss the difficulties in defining the right to privacy, the way in which the Israeli legislature chose to formulate the laws, and the approach taken by the courts in interpreting the provisions of those laws. Part 3 will examine the benefits and possible threats to the right to privacy, resulting from the use of UAVs, and consider why they constitute such a broad, significant threat to privacy, in comparison with existing measures, such as manned aircraft or closed-circuit television (**"CCTV"**). Part 4 will examine the ability of Israeli law to address the breach of privacy as a result of the use of UAVs. Part 5 will review the spectrum of means through which Israeli law could provide protection to the right to privacy, as it relates to the operation of UAVs. Part 6 will present the conclusions and a list of operative recommendations regarding the way in which the potential damage to the right to privacy, caused by the use of UAVs for civilian purposes, can be mitigated.

Two main conclusions ensue from the analysis set out below. The *first* conclusion is that, in many respects, the introduction of UAVs into the civilian market represents a new type of threat to the right to privacy. Indeed, the concept of assembling photographic equipment on traditional aircraft and using other related technologies to monitor subjects on the ground is not new. Nevertheless, the combination of innovative photographic capabilities, the unique characteristics of UAVs and the anticipated widespread use of UAVs in a civilian context, greatly magnifies the potential risk to the right to privacy.

The *second* conclusion is that in order to successfully mitigate the potential risk to the right to privacy, resulting from the use of UAVs for civilian purposes, it is necessary to establish a new set of statutes, rules and guidelines. Governments and policy makers should understand that alongside its potentially important benefits, the operation of UAVs endangers the fundamental right to privacy. The companies which are responsible for the design, manufacture and marketing of UAVs should not be motivated purely by profit but should also take into account issues of privacy. Finally, individuals and commercial companies which use UAVs for civilian purposes, should agree to limit their use in the event that the potential damage to the right to privacy is outweighed by the potential benefits resulting from such use. Such agreement can either be voluntary (i.e., as a result of educational programs explaining the risks associated with the use of UAVs) or involuntary (i.e., as a result of statute based restrictions).

2. The right to privacy – difficulties in definition and the Israeli experience

2.1. *The vagueness of the right to privacy*

The right to privacy is a vague right, since it is dependent on two dynamic, variable factors. The *first* factor is the social variable, while the *second* factor is the technological variable.[39]

As with other fundamental rights, the right to privacy is society dependent. *This social element* has two aspects. The *first* aspect is sociological–societal, which is clearly reflected in the Israeli case law, in light of the shift in Israeli society from a collective, socialist society to one that promotes the individual. Therefore, it is not surprising that legislative regulation of the right to privacy, with its emphasis on the individual, only took place in 1981, with recognition of privacy as a fundamental right only occurring in 1992.

The *second* aspect, reflected in the context of privacy in society, relates to the connection between a societal norm and its legal expression. This aspect reflects the history of the community under discussion, its culture, current way of life and its shared values. Israel's constant need to defend itself has led to a sanctification of defense needs, at times, even at the expense of the right to privacy.[40] In the United States, historical roots and an aversion towards centralized (English) rule led to the interpretation of the right to privacy as a liberty, and particularly as a constraint on the administration's ability to infringe the rights of American citizens, *inter alia*, through the Fourth Amendment to the United States Constitution. On the other hand, neither the United States Constitution nor federal law offers complete and comprehensive protection of the right to privacy.

In contract, central to the model adopted by the European Union is the perception of privacy as an element of human dignity. The dictatorships that led to the Second World War, and the misuse of information collected about European citizens, formed the backdrop to the approach recognizing the right to privacy as a fundamental constitutional right.[41] In this, the constitutional arrangements regarding the right to privacy in Israel and the European Union are similar. As shall be demonstrated in Part 3 below, the historical-social factor will have a substantial impact on the ways in which society addresses the risk of privacy breaches due to the use of UAVs.

[37] Ali Winston, *Facial recognition, once a battlefield tool, lands in San Diego County*, The Center for Investigative Reporting (Nov. 7, 2013) http://cironline.org/reports/facial-recognition-once-battlefield-tool-lands-san-diego-county-5502.

[38] Philip Sherwell, *First Conviction Using Drone Evidence in US*, Telegraph London (Jan. 30, 2014) http://www.smh.com.au/world/first-conviction-using-drone-evidence-in-us-20140130-hvag9.html. *See* also Marc J. Blitz, *The Fourth Amendment Future of Public Surveillance: Remote Recording and Other Searches in Public Space*, 63 Am. U. L. Rev. 21 (2013).

[39] Birnhack, *supra* note 9, at 14.

[40] Thus, for example, the Criminal Procedure Law (Enforcement Powers – Communication Data), 2007 SH No. 2122 p. 72 allows the police to obtain personal data about any person from cellular and internet service providers – including whom the person contacted, his location, with whom he corresponded by e-mail, and which websites he visited. *See* also: Omer Tene, *Communications Data and Personal Information in the 21st Century*', *in* Legal *Network: Law and Information Technology* 287 (Niva Elkin-Koren and Michael D. Birnhack Birnhack (eds.), 2011) (Isr.).

[41] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 Yale L. J. 1151 (2004).

As with the right to freedom of expression (and additional fundamental rights), the right to privacy has a mutual, bi-directional relationship with **technology**.[42] It is often argued that technology renders legal discussions, including those on the nature and scope of the right to privacy, theoretical. For example, it has been argued that there is no privacy on the internet[43]; that if one does not wish it known that a search has been made on the web, then it is best not to search it.[44] Those who would prefer the disappearance of the right to privacy argue that its disappearance is necessary to ensure economic efficiency.[45] This argument has also been raised in connection with the use of UAVs.[46]

As alluded to at the beginning of the previous paragraph, technology is not detached from values, including that of privacy. There are technologies (including encryption) that allow greater privacy. On the other hand, there are technologies that have the power to reduce privacy, such as CCTV.[47] However, unlike fixed cameras, UAVs are not dependent on public infrastructure or on private initiatives. Furthermore, unlike CCTV, UAVs can identify body heat, chemical substances or the existence of concealed weapons and may fly undetected.[48] We can demonstrate the balance between technology that restricts privacy and that which extends privacy in the context of facial recognition technology, in connection the use of UAVs.[49]

2.2. *The various approaches to reducing the vagueness of the right to privacy, and their influence on the possibility of breach of privacy by UAVs*

The article briefly presents various approaches that seek to reduce the vagueness in defining the right to privacy. This discussion is important in the context of UAVs for three reasons. The *first* is that an understanding of what is included in the right to privacy is essential to allow an understanding of whether, and under what circumstances, the use of UAVs constitutes a breach of privacy. The *second* reason is related to the fact that, at various points in time, the Israeli legal system has adopted each of the approaches that will be presented. The *third* reason is related to the fact that the Israeli legislature does not make the operation of UAVs by civilian entities (public authorities, corporations and individuals) conditional on ensuring the privacy of Israeli citizens. That being the case, it will be necessary as well as beneficial to examine alternative arrangements from a comparative point of view. In order to understand the full significance of the solutions adopted in the United States and Europe, and to examine their appropriateness for Israeli law, we need to examine how the right to privacy has been interpreted in those legal systems.

