Spioneren met hobbydrones en andere technologieën door burgers: een verkenning van de privacyrisico's en reguleringsmogelijkheden

Maša Galič, Merel Noorman, Bart van der Sloot, Bert-Jaap Koops, Colette Cuijpers, Raphaël Gellert, Esther Keymolen en Thierry van Delden

Universiteit van Tilburg

TILT – Tilburg Institute for Law, Technology, and Society

Postbus 90153

5000 LE Tilburg

m.galic@uvt.nl

Tel: 013 466 3534

7 mei 2020

Summary

1. Background and research question

Spy products such as miniature cameras, eavesdropping devices and location trackers enable citizens to spy on, that is covertly surveil, each other. However, citizens can also covertly surveil others with the use of products that are not directly designed for spying, but that are very suitable for it, such as hobby drones with sensors. As such, it makes sense to distinguish between **spy products in a narrow sense** (that is, devices designed or adapted primarily for the surreptitious gathering of information about persons) and **spy products in a broad sense** (that is, devices that can be used to covertly collect information about a person, but of which such covert collection of information is not the main purpose of design or use). Examples of the former are spy-cams or eavesdropping devices in the shape of everyday of objects and location trackers (both physical devices and spyware). Smartphones and drones are examples of the latter.

The wide availability of both types of products on the market, both in physical spy-shops and in web-shops, and the fact that they are becoming increasingly cheap, has led to a stark increase in the possibility and opportunity to spy on others. As sensors are becoming increasingly small, they can be hidden or built into any everyday object imaginable, from a shampoo bottle to a cuddly toy, and secretly placed in houses and toilets, as well as on people's smartphones (‘spyware’). The constantly improving quality of recording makes it possible to spy on others from greater distances, and new capabilities enable penetrating physical barriers, such as walls. Finally, the possibility to surreptitiously record and disseminate information is by now almost unlimited. Spy products can record for increasingly long periods of time, remotely and in real-time. Such recordings can then be adapted (think of deep fakes) and/or spread globally via the internet with a matter of clicks.

The main question investigated in this report is *how the regulation of hobbydrones and spy products in a narrow sense can be optimised in light of protecting citizens’ privacy.* Answers to this question are based on desk research, legal analysis on Dutch, German and French law and the acquis of the European Union, internet quickscans, two focus groups on hobby drones and 10 semi-structured interviews with stakeholders connected to hobby drone flying and experts on drones (including academics, practitioners, organisations).

The distinction between spy products in a narrow and broad sense is particularly useful for the goal of this study: the inventory of regulatory options. Spy products in a narrow sense can namely be **regulated at the source** (‘upstream regulation’; e.g. licensing requirements or prohibition of sales or possession), whereas spy products in a broad sense can best be **regulated at the end** (‘downstream regulation’; e.g. criminalisation of malicious use and awarding damages).

This report assessed the privacy risks in horizontal (citizen-citizen) relations, evaluated potential lacunae in the Dutch legal system and specified regulatory options to remedy those lacuna's, using Lessig's well-known categorisation of regulation through the market, social norms, code (or architecture) and law.

2. Privacy risks in horizontal relations

Numerous types of spy products available globally on the market can intrude into persons' privacy (that is, 'the ability to be yourself') in a number of ways.

Firstly, spy products enable making recordings within citizens' homes and other private places, such as cars or hotel rooms. They can secretly record images or sound both from the inside (e.g. by placing a listening device in the shape of a wall clock in the kitchen) or the outside of the home (e.g. by drones 'peeking' through windows or through infrared cameras). This puts pressure on the idea of the dwelling as an enclosed private space ('one's castle'), and therefore **spatial privacy**, because the occupant of the dwelling loses control over who has access to that space.

Second, spying within (or inside) the home may also intrude upon intimate matters and thus **bodily privacy**. For example, drones can record persons while they are sunbathing topless in one's backyard. In addition, it should be noted that such intimate images can also be recorded in public and semi-public space. Think of a drone flying over a nudist beach or of hidden cameras in saunas and changing rooms of fitness venues.

