## Summary

Fundamental rights, such as the right to privacy, are primarily aimed at the protection of citizens against the state. But citizens may also violate the fundamental rights of others. For that reason, it is imperative to assess the extent to which fundamental rights (more specifically, the right to privacy) provide protection in 'horizontal relationships'. The issue of horizontal privacy was raised in the '*initiatiefnota onderlinge privacy*'. The topic of privacy violations in horizontal relationships is aimed at violations committed in the context of (i) actions of citizens towards each other and (ii) the relationship between citizens and legal persons (companies, associations, etc.). The protection of horizontal privacy is differentiated from the protection of vertical privacy, which concerns the relationship a citizen has with the state.

This research addresses a problem statement that can be divided into three sub-statements:

- What lessons can be learned from the approach taken by other European countries with regards to the protection of horizontal privacy?
- To what extent can these solutions be applied in the context of the Netherlands?
- Are there any undesirable consequences or side-effects associated with the opportunities to provide effective protection to horizontal privacy in the Netherlands?

The countries that are involved in the legal comparative analysis are: Germany, Poland, Sweden and the United Kingdom.

To address the problem statement, the following questions require answering:

- What is 'horizontal privacy' and how is it conceptualized in the Netherlands and the investigated European countries?
- What are the protected interests that may be affected by the impairment or violation of horizontal privacy?
- What are the current impairments to these interests?
- What are the various forms of prevention, enforcement and prosecution of violations currently used?
- What forms of cooperation exist between citizens, businesses and the government to combat the violations of horizontal privacy?
- How has the protection of horizontal privacy been designed in Germany, Poland, Sweden, and the United Kingdom?
- To what extent are protective measures from these countries useful in the context of the Netherlands?
- What are the potential negative effects of implementing these measures to better protect horizontal privacy?

The scope of this research is limited to 'digital' privacy violations. In this research, we focus on the (i) citizen-to-citizen relationship and (ii) the citizen-to-private legal person relationship (more specifically, the relationship between business and consumers/employees). However, the emphasis is placed on the discussion and analysis of privacy violations committed by citizens towards each other.

**Violations of horizontal privacy**

The privacy of citizens in horizontal relationships can be violated in any number of ways. This research makes a distinction between the actions leading to the invasion of privacy and the consequences that this can have for the individual and society as a whole (the values and interests that as a result are likely to be affected).

Actions that may affect the privacy of citizens that we have identified are: observation, the collection and registration of data, analysis and decision-making, creation, the sharing and publication of data and interaction and communication.

*Observation*

Privacy violation typically starts with the observation of individuals and their behavior. In the digital era, observation is not limited to literally 'watching' an individual (whether or not aided by technical resources) but also concerns the following of an individual on social media and monitoring an individual's behavior on the Internet.

*Collection and registration*

Observation often goes hand in hand with the actual collection and recording of (personal) data. Relevant examples are the recording of images or conversations on a mobile phone but also includes the registration of traffic data or the location of an individual.

*Analysis and decision-making*

Depending on the purpose, registered data can be analyzed. This is particularly relevant in the context of a citizen's relationship with businesses, because it is primarily these businesses that are engaged in the analysis of personal data and using this analysis to inform their (automated) decision-making. The underlying purpose is generally to gain insight into the behavior and desires of consumers.

*Creation*

In addition to the observation and registration, data concerning individuals can also be created. Good examples are the creation of photomontages, cartoons, and even memes. One could also think about creation and dissemination of statements and/or expressions and how they can be (mis)attributed to an individual.

*Sharing and publication*

Many violations of horizontal privacy concern the sharing of data (photos, text, videos, sounds). Data can be shared with a single person, a (relatively) limited group (a private WhatsApp groupchat), or a large and undefined group (Facebook, Instagram, or Twitter). The sharing of data exposes information relating to an individual (or exposes their identity) with the result that it (undesirably) becomes public.

*Interaction and communication*

Direct interaction and communication with a person can also affect his or her privacy. Through digital means of communication it becomes possible to contact an individual at any moment and to communicate with (or about) them. This kind of interaction can, depending on the nature and frequency of the communication,

result in the violation of that individual's privacy. Prominent examples are stalking, cyber-bullying, the communication of offensive insults or threats.