The conceptual approach to privacy, which was first presented by Warren and Brandeis,[50] sought to address the lack of a complete and comprehensive definition of privacy, apart from some exceptions established in the American Bill of Rights, by identifying the individual's inviolate persona as the common denominator across the various branches of law. According to the authors, the individual's persona includes an interest in controlling the publication of information about himself, his works, his writings and his image. From that interest derives the right to be left alone, which encompasses the individual's control of private information about himself and his personality. Against the conceptual approach, it has been argued that if the right to privacy is only an interest protected under other branches of law, there is no reason to recognize this interest as a separate right.[51]

An example that demonstrates the problems associated with the conceptual approach can be found in Israeli legal rulings, in the *Vaknin* case.[52] This ruling addressed the conduct of prison guards at a military prison who, by forcing a prisoner to swallow salt water, caused him to vomit up a package of drugs, which subsequently was used as evidence against him at trial. The Supreme Court faced the question of whether the act of "making the prisoner drink" the salt water constituted an "other nuisance" as defined in Section 2(1) of the PPL. Such a definition would have led to the invalidation of the evidence, by virtue of Section 32 of the Privacy Protection Law, which states that: "*Material obtained through breach of privacy shall be invalid for use as evidence in court, without the consent of the victim, unless the court permits the use of the material, for reasons that shall be recorded, or if the infringer, who was a party to the proceedings, had a defense or exemption pursuant to this law.*"[53] The Court ruled that the package of drugs was admissible as evidence. The Court based its ruling on a narrow, formalistic approach, determining that the act of "*making him drink*" did not come under the definition of the PPL. "*Other nuisance*" as defined in the section, was not intended to include the causation of violent injury to an individual's person, which in itself was the criminal offense of assault. Infringement of an interest which was protected under other legislation, in this case the crime of assault, found in the Penal Law,[54] was not included within the provisions of the Privacy Protection Law, since it was inconceivable that the whole of the Penal Law (or, for the purposes of the specific case, tort and property law) would also constitute a nuisance as defined in

[42] Michael D. Birnhack, Private Space: The Right to Privacy, Law & Technology 43 (2010) (Isr.).

[43] Polly Sprenger, *Sun on Privacy: Get Over* It, Wired (Jan. 1, 1999) http://www.wired.com/politics/law/news/1999/01/17538.

[44] "Google CEO Eric Schmidt on Privacy", YouTube http://www.youtube.com/watch?v=A6e7wfDHzew.

[45] Richard A. Posner, *An Economic Analysis of Privacy*, *in* Philosophical Dimensions of Privacy: An Anthology 333 (Ferdinand David Schoeman ed., 1984).

[46] *See* discussion at Part 4 below.

[47] Benjamin J. Goold, *Privacy Rights and Public Spaces: CCTV and the Problem of the "Unobservable Observer"*, 21(1) Crim. Just. Ethics (2002). CCTV cameras are common in the England *see*, *Britain is 'surveillance society'*, BBC News (Nov. 2, 2006) http://news.bbc.co.uk/2/hi/uk_news/6108496.stm.

[48] *The Future of UAVs in America: Law Enforcement and Privacy Considerations, Before the S. Comm. On the Judiciary* (Mar. 20, 2013) (written statement by Ryan Calo, Assistant Professor University of Washington School of Law).

[49] *See* discussion at Parts 4 and 5 below.

[50] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

[51] Amy L. Peikoff, *The Right to Privacy: Contemporary Reductionists and Their Critics*, 14 VA. J. Soc. Pol'y & L. 474 (2006).

[52] FH 9/83 *Military Court of Appeals v. Vaknin* 42(3) PD 837 [1988] (Isr.).

[53] Compare Court's holding in *Isacharov*, *supra* note 99 below.

[54] Penal Law, 1977 SH No.864 p. 226 (Isr.).

the PPL.[55] Worth noting is the minority opinion of Justice Sheinbaum, according to which "*even if we were to say that the words used by the legislator could suffer such a limited interpretation, they should not be so interpreted unless such interpretation is required to expand relief, enhance justice, and preserve human rights from being infringed*".

The Israeli legal system distanced itself from the conceptual interpretation of privacy following the adoption of Basic Law: Human Dignity and Liberty,[56] which explicitly enshrines the right to privacy. Thus, Section 7 of the Basic Law states: "*(a) all persons have the right to privacy and to intimacy; (b) there shall be no entry into private premises of a person who has not consented thereto; (c) no search shall be conducted on the private premises of a person, nor on his body, in his body, or in his personal effects (d) there shall be no violation of the confidentiality of conversation, or of the writings or records of a person*". The constitutional status of the right to privacy, as derived from the dignity of the individual, is expressed in a series of judicial rulings. Thus, for example, in the *Jane Doe case*,[57] the Court considered the situation where a husband photographed his wife, whom he was in the process of divorcing. The photograph showed that, following the separation of the couple, the wife had committed adultery in the jointly owned apartment. The Court had no difficulty in disqualifying the evidence by virtue of Section 32 of the PPL, stating that: "*The right to privacy is one of the most important human rights in Israel […] it is one of the liberties that shapes the nature of Israel as a democratic regime […] it is recognized by Israeli common law as a human right […] By virtue of the Basic Law, privacy has become a constitutional-supra-constitutional right*".

Alongside the definition in the Basic Law, Section 2 of the PPL sets out a closed list of situations that would be considered a breach of privacy (including "other nuisance" considered in the *Vaknin* judgment). In this, the Israeli legislature has adopted an approach similar to other legal approaches in the world, which refrain from giving a positive definition of privacy, and instead specify situations which would be considered as a breach of privacy. This approach is known as the *categorization of privacy*. Examination of the instances listed, allows us to identify the protected areas, and categorize them. Nonetheless, in light of the expansive interpretation in the *Jane Doe* case, where a matter does not fall within the list set out in Section 2 of the PPL, the court is still able to bring it within the constitutional boundaries of privacy based on Section 7 of Basic Law: Human Dignity and Liberty.

In keeping with this categorization, Prosser[58] stated that the right to privacy falls into the four following categories: (a) intrusion upon seclusion (i.e. within one's private domain); (b) appropriation of a name or likeness for profit; (c) public disclosure of private facts; and (d) presentation of an individual in a false light. Israeli law adopted this categorization.

Over time, and in light of the vagueness of the right and the inability to apply new situations arising, *inter alia*, from the development of new technologies,[59] Prosser's categorization has been replaced by an approach that defines privacy on the basis of the kinds of human activities under discussion. Thus, privacy applies in: (a) *places* – pursuant to Section 7(b) of the Basic Law and Section 2(3) of the PPL, which forbids photography in a private domain, as opposed to Section 2(4), which forbid publication of a photograph taken in the public domain if it is demeaning or humiliating. Privacy within a place lies at the heart of the right to privacy of the American citizen, and allows the protection of occurrences taking place within one's home, even if these are perceived to be immoral, and even in instances of illegality[60]; (b) *the media* – communications between individuals are protected by virtue of Basic Law: Human Dignity and Liberty and Section 2(2) of the PPL, which states that prohibited wiretapping is also a breach of privacy, while Section 5(2) states that copying the content of a letter, including an electronic communication, is also an infringement; (c) *information* – this is protected by virtue of the various alternatives listed in Section 2, including Section 2(9): "*Use of information about a person's private affairs, or their transmission to another person, not for the purpose for which they were given*", and Section 2(11), "*Publication of a matter touching on a person's privacy, or his health, or his conduct in private*"; and (d) *decisions* – Israeli law does not recognize the category of "decisions" as part of the right to privacy.