Third, citizens' **communicational privacy** can be interfered with, inter alia, by placing listening devices in a home or an office, which can record private conversations either of persons present or via the phone. Another way to do so is by placing tracking apps (spyware) on someone's smartphone, allowing one to eavesdrop on every conversation, e-mail exchange or other private communication transmitted via that device.

Fourth, the possibility to record images, sounds and tracking location in private, public and semi-public space, combined with the (feeling of) loss of control by citizens and the impossibility of knowing for sure whether and when such recordings might be made, can lead to a notable change in people's behaviour. Persons who (think they) are surveilled may begin to behave in an increasingly inhibited manner (for instance by dressing more conservatively), may reveal less in conversations, and may even hesitate to associate with certain friends both in public or private (for example, if they think that a jealous ex-partner is tracking their movements). This leads to an interference with citizens' **behavioural** and **associational privacy**.

Fifth, and perhaps most obviously, spy products enable the collection and processing of information, putting citizens' **informational privacy** at risk. Once information has been captured and/or aggregated, it can then be further disseminated. This may involve publishing the

information online or sharing it with third parties, which can damage a person's reputation. Threatening with such actions can be used for blackmail, either for monetary gain or other (malicious) purposes.

Finally, it is important to consider **the cumulative effect of privacy violations**. While each recording in itself can reveal relatively little (intimate) information, when tens or hundreds of different 'harmless' sources of information are combined, they can paint a rather concise picture of someone's private life. For example, information collected by location tracking for a week can reveal a lot about a person's professional and personal life: where they live and work, how they spend their time in the evenings and weekends, whom they spend time with, and so on.

3. Gaps in legal protection in the Netherlands

In order to address the aforementioned privacy risks, we have investigated possible gaps in legal protection in the Netherlands. We have examined existing privacy and data protection legislation, criminal law, private law, the portrait right, general local ordinances and drone regulations. Because many of these rules stem directly or indirectly from EU Directives and Regulations, and the rules by the Council of Europe, the findings of this report as to the legal lacunae and regulatory options may have significance for many European countries.

This research shows that the current (or upcoming) legislation offers substantial protection against most of the identified privacy risks. In fact, most current use of hobby drones and spy products for the purpose of spying on others already violates existing laws. Nevertheless, a few smaller gaps (or lacunae) in the laws do exist, mainly requiring clarification or a slight broadening of scope.

Research carried out for this study, however, shows that the **main gap** relating to the regulation of hobby drones and spy products concerns **a lack of compliance and enforcement of the existing rules**. This is due to a combination of factors. Firstly, in the case of covert recordings the obvious problem is that the victim often is unaware that she is being spied upon. This is particularly the case regarding spy products in a narrow sense, which are designed for surreptitious surveillance. However, even if the victim does become aware of the spying, for example because recorded images have been placed online, it is often very difficult to determine who is responsible for the spying (and the placing online) and, moreover, to prove this in criminal or private legal proceedings afterwards.

Secondly, the amount of **compensation** granted in private law proceedings for immaterial damage suffered from the intrusion into privacy is currently very low. This means that even in case victims are aware of and can prove a causal link between the spying and the immaterial damage, the awarded monetary compensation is often low. This may mean that beginning legal

proceedings is not considered a worthwhile endeavour, because legal proceedings amount to a significant emotional and financial burden.

Finally, **possibilities for enforcement** are also limited because non-compliance with the law through the use of drones and spy products often involves relatively a high number of relatively small incidents. As such, it cannot be expected of the Data Protection Authority to investigate every photo, video or sound recording taken by a citizen using a drone or a smartphone, and to check whether it was done lawfully. It also cannot be expected of the Public Prosecution to prosecute every surreptitious and unlawful recording. Based on our interviews and focus groups, municipalities also find it difficult to enforce the rules concerning the prohibition of spying and nuisance in the general local ordinances. Even in the case of drones, which are the most visible of all spy products, Special Investigation Officers need to perceive the nuisance caused by the drone personally. However, it is impossible for them to constantly monitor the streets and skies in order to spot drones and to then follow them to their rightful owner. Enforcement of the law will thus provide protection only against the most intrusive incidents in which, for example, people's physical or spatial privacy is at stake.

