International Review of Law, Computers & Technology

ISSN: 1360-0869 (Print) 1364-6885 (Online) Journal homepage: https://www.tandfonline.com/loi/cirl20

Capturing licence plates: police-citizen interaction apps from an EU data protection perspective

Jonida Milaj & Gerard Jan Ritsema van Eck

To cite this article: Jonida Milaj & Gerard Jan Ritsema van Eck (2020) Capturing licence plates: police-citizen interaction apps from an EU data protection perspective, International Review of Law, Computers & Technology, 34:1, 1-21, DOI: 10.1080/13600869.2019.1600335

To link to this article: https://doi.org/10.1080/13600869.2019.1600335

Published online: 15 Apr 2019.

INTERNATIONAL REVIEW OF LAW, COMPUTERS & TECHNOLOGY
2020, VOL. 34, NO. 1, 1–21
https://doi.org/10.1080/13600869.2019.1600335

Capturing licence plates: police-citizen interaction apps from an EU data protection perspective

Jonida Milaj and Gerard Jan Ritsema van Eck

Security, Technology, and e-Privacy (SteP) Research Group, University of Groningen, Groningen, Netherlands

ABSTRACT

A Pokémon Go-like smartphone app called 'Automon' was unveiled in October 2017 as one of several new initiatives to increase the public's contribution and engagement in police investigations in the Netherlands. Automon is designed in the form of a game that instigates participants to photograph license plates to find out if a vehicle is stolen. The participants in the game score points for each license plate photographed, and may also qualify for a financial reward if a vehicle is actually stolen. In addition, when someone reports that a vehicle has been recently stolen, game participants that are in the vicinity receive a push notification and are tasked with searching for that particular vehicle and license plate. This paper studies the example of the Automon app and contributes to the existing debate on crowdsourced surveillance and the involvement of individuals in law enforcement activities from an EU law perspective. It analyses the lawfulness of initiatives that proactively require individuals to be involved in law enforcement activities and confronts them for the first time with European Union (EU) data protection standards. It is concluded that the Automon app design does not meet the new legal standards.

ARTICLE HISTORY
Received 19 November 2018
Accepted 25 March 2019

KEYWORDS
Police Directive; participatory surveillance; ANPR

Introduction

> So can we make an app, Automon, and make it a game to find stolen cars back who are somewhere in Holland? (Bart Driessen, Dutch national police force)

In October 2017 the Dutch police chief Erik Akerboom revealed several new initiatives to increase the public's contribution and engagement in investigation activities (van den Heuvel and van Wely 2017; Vries 2017). One of these initiatives is the development of a Pokémon Go-like[1] smartphone app called 'Automon' (Figure 1).[2] Automon is designed in the form of a game that instigates participants to photograph license plates to find out if a vehicle is stolen. The participants in the game score points for each license plate photographed, and in case the car is indeed stolen they might also qualify for a financial reward. In addition, when someone reports that a car has recently been stolen,

CONTACT Jonida Milaj j.milaj-weishaar@step-rug.nl Security, Technology, and e-Privacy (SteP) Research Group, University of Groningen, Oude Kijk in 't Jatstraat 26, Groningen 9712 EK, Netherlands

game participants from the neighbourhood receive a push notification and are tasked to search for that specific license plate. The more stolen cars you find, the higher your score, and the more money you can collect.

The launch of Automon is indicative of broad trends within policing and society. Participation can be said to be a general characteristic of surveillance (Albrechtslund and Lauritsen 2013, 314) and the involvement of individuals in police activities is not a new phenomenon. Distributing labour between law enforcement and individuals is considered fruitful as it relies on a multitude of watchers and has the advantage of achieving a particular goal that could otherwise be difficult to achieve because of the limited resources available to law enforcement. The Automon app is also a form of crowdsourcing, though it is particularly interesting as it differs from usual crowdsourcing practices. Normally in crowdsourced policing individuals are asked *ex post* to contribute valuable evidence they might have captured with their devices while being part of an event at the right time and place. The Automon app, on the other side, proactively asks individuals to collect evidence, and thus to turn into surveillants. By gathering evidence, individuals collect, retain and share with law enforcement personal data of others. The simple participation in a game with the scope to assist law enforcement in their activities could turn individuals into data controllers or processors and impose upon them the rights and obligations prescribed by the applicable laws and regulations.