Given the present and future capabilities of UAVs, the classification of privacy based on categories is not free of difficulties. Thus, for example, it would be appropriate to view privacy as applying not to places, but to the people acting within those places. Shall we adopt the rule that a person's privacy has not been infringed, since photography from the UAV was not carried out within the private domain of the subject of the photograph? What would be the rule when the photograph is of a guest in someone else's home? Furthermore, physical delineation does not help us rule in intermediate cases, in which the individual is photographed in places that do not fall into the categories of private domain or public domain, such as photography from a UAV, or interception of a telephone call from a public telephone booth using equipment assembled on a UAV; or in instances in which the photograph is made of an area of a house that is visible only from the air, or by means of thermal imaging. A further difficulty relates to the interception of communications data (as opposed to the content of the conversation), which do not enjoy the same level of protection as the content of the communication.[61]

An alternative approach views privacy as a means for the individual to retain control of himself, and particularly of information about himself (including photography, letters, recordings, and any of an individual's actions).[62] In light of the

[55] The Supreme Court holding in CrimFH 9818/01 *Biton v. Sultan* 59(6) 554 [2005] (Isr.) was based on a similar approach.

[56] Basic Law: Human Dignity and Liberty, 5752–1992, SH No. 1391 (Isr.).

[57] HCJ 6650/04 *Jane Doe v. National Rabbinical Court* 61(1) PD 581 [2006] (Isr.).

[58] William L. Prosser, *Privacy (A Legal Analysis)*, 48 CAL. L. REV. 383 (1960).

[59] Birnhack, *supra* note 9, at 28.

[60] *Stanley v. Georgia* 394 U.S. 557, 565 (1969). With respect to the right to privacy at home the Court held that: "*fundamental is the right to be free, except in very limited circumstances, from unwanted governmental intrusions into one's privacy*" particularly the right to satisfy [one's] intellectual and emotional needs in the privacy of his own home".

[61] Birnhack, *supra* note 9, at 34.

[62] *Id.*, at 41. *See* also ALAN WESTIN, PRIVACY AND FREEDOM (1967).

technological era in which we live, at a time when decisions by the state, market decisions, and decisions within various social circles are made on the basis of prior knowledge about us and our patterns of behavior, information becomes the main currency and tool for control. According to the privacy as control approach, the individual himself controls what will happen to the information relating to him. Adopting this definition means that where information has been collected about an individual in a certain place through the use of a UAV, that individual will control the information, whether or not he is the owner of the particular place.

The approach that views control of information as the realization of privacy was adopted in the framework of the provisions of Chapter 2 of the PPL. The European Union recognized the constitutional status of the individual's right to privacy of his personal information at the level of a fundamental constitutional right, in a number of directives. The Data Protection Directive (95/46/EC) establishes detailed rules for maintaining the privacy of the subject of the data. In 2002, the Directive on Privacy and Electronic Communications was enacted, expanding the doctrine of data protection to internet and cellular service providers.[63] In addition, Article 8 of the European Convention on Human Rights states as follows: "*Everyone has the right to respect for his privacy and family life, his home and his correspondence*". These sources will, in the future, influence and shape the rules relating to the ability to operate UAVs in the civilian market, and the use of data collected through them.[64]

On the other hand, under the American approach, which favors the free movement of information, personal data collected in databases is considered the property of the database owner, which he is entitled to trade in. In a way that is substantially different from European (and Israeli) law, the establishment of databases is not considered one that raises issues of privacy, and hence is not regulated comprehensively, unless particular circumstances apply.[65]

Part 5 considers whether it is possible to protect, or alternatively minimize, the breach of privacy as a result of the use of UAVs, by setting rigid provisions regarding the establishment and use of databases. The section discusses potential ways of coping with breaches of privacy as a result of the use of UAVs.

3. Possible benefits of the use of UAVs and possible threats to the right to privacy

As explained in Part 2 above, there is a close, bi-directional connection between privacy protection laws and technology. In this section, we turn to a discussion regarding the advantages and disadvantages inherent in the use of UAVs, where an advantage from one point of view may, in certain circumstances, constitute a disadvantage from another perspective.

Those who argue that UAVs have only had a marginal impact on the right to privacy, base their approach on the following two points. Central to the *first* argument is the finding – true in and of itself – that, for decades, public authorities throughout the world have made use of helicopters and manned aircraft, equipped with cameras, to carry out observation, surveillance, and law enforcement activities. Furthermore, over recent years we have witnessed the installation of various surveillance systems, such as CCTV cameras intended to deter and (where necessary) document offenders during the commission of their crimes.[66] Hence, the use of UAVs as an alternative to the above should not be considered a factor that negatively affects the delicate balance between the desire to ensure the public's wellbeing, and the right to privacy.

The *second* argument places emphasis on the inherent advantages (economic and in terms of saving human life) and efficiencies that could come about as a result of the use of UAVs. In this context, it should be mentioned that UAVs are operated by remote control and, as such, are not subject to human limitations, including the possible risk of loss of human life in the case of flying in dangerous regions. According to a document prepared for the European Union Commission,[67] the advantages inherent in the use of UAVs by civilian bodies can be presented under the following four categories: (a) **civil:** monitoring, prevention and warning of crises due to natural disasters (floods, earthquakes, fires, nuclear disasters such as the Chernobyl disaster). The occurrence of a crisis, of the type already mentioned, requires rapid response capability, visual contact with the survivors, and communications in disaster-hit areas – all these can be achieved more easily through the use of UAVs. UAVs may also be used to shorten the time period for the delivery of packages[68]; (b) **defense**: routine activity of the coast guard (particularly in countries such as the United States and Europe, which have extensive coastlines) and supervision of sites such as ports, airports, and oil and gas fields, which are a preferred target for

[63] OJ L 281, 23.11.1995, p. 31.

[64] Convention for the Protection of Human Rights and Fundamental Freedoms art. 6.1, Nov. 4, 1950, 213 U.N.T.S. 221.

[65] For a comprehensive review of the differences between the United States and Europe regarding data protection *see* Joel R. Reidenberg & Paul Schwartz, Data Privacy Law (1996); Whitman, *supra* note 36.

[66] For the restrictions regarding the use of CCTV in Israel *see* Israel Law, Information and Technology Authority ("**ILITA**") Guidelines regarding the "Use of Security and Surveillance Cameras and the Collections of Images Recorded by Them" (Apr., 2012) http://www.justice.gov.il/NR/rdonlyres/34A1D5CF-493A-4E02-850D-74F7FAE50B27/37913/42013.pdf (Isr.).

[67] Roadmap for the Integration of Civil Remotely-Piloted Aircraft System, *supra* note 21, at 29–34.

[68] Doug Gross, *Amazon's Drone Delivery: How Would it Work,* CNN (Dec. 2, 2013) http://edition.cnn.com/2013/12/02/tech/innovation/amazon-drones-questions/; *Deutsche Post completes first drone flight*, The Local Germmany's News in English (Dec. 9, 2013) http://m.thelocal.de/20131209/deutsche-post-completes-drone-delivery-flight. *See* also Associated Press, *Craft brewer Lakemaid Beer's drone delivery hopes put on ice*, CBSNews World (Feb. 2, 2014) http://www.cbc.ca/news/world/craft-brewer-lakemaid-beer-s-drone-delivery-hopes-put-on-ice-1.2520252 describing a craft brewer who wanted to use drones for the purpose of delivering a 12-pack of its brew to anglers on Minnesota's Lake Mille Lacs. As a result of the FAA order, the craft brewer was forced to cease the operation of the UAV. Compare with Hamish Mckenzie, *Amazon Wants to use Drones by 2018. An Australian Startup will do it by March*, Pandodaily (Dec. 2, 2013) http://pando.com/2013/12/02/amazon-wants-to-use-drones-by-2018-an-australian-startup-will-do-it-by-march/.

terror organizations such as al-Qaeda[69]; (c) **environmental:** protection against nuisances (originating in nature, or man-made) that influence air or water quality; in addition to the economic advantages deriving from the above one may note the contribution of UAVs to economic development and growth in the employment market, and their influence on areas apart from the aviation industry[70]; and (d) **commercial:** such as photography of real estate, trespass, etc.

