Editorial

The danger that with developments in mass surveillance, biometric passports and ever-expanding registration systems, a Big Brother society may emerge is widely recognised. Equal attention is paid to privacy risks posed by data companies such as Google, Facebook and Microsoft: technology giants that have more data, power and resources than most governmental organisations do. That is why regulators and civil society organisations have called for action not only to preserve so called vertical privacy, ie privacy protection in citizen-state relationships, but also to preserve so called diagonal privacy, ie privacy protection in relationships between citizens and large multinationals.

Although the dangers of privacy violations committed by citizens have never been off the radar fully, horizontal privacy has recently gained new momentum. That should not come as a surprise. Although there have been discussions over the right to be let alone in horizontal relationships since the advent of photography, and certainly since the 1960s, when small spy products such as directional microphones, zoom lenses and various types of cameras appeared on the consumer market, a number of important developments are unfolding.

On the one hand, the tools that enable citizens to easily collect and disseminate data about each other, such as products designed specifically for these purposes (so called spy or espionage products) and products that offer far-reaching possibilities to do so (smartphones, drones, smart doorbells, etc.), are becoming increasingly available and accessible to ordinary citizens. Whereas in the past, such products were mainly for sale in specialised shops, nowadays such equipment can easily be obtained via Amazon, specialised websites for spy products and a myriad of Chinese online sellers. On the other hand, costs have continued to dwindle, so that economic barriers to the purchase and use these products have been removed almost completely. Both developments have resulted in a democratisation of these products.

In addition to a strong quantitative increase in the possession and use of such products by citizens, qualitative changes are evident. Firstly, products such as cameras and microphones are becoming smaller and smaller, sometimes only being a few millimetres in size. Consequently, recording devices can be and are hidden in or built into everyday objects, such as a bottle of shampoo or a teddy bear. This makes it increasingly easy to monitor others in intimate spaces and atmospheres, such as a locker room or sauna. Secondly, recording technologies are becoming increasingly precise, which not only improves the quality and resolution of the recorded image and sound; it also makes it possible to spy on others from ever greater distance. Sound recording devices are able to pick up conversations through walls just as HD quality infrared cameras can be used to recognise people through walls. Thirdly, recording products can in-

DOI: 10.21552/edpl/2020/3/3

creasingly squeeze past physical barriers; for example, a mini-drone can simply fly over the garden fence and float through a person's open bedroom or bathroom window to take shots.

These developments in terms of cost, availability, recording quality and size are expected to continue in the near future.

In addition, the information infrastructure within which the collected information can be disseminated has also changed radically in recent decades. The devices themselves can take longer and longer recordings without having to be recharged and the products make it possible to read the recordings from a distance. Such recordings can be easily distributed via and published on the Internet, with some products allowing for live streaming. There are hardly any technological or economic barriers to publishing images or sound recordings via YouTube, Instagram, Facebook or other forums. In addition, apart from the deliberate recording and publication of the recordings by citizens, technological products are often poorly secured, so that all too often security cameras or IoT-devices, without the knowledge of the citizen who has installed them, for example in or on his home, broadcast live data-streams on the Internet.

Not only is hardware such as GPS trackers that can be attached to objects or persons, smoke detectors with cameras, pens with sound recording functionalities, widely available, but spy software is also being advertised. This includes tools to monitor children, spouses and employees, which offer the possibility to view all incoming and outgoing text messages from the phone the software is installed on, tracking which websites have been visited, what has been viewed on the site and at what time, viewing the live location of the phone, getting an overview of all incoming and outgoing calls with number display and a time and date, seeing who has been added to the contact list, view the name, phone number and the time when a person was added to the contact list, the possibility to record the room where the phone is located, reading all WhatsApp messages with date, time and the name of the third party, recording phone calls, seeing photos and videos being made and getting a copy of every e-mail sent.

The available information infrastructure has created a culture in which self-recording and sharing such recordings with friends or the whole world has become the standard. Instagram, Tiktok, Facebook and the various sites of vloggers revolve around making recordings about their private lives, often with the presumption that this form of information sharing will lead to more friends, acclaim or success. Often the more intimate the information is, the more followers, views or likes are acquired. Through quantified-self techniques, people are also able to record and share more and more data about themselves in online communities. This means that an ever-increasing amount of data and intimate information is being shared by people themselves, making it increasingly easy for other citizens to abuse those data and increasingly unclear to third parties whether intimate information or recordings on the Internet have been made and disseminated by a person herself or by others. The development of an online information culture has also led to a blurring of previously established ethical and moral

boundaries. Finally, the anonymity offered by the Internet and the distance between the person disseminating information and the person to whom it relates lower the threshold for violating each other's privacy.