4. Regulatory options

Consequently, while Dutch law already offers substantial protection against privacy risks stemming from use of hobby drones and spy products in a narrow sense, there are also several smaller and some larger gaps, which may still be filled by the legislator. We also suggest possibilities for the regulation of spy products in a narrow sense based on examples from France (a licensing system for audio-surveillance equipment) and Germany (a prohibition of certain types of image- and sound-recorders). Considering that the main identified gap concerns compliance and enforcement, the law on itself cannot sufficiently address it; other types of regulatory tools also need to be employed. We therefore structure our recommendations for regulation according to Lessig's four types of regulatory tools: market, social norms, code and law.

Market

One regulatory option is to leave the protection of privacy up to the market. For instance, almost all web-shops that sell spy products also offer **anti-spying products**, such as jammers (devices that transmit signals on certain radio frequencies in order to disrupt communication between devices) and devices that can detect hidden recording devices. One option is thus to leave it up to citizens themselves to protect themselves against spying fellow citizens by purchasing such devices. However, relying too much on this option may not be desirable as it would lead to a kind of arms race between citizens, where the question of whether someone's privacy is adequately protected depends on how much she is able to invest (in terms of money, expertise and time) in anti-spying products.

Another type of market regulation can be found in the **information concerning privacy available on sellers' and producer's websites**. Several examined websites selling or producing drones include links to local drone legislation. Some also include a part on the website dedicated to 'proper use' of drones with reference to privacy. Several drone manufacturers are also working on privacy-by-design solutions, either of their own accord or as a response to (upcoming) legislation. Companies also exist that provide **training courses** both for recreational and professional drone pilots, in which privacy plays a role. The upcoming EU drone regulations are likely to increase the demand for training, as they make it compulsory for most drone pilots to pass at least a theory exam.

The situation is very different in relation to the examined web-shops selling spy products in a narrow sense. These web-shops offer little or no explanation to buyers as to what is allowed or not according to the law. Companies also declare that they cannot be held liable for unlawful use of spy products purchased from them, placing the burden on the individual to check, what types of use of the product (or the product itself) are legal in their country. Furthermore, several web-shops directly encourage activity which is illegal, at least in most countries around the world, in their advertisements. For instance: 'With a spy camera you can follow all movements in a home, meeting room and at work unnoticed.' Therefore, leaving the protection of privacy purely or mainly in the hands of these sellers ('the market') may not lead to the most satisfactory outcome.

Social norms

Efforts could also be made in order to create more awareness about privacy risks stemming from the use of hobby drones and spy products in narrow sense. For example, **national awareness campaigns** could be launched, trying to increase the awareness of citizens of the dangers of spy products and make them aware of what is what is not allowed. Websites could be launched that focus on the privacy aspects of spy products and the legal obligations stemming from their use. Such sources of information are particularly important in relation to the upcoming EU drone regulations, which introduce a wide range of obligations that are very complex and difficult to understand. Such awareness-raising campaigns are likely to be effective when it comes to the use of spy products in which people generally have no intention of violating the privacy of others; thus, especially in relation to spy products in a broad sense, such as drones. Concerning spy products in a narrow sense, which are made for covert monitoring of others, such awareness campaigns are likely to be less effective, because unfamiliarity with the legal framework is not the problem.

Based on this research, **initiatives by civil society organisations, associations and individuals** are also a valuable source of information concerning privacy. For instance, novice drone pilots often visit the websites of such associations (e.g. dronewatch.nl) to obtain information about what may and may not be done with drones. Forums are also a good place for hobby drone pilots to communicate with each other, offering rich sources of information, also in

relation to privacy. There are several ways through which the government could support such initiatives, such as through monetary support, organisation of workshops, etc. Again, such initiatives are likely less effective with communities that use spy products in the narrow sense, which are more likely to offer advice on the best ways to spy on others.

Code

Techno-regulation could play an important role in maintaining horizontal privacy. The EU regulations on drones already envision several technical solutions, such as **geofencing**, **unique serial numbers** of drones and a **remote identification system** (enabling remote identification of drones). For example, geofencing can be used to prevent drones from entering certain zones. The unique serial number and the remote identification system are, however, not required for drones with or without a sensor weighing less than 250g. It may, however, be desirable to make these technical requirements mandatory for all drones that can record personal data, no matter the weight. These technical solutions would namely enhance the possibility to identify the drone pilot that is intruding into others' privacy. It should be noted that, techniques such as remote identification and geofencing can be switched off with a few simple interventions. These technical solutions thus will not succeed in preventing all, especially the more tech-savvy, citizens spying on others. Nevertheless, they will help the average hobby drone pilot to reduce the risk of (accidental) privacy breaches.