Thus, it is not surprising that according to a recent poll, 57% of the general public supports the use of UAVs for any of the activities listed above, 88% supports the use of UAVs for search and 63% supports their use in fighting crimes.[71]

Apart from the advantages described in the previous paragraph, the use of UAVs entails a potential risk to the right to privacy. It must be emphasized that although of different sizes,[72] all UAVs have photographic equipment, extended flying capabilities and the ability to carry out surveillance. This is not meant to suggest that the harm which may be caused by larger UAVs (with longer flight time capabilities) is more or, conversely, less severe than that ensuing from UAVs the size of a wasp (which are capable of entering private homes without the target being surveilled, noticing them). Each class of UAV represents a different risk to the right to privacy.

Arguments against the use of UAVs can be categorized into the following groups: (i) **the psychological perspective:** people who are being watched tend to behave differently and make different decisions than they would, were they not being observed.[73] Assuming that the number of UAVs equipped with cameras will rise significantly, the influence of the chilling effect on behavior will expand, and cause changes in people's behavior patterns adversely affecting the fundamental right to human dignity; (ii) **the technological perspective:** innovation and technological breakthroughs, particularly in connection with information and communications technologies, have created new economic models and tools that influence the life of the individual.[74] The argument is that UAVs negatively reinforce this phenomenon, since they constitute an ideal platform combining technical capabilities and existing and future technologies. Furthermore, as with other technologies, it may be assumed that in the case of UAVs, there will be those who seek to abuse their capabilities, for example, by attempting to hijack and take control of a UAV and its photographic capabilities.[75] In this context, the following three examples of *existing technologies* that will eventually be integrated into UAVs sold on the civilian market, illustrate how UAVs may damage the individual's right to privacy: (a) the use of *biometric data*, the source of which is the human body, which allows verification and identification based on finger veins, fingerprints, iris scans and facial patterns. Although the use of biometric data is not new, in recent years there has been a trend to expand biometric databases, both in the private and public sectors, alongside criticism and concern regarding misuse of the data and leakage of personal biometric data into hostile hands.[76] The most problematic aspect in the context of biometric data is the use of facial recognition technology in the context of CCTV,[77] the integration between facial recognition technology and social media such as Facebook and LinkedIn, leading to intrusive monitoring of the life of the individual. Furthermore, by means of "behaviometrics" a person's behavior is studied in line with his biometric characteristics (such as voice, retina). The use of UAVs may intensify the use of the various technologies, and lead to excessive incursion into the privacy of the individual[78]; (b) *photographic technologies* developed for UAVs, including lenses that allow zoom photography from such heights that prevent the subject of the photograph from discerning that he is being photographed (and due to the high resolution, even the smallest objects can be identified at high quality)[79]; *night vision* – photography in total darkness, thus solving the limitations on human sight at night; *see-through-imaging* –

[69] *Report: Israel Will use UAVs to Protect its Gas Fields*, Globes (Aug. 9, 2011) http://www.globes.co.il/news/article.aspx?did=1000671967 (Isr.).

[70] John Villasensor, *Privacy, Security, and Human Dignity in the Digital Age: Observations From Above: Unmanned Aircraft Systems and Privacy*, 36 Harv. J. L. & Pub. Pol'y 457, 458 (2013).

[71] Joe Eyerman, Clark Letterman, Wayne Pitts & John Holloway, Unmanned Aircraft and the Human Element: Public Perceptions and First Responder Concerns (Institute for Homeland Security Solutions, June 2013) http://sites.duke.edu/ihss/files/2013/06/UAS-Research-Brief.pdf.

[72] UAVs may appear in bug-sized "nano drones" as well as vehicles the size and weight of large business jets. *See* Bart Elias, Pioltless Drones: Background and Considerations for Congress Regarding Unmanned Aircraft Operations in the National Airspace (Congressional Research Service, Sep. 10, 2012) https://www.fas.org/sgp/crs/natsec/R42718.pdf. *See* also Michael Anissimov, *DARPA Funds Nano-UAV Hummingbird*, Recent Articles (Sep. 16, 2009) http://hplusmagazine.com/2009/09/16/darpa-funds-nano-uav-hummingbird/.

[73] Protecting Privacy From Aerial Surveillance: Recommendations for Government Use of UAV Aircraft (American Civil Liberties Union) (Dec. 2011) http://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf (hereinafter Protecting Privacy From Aerial Surveillance). *See* also Ryan Calo, *People Can be so Fake: A New Dimension to Privacy and Technology Scholarship*. 114 Penn. St. L. Rev. 809, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1458637.

[74] Omer Tene, *Privacy: The New Generations*, Int'l Data Privacy L. (2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1710688.

[75] A hacker has recently shown how easy it is to use one UAV to hijack another. The software that enabled the hacker to take control of the UAV is now available for anyone to downwload. *Attack of the Zombie Drones*, One Per Cent (Dec. 11, 2013) http://www.newscientist.com/article/mg22029475.100-one-per-cent.html#.UuMwMxDA6M8.

[76] Omer Tene, *Israel's Biometric Database Law: Risks and Opportunities*, 17(2) Hamishpat L. Rev. 421 (2013) (Isr.). *See* also Tamar Gidron & Uri Volovelsky, *The Public Debate on the Process of Creating a Biometric Database in Israel, in The 2013 CLSR-LSPI Seminar on Electronic Idendity: The Global Challenge – Presented at the 8th International Conference on Legal, Security and Privacy Issues in IT Law (LSPI) November 11-15, 2013, Tilleke & Gibbins International Ltd., Bangkok, Thailand, Comp. L. & Security Rev.* (forthcoming, 2014).

[77] For a review of the different types of UAVs and capabilities *see* Protecting Privacy From Aerial Surveillance, *supra* note 73, at 2.

[78] For a discussion regarding new types of technologies, see Tene, *supra* note 74.

[79] Joshua Kopstein, *DARPA'S 1.8 Gigapixel UAV Camera is a High-res Fourth Amendment Lawsuit Waiting to Happen*, The Verge (Feb. 1, 2013), http://www.theverge.com/2013/2/1/3940898/darpa-gigapixel-UAV-surveillance-camera-revealed.

technology allowing one to view what is happening within buildings; *video analytics* – technology allowing one to carry out surveillance of individuals and vehicles by means of FRT; *distributed video* – the operation of a number of inexpensive UAVs, working in coordination, and which spread a video network over a city, allowing one to view what is happening in a whole town from a bird's eye view[80]; (c) *position based services* – by means of GPS, IP addresses, or by means of UAVs, it will be possible to offer clients services based on their geographic location (such as discounts in restaurants, or up-to-date information on traffic conditions).[81] Data collection, carried out constantly, and independently of the use of cellular devices, renders the notification and opt-in mechanisms adopted in certain countries (such as in the European Union) ineffective.[82] This difficulty will only intensify and expand as a result of the use of UAVs that are not subject to technological or technology limitations on the ground. Apart from the potential damage to the right to privacy, a possible side-effect of the use of the above-mentioned technology is the introduction of automated enforcement whereby the operation of UAVs in the civilian sector will continue the trend toward automation of law enforcement without human intervention.