This paper contributes to the existing debate on the involvement of individuals in law enforcement activities by analysing it from an EU law perspective. Taking the example of the Automon app as a case study, it will analyse for the first time the lawfulness of initiatives that proactively require the involvement of individuals in investigation activities and will confront them with the data protection standards of the European Union (EU).[3] This legal analysis is augmented by the presence of discussions based on surveillance studies and science and technology studies. The presence of these other fields of study helps to better understand the individuals' involvement in surveillance activities.

After this short introduction, section two provides background information on the role of technologies in the involvement of citizens in police activities, crowdsourced surveillance and digilantism.[4] Section three analyses the Automon app in light of the current legal framework at EU level, including insights from the case law of the European Court of Human Rights (ECtHR). Before turning to the conclusion (section five), in section four the legal implications of the findings of the previous sections are discussed.

The Automon app: surveillance, game, or both?

> Lots of people, elderly, but also youngsters were running on the street looking after Pokémons. So we said: Hey, if they are looking after Pokémons, can they go after stolen cars? (Bart Driessen, Dutch national police force)

This section introduces the Automon app under scrutiny in this paper. Throughout the section other apps, technological solutions, and academic literature from various disciplines will be used to sketch the background against which the Automon app can be understood. This underscores the wider relevance of the analysis, and the importance of understanding the legal ramifications of the app: Many similar apps, often for slightly different purposes or target audiences, have already been developed and many more can be expected.

Figure 1. A screenshot of the map view in the Pokémon Go game published by Niantic, Inc. Screenshot taken by the authors on an Android device on 1 May 2018.

Note that the description of the Automon app in this paper is primarily based on a telephone interview conducted in June 2018 with Police Commissioner Bart Driessen, who is responsible for the development of the Automon app within the Dutch national police force. This interview was followed up with several questions over email, stretching into January 2019. At that point a beta version of the app had been finished and a decision

was being awaited on small-scale field testing in a regional police unit. It is possible that as a result of these tests the app will undergo significant changes before being released publicly. The authors have not been able to test the app themselves. Throughout the article it is indicated where information from the interview and email correspondence has been used.

First, the background of the Automon app is discussed: what problems does it, and others like it, hope to solve? In the next subsection, the importance of the selection of users and how they are instructed is considered. In the final subsection, attention is paid to how they are enticed to keep using the app.

Background

A typical Automon app usage scenario could begin with the user spotting a suspicious vehicle.[5] The user opens the Automon app and takes a picture of the car, after which Automatic Number Plate Recognition (ANPR) software embedded in the app picks out the number plate and reads it. The number plate and some information on e.g. the app user and the location where the photo is taken are then sent to the police server where the number plate is compared with the publicly accessible database of the *Rijksdienst voor het Wegverkeer* (*RDW*, state service for road traffic) to check whether the vehicle is stolen. If this results in a 'hit' either a police patrol car is deployed immediately or a towing company is contacted to secure the vehicle. The user is rewarded for his efforts with some points that can be used for an in-app car-related collection game, whether the vehicle was stolen or not. Finally, she/he might be able to claim a monetary reward from insurance companies if the car indeed was stolen.

Although these core mechanics are very simple, serious investments in time and money are needed from the Dutch National Police Force to make this app a reality. As such, a close look at the app can tell us much about what is considered important at this particular moment by the Dutch Police (Lupton 2014). As Bart Driessen of the Dutch Police noted in the telephone interview, these investments are made because a key goal for the Dutch police is getting ordinary citizens involved in tackling crime. The police depends on information from the public for most of its work, and the public is mostly very willing to provide it. He estimated that about eighty to ninety percent of all suspects in the Netherlands are caught red-handed after a call from a concerned citizen. However, when it comes to vehicle theft, the public doesn't have the tools to recognise stolen cars: 'If you don't tell the public what is stolen, they can't look for it, and they cannot call us when they see somebody with stolen property.'