Technical measures to prevent privacy breaches are less suitable in relation to devices that are designed primarily for spying on others. Considering that spy products in a narrow sense are primarily intended to surreptitiously collect data about others without permission, implementing the above technical requirements would negate the raison d'être of such products. Legal rules, such as prohibitions and licensing regimes, are therefore more suitable to regulate these products.

Law

There are a number of points in Dutch **criminal law** that require clarification and possibly adjustment.

- First, it is somewhat unclear whether the prohibition of covert surveillance in private and public space also covers recordings made with a drone (the same applies to recordings made with a smartphone). Considering the **requirement of surreptitiousness**, it is unclear to what extent recording drones can be regarded as covert. Although it is relatively known that many or most drones have cameras, it is difficult or impossible to know, whether in a concrete instance a recording is actually being made, and people can hardly effectively protect themselves against unwanted recordings.
- Another point that would merit attention from the legislator concerns the scope of the prohibition of recording of conversations, which is currently forbidden only when it concerns

the recording of conversations of others, that is conversations in which the spy itself is not involved. However, one can also covertly record a conversation in which one is participating. The legislator might thus consider switching from a so-called one-party consent model to an **all-party consent model**.

- Considering that drones are also used to commit certain crimes such as burglaries (for example, by flying around the house to check whether someone is at home or whether a window is open), the legislator could also consider introducing a **criminalisation of covert observation of objects** such as houses, barns, sheds (rather than persons) as a preparatory act of committing certain crimes.
- Finally, the surreptitious placement of physical location trackers on another citizen's car is currently only punishable if an object is damaged during installation. The legislator could consider introducing a **direct prohibition of physical location trackers** in the Criminal Code, similarly to how digital location trackers are prohibited.

However, as noted in section 3, the main shortcoming in relation to privacy protection stemming from the use of drones and spy products concerns enforcement and compliance with the current legal framework. This main gap can generally be addressed in two ways: (1) a greater focus on ***ex post* enforcement and compensation** (downstream regulation) and/or (2) a greater emphasis on ***ex ante* regulation of the sale and purchase** of spy products (upstream regulation). The first will be particularly important with regard to spy products in a broad sense, including drones, while the second will mainly apply to spy products in a narrow sense.

Among the *ex post* options, the legislator could consider, whether compensations for immaterial damage in cases of privacy violations in **private law** proceedings are high enough. For many citizens, the effort and costs involved in litigation do not outweigh the possible damages awarded, which are currently very low. A possible solution would be to set higher compensation guidelines for courts or to lay down a minimum amount for privacy violations caused by spying.

In relation to the **general local ordinances**, this study has found that there is uncertainty among municipalities about how new types of spy products, especially drones, can and should be regulated by local ordinances, and to what extent the newly introduced rules will stand up in court. In view of this lack of clarity, the Dutch Association of Municipalities could provide guidance on the possibilities of regulating drones and spy products in a narrow sense through existing or additional provisions in the local ordinances.

Considering the limited possibilities to enhance enforcement (as a type of ex post regulation), possibilities of ***ex ante* regulation** should be looked at more closely.

With respect to drones, an obligation might be introduced for drone pilots to register. While such an obligation already exists (and will enter into force with the forthcoming EU Regulation on drones in July 2020), the Dutch legislator might also consider broadening the obligatory

requirement for **unique serial numbers** and the **remote identification system** in the EU Regulation on drones to all drones with a sensor thus facilitating the identification of the drone pilot.