It is clear that these developments pose a number of privacy risks. Locational privacy can be undermined both by espionage products that secretly record images or sound from inside and from outside the home, by IoT-devices, such as smart meters, smart fridges, and smart sex toys, that can be hacked and by the fact that when citizens go to other peoples' private homes – eg of friends or an apartment rented via Airbnb – they may be filmed there, through a camera built into the clock, smoke detector or bathroom mirror. Obviously, such recordings, or recordings made in saunas and locker rooms or, for example, by drones flying over nude beaches, may infringe upon people's bodily privacy.

The recording of images and sounds in private, public and semi-public space, combined with the loss of control by citizens and the impossibility of knowing for sure whether and when such recordings are made can also lead to a change in behaviour. People who are spied upon in their private environment start to behave differently, hesitate to invite friends back home and dress more chaste or take precautionary measures. Recording data can also lead to aggression. For example, there have been a number of incidents involving people who destroy neighbours' drones flying over. Importantly, behavioural changes do not only result from actual recordings, but may also occur when a recording device is not on or does not allow for personal identification, but citizens belief otherwise or are unsure.

An important privacy problem with covert filming is that information about a person is collected against her will and without her knowledge. This is particularly problematic when it comes to secrets or private matters, which can lead to reputational damage. However, data need not be used or misused to pose privacy risks. The mere fact that the teenage neighbour playing around with his drone has seen his neighbour sunbathing topless can be a privacy problem, even if he immediately destroys the images. Gathering information about others shifts power relations, because one citizen knows more about the other than the other about the first. There is also the problem that the anonymity and distance of communication on the Internet removes a number of important barriers. For example, most people are reluctant to make horrific accusations directly to someone's face, while this is much more common on the Internet. It is also known that in the case of bullying, the reaction of the person being bullied often has a moderating influence on the bully(s), while this reaction is often invisible with cyberbullying.

Finally, it is important that even if a single recording reveals little (intimate) information about a person, tens or hundreds of different innocent sources of information taken together can give a very concise picture of a person's (private) life. The same applies to the nuisance and fear that people experience. The knowledge that there is a small chance that someone has purchased an expensive and highly specialised prod-

uct to follow you, as was the case until a few years ago, is fundamentally different than the knowledge that you could be constantly watched by almost all fellow citizens. Seeing a drone fly over your backyard once a year is surmountable; if, however, that happens several times a week, a permanent sense of discomfort can slip into a person's life.

When discussing new forms of regulation to tackle these issues, two complex points need to be addressed: the choice between ex ante and ex post regulation and the question of who should be the primary norm addressee. With respect to both points, no easy answers are available.

As to the first point, it is clear that the problem with the regulatory regime vis-à-vis horizontal privacy violations is not the regulation as such; almost all privacy problems in horizontal relations are in fact regulated, through the GDPR, criminal law or general tort law. The problem is not the absence of material legal provisions, but the lack of enforcement of those rules. It is evident that one of the primary causes of this enforcement gap in horizontal relations is the fact that by far most existing rules can be categorised as ex post forms of regulation. Arguing in favour of more ex ante regulation is, inter alia, the fact that although citizens are generally aware of privacy rules - certainly the more extreme violations prohibited through criminal law are intuitive enough to be deemed general knowledge - not every citizen is aware that, when publishing a selfie on a website on which others can be seen in the background, she is legally obliged to inform those others; not every citizen understands that when placing a security camera above her front door which also films the sidewalk, the GDPR applies; not every hobby drone pilot will be aware that sharing landscape images on which people can be seen may qualify as libellous behaviour. An additional reason to invest in ex ante regulation is that many recordings are made without the intention of collecting data about others. More generally, ex post regulation entails that the collection, processing and publication of information can only be assessed legally after these actions have materialised. The problem in relation to privacy in horizontal relations is, obviously, that more and more everyday products enable citizens to collect and disseminate data about others and that almost all citizens have these products and use them on a daily basis. Estimates have it that about 75% of the population use, on a daily basis, products that are or could be used to collect data about others, such as a smartphone, (security) camera, drone or specialised spy product. It is practically impossible to ascertain what recordings they have made each and every day and whether these are lawful. That implies a number of things. Firstly, that the attention and energy, if any, with respect to enforcing privacy norms in horizontal relations goes almost exclusively to the handful of more extreme violations (often related to bodily privacy), while the vast majority of the not acutely problematic recordings remains unaddressed. This also means that in time, these minor privacy violations will be normalised. Secondly, privacy violations are addressed after they have materialised. Not only has the damage already been done, starting a legal battle may actually result in more attention being paid to the violation and the private information disclosed, for example because a sensational case may attract the attention of the media.