An interesting early example of a similar tactic was the call from the police to submit images, and tag people in submitted images, during riots in Vancouver that broke out in 2011 after the Vancouver Canucks lost the Stanley Cup finals to the Boston Bruins. During and immediately after the riots, many people used their smartphones to make pictures of the participants and to document the turmoil, which were then shared on social media, such as a Facebook page dedicated to the riots (Schneider and Trottier 2012). This gave the police the possibility to identify many rioters with pictures and names on the bases of comments of other social media users even as the riots continued. Although this shows the willingness of the public to share information with the police, it also points to some limitations that the Automon app tries to take away. The ad-hoc nature

of the appeal – perhaps suitable for extraordinary events like a mass riot, but wholly inadequate for more ordinary and continuous problems such as car theft – is replaced by a more permanent call for action, and the reliance upon platforms that are owned and operated by outside companies is reduced.

On the one hand, then, Automon is a tool given to interested citizens in order to help them support the police. On the other hand, it is also a tool to channel that support, as police forces and individual police officers within them often hold varying views on the reliability of citizens, citing fears of vigilantism and other forms of 'cowboy-ish' behaviours when citizens are actively involved in neighbourhood watch groups (Pridmore et al. 2018, 14). Therefore, the police prefers to be involved in such bottom up initiatives, often joining the WhatsApp conversation of a neighbourhood watch group, or keeping in close contact with moderators and other group leaders (Pridmore et al. 2018, 12–16; Spiller and L'Hoiry 2018).

An interesting counter-example to the Vancouver riots which illustrates these fears is formed by the Boston bombings in April 2013. Shortly after two bombs exploded at the finish line of the Boston marathon and killed three people, a collective effort was started on online forums, most notably Reddit.com, to support law enforcement authorities by identifying the bombers (Cassa et al. 2013; Lee 2013; Davis, Alves, and Sklansky 2014; Starbird et al. 2014). However, several people were wrongly identified as suspects, and three days after the bombing the Boston police felt forced to release photos of the actual suspects – two brothers – in order to prevent retaliatory violence against those wrongly targeted. Upon seeing their photos on the news the suspects panicked and fled, killing one police officer in a botched attempt to steal his gun (Montgomery, Fisher, and Branigin 2013; Montgomery, Horwitz, and Fisher 2013). After a tense 22 hour manhunt, including a shootout where a police officer sustained fatal wounds from an improvised hand grenade and where one of the suspects died after being run over by his brother who was fleeing the scene in a stolen SUV, the remaining suspect was arrested.

Similarly, in the aftermath of the November 2015 terrorist attacks in Paris, the Brussels police had to ask Twitter users to remain silent because tweets could give away police movements in real time – to which the public dutifully responded by flooding related hashtags with cat pictures (Rawlison 2015). Although these two terrorist attacks and subsequent manhunts are perhaps not typical of the police investigations they were covered extensively in the news, including in the Netherlands, establishing a narrative where mobs of internet detectives can run amok and cause real harm to ongoing police investigations and police officers.

In the view of the Dutch police, then, the Automon app responds to an already existing willingness amongst the public to contribute to police work and channels that support (see e.g. Timan and Albrechtslund 2018, 855). However, seen from a more critical perspective the Automon app also fits in an ongoing trend of using networked computing technologies to responsibilise citizens for government tasks (e.g. Koskela 2011; van Brakel and de Hert 2011; Marx 2013; Trottier 2014; Mantello 2016; Larsson 2017; Purenne and Palierse 2017; Vera and Torsten 2017; Cardullo and Kitchin 2018; Millie 2018, 201; Pridmore et al. 2018). Mantello (2016, 2) poignantly called such forms of surveillance '*Ikeaveillance* [which] encourages citizens to do the securitization footwork of the state by offering them the opportunity to participate in do-it-yourself, reward-centered, pro-active, networked and, at times, and [*sic*] gamified versions of automated governance' (italics in

original). On this view, the app mostly exists to offload what should be police tasks to an untrained and unpaid volunteer workforce that cannot – but perhaps should, as we shall see in the next section – be held accountable.