Regarding *ex ante* regulation of spy products in a narrow sense, two types of instruments are particularly suitable. The Dutch legislator could follow the example of France and establish a **licensing system for both buyers and sellers of spy products in the narrow sense**. Such a licensing system requires each spy product to have a unique identification number and can thus facilitate the identification of persons conducting the espionage. While the French licensing obligation only applies to spy products in a narrow sense that enable audio recording, the Dutch legislator could consider broadening its scope to include spy products enabling visual observation and location tracking. Additional rules could also be introduced, such as a mandatory explanation at the time of sale of what is or is not allowed with regard to the use of such products, comparable to pharmacists, who have to explain the correct use, dangers and risks of the products they sell. Of course, such a licensing system should not be seen as a panacea to the spying problem, considering that the sellers or buyers of spy products can fairly easily circumvent the licensing requirement by ordering a product from a foreign online shop (such as Alibaba.com) or by setting up their company in a country without such a requirement.

Following the example of Germany, the Dutch legislator could also consider simply **prohibiting the production, distribution and use of particular types of spy products in a narrow sense**. The German prohibition specifically applies to spy products suitable for the surreptitious interception of others' private conversations and surreptitious recording of others' images, which need to be shaped as an everyday object or embedded in one. This includes, for instance, spy cams in the shape of pens or dolls with a hidden listening device. However, the German ban does not include spy products that can be hidden 'in plain sight' due to their (increasingly) miniature size, such as a spy cam shaped as a black box the size of 1,5cm³. Furthermore, the German prohibition only applies to spy products that can transmit data wirelessly; a spy product that can surreptitiously record data but transmits it via USB does not fall within the scope of the prohibition. The Dutch legislator might thus consider broadening the prohibition to include spy products, which are particularly suitable for spying due to their miniature size, and, which cannot be read out wirelessly, but can be read out in any other way. By introducing these two additions, circumventing the ban (both for sellers and buyers) would become much more difficult. Finally, the Dutch legislator could follow the German example by designating a specific authority (in Germany this is the *Bundesnetzagentuur*) with clearly defined powers and a clear point of contact for handling complaints, withdrawing products, imposing fines or ordering the destruction of products.


1: Prohibition
• First, it could be examined, whether and which products could be prohibited, either at the moment of production or at the point of sale.
• In particular, everyday products with sensors as well as miniature microphones and cameras that can be hidden in everyday objects could be considered.
2: Licensing
• Second, the extent to which the sale and use of non-banned products could be put under a licencing obligation could be explored.
• In particular, possibilities for a licencing regime concerning physical and virtual spyshops, and the use of drones in residential areas could be explored.
3: Technical requirements I
• Third, it could be investigated to what extent technical requirements that would make certain actions and recordings impossible (or at least, much more difficult), such as geo-fencing with regard to no-fly zones or the automatic blurring of faces or persons in drone-cameras, could be imposed.
4: Technical requirements II
• Fourth, it could be explored to what extent technical requirements could be imposed on products in order to reduce the stealthy characteristic of recording equipment.
• This could include, for example, an obligation to emanate an acoustic or light signal, when a product begins to record.
5: Criminal law
• Fifth, it could be examined to what extent criminal law provisions need to be adapted, particularly in regard to the extent that recordings by visible cameras should be covered by the prohibition of covert surveillance, whether covert recording of conversations by a participant in a conversation should also be prohibited, and to what extent the installation of physical location trackers should be punishable.
6: Guidelines
• Sixth, it could be examined to what extent more clarity could be provided on the interpretation of the current regulatory framework with regard to spy products and drones.
• In particular, this could include the development of a model provision in the General Local Regulation by the Dutch Municipalities Association and guidelines by the Personal Data Protection Authority with regard to data protection law.
7: Awareness
• Seventh, it could be explored to what extent efforts to create more awareness could be made, for example by means of national campaigns, by placing prohibition signs or by developing apps that would enable drone users to quickly and easily see where they are and are not allowed to fly.
8: Auditing
• Eighth, it could be investigated to what extent drones and other spy products could be equipped (as a default) with technical-procedural mechanisms allowing audits and controls, such as logging the use and location of the device.
9: Enforcement
• Ninth, ways to strengthen the enforcement of the legal framework could be explored, for instance by developing a joint strategy between municipalities, the Personal Data Authority and the Public Prosecution Service.
10: Compensation
• Finally, it could be investigated, whether it is possible to grant citizens a standard allowance in the event of unlawful data collection by fellow citizens by means of drones and other spy products.