**Values and interests**

The right to privacy is a comprehensive right. Not only does the right to privacy have a broad scope, it also functions as an 'umbrella right' which serves to protect a wide range of values and interests. The current research has identified the relevant values and interests and divided them into the following groups: dignity and reputation, confidentiality and control, personal autonomy, the development of identity and emotional relief, maintaining (intimate) relationships, security, economic equality, and the prevention of nuisance.

*Dignity and reputation*

Dignity (or personal honor) and reputation form components of the right to privacy as set out in Article 8 of the European Convention on Human Rights. Honor and dignity refer to the value one has in his or her own eyes. Reputation concerns the value that one has in the eyes of others.

*Confidentiality and control*

A crucial element of the right to privacy is the possibility to restrict and exclude the access of others to one's private life (which includes information and communication). This control of private life enables an individual to temporarily withdraw from social interaction and also enables them to selectively share information and aspects of their personality. Confidentiality and control play an important role in the relationship between individuals and legal persons. For example, when companies collect personal data relating to individuals, these individuals lose control of their information.

*Personal autonomy*

Privacy is an important requirement for the preservation of personal autonomy. As others gain more knowledge about an individual (his or her interests, weaknesses, preferences, habits, contacts, *et cetera*), it becomes easier to exercise power over this individual (or manipulate them).

*Development of own identity and emotional relief*

A more specific element of the personal autonomy is the possibility for an individual to develop their own identity, free from the pressure and influence of others. The right to privacy creates a space to experiment with a personal identity and (temporarily) escape the pressure of societally acceptable or expected behavior.

*Maintaining (intimate) relationships*

Confidentiality is a condition for social relationships. For example, friendships are in large part formed by the exclusive transfer of information.

Another aspect of the right to privacy that affects relationships is the so-called *associative privacy*. Associative privacy concerns the relationships and contacts that individuals maintain. When these contacts are made public, especially without providing the necessary context, maintaining these contacts in the future is made difficult.

*Security*
The most extreme cases of violations of horizontal privacy can also create a threat to the safety of the victim or their sense of security. Examples are the communication of communicating offensive insults, threats, harassment (stalking) and cyber-bullying.

*Economic equality*
Where it concerns the relationship between a (potential) client and a business, the economic position of the client is particularly susceptible to privacy violations. Information asymmetry provides businesses with a dominant position in comparison to the consumer. This position can, among other things, be exploited in the form of price discrimination or *nudging* clients towards certain groups of products.

*The prevention of nuisance*
The prevention of nuisance is also an interest protected by the right to privacy and data protection. From the perspective of the commercial industry, relevant examples include the sending of unsolicited commercial communications and personalized advertising.

**Categorizing horizontal privacy violations**
Set out below is a categorization of horizontal privacy violations, determined on the basis of (i) actions with potentially violating effects and (ii) the aforementioned interests and values that are at stake.

| **Horizontal privacy violations (citizen-to-citizen)** | | |
|---|---|---|
| *Actions* | *Manifestations* | *Affected values / interests* |
| Observation | Covert observation, filming in the public space, eavesdropping, espionage | Confidentiality and control, trust in intimate relations, identity and emotional release, personal autonomy, (sense of) security, dignity |
| Collection and registration | Covert observation, filming in the public space, eavesdropping, espionage | Confidentiality and control, trust in intimate relations, identity and emotional release, personal autonomy, (sense of) security, dignity |
| Analysis and decision-making | Profiling and automated decision-making | Confidentiality and control, dignity and reputation, personal autonomy |
| Creation and sharing | Libel, defamation, slander, hate speech, threats, extortion, revenge porn, sextortion, deep fakes, fake endorsements, fake news. | Confidentiality and control, trust in intimate relations, identity and emotional release, personal autonomy, (sense of) security, dignity and reputation |
| Interaction and communication | *Trolling*, harassement (stalking), cyberbullying | personal autonomy, (sense of) security, dignity and reputation |

| Horizontal privacy violations (citizen-to-business) | | |
|---|---|---|
| *Actions* | *Manifestations* | *Affected values / interests* |
| Observation | Monitoring online behaviour, Wifi tracking | Confidentiality and control, personal autonomy |
| Collection and registration | Customer relation management, registration of consumer behaviour | Confidentiality and control, personal autonomy |
| Analysis and decision-making | *Nudging*, *profiling*, automated decision-making | Confidentiality and control, personal autonomy, dignity and reputation |
| Creation and sharing | Selling personal data, black / whitelisting | Confidentiality and control, personal autonomy, dignity and reputation |
| Interaction and communication | Unsolicited (commercial) emails | Sense of security, avoiding nuisance |