Such responsibilisation campaigns often take the form of crowdsourcing. Crowdsourcing is the distribution of many small tasks to participants in order to obtain a cumulative result, such as Google's reCAPTCHA program in which website users can prove they are not bots by clicking on images of e.g. vehicles and traffic signs and thereby contribute to a machine learning dataset to be used by self-driving cars. When smartphones are used in crowdsourcing applications, it is often called crowdsensing, a term first coined by Ganti, Ye, and Lei (2011). Crowdsensing is especially well-suited for collecting data from public places as people often carry their smartphones with them wherever they go. Crowdsensing application can be anything from fully participatory to fully opportunistic (Ganti, Ye, and Lei 2011, 32). Whereas participatory applications require the active involvement of the smartphone user to upload sensor data, opportunistic crowdsensing applications require minimal effort. Crowdsensing applications are also often Location Based Services (LBS): 'computer applications (especially mobile computing applications) that deliver information tailored to the location and context of the device and the user' (Huang et al. 2018, 1). Examples include navigation apps and certain social network such as FourSquare. Often, the relationship between the LBS-app and the user is reciprocal but not necessarily equal: not only does the app user receive tailored information but location (and other) data is collected in an opportunistic crowdsensed manner from her to make the app more valuable to other users and, consequently, its owners. Take for example Google Maps, which uses location data to show a map of the direct surroundings of the user. At the same time, it uses this data to calculate traffic conditions.

Such a reciprocal relationship also exists within the Automon app. On the one hand, the users gain the possibility to receive a financial reward for spotting a stolen car, a game embedded in the app, and the possibility to fight crime in their direct surroundings or work environment (see the below sub-section). On the other hand, the police receives the location of stolen vehicles and consequently the possibility to apprehend more criminals without investing heavily in its investigation capabilities. The app user must participate actively before this data-sharing takes place and, in contrast to some of the examples in the previous paragraph, is completely transparent. This transparency, however, does not absolve the Automon app from Ikeaveillanism which, as will be discussed in the legal analysis below, also has important legal repercussions under the new personal data protection regime of the EU.

Directing the surveillant gaze

When citizens are enrolled in surveillance practices, they must learn how to apply a 'surveillant gaze' (Marx 1988; Foucault 1995) to their surroundings. They must learn to spot what is suspicious, out of place, and in need of further scrutiny because it does not belong in the normal state of affairs (Curry 2004; Larsson 2017, 97). Automon users receive points for merely scanning a number plate; the app stops short of asking from its users anything beyond this gaze. Bart Driessen pointed out that, if a stolen vehicle is found with the app, users are also not supposed to actively engage with it beyond alerting the authorities (See also Larsson 2017, 103):

> The Automon app users go after stolen cars, [however] no chasing, no fighting, only observation is what's really going on.

How does the app direct this surveillant gaze that is central to the app and its usefulness for the police? One way in which the Automon app does this is by sending out notifications. These notifications are pushed out to users who are close to where a car theft has recently taken place and contain a description of the car to look out for. Not only does the app direct the gaze of the users when a car has recently been stolen nearby, it also urges surveillance of the streets for stolen cars as a quotidian practice (See also Lyon 2018) as explained by Bart Driessen:

> So we have some help function [in the Automon app] to say, okay, when is it useful to make a picture? So you can see on the car, for instance, a broken window, or the lock is broken, or something else is going on when a car is standing in the street, standing there for a few days and nobody knows where that car is from. We say, okay, that it's possible that it's stolen, so make of that kind of car pictures.

Because of their openness to interpretation and lack of enforcement mechanism within or outside of the app, these instructions for quotidian surveillance are more like guidelines than actual rules (Verbinski 2003). Users are free – and even encouraged (see the next subsection) – to interpret them broadly and scan as many number plates as they like in order to score more points for the in-app collection game.

As the discretionary power to (not) surveil lies squarely with the users, the makeup of the user base is very important: a car that looks suspicious to one person might seem perfectly normal to the next. It will be the users that direct the surveillant gaze according to their sense of what a normal car should look like (Larsson 2017, 98, 102; Ritsema van Eck 2018, 163–164). Unfortunately, describing the actual makeup of the user base of Pokémon Go is not possible at the time of writing, as the app is still in development. Bart Driessen did point out that initially the app will be actively marketed to two groups of users: those who work in the car industry and gamers.