Ex ante regulation would solve some of these problems and reduce significantly the number of horizontal privacy violations. However, what makes this type of regulation difficult, is that almost any product or service can also be used for legitimate purposes. This certainly applies to everyday products, such as a smartphone, drone or security camera, but even a mini camera that can be hidden in the cap of a bottle of shampoo can be used legitimately, for example by someone who wants to film herself in the shower and send that clip to a loved one. Recording equipment hidden in a clock can be used to catch the medical personnel that is stealing from grandma's purse. Microphones built into pens can be used by undercover journalists. Ex ante bans on products make these legitimate applications impossible; ex ante verification of the legitimacy of the concrete use of these products or the actual recordings being made is both virtually impossible given the amount of recordings and will also involve margins of error. As a consequence, considerable numbers of recordings will not be published while not being unlawful (eg Facebook blocking old paintings with nudes). Ex ante evaluations over legitimacy obviously also raise the question: which party assesses whether a product or application is legitimate and on the basis of which legal or moral standard? What complicates ex ante evaluations of the use of products is that although products and services are regularly used without the consent of the person concerned, there may be a privacy infringement even with initial consent. Consent is often given for an explicit or non-explicit purpose, while images are often used for other purposes. It is not easy for a third party (the Data Protection Authority, an internet intermediary, etc.) to determine whether images have been created with consent and, if so, for which purposes consent has been obtained. Finally, although ex ante regulation is easier to enforce, it still offers no guarantees; a ban on the sale of espionage products in the EU, for example, still does not preclude people from buying all kinds of products via Chinese online sellers.

Secondly, three parties could play a role in monitoring and enforcing privacy standards in horizontal relationships - citizens themselves, the state and the intermediaries - but there are obstacles to each of them doing so effectively.

While every citizen has a wide range of procedural and complaint rights, it is by no means always clear to citizens that their data have been collected; rather, most citizens are oblivious to the fact that they figure in the background of a selfie, that they are captured by a security camera hidden in a tree or that they have been spied upon with the use of specialised technologies. Even if they do, it is not always clear who can be held responsible. Whose drone just flew over the garden? Who exactly placed the anonymous comment on a discussion platform? Even when a video showing two exlovers having sex has ended up on a porn website against one person's knowledge, it is not necessarily the other person who is the perpetrator. For example, the devices of either of them may have been hacked. In order to find out the identity of the citizen that has recorded and/or published personal data about others, the cooperation of internet intermediaries is often necessary, but they are not always eager to cooperate (without court order) because of the privacy interests of the third party. This often means that two lawsuits are necessary, one to find out the identity of the perpetrator and an-

other to take the perpetrator to court (and sometimes a third or a fourth to remove copies of that content from other internet sites). This requires time, money and energy that citizens often lack, while the parties that provide facilities for making, processing and distributing recordings, such as Google, Facebook and Apple, have very deep pockets. The cost of lawsuits means that, in any case, the more common violations of privacy will generally not be addressed. For example, it is highly questionable whether the mere fact that a drone has made recordings of the neighbours in their backyard, while those recordings have been erased immediately, will be seen as a violation of privacy, because the damage is so limited. Even if the damage can be demonstrated and a privacy violation is found, the problem is that compensation will usually be low, making it hardly worth the effort for ordinary citizens' to engage in these legal procedures.

As far as intermediaries are concerned, some have already introduced forms of ex ante verification, but this is both very time-consuming and costly. What is more, these systems force them to become both judge and executioner. The problem with conflicts in horizontal relationships is that it is seldom evident whether a breach of privacy has taken place. An internet intermediary can usually not tell from a recording whether or not it is unlawful. An amateur clip with two lovers having sex may have been taken and distributed with mutual consent; an online blog with a photo of slightly inebriated people does not have to be a problem for those people; publishing recordings of a private conversation with third parties may serve a legitimate purpose. Usually, only the citizen who is affected knows whether a recording or publication is unlawful. In addition, there are many difficult legal questions. Is it possible to identify a person through the recordings of a drone, so that the GDPR applies? Does it serve a legitimate interest for a person to use a security camera to record people entering her yard? To what extent is the covert recording by a journalist legitimate in relation to the freedom of expression? Is insulting someone or revealing certain private information about others permitted? Different interests are often at stake for different citizens, so that the choice to comply with one person's request is almost always a choice to limit the rights or interests of the other. (Obviously, it should not be ignored that most companies make profit when distributing controversial or sensitive information, giving them an incentive to tolerate rather than to restrict such recordings). Finally, intermediaries are often located in foreign jurisdictions and are bound to dozens and sometimes hundreds of legal regimes. It is virtually impossible for them to implement and enforce every normative regime, not in the last place, because those regimes may conflict, for example when a US citizen exercises her freedom of expression and an EU citizen exercises her right to data protection.