**The horizontal application of the right to privacy**

The intention with the creation of the classical fundamental rights was that these were only applicable with regards to the state. The underlying rationale was that citizens and private legal persons were more or less equal and could challenge any infringement of their rights caused by the other through civil law. This view has changed with the passage of time. The horizontal application of fundamental rights is recognized in the jurisprudence of the European Court of Human Rights (ECtHR), the national legal order of the Netherlands, and the legal orders of the European countries investigated for this research. The common thread is that recognizing the general rights relating to personality derives from human dignity. These rights relating to personality can be invoked against anybody.

In the European countries investigated for our research, the recognition of the horizontal application of fundamental rights finds different constructions. In Germany, the horizontal application of fundamental rights is derived from the constitutional protection of human dignity. The German Constitutional Court found that these constitutional protections could be invoked against anybody. In Poland, the horizontal application of fundamental rights is enshrined in its constitution. In the United Kingdom, the horizontal application is recognized through the *Human Rights Act 1998* and the associated jurisprudence. In Sweden, the judgments of the ECtHR have created the acceptance of the horizontal application of fundamental rights.

The Supreme Court of the Netherlands has also accepted the horizontal application of fundamental rights. According to the Court, the horizontal application of these rights is derived from the general rights relating to personality which find their origin in the concept of human dignity.

The development in the United Kingdom and Sweden shows the influence of the European Convention on Human Rights (ECHR) and the ECtHR concerning the horizontal application of fundamental rights. The ECtHR's construction of the horizontal application of fundamental rights begins with the positive obligation of Contracting Parties to protect fundamental rights. The second way the ECtHR ensures the horizontal application of fundamental rights is through the enforcement of treaty-compliant interpretation by national courts. Where national courts pay insufficient attention to the protection of the fundamental rights of citizens (including in horizontal relationships), the ECtHR will find that the state has failed to fulfill its Treaty obligations.

We conclude that on the basis of both developments in the national legal order and the operation of the ECHR, the horizontal application of fundamental rights has been accepted both in the Netherlands and the European countries in our analysis. Poland and Germany have the most explicit recognition of the horizontal application of the right to privacy. We doubt whether further constitutional codification of the horizontal application of the right to privacy (based on the Polish model) or the introduction of an independent right to informational self-determination (based on the German model) is necessary or useful. Explicit recognition of the horizontal application of fundamental rights in the Dutch Constitution would appear to primarily be symbolic because of the already present recognition at the level of the ECtHR. The same applies to a right to informational self-determination. The right to privacy is not absolute and can be restricted by other rights. Introducing a right to informational self-determination is therefore, in the words of the Franken Commission, little more than a question of 'giving a lot and then taking a lot back'. In addition, it should also be borne in mind that, with the binding European data protection legislation (the General Data Protection Regulation), the room for introducing a national right to informational self-determination is very limited.

**The protection of the right to privacy in formal legislation**

The constitutional protection of horizontal privacy is given actual shape in subordinate legislation. Examples are data protection law, civil law, and criminal law.

*Data protection law*

Both the right to privacy and the right to data protection are broad in scope and may conflict with other (fundamental) rights in horizontal relationships. In the relationship between citizens and businesses, this concerns a conflict with the freedom of enterprise, and, in the horizontal relationship between citizens, it primarily concerns the freedom of expression. In the event of such a conflict, a judge will have to assess on a case-by-case basis whether such a restriction of the right to privacy is legitimate.

Data protection law, more specifically the General Data protection Regulation (GDPR), is particularly relevant in the relationship between citizens and commercial industry. The GDPR does not apply when citizens process personal data for purely domestic purposes. However, the GDPR does apply if the data is processed outside this personal sphere (e.g. through the publication on the Internet).

If it concerns the processing of special categories of personal data, through which sensitive matters about an individual are made clear, the processing is in principle not permitted, unless the individual concerned

has provided, for instance, explicit consent. If it concerns the processing of 'ordinary' categories of personal data, it may also concern a legitimate interest of the data controller that outweighs the interest of the data subject. This may be the case when camera images are made in and around the house for the purpose of home security. The extent to which this applies in the case of recreational purposes cannot be unequivocally stated and will have to be assessed on a case-by-case basis. It will hardly ever be possible to rely on this lawful basis for processing if the processing of personal data is done with the aim of causing damage to the data subject or placing them at a disadvantage.