With regards to the first group, it is difficult to predict how they will utilise their surveillant gaze. On the one hand, some car dealerships might be more than happy to scan the license plates of all cars offered to them in order not to be complicit in criminal activities. A possible motive for this course of action is that all businesses who encounter suspicious transactions are obliged to report them[6] and the ANPR-capabilities of the app might be a time-saving way of ensuring compliance. On the other hand, businesses might choose not to jeopardise lucrative partnerships despite concerns over the origin of (some of) the cars being offered to them. Furthermore, the game-like user interface of the app might dissuade well-meaning employees from using it out of fear to be seen playing games on their smartphones during work, either by their boss or by visiting customers. Finally, cars are (re-)sold through a multitude of channels and it seems probable that a criminal, if in possession of a stolen car that she/he wishes to sell, will avoid official channels where the Automon app might be used. As Bart Driessen pointed out in the telephone interview, many stolen cars are swiftly exported to e.g. Africa and Russia. In those cases, the many narrowly focused surveillant gazes will still miss that which lies just outside their field of vision (Latour 2005, 181).

The second group to which the app will be marketed are gamers (Figure 2). In this manner, the police hopes to benefit from the popularity of Pokémon Go and other

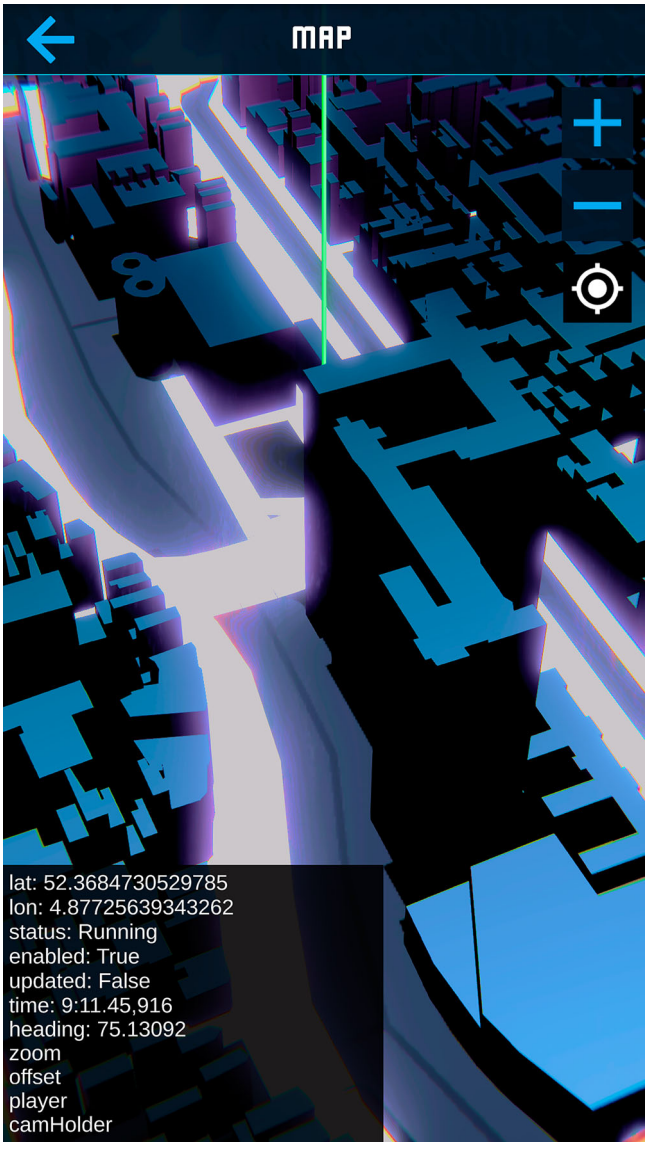

Figure 2. A screenshot of the map view in a prototype of the Automon app. Notice how it uses a stylised map in a similar manner to Pokémon Go (see Figure 1), albeit with a cooler colour scheme. Screenshot provided by the Dutch Police.

mobile games. However, it is not clear how this will be done. If the police aims to approach gamers directly, then the police must be able to first identify them. Besides the data processing activity that this will require one might also ask: What sets apart a gamer from a non-gamer? The label of 'gamer' hardly discriminates in today's world. Pokémon Go, which was downloaded over 800 million times worldwide (Harris 2018), itself is a demonstration that especially casual mobile gaming has become a mainstream activity.[7] Furthermore: how will the police market to this group? Assuming that 'gamers' and 'non-gamers' exist, it is not clear how the police will identify the former and

approach them to enrol them. If the police aims to approach gamers indirectly, then the call must be sent to the general public at large. Those that are willing to collaborate with the police and that are gamers or that are willing to play this particular game will be enrolled. The composition of this part of the projected user base thus also remains unclear, as will their surveillant gaze.