The concern is that law enforcement will be entrusted to technological systems that lack the ability to weigh up fairly the external circumstances that occurred when the offender committed the crime, and whose performance may be influenced by bugs or faults in the operating software.[83] (iii) **the economic perspective**: this perspective complements the psychological and technological perspectives discussed above. The cost of purchasing, operating and maintaining manned aircraft constitutes a hurdle that limits the ability to carry out aerial surveillance. On the other hand, the development and availability of photographic technologies that can be fitted easily and at low cost to UAVs, the ability to operate the UAVs without a human pilot, along with the low cost of purchasing, holding and maintaining the UAVs, generally eliminates the economic hurdle preventing ongoing, permanent surveillance by law enforcement agencies, commercial bodies and private individuals[84]; (iv) **the social perspective**: in the future, UAVs will significantly increase the phenomenon of voyeurism by law enforcement agencies, and particularly, by individuals.[85] Hence, it is not surprising that a survey conducted in the United States in 2012 found that 42% expressed significant concern that their privacy would be infringed were permission to be granted to law enforcement agencies to make use of UAVs for enforcement and policing purposes.[86] In this context, we note that publication of a demeaning or intimate image, before an injunction can be granted, renders such an injunction moot.[87] Furthermore, publication of harmful information may take place over the internet, without it being possible to monitor the identity of the person publishing it. Like other technological means, such as CCTV, UAVs may be used for discriminatory purposes based on skin color, ethnicity or race[88]; and (v) **the normative-legislative perspective**: this issue will be discussed in greater detail below as part of the survey of means and approaches to limiting the risks inherent in the use of UAVs in the civilian sector. Nonetheless, it is worth emphasizing briefly that traditional legislation in the field of privacy is not prepared to cope with the negative influences arising from the use of UAVs. Moreover, the use of UAVs is not limited and in the absence of effective tools, cannot be limited to governmental bodies. UAVs are marketed and sold to the private sector and operated by it, whether for commercial reasons or reasons connected to governmental outsourcing.[89] There is no reason to assume that the standard of care and self-restraint adopted by the government will also be adopted by commercial entities seeking to maximize their profits.

4. Does Israeli law have the tools to successfully deal with the influence of UAVs on the right to privacy?

The discussion so far has focused on presenting the vagueness that exists in defining the right to privacy; the attempts to lessen that vagueness in the various legal systems; the advantages inherent in the use of UAVs in the civil aviation market and the real risks to the right to privacy arising from the use of UAVs (use that is expected to increase in the foreseeable future).

We shall next turn to the issue whether the PPL provides adequate protection against the potential risk arising from the use of UAVs for civilian purposes. Since the Israeli legislature and the Israeli courts have yet to express their opinion on this matter, the following discussion will include a description of the solutions adopted in other countries and attempt to apply these solutions to the situation in Israel.

The discussion will also include an examination of the protection given to private information, both at the *data collection* stage and at the stage of *data processing and storage* in

[80] For a complete description of UAVs current and future technologies, *see* PROTECTING PRIVACY FROM AERIAL SURVEILLANCE, *supra* note 73, at 2.

[81] REPORT: MOBILE LOCATION BASED SERVICES: APPLICATIONS, FORECASTS & OPPORTUNITIES 2010–2014 (Mar. 1, 2010, Juniper Research) indicating that the mobile location-based services shall exceed USD 12bn by 2014, https://www.juniperresearch.com/reports/mobile_location_based_services.

[82] Tene, *supra* note 74.

[83] PROTECTING PRIVACY FROM AERIAL SURVEILLANCE, *supra* note 73, at 12.

[84] A UAV system that includes a ground operating computer and the UAV can cost less that USD 50,000. A police helicopter performing the same function will cost up to USD 1,000,000. *See* PRIVACY AND UAVS: UNMANNED AERIAL VEHICLES 19 (Information and Privacy Commissioner, Ontario, Canada, Aug. 2012).

[85] *Id.*

[86] UNMANNED AIRCRAFT SYSTEM: MEASURING PROGRESS AND ADDRESSING, *supra* note 28, at 32. Cf., the results of the poll ordered by the Institute for Homeland Security Solutions, note 70 above.

[87] Tamar Gidron & Hiroko Onishi, *Protection of Personal Rights through Judicial Pre-Publication Orders: A Comparative Israeli and Japanese Perspective*, *in* CONTEMPORARY PRIVATE LAW 127 (Sylvia Kierkegaard ed., 2012).

[88] Rachel L. Finn & David Wright, *Unmanned Aircraft Systems: Surveillance, Ethics and Privacy in Civil Application*, 28(2) COMPUTER L. & SECURITY REV. 184 (2012).

[89] Azmat Khan, *Should the State Dept Outsource Drone Operations to Private Contractors?*, FRONTLINE (Jan. 30, 2012) http://www.pbs.org/wgbh/pages/frontline/foreign-affairs-defense/should-the-state-dept-outsource-drone-operations-to-private-contractors/.

various databases. As will be explained in greater detail, the issue of the regulations imposed on collection and storage of private data, is essential to the protection of private information and particularly information collected by UAVs.

Israeli law, like the laws in other countries, deals with possible breaches of privacy (including through the use of UAVs) by establishing various restrictions and obligations, depending on the entity posing the threat to privacy.

The *first* circle of entities relates to the State including its authorities and semi-governmental bodies. The *second* circle relates to commercial companies. The *third* circle relates to individuals.

The licensing of pilotless aircraft in the State of Israel is regulated under the general legislative framework for licensing aircraft, and the regulations enacted thereunder.[90] The authority of the CAA to grant permits and approvals for the operation of aircraft, including UAVs, is based on Section 4(2)(a) of the Civil Aviation Authority Law,[91] which states as follows: "*To grant licenses, permits and approvals in the field of civil aviation, pursuant to air navigation laws, including for aircraft and aviation equipment*". The definition of "*aircraft*" under the Air Navigation Law is sufficiently broad to include UAVs: "*Aircraft – a device or installation having the ability to be supported in the atmosphere by the reactions of the air […] with the exception of hovercraft*". It should be emphasized that "*hovercraft*" includes "*radio powered, unmanned model aircraft, serving or intended for leisure or sports purposes*" and hence UAVs intended for leisure or sports are not subject to regulation by the Civil Aviation Authority. Nonetheless, the operator of a UAV of this type is required to maintain visual contact with the UAV. This condition restricts, even if it does not prevent, the risk of breach of privacy.

The statutory provision also explicitly includes equipment by which a UAV is operated, and therefore it is subject to any conditions that may be set.[92] Section 18 of the Air Navigation Law states that a license for aerial operations will be granted if the Director of the Civil Aviation Authority ("**CAA**") is satisfied that the operator of the UAV is capable of carrying out the requested action safely. *Privacy considerations, unlike safety considerations, are not considered by the Director of the CAA* when reviewing an application for the installation of equipment on a UAV.

Reviewing the legislation that was traditionally enacted to regulate manned aircraft, leads to an interesting and important interim conclusion regarding the possible regulation of UAVs in Israel. Israeli legislation recognizes the authority of the CAA to establish rules for the use of UAVs for commercial purposes. *However, it does not explicitly empower the authority to weigh up the potential extent of harm to the right to privacy, when deciding whether to permit the use of a UAV*. This finding is strengthened by the fact that once a permit is granted, the CAA may not terminate the permit on the ground that the UAV operator breached an individual's right to privacy.