Where the GDPR is applicable, there are a number of obligations for the data controller that go beyond having a legitimate purpose for processing. An important example is informing the data subject when personal data is processed for purposes beyond those for which they were originally collected. This disallows the covert processing of personal data for any other reason than the original purpose of collection. Another obligation is the taking of appropriate technical and organizational security measures.

The high degree of harmonization within the field of data protection law has left this research with an absence of any noteworthy differences that could be relevant for this research.

*Criminal law*
The legal comparison shows a reasonable uniformity when it comes to the criminal sanctioning of horizontal privacy violations. In all of the European countries analyzed for this research, crimes of expression (libel, slander), crimes of indecency (voyeurism, revenge pornography, violation of honor), and crimes against freedom (threats, extortion) are punishable. On the basis of the comparative law analysis, there appears to be no major discrepancies in the criminal law standards of horizontal violations of privacy in the Netherlands with respect to other countries. There are, however, a number of aspects with regards to standard setting of horizontal privacy violations in respect to criminal law that may be of interest to the Dutch legal practice.

To begin, the Netherlands has a more limited criminal liability for the creation and dissemination of sensitive information. In the Netherlands, the offense is primarily limited to the making and distribution of images of a sexual nature (Article 139h of the Criminal Code). The capturing and distribution of images of, for example, people in need of help, or distributing data concerning someone's state of health, are acts that are not independently punishable. However, under certain circumstances, the dissemination of such information can fall under the criminal definition of libel. However, a precondition is that the victim's honor or good name be tarnished. Where the information has been obtained illegally (e.g. by copying data or secretly filming individuals), it will offer a possibility for criminal prosecution in the Netherlands.

Unlike Germany and Sweden, the filming of individuals in need of help is not independently punishable in the Netherlands. Although under certain circumstances, the failure to provide assistance can lead to a criminal charge. This should concern a situation in which the individual filming could have provided assistance and was aware of this. This does not solve the problem of bystanders who film victims, where emergency services are already at the scene. It is possible to be charged with an offense of obstruction, under Article 426bis of the Criminal Code, although the individual filming would have to have obstructed others in their freedom of movement. A possible negative consequence of criminalizing the filming of

individuals in need of assistance (e.g. traffic accident victims) is that it may make it more difficult to clarify offenses. The captured images of bystanders may also play a role with regards to relevant liability and insurance issues. This should be taken into account in the context of potential criminalization.

The extent to which offensive behavior and obscenity is criminalized is in large part culturally determined. On one hand, the aim is to protect morality within society and, on the other hand, to prevent individuals from being shocked or offended by certain behavior or information. The United Kingdom and Poland have regulations in place that allow the government to take action against the dissemination of offensive or obscene images, especially when they are aimed at causing irritation or unnecessary stress. In the Netherlands, the sending of offensive material may violate the honor of an individual (Article 240 Sr), but its application is limited to the sending of pornographic material. In both Poland and the United Kingdom, the absence of this limitation means that there are more opportunities to take action against unacceptable online behavior. For example, serious forms of pranking or trolling could fall within the scope of the offense and its definition if the public is sufficiently offended. In the Netherlands, this type of behavior is not independently punishable. However, depending on the circumstances of the case, this type of behavior may be punishable, in particular when maltreatment or destruction is involved. Whether the unacceptable behavior should be subject to broader criminalization in the Netherlands is ultimately a political issue. Wider criminalization for the disclosure or dissemination of information does offer more possibilities to counter horizontal privacy violations. Although on the other hand, freedom of expression might be threatened if there is no clear definition of what is considered obscene, harmful, or otherwise hurtful. In addition, there is also a danger this broader criminalization might lead to arbitrary application.

Furthermore, in the European countries analyzed for this research, it is clear that many crimes of expression are not crimes conditional on a complaint like in the Netherlands. This offers the government more possibilities to act autonomously in setting standards. Even here, the question surrounding whether this is desirable with a view on safeguarding the freedom of expression, because it provides the government with more leeway to take direct action against (minor) violations of privacy. Finally, in a number of countries the penalties for crimes against expression crimes (e.g. libel and slander) are higher than in the Netherlands.