Despite this uncertainty, two general hypotheses can be postulated about how gamers[8] might use their surveillant gaze: First, if they try to score points in Automon, they might scan as many number plates as possible. This would entail a rather unselective surveillant gaze, aimed at any number plate in reach. Second, the competition from the mobile gaming market is fierce, oversaturated as it is with engaging games produced by large teams of designers. If a user approaches Automon as a game rather than as a tool to support the police, the unique qualities are quickly lost and other games might be more rewarding to play. The surveillant gaze would then become distracted and drift away.

Taking a broader view, in the academic literature bias and discrimination are seen as concerning by-products when surveillance technologies are put in the hand of citizens. Locative social media are mostly used in white and high income areas (Anselin and Williams 2016, 318). This could lead to more police resources being spent on those areas compared to low-income areas (Joh 2014, 2016). It remains to be seen whether this effect carries over to locative participatory surveillance apps, but at the very least smartphone ownership is presupposed. Excluded are those who do not possess a smartphone, or the necessary skills to install and use apps. Furthermore, Purenne and Palierse (2017, 88) found that such tools are used to keep those who are 'others' out of homogenous areas. It is possible that the app aims the surveillant gaze at cars rather than people will dampen this effect. It is equally possible, however, that people who are part of a disadvantaged group find their number plates will be scanned more often (See also e.g. Gandy 2000, 2006; Ritsema van Eck 2018, 168–169). After all, can 'someone like that' really afford a 'car like that'?

Gamification and rewards

Users will primarily experience the Automon app as a game. Compare for instance the user interface design of the garage in 'Asphalt 9,' a popular smartphone racing game, with that of Automon in, respectively, Figures 3 and 4. Presenting the app as entertaining and exciting is done in order to maintain the surveillant gaze once it is established; The Automon app needs to fight for attention with myriad distractions both on and off the smartphone screen. Two main rewards have been built into the Automon app in order to encourage users to continue using the app and scan as many number plates of suspicious cars as possible: in-game points and, in certain cases, a monetary reward.

The gamification mainly takes the form of a 'Pimp my Ride' style game, in which gamers can 'pimp up' cars in the virtual garage in the app using in-game currency, buying increasingly desirable cars and car parts (see Figure 4). Note that, in contrast to many racing games which employ similar upgrading mechanics, it seems there is no benefit to buying more cars or upgrading them. In-game points can be earned by scanning number plates, and certain special actions and milestones, such as scanning fifty number plates, might earn the player bonus in-game points.

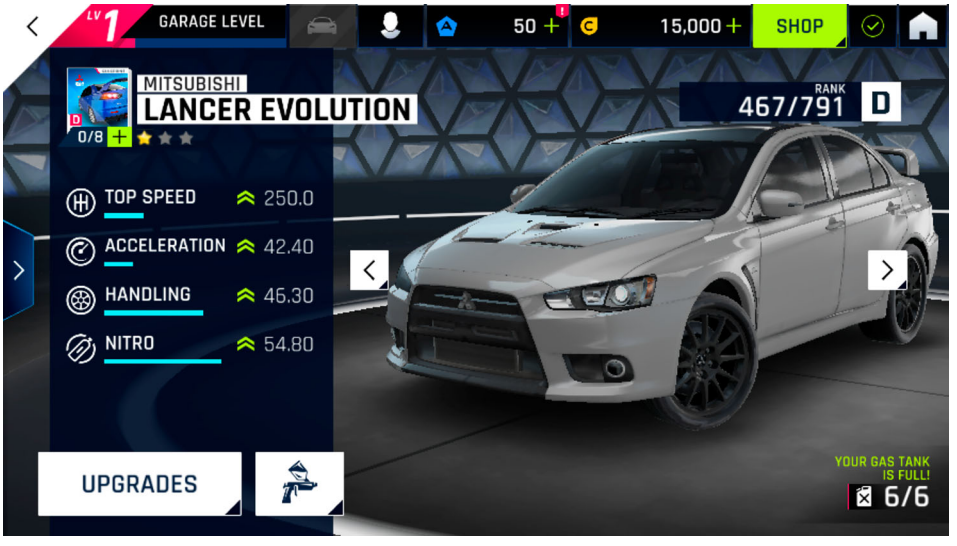

Figure 3. A screenshot of the garage view in the Asphalt 9 mobile racing game published by Gameloft SE. Screenshot taken by the authors on an Android device on 19 October 2018.