Finally, for public authorities, such as the Public Prosecutor's Office and the Data Protection Authority, many of the aforementioned problems apply equally. The time, effort and resources that it takes to assess the legitimacy of recordings, the ambiguity about whether or not consent is given for recordings and publications and the various complex legal questions that arise, the question of whether it pays off to go after relatively minor breaches of privacy in horizontal relationships and the problem that a

choice to protect the right of one citizen may have consequences for the interests others. Another question is whether strict monitoring of all kinds of minor breaches of privacy is actually helpful. At one point, the cure may become worse than the disease. For example, giving government services more power and resources to monitor everyday use of technology and applications can lead to a Big Brother society in which the government closely monitors citizens' everyday activities.

A hopeless situation? Luckily, the two forewords in this edition offer fresh ways to look at privacy, namely through the lens of the old. Sarah E. Igo, author of *The Known Citizen: A History of Privacy in Modern America*, suggests that there are four ways that a historical sensibility can and should be brought to bear on our discussions about the contemporary state of data privacy. She suggests that knowledge of history not only offers us precedents and analogies, but that a historical perspective also helps us recognize the broader forces undergirding seemingly separate developments, it destabilizes our working concepts in productive ways and reacquaints us with important debates and ideas that have been lost. Almost all contemporary privacy dilemma's, she suggests, are not new entirely but have their roots in the shadows of our past. Angela Vanhaelen, author of a number of books including *Making Space Public in Early Modern Europe: Performance, Geography, Privacy,* turns our gaze towards a painting of Vermeer. She suggests that Vermeer's painstaking attentiveness draws awareness to the invisible mysteries of bodily privacy, to inner feelings and intimate secrets. As viewers, we are positioned as voyeurs who spy on a personal moment that we cannot quite decipher. Might this be one of the first artful reflections of the separation between public life and the private and mysterious life that can never be brought to light in full?

This issue also contains five academic articles. Leanne Cochrane, Lina Jasmontaite-Zaniewicz and David Barnard-Wills explore the data protection authorities' role as leaders and educators, particularly in relation to awareness-raising efforts with Small and Medium-sized Enterprises. They make several suggestions for improving their current role and approach. Peter Alexander Earls Davis analyses the applicability of the GDPR to smart billboards. He suggests a novel interpretation of the term 'identified', so as to ensure that smart billboards do in fact fall under the GDPR. Tiago Sergio Cabral has studied the impact of the right to erasure under the GDPR in the development of artificial intelligence in the European Union. Anna Rita Popoli examines the various forms of liabilities that accredited certification bodies may incur in operating in the field of data protection, while also trying to offer some suggestions to improve the harmonisation in the pathological phase of litigation in certification mechanisms. Finally, Joanna Strycharz, Jef Ausloos and Natali Helberger discuss the results of a large survey on individual knowledge of, reactions to, and rights exercised under the GDPR in the Netherlands. The results show high awareness of the GDPR and knowledge of individual rights, while at the same time, there is doubt about the effectiveness of their individual rights.

Then, as always, special mention should be made of EDPL's reports section, reflecting on some of the most important developments in the EU. This edition has a report on

Croatia, Italy and two on the United Kingdom. Alina Škiljić discusses the Croatian application for contact tracing, Angela Busacca reflects on Covid-19 emergency response and the effects on the Italian workplace, David Erdos evaluates the issue of legal accountability of the UK Data Protection Authority and finally Lorna Woods analyses recent developments concerning facial recognition in the UK. In our long standing GDPR implementation series, Martin Zahariev and Radoslava Makshutova cover Bulgaria and finally, in the practitioners' corner, Alvaro Moreton and Ariadna Jaramillo evaluate how private information recorded by voice-enabled systems can be identified.

In the book review section, led by Gloria Gonzalez Fuster, our own editor Axel Freiherr von dem Bussche has taken up Jef Ausloos' The Right to Erasure in EU Data Protection Law and Chiara Angiolini discusses Marcin Betkier's new book Privacy online, Law and the Effective Regulation of Online Services.

For those interested in submitting an article, report, case note or book review, please e-mail our executive editor Jakob McKernan (<mckernan@lexxion.eu>) and keep in mind the following deadlines:

- Issue 4/2020: 1 October 2020;
- Issue 1/2021: 15 January 2021;
- Issue 2/2021: 15 April 2021;
- Issue 3/2021: 15 July 2021.

I hope you enjoy reading this edition of the European Data Protection Law Review!

Bart van der Sloot
Tilburg Institute for Law, Technology, and Society (TILT)
Tilburg University, Netherlands