To summarize, we can state that violations of horizontal privacy from a criminal law perspective can be addressed effectively. Although, the question is to what extent the existing protection is actually enforced in practice. This question was not the subject of the current research but its importance is evident when assessing the effectiveness of the protection of horizontal privacy in the context of criminal law.

*Consumer protection law, administrative law and competition law*
Consumer protection law focuses on the protection of consumers, who are often regarded as the weaker party in their relationships with entities in the commercial industry. Citizens are protected in their diagonal relationships against service providers who abuse their power or act in a misleading or deceptive way. Competition law takes the same stance. Through competition law, large (internet) companies such as Facebook, Microsoft, and google can be tackled for abusing their dominant position. It is not without reason that the European Data protection Supervisor, among others, has stressed that that in Big Data processes there will often be a confluence of data protection, consumer protection, and competition law.

For that reason, there have been calls for increased cooperation between the administrative authorities responsible for the supervision of compliance within these fields of law. In the Netherlands, the relevant authorities are the Autoriteit Persoonsgevens (the Data Protection Authority) and the Autoriteit Consument en Markt (the Authority for Consumers & Markets).

The question becomes to what extent is it realistic for these three legal fields to play a major role in horizontal relationships; it is apparent that diagonal relationships (the relationship between citizens and large commercial entities) can be placed within this framework, but this is not the case with the relationship between citizens. Even if supervisory authorities would be able to enforce these requirements in all horizontal relations, it is both impractical and likely undesirable for governmental agencies or public officials to monitor the everyday use of everyday products in horizontal relationships such as smartphones, drones and IoT devices.

*Civil law*
Civil law in both the Netherlands and the countries analyzed for this research provides many opportunities for enforcement action against violations of horizontal privacy. The most important enforcement action can be found in tort law. If the victim of a horizontal privacy violation suffers harm, the defendant has an obligation of compensation. This does not only apply to pecuniary damages, but on the basis of article 6:106 of the Dutch Civil Code and the associated jurisprudence, it also applies to harm to reputation and immaterial damages. However, the mere violation of the right to privacy will not immediately result in a right to compensation; it must either be a gross violation from which it is to be expected that damage will follow, or the plaintiff must be able to substantiate that harm was caused.

Civil law has two limitations with regard to the protection of horizontal privacy. First, civil law is primarily reactive in nature and while it is possible to proactively take action against horizontal privacy violations, such as the prohibition of unlawful press publications, it will often not be known in advance that a citizen will commit a privacy violation. In that event, the enforcement action remains with tort law to retroactively obtain compensation for any harm caused. The second limitation lies in the possibilities for the injured party to actually exercise his or her rights. Proceedings before a court are costly and the outcomes are unclear. Horizontal privacy violations are in many cases committed anonymously or through the use of pseudonyms on the Internet, making independent actions by citizens even more difficult. The problem of difficult or costly litigation is partially addressed by the possibility of collective proceedings, although this option is only available for a limited category of privacy infringements.

Finally, it should be noted that going to civil court (or filing a criminal complaint) is not always a realistic option for injured parties. In sensitive cases, such as the distribution of nude images, the victim may choose not to go to court because of the inevitable confrontation with the culprit and the openness of the court proceedings. In a twist of irony, the procedure could cause a continuation or further aggravate the violation of privacy. Shielded or non-public procedures could address these problems, although at the cost of the openness and transparency of the judicial system.

**The role of producers, distributors, and internet intermediaries**

*Liability of producers and distributors*
In the Netherlands and most countries analyzed during this study, we have not come across any legal provisions prohibiting certain types of products (such as eavesdropping devices, spycams, stalkerware) in advance or the setting out of specific rules for their sale. It is only Germany who has a (limited) ban on the use of equipment that can (also) be used to eavesdrop on individuals. In addition, under the rules on product liability, no action can be taken against producers of hardware and software, even if they are clearly intended to commit violations of horizontal privacy.

*Liability of internet intermediaries*
With regards to the role of internet platforms in combating horizontal privacy violations, the question is to which extent they are liable for the behavior of their users and what their corresponding responsibility is to prevent the commission of these violations. According to the current European regulations (specifically, the e-Commerce Directive), the fundamental principle is that internet platforms are not liable if they are not aware (or should have been aware) that unlawful conduct has taken place and they act promptly to remove the infringing material in question once they do become aware.