The "*principle of administrative legality*" is a fundamental principle in the Israeli legal system, as well as in all other democratic legal systems. Under this principle, an administrative authority, such as the CAA, is limited to implementing powers specifically granted by a binding law to that administrative authority.[93] Thus, in line with the discussion in the previous paragraph, the CAA is not empowered to set conditions which are intended to ensure that the right to privacy is not infringed as a result of the operation of UAVs. It seems that the Israeli legislature's approach is correct and corresponds to the approaches adopted in the United States and the European Union, according to which the role of the different aviation authorities is not to establish rules, but to ensure enforcement of the rules and guidelines set by those bodies responsible for privacy matters.[94]

In the first circle, the operation of a UAV by *a state authority* (or a dual-nature body) for purposes of search and surveillance is subject to the general provisions applicable to the execution of searches and wiretaps.

Israeli courts have yet to address the question of whether evidence obtained by means of UAV photography will be considered admissible. At the same time, assumptions can be made as to how the Israeli courts would assess the question of the admissibility of such evidence. Section 25 of the Israeli Criminal Procedure Law,[95] states that where one of the four situations listed in the section exists, a police officer may conduct a search "*in any house or place*" even if the police officer does not hold a search warrant. For example, Section 25(a) states that a police officer may carry out a search without a warrant if "*the police officer has reason to assume that a crime is being committed there or that a crime has recently been committed there*". The "*reason to believe*" test is an *objective test*, in which the court is called upon to evaluate the reasonableness of the police officer's discretion in carrying out the search, so as to determine the question of the search's legality.[96] In the ruling in the *Ben Moshe* case,[97] the Court was presented with the question whether the consent of a suspect to a search of his home would be considered sufficient to grant legal validity to the search, even if the police officer did not have reason to believe that a crime had taken place. The Supreme Court, in a majority decision, held that, for the suspect's consent to be valid for the purpose of legalizing a police search, the consent had to be "*informed consent*"; a process in which the police officer explains to the suspect that he is entitled to refuse the search, and that such refusal will not be used against him in a court of law. Application of the provisions of Section 25 and the *Ben Moshe* doctrine, in regard to photography by means of a UAV, leads to the conclusion that, where the court is persuaded that the police officer had reason to suspect that a crime was being committed at the time the photographs were taken or that a crime had been committed not long before the photographs were taken (or one of the other alternatives listed in Section 25), then the UAV evidence would be admissible. In regard to

[90] Air Navigation Law, 2011, SH No. 2296 p. 830 (Isr.).
[91] Civil Aviation Authority Law, 2005 SH No. 1980 p. 130 (Isr.).
[92] Section 1 Air Navigation Law.
[93] Daphne Barak-Erez, Administrative Law 98–99 (2010) (Isr.).
[94] Margot E. Kaminski, *UAV Federalism: Civilian UAVs and the Things They Carry*, 4 Calif. L. Rev. Circuit 57 (2013).
[95] Criminal Procedure (Arrest and Searches) Ordinance (New Version), 1969 (Isr.).
[96] HCJ 465/75 *Dgani v. Ministry of Police* 30(1) PD 337, 349–353 (1975) (Isr.).
[97] CrimFH 10141/09 *Ben-Haim v. State of Israel* (Mar. 6, 2012), Nevo Legal Database (by subscription) (Isr.).

"informed consent", the interpretation given to the term may be expanded on the basis of the American approach, and we may determine that aerial photography of a part of the house that is not concealed would be considered informed consent of the property holder to photography and the admissibility of the photos taken by the UAV as evidence. This gives expression to the theory of *privacy as control*, which establishes that realization of an individual's control over his autonomous self is only possible when the individual knows, understands and grants his consent to the action of photography by a UAV.[98] In this context, it is again worth mentioning that, in keeping with Section 32 of the PPL, material obtained through breaches of privacy is invalid for use as evidence in court (unless one of the exceptions listed in that section applies).

Nonetheless, it cannot be concluded that all evidence unlawfully obtained by means of UAVs will automatically be disqualified. In line with the determination in the *Isacharov* case,[99] the "*doctrine of the fruit of the poisonous tree*"[100] has *not been rejected in Israel*. That being the case, the court will draw a balance between the infringement of the constitutional right to privacy on the one hand, and the public and social interest involved in disqualifying evidence on the other hand. Further, the court will give weight to the question of whether the evidence is "real evidence," which is not subject to dispute, and has an independent existence, apart from the illegality involved in the operation of the UAV. It should be emphasized that data from UAVs, collected by authorities and stored in databases, may lead to a breach of privacy. This topic will be considered below, in connection with databases operated by commercial entities.[101]

As mentioned above, another way in which UAVs may infringe privacy is by intercepting telephone conversations. Section 7 of Basic Law: Human Dignity and Liberty, discussed in the previous section, also protects against unlawful wiretapping. According to Section 2(2) of the PPL, an unlawful wiretap is a breach of privacy. Based on Section 2(5) of the PPL, copying the content of a letter (including an electronic message) constitutes a breach of privacy. The Secret Monitoring Law[102] regulates the general rule under which a court order is required to carry out a wiretap, and the circumstances in which evidence may be admissible, although unlawfully obtained.

In the *second* circle, we examine the operation of UAVs by *commercial entities*. In the case of photography from UAVs operated by commercial entities, the emphasis is on their storage in databases, and the applicability of the provisions of Chapter 2 of the PPL – "*Protection of Privacy in Databases*" – to the photographs. In this regard, Israeli law is similar to European law which applies the provisions relating to databases both to public and private-commercial entities. In contrast, American law completely refrains from imposing obligations in connection with the administration of databases held by private entities, and imposes certain obligations on government databases.[103] According to the Australian Privacy Act,[104] when a private organization intends to use drone technology, it must comply with the local Privacy Act. Thus, the operation of a UAV requires that the operator will provide notice to the affected individuals about the collection of personal information, that the information collected will be secured and that the disclosure of such information will be in line with the provisions of the local Privacy Act.[105]

The fact that Israeli law imposes restrictions on the use of private information stored in designated databases symbolizes the significance of privacy as a form of control in the Israeli legal system. It should be emphasized that there are differing opinions as to the value of collecting data and including it in databases.[106]

[98] *See*, for example, the ruling in *California v. Ciraolo*, 476 U.S. 207. Birnhack, *supra* note 9, at 50.

[99] CrimA 5121/98 *Isacharov v. Military Prosecutor* 61(2) PD 461 [2006] (Isr.). Such a conclusion is consistent with Section 3 of the PPL which defines "consent" as informed consent, whether explicit or implicit.

[100] For the application of the rule in American legal sytstem *see Nardone v. United States*, 308 U.S. 338, 60 S. Ct. 266, 84 L. Ed. 307 (1939); *Murray v. United States*, 487 U.S. 533 (1998); *Hudson v. Michigan*, 547 U.S. 586 (2006). *See also* Victor R. Quiros, *The Impact of California v. Hodari D. upon Police Pursuits in California: The Fruit of the Poisonous Tree Is No Longer Poisonous*, 19 W. St. U. L. Rev. 641 (1992).

[101] In the European Union, greater emphasis is given to the dissemination of personal information than to its collection *per se*. *See* the discussion in Roadmap for the Integration of Civil Remotely-Piloted Aircraft System, *supra* note 21, at 22.

[102] Secret Monitoring Law, 1979.

[103] Commission Decision, Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequate Protection of Personal Date by the state of Israel with regard to Automated Processing of Personal Data (Jan. 31, 2011), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:027:0039:0042:en:PDF. Section 12 states: "The State of Israel should therefore be regarded as providing an adequate level of protection for personal data as referred to in Directive 95/46/EC with regard to automated international transfers of personal data from the European Union to the State of Israel".