The monetary reward on the other hand would only be given out if a user scans the number plate of a stolen car, which would then lead to the successful retrieval of the car in question. As this might save an insurance company from having to pay out a claim, it could utilise (part of) these savings to reward the user who scanned the license plate. When the interview with Bart Driessen was being conducted, the details of the monetary reward were still being negotiated with insurance companies, some of which were hesitant to cooperate. In order for the monetary reward to be paid out, some personal

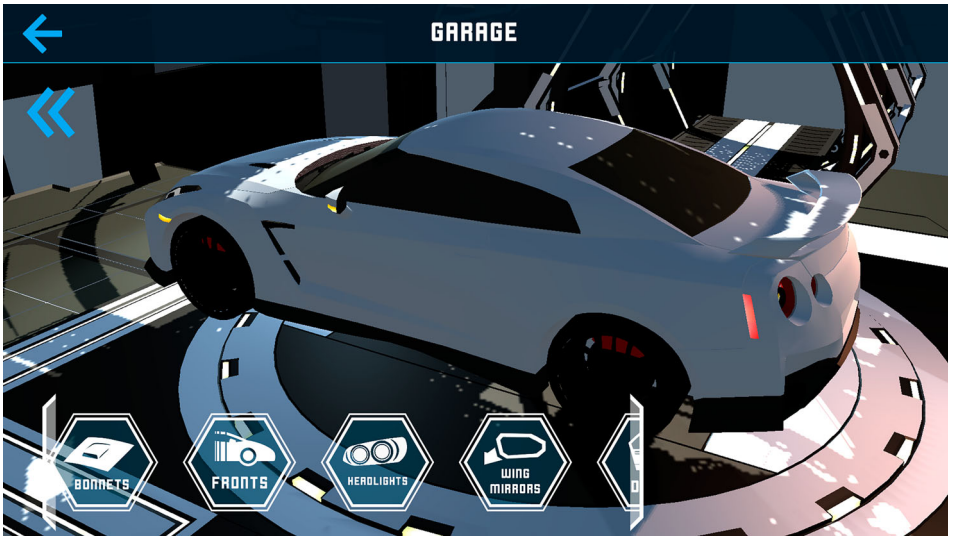

Figure 4. A screenshot of the garage view in a prototype of the Automon app, showing a car which can be upgraded, or 'pimped', using in-game currency. Screenshot provided by the Dutch Police.

data must be stored on the police server in order to be able to identify the user who scanned the number plate.

Gamified participatory surveillance is not without its critics, such as Julie E. Cohen, who argues forcefully that gamification should not be confused with innocuous play (2016, 210–211). Whereas play is 'quite consciously outside "ordinary" life as being "not serious"' (Huizinga 1980, 13), the Automon app outsources a task of law enforcement to the public, packaged as an entertaining pastime. However, play 'is an activity connected with no material interest, and no profit can be gained by it' (Huizinga 1980). There is then a tension between the playful experience of scoring points and upgrading cars on the one hand, and the very serious interests of the police and insurance companies on the other hand.

Before engaging in the legal analysis, it can be concluded that the police seems to be betting on two horses with regards to various aspects of the Automon app. The police wants to collect as many number plates as possible, but not become engulfed in a torrent of useless data provided by over-eager participants. Similarly, the police aspires to steer the surveillant gaze of the Automon app users towards cars that might be stolen property, but also rewards the bulk scanning of number plates with in-game points. Finally, in the hopes of solving the quite serious problem of car theft, the police has chosen a whimsical, game-like form. As a result of these divergences, the Automon app is neither a dedicated surveillance app, nor a dedicated game.