For the time being, it appears that parties such as Facebook and Twitter can invoke their exemptions of liability under Article 14 of the e-Commerce Directive with respect to content posted by users. Pursuant to Article 15 of the same Directive, these internet platforms are also not obligated to proactively monitor their platforms for harmful content. However, they may be required by national courts to implement measures to prevent future violations, despite the harm having already been caused. It is questionable whether this sufficiently solves the problem of horizontal privacy violations, because the measures must concern the removal of content that is identical or similar to that which has already been brought before the courts. This means that a court ruling will be necessary for each violation of horizontal privacy.

In order to stimulate internet platforms to increase their enforcement actions, there might be room to consider the introduction of a good Samaritan clause (as proposed in the Communication on combating illegal content online). A potentially harmful side effect of such a clause would be to provide internet platforms with more power and control over the content placed on their platforms. They will enjoy more 'editorial freedom' without any of the corresponding liability. If the route of introducing a good Samaritan clause is pursued, it will be important to delineate the corresponding responsibilities and limits of such a clause.

A more far-reaching step is the introduction of a proactive duty of care. The ECtHR in its *Delfi* ruling did not preclude the taking of proactive measures, although this case was in the context of another type of internet service (a message forum which belonged to a major internet portal providing daily news). The Member States of the European Union are currently working on changing the liability regime for internet intermediaries through the Digital Services Act. It is expected to include a 'duty of care' for internet platforms, although its precise meaning and what it will entail are not yet clear.

The introduction of a possible duty of care to help address violations of horizontal privacy highlights another challenge. In contrast to works protected by copyright, it is often difficult to determine when a privacy violation has taken place. Expressions and their effect on the privacy of a data subject are strongly context specific. This complicates the ability of intermediaries to assess whether an expression is unlawful, especially when they are made on a large scale and therefore its detection is likely to be automated. This may result in internet platforms preferring to choose broad parameters to avoid liability, which will consequently have a negative impact on the freedom of expression.

Germany appears to take a much stricter approach to dealing with illegal online content; through the *Netzwerkdurchsetzungsgesetz* (the Network Enforcement Act). Sweden, through its interpretation of the old BBS legislation, also has legal possibilities to hold internet platforms liable for criminal violations of horizontal privacy. It can be said that the legal 'stick' through which rapid and effective action can be taken against violations committed on internet platforms is more readily present in Sweden and Germany, as opposed to the Netherlands. However, it remains dependent on whether it concerns a violation of horizontal privacy that is criminalized.

In addition to measures taken by internet platforms themselves (such as the removal, blocking, or filtering of content), users can also take action against violations of their privacy. Individuals can, on one hand, exercise their rights under the GDPR (in particular, the right to erasure as set out in Article 17 of the GDPR) and, on the other hand, leverage the possibilities offered by the Civil Code (e.g. through an action in tort law).

The problem with exercising these rights is that the injured party must focus primarily on the internet platforms instead of the user who committed the violating act. Particularly when it comes to obtaining compensation, this raises the threshold that injured parties need to meet in order bring an action because they will first be required to go through proceedings against the platform (e.g. to obtain user data) before they can start proceedings against the user who committed the violating act.

**Other mechanisms**

In addition to laws and regulations, there are other available mechanisms aimed at regulating privacy in horizontal relationships. These mechanisms concern self-regulation, awareness and education.

*Self-regulation*

While we (as researchers) have less insight into initiatives in smaller social contexts, self-regulation seems to be particularly focused around online services. Self-regulatory initiatives by producers and distributors of hardware and software that is specifically suited to infringe privacy have not been found.

Self-regulatory initiatives to protect privacy in horizontal relationships are of particular relevance in the context of online services. These are internet platforms and other service providers that work independently or in a public-private context to regulate online content. Public-private initiatives to regulate online content are focused on child abuse images, racist or xenophobic content (hate speech), and terrorist content (glorification or incitement of terrorism). Other violations of horizontal privacy (such as the communication

of insults or revenge pornography) are mainly regulated by internet service providers through community standards and abuse policies.

Although self-regulation through Terms of Use can be a powerful tool to counter horizontal privacy violations, there are also concerns about potential and undesirable side-effects. For example, the UN Special Rapporteur on Freedom of Expression warned that internet platforms can regulate themselves too independently on the basis of their community standards.