[104] *Privacy Act 1988* (Cth).

[105] Letter from Timothy Pilgrim, Australian Privacy Commissioner, to Hon Nicola Roxon, Attorney General (Sep. 2012) http://www.oaic.gov.au/news-and-events/statements/privacy-statements/regulation-of-drone-technology/correspondence-attorney-general-regulation-of-drone-technology-september-2012. For a comprehensive discussion of the Australian position, *see also* a marginal reference to the privacy concerns arising from the use of UAVs in Serious Invasions of Privacy in the Digital Era 52 (Australian Government – Australian Law Reform Commission, Issues Paper 43, Oct. 2013) http://www.alrc.gov.au/sites/default/files/pdfs/publications/issues_paper_43.pdf. For a comprehensive discussion of the introduction of UAVs into Australian airspace and privacy concerns see additional papers in this issue of CLSR viz., Roger Clarke & Lyria Bennett Moses 'The regulation of civilian drones' impacts on public safety' and Roger Clarke & Lyria Bennett Moses 'The regulation of civilian drones' impacts on public safety' and Roger Clarke 'The regulation of civilian drones' impacts on behavioural privacy' [2014] 30 COMPUTER LAW & SECURITY REVIEW 263-285.

[106] *See* Fred H. Cate, Privacy in Perspective (2001) describing the benefits resulting from the use of information. Excessive defense of privacy is claimed to prevent efficient law enforcement and to impede economic efficiency based on a free flow of information to be collected, stored and sold. Privacy may also hinder law enforcement and national security operations and curtail freedom of information. *See* Roadmap for the Integration of Civil Remotely-Piloted Aircraft System, *supra* note 21, at 21.

In order to understand the level of protection afforded by Israeli law to private information stored in databases, several substantive provisions of the PPL should be noted and briefly discussed in connection with the right to privacy. Section 7 of the PPL defines "*data*" as: "*data on the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of a person*"; "*sensitive information*" is defined as "*data on a person's personality, private family relations, state of health, economic condition, opinions and faith*"; and "database" is defined as "*a collection of data, kept by magnetic or optical means and intended for computer processing*".

In view of the way in which UAVs are used, the material collected by them constitutes data which is stored in databases, as defined by the PPL. In the context of such data storage, the PPL imposes *three* obligations on the administrator of the relevant database: (a) to register the database in the Registry that will be open to public scrutiny; he must do so if the information included in the database is sensitive; collected indirectly from people; without their consent; or in instances in which the database belongs to a public body[107]; (b) to make a request to a person subject to the collection of information for such information, with a view to keeping it in a database; inform the person as to whether he is under a legal duty to deliver that information; inform the individual as to the purpose for which the information is requested; and inform the individual to whom the information is to be delivered and the purposes of such delivery.[108] It is also important to note that information collected for one purpose may not be used for a different purpose.[109] Finally, (c) to protect the data and keep it confidential.[110]

The discussion in the previous paragraph gives the mistaken impression that the PPL provides a suitable solution for safe storage of UAV collected information in designated databases managed by commercial entities. The following *three* examples demonstrate that the current language of the PPL must be revised if it is to provide adequate protection against possible infringement of the right to privacy due to the use of UAVs in the civilian market. (a) According to Section 13 of the PPL, the subjects of the data collection have the right to access and peruse it, or demand its correction, should the information be wrong. However, the obligation to notify the individuals concerned *does not* specify the form of that notice; for example, there are no requirements regarding fonts or marking of key words. Therefore, the likelihood of the subject of the data collection considering or even bothering to read the notice is extremely low. (b) Section 7 of the PPL states that the data administrator shall provide "*protection of the integrity of data, or protection of the data against exposure, use or copying, all when done without due permission*"; however, the law does not specify the nature of these requirements, and therefore there is no certainty as to the measures which the data administrator is required to pursue. (c) The ability of the individual to demand compensation, should the data administrator fail to meet his obligations, is subject to proof of damages, yet in many instances the damage is intangible or has not yet materialized.[111]

The question of whether photography using UAVs, performed by *individuals*, as part of the *third* circle, constitutes a breach of privacy will be examined in line with the provisions of Section 2(3) of the PPL, which prohibits photography in the private domain and Section 7(b) of Basic Law: Human Dignity and Liberty, which states that "*There shall be no entry into the private premises of a person who has not consented thereto.*" Thus, Israeli law provides protection to the subject of the photograph (including in cases where the photograph was taken by a UAV), in circumstances where the photograph was taken in the *person's home*.[112] However, when it comes to photography by a UAV, carried out in the *public domain*, the subject of the photograph has to show that the photograph is demeaning, and this test is based on the reasonable person test.[113]

Section 4 of the PPL states that breach of privacy constitutes a civil wrong, and the provisions of the Torts Ordinance would apply to it.[114] Alternatively, Israeli law protects the independent right to autonomy as an independent class of tort, derived from human dignity, for the purpose of calculating tort compensation. A potential plaintiff who was photographed without his consent, would pose a challenge to the court, were he to sue for breach of his right to autonomy by reason of having been photographed by a UAV.[115] Compensation for breach of autonomy once again reflects privacy as control, since photographing a person in the public domain, without his consent, constitutes expropriation of the subject's control of information about himself, and thus a breach of his privacy. Hence there is a need for knowledge, understanding and consent.[116] In addition, the operation of the UAV is subject to the various wrongs listed in the Torts Ordinance (including trespass on property).[117]

[107] Section 8(c).
[108] Section 11.
[109] According to Sections 2(9) and 8(b) of the PPL.
[110] Section 16.
[111] Birnhack, Private Space: The Right to Privacy, Law & Technology at 235.

[112] Similar to the English common law approach which protects the private home against government intrusion. Compare to the principle contained in the US legal doctrine known as "Castle law" or "defense of habitation law".
[113] Section 2(4). Roadmap for the Integration of Civil Remotely-Piloted Aircraft System, *supra* note 21, at 20. *See* also the Australian Privacy Comissioner's letter to the Attorney General, *supra* note 100 stating that while the Australian Privacy Act 1998 covers private sector organizations' use of drones it does not cover the actions of individuals in their private capacity, including the situation where individuals use drones. Other Australian local laws that protect individuals against unlawful surveillance, stalking and harassment do not provide sufficient regulatory protection including appropriate restrictions on unreasonable use.
[114] Section 5 of the Law states that a breach of certain provisions of the Protection of Privacy Law is a criminal offense, and that such a breach is deemed to be deliberate (including the case where a photograph is taken when the subject of the photograph is in the private domain).
[115] The Israeli legal system, in many senses, uniquely recognizes a breach of autonomy as a principal tort, derived from the right to human dignity. In other countries the right is recognized, but included in the framework of compensation for other torts. *See* for example, the judgment given in CA 2781/93 *Daka v. Carmel Hospital* 53(4) PD 526 [1990] (Isr.).
[116] Birnhack, *supra* note 9, at 50.
[117] Section 29 of the Civil Wrongs Ordinance, 1968, D.M.I. 266 (Isr.). For a discussion regarding the implementation of American tort law with respect to the use of UAVs by individuals *see* Villasensor, *supra* note 70, at 500.

5. Proposed solutions for addressing potential breaches of privacy arising from the use of UAVs

The two main conclusions which can be drawn from the discussion so far may be summarized as follows: (i) the civilian use of UAVs would infringe the fundamental right to privacy, albeit the issue of the precise scope of that breach requires both additional research and, more importantly, sufficient time to better examine the practical impact of civilian use of UAVs on privacy; (ii) given the advantages inherent in the civilian use of UAVs, and the desire to avoid a chilling effect, it is essential to effect a solution that would enable the use of civilian UAVs while concurrently protecting the right to privacy.

The Israeli legislature may choose a solution from a broad spectrum of possibilities. The discussion in this section will be based largely on solutions offered in the United States and the European Union, primarily because of the relative similarity between the latter legal systems and the Israeli legal system and, of course, in light of the fact that all the countries concerned face similar challenges arising from the civilian use of UAVs.

5.1. *Technological and social solutions*

(i) "Privacy by Design (PbD)": "This principle means that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal."[118] The advantage of adopting PbD is that preventive measures will be taken in relation to the use of UAVs, rather than reactive steps such as monetary compensation for breaches of privacy. Thus, for example, the use of UAVs will have to be limited to certain geographic areas and to limited periods of time. There will have to be transparency in terms of the rationale and goals to be achieved through the use of UAVs. Measures must be taken to ensure that the cameras installed on the UAVs are not aimed at windows, and that the operator does not aim or focus on areas where there is a greater expectation of privacy (such as private dwellings). In addition, to the extent that the use of UAVs involves the collection of photographic or video images that include the faces of individuals, the organization operating the UAV must make use of anonymous video analytics.[119] In those instances in which it is determined that the use of a UAV is to be permitted, for example, for defense purposes, it must be ensured that the process of viewing the resulting images is carried out in line with a "*Privacy Protected Surveillance using Secure Visual Object Coding*" process[120]; (ii) *Privacy by Assessment*: a structured process assisting organizations in evaluating the influence that new technology, to be integrated in UAVs for the civilian market, will have on the individual's privacy[121]; (iii) *Education*: states must actively take steps to educate the public regarding the benefits associated with the use of UAVs and, concurrently, educate their potential civilian operators about the damaging consequences which their actions may have for the right to privacy. In this way, the state may successfully mitigate public fears concerning the use of UAVs in the civilian market.[122]

5.2. *Legislative solutions*

(i) Rectifying the shortcomings of the PPL in relation to databases, bringing them into line with the various European directives for data protection, as proposed by the *Schoffman Committee*[123]; (ii) enacting a special law that will list the obligations and requirements to be imposed on operators of civilian UAVs, with strict limitations on the type of technology, and in particular the camera lenses, which may be installed and assembled on a civilian device. Thus, for example, consideration should be given to amending the search laws and determining that, as a general rule, law enforcement agencies would only be able to make use of UAVs after obtaining a search warrant. Further, consideration should be given to the types of data that UAVs will be allowed to collect; procedures for deleting data that is not relevant to the specific purpose for which the civilian operator received a permit; the period of time for which the data could be kept; and the specific circumstances under which the UAV collected data might be used.[124] Similarly, conditions for obtaining a UAV commercial operation license will require prior publication on a designated website; the conditions should refer to the purposes of operation and the dates on which the service will be carried out. Thus, for example, ILITA, the public body responsible for privacy protection on behalf of the State of Israel, made the operation of the *Google Street View* service in Israel conditional upon prior notice being given in the national press as to the nature of the service and its dates of operation. A similar solution can be adopted with respect to the use of civilian UAVs.

Additionally, the ILITA restrictions as to the transfer to Google Inc. of data received from operating the *Google Street View* service; the blurring of faces and license plates captured

[118] A Digital Agenda for Europe 17 (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Aug. 26, 2010) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF.

[119] This is software that processes the video film, searching, at the pixel level, for images that are similar to human faces. Where there is a match, the software automatically deletes the relevant frame. *See*, Privacy and UAVs: Unmanned Aerial Vehicles 19.

[120] *Id*. To view the pictures, the viewer must enter personal details known only to the user.

[121] *Id*. at 17.

[122] Stephen R. Brown, *It's drone season! Colorado Town to vote on License to shoot down unmanned aircraft*, Daily News (Dec. 10, 2013) http://www.nydailynews.com/news/national/colorado-town-vote-license-shoot-drones-article-1.1543030.

[123] The Schoffman Committee was set up to examine the appropriate legal arrangements for regulating the field of databases in Israel. *See* Schoffman Report (Jan., 2007) http://www.justice.gov.il/NR/rdonlyres/74594019-306F-4578-B604-189BE42EA1A0/8153/DochDB.pdf (Isr.).

[124] The United States Congress considered a series of bills aimed at ensuring that the right to privacy would be maintained in the UAV age. *See* UAVs in Domestic Surveillance Operations, *supra* note 13, at 20.

by the service and adoption of the PbD model, mentioned above, can all be applied to the use of civilian UAVs.[125]

5.3. *Voluntary solutions*

The voluntary adoption of rules by organizations operating UAVs may lessen public opposition to their use. Thus, for example, the Association for Unmanned Vehicle Systems International calls for an undertaking to respect the privacy of individuals.

6. Conclusion

The principal conclusion arising from the detailed analysis above is that the use of UAVs in the civilian market will, in the near future, pose an enormous challenge to the right to privacy. There is a broad spectrum of opinions and ideas as to how we may cope with the risks inherent in the use of UAVs for civilian purposes. In light of the complexity of the subject, and the fact that the use of UAVs in the civilian market also carries with it advantages (as well as disadvantages), and also in light of the fact that civilian use of UAVs is still in its infancy, legislatures and courts need not rush to enact strict laws and rulings as to the time and manner in which such use will be allowed.

Nevertheless, it is already possible to present four insights. The *first* insight is that technological progress, in this case the use of UAVs for civilian purposes, is inevitable. The *second* insight refers to the problematic situation whereby the regulation of UAVs is the sole responsibility of local aviation authorities. Without derogating from the importance of safety considerations, regulatory authorities that lack the proper knowledge and tools to cope with the potential risk to the right to privacy, should not be assigned the task of regulating the use of UAVs for civilian purposes. In other words, governmental bodies, such as ILITA, which have the relevant technological and privacy knowledge and experience, should be consulted and granted a leading role in shaping the rules and guidelines regarding the use of UAVs for civilian purposes. The *third* insight is that the ability to limit (even if not prevent) breaches of privacy requires a combination of legislative-regulatory, technological, and social measures. Finally, the *fourth* insight is that the effectiveness of the solutions to be adopted to mitigate the risks associated with the use of UAVs for civilian purposes depends on the ability of the states, commercial bodies and individuals to coordinate their operations.

Within the framework of the solutions presented in this article, special emphasis should be given to the role which must be fulfilled by local governments when regulating the use of UAVs for civilian purposes. Governments and policy makers should initiate public discussions with all entities involved in the design, manufacture and use of UAVs, including the "non-profit sector". One can hope that the result of such discussions would be the voluntary wide-spread acceptance of rules and guidelines for the design, manufacture and use of UAVs in the civilian market. These rules and guidelines should, and must, find their way into local by-laws and regulations. Alternatively, in the event that no agreement is reached on the conditions for the operation of UAVs for civilian purposes, and as a temporary solution, local legislators and policy makers should enact a regulatory regime that ensures a proper balance between the right to privacy, on the one hand, and the benefits associated with the use of UAVs, on the other hand. Finally, manufacturers and companies that market UAVs should consider the repercussions of using certain technologies and photography equipment assembled on UAVs, within the framework of a comprehensive PbD procedure, before marketing the UAVs in the civilian market.

[125] ILITA Guidelines Regarding the Registration of Google Street View Database in Israel (Oct. 10, 2011) http://www.justice.gov.il/MOJHeb/ILITA/News/streetviewauthorized.htm.