*Awareness and Education*
In the field awareness and education, there is a fairly uniform picture when looking at the different European countries analyzed for this study. This can be partly attributed to the fact that a lot of awareness raising iniatives, especially information directed at children, is coordinated at a European level. This enables countries to adopt successful campaigns from each other and exchange lessons learned.

**Overview of standardization and legal protection of horizontal privacy**
On the basis of our research, we set out the following overview of violations and the associated standards and legal protection:

| **Standardization and the legal protection of privacy in horizontal relationships** | | | | | | |
|---|---|---|---|---|---|---|
| **Type of violation** | **Examples** | **Standards and protection** | | | | |
| | | Laws and regulations | | | | Other mechanisms(self-regulation) |
| | | Criminal law | Data protection law | Administrative law, Competition law, and Consumer protection law | Civil law | |
| Observation, collection, and registration | Voyeurism, (covert) video surveillance, eavesdropping,use of spyware and stalkerware, fencing information, filming of victims | Computer hacking (138ab Sr), overname gegevens (138c Sr), eavesdropping (139c Sr), covertly recording conversations (139a, b Sr), covert camera surveillance (139f Sr), data fencing (139e, g Sr), harassment (285 Sr) | Illegitimate processing, right to erasure (Article 17 GDPR) | Administrative law (APV), consumer protection, product safety, unfair trade practices | Tortious act, violation of portrait rights | *Naming and shaming* |

| | | | | | | |
|---|---|---|---|---|---|---|
| Analysis and decision-making | Profiling and automated decision-making | | Illegitimate processing, right to erasure (Article 17 GDPR), ban on automated decision-making (Article 22 GDPR) | Consumer protection | Tortious act | |
| Creation and sharing | Insults, *deepfakes*, false advertising. attribution of expression to an individual, identity theft, revenge pornography | Defamation, incitment and hate speech (137c en d Sr), insult (266 Sr), libel (261 Sr), slander (262 Sr), revenge porn (139h Sr), | Illegitimate processing, right to rectification (Article 16 GDPR), right to erasure (Article 17 GDPR) | - | Tortious act, rectification right, portrait rights. | Violating Terms of Use of platforms, *naming and shaming* |
| Interaction and communication | Stalking, threats, *sextortion*, cyber-bullying. (further: insults, libel, slander) | 285 Sr, threats (317 Sr), revenge porn (139h Sr), fraud (225 Sr, 326 Sr) | Illegitimate processing, right to rectification (Article 16 GDPR), right to erasure (Article 17 GDPR) | - | Tortious act, | Violating Terms of Use of platforms, *naming and shaming* |

**Integrating foreign legal concepts into the legal order of the Netherlands**

Our research has shown that the regulation of horizontal privacy in the legal system of the countries analyzed is more or less the same. The ability to adopt 'lessons learned' in this case is limited. Legal concepts that might contribute to better protection of horizontal privacy lie primarily in criminal law and the rules addressing the liability of internet platforms.

A first criminal provision that can be considered is the broader criminalization for the publication and distribution of offensive or obscene content, following the example of Poland and the United Kingdom. The main advantage of this possibility is the increased degree of flexibility for government to act autonomously in the enforcement of standards. Although, it brings with it a major risk in that its introduction will create legal uncertainty. In the absence of a clear definition and delineation of material considered to be obscene, offensive, hurtful or otherwise harmful, there will always be a risk of censorship or arbitrary enforcement.

A second criminal provision that may qualify for integration into Dutch criminal law is the filming of individuals in need of assistance. Introducing a ban on the filming of individuals requiring assistance will have a potential effect on the freedom of expression. If the provision is sufficiently qualified and provides exemptions in the context of, for example, the press, it is likely that an appropriate balance can be struck between the right to privacy and the right to freedom of expression. Another consequence that should be taken into account is that images of bystanders can contribute to clarifying the alleged crime or to better understand the circumstances surrounding an accident. In the context of potentially broadening criminalization, these are important considerations to take into account.

If the legislator chooses to impose stricter requirements on internet platforms, the German Network Enforcement Act can serve as an example. Although the consequences of the law (both positive and negative) have not yet been clearly established, it can be expected that such provisions affect the freedom of expression. Additionally, measures aimed at internet platforms can also affect the freedom of enterprise and potentially influence the economic climate and innovation in the Netherlands.

**Legal concepts not borrowed from abroad**

While certain legal concepts can be borrowed from abroad, there are number of proposals that have emerged from our own analysis of Dutch and foreign legal protection.

A first option is the exploration of stricter requirements for the sale of products and services that are primarily made to infringe the private life of individuals. Prime examples include spycams, monitoring beacons, and stalkerware. Restrictions could be placed on the sale of such products to private individuals, additional notification requirements could be introduced, or a licensing system for sellers and/or users. These measures stop short of a complete ban.

Second, the extent to which technical requirements could be imposed to make certain recordings impossible (or, in any case, substantially more difficult) could also be a topic worthy of exploration. This could for instance include geo-fencing with regard to 'no-fly zones' for drones, or the automatic blurring of faces when using cameras in specific areas. There could also be a further investigation into the extent to which technical requirements can be imposed on products in order to reduce their stealthy nature. An example is the mandatory issuing of a sound or light signal when a products start recording. By referring to Article 25 of the GDPR, there is already a (potential) legal basis for the enforcement of such measures.

**Future regulation of horizontal privacy violations**

When it comes to legal measures aimed at providing better protection for horizontal privacy, there are roughly two options to choose from: (1) take measures aimed reducing the opportunities to violate privacy (*ex ante*, preventative measures), and (2) take measures aimed at more effectively ending privacy violations and compensating victims (*ex post*, reactive measures).

The first option and category of measures may include banning certain products or services or making the sale or purchase of such products subject to licensing requirements as described above. A drawback of this approach is that most products (e.g. smartphones or drones) can be used for both legitimate and illegal purposes. This makes it problematic to prohibit certain products or services in advance or to further regulate their sale and use.

The option of *ex post* regulation brings with it the advantage that the lawful application and use of technology are not prohibited beforehand. However, the associated disadvantage is that the applications are so diverse that it is virtually impossible to test the legitimacy all potential uses of technology in horizontal relationships (either by citizens themselves, or by civil rights organizations or governmental bodies). Furthermore, the harm has already been caused by the time legal action can be taken. At best, the citizen can recover damages, although it will often prove difficult, because: (i) the culprit cannot always be

identified due to obstacles in obtaining evidence, (ii) the harm and corresponding damages are not quantifiable or easy to interpret, and/or (iii) the individual simply does not wish to draw even more attention to what has been exposed with the invasion of his or her privacy.

A compromise would be to not focus on the commission of the privacy violation but rather on the further dissemination of unlawfully obtained information about other citizens. internet services and platforms in particular have an important role to play in this respect. The question becomes to what extent these platforms (should) play a proactive role to prevent violations of horizontal privacy. While a general duty of care already exists, it remains in many regards unclear how far it applies in the digital context.

**Legal protection in practice**

Although the horizontal application of fundamental rights is recognized, the notion that the parties involved are more or less equivalent and therefore should be able to sort any issues amongst themselves remains. Although testing the effectiveness of privacy protection measures was not the assignment for this study, the result is that we can question the level of actual legal protection provided to citizens. On one hand, it is difficult for citizens to take action against violations of their right to privacy, while on the other hand, the capacity of the government (such as the police, judiciary, and regulators) to enforce the current standards is limited. Possible reinforcement of the right to privacy in legislation and further regulations can therefore never be considered in isolation from the actual challenges faced by citizens or the capacity of the government in its enforcement.

It is also important to focus on the development of societal norms in the digital context. In contrast to the physical world, the norms in the digital world have not yet been fully developed. The relative absence of authoritative institutions also play a role in the emergence and persistence of privacy violations. Awareness and self-regulation can help to form and maintain norms and values in places where governmental presence is less pronounced.

More generally, it can be stated that it is precisely in the digital environment that the legislator must invest in mechanisms to, at an early stage, identify technological developments, new applications, and their consequences. If legislation is delayed for years, by the time a new law or provision enters into force, the technology that was supposed to be addressed is already out of fashion or has become so widespread and widely used that it becomes impossible to set any substantial or meaningful limits to it. In view of the great importance of digitization of the Netherlands, continued discussion on technological developments and their impact on society, for instance through a Parliamentary Committee on the Digital Future, is advised.