Legal analysis

After discussing the merits and demerits of the Automon app and its double function as a game and a surveillance tool, this section takes a legal approach and analyses the compatibility of the app with the EU data protection framework. With the introduction of the app, law enforcement aims to benefit from the willingness of the individuals to collaborate. However, the new data protection regime in the EU might create further legal implications that were not discussed at the time the app was initiated. Attention is paid in this section especially to the GDPR and to the Police Directive. The section will first analyse the nature of the data collected via the Automon app. Then, it will establish the applicable law. Finally yet importantly, the legal positions that the applicable legal rules assign to the various actors involved are analysed. The analysis presented here has a wider applicability than just to the Automon app as the trends described in the 'Background' subsection above will probably lead to a multitude of similar initiatives by police forces throughout Europe.

Automon app data as personal data

In order to establish if the EU data protection framework is applicable, we must first establish whether the data collected via the Automon app qualify as personal data. As explained in the interview by Bart Driessen, the number plate is the only data that the app will collect and that will be further processed. Thus, we need to assess if number plates qualify as personal data. Personal data are defined in the GDPR, article 4(1) and the Police Directive, article 3(1), as any information relating to an identified or identifiable natural person. An identifiable person is further defined as him who can be identified, directly or indirectly, in particular: '… by reference to an identifier such as a name, an identification number,

location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

The verification of these conditions is obvious for number plates since their *raison d'être* lies in facilitating the identification of the person to whom a vehicle is registered.[9] In the EU legal framework for data to qualify as personal, identification should be possible by the controller or any other person with 'means reasonably likely to be used […] to identify the natural person directly or indirectly'.[10] In the case of number plates, the obvious means of identification are the vehicle registration databases that each Member State is required to maintain.[11] For an Automon app user the access to the vehicle registration database is possible only in very specific situations in the presence of a legitimate interest.

For law enforcement (which qualifies as the data controller in this case; see the subsection 'Automon app users under the Police Directive' below) such access to the RDW database is much easier. Advocate General Sánchez-Bordona in his opinion in *Breyer* explained that 'reasonable' in cases of indirect identification of individuals should be understood to denote at least that those means are lawful.[12] The Court of Justice followed this line of reasoning in its decision.[13] Whether the police actually uses this authority either in general or in specific cases does not matter.[14] In the example of the Automon app, the police can indirectly identify the owner of any vehicle in the RDW database using the number plates provided by Automon app users. Therefore, all number plates are personal data. Finally, the police will have files on any stolen vehicles, making direct identification possible for those number plates that belong to stolen vehicles. Thus, number plates qualify as personal data: The strict European personal data protection framework should be applied to what might seem an amusing diversion.

GDPR or Police Directive?

Data protection laws first emerged to protect individuals against the effects of the ever-increasing exposure of their personal information to public authorities; later, they were expanded to also include protections against interferences by the private sector (Gstrein and Ritsema van Eck 2018, 79). Thus, individuals have traditionally been the 'beneficiaries' of data protection. Over time, however, the role of the individual has shifted. Due to the rapid development of technology and its increasing availability, individuals have acquired capabilities that were previously reserved for the state or large private organisations. As such, individuals today are not only data subjects but also potential data controllers and processors.

Despite the fact that there are no specific rules at EU level regulating the collaboration between law enforcement and citizens, the legislation on data protection is very broad and accommodates such situations. In their work on community policing in EU law, Al-Sharieh and Mifsud Bonnici (2018, 182) find the legal bases for such activities broadly in the rule of law and the crime prevention framework.

Generally, the GDPR applies when individuals process personal data of their fellow citizens.[15] In principle, this would be the case also when individuals in a public space capture with their cameras images of number plates. Exceptions to this general rule are the processing of personal data that take place in the course of purely personal and household activities,[16] processing of data that falls in the area of Common Foreign and Security Policy,[17] and processing for law enforcement activities for the scope of prevention,

detection, investigation and prosecution of crime.[18] In the latest case, the Police Directive applies.[19]

There are no indications that the Automon app collects and processes data for foreign, security and defence policy purposes. If the app had only one function, the gaming one, the exception of purely personal and household activities would have been valid, but the double function of the app as a game and as a surveillance tool changes the situation. The fact that the data are sent to the RWD for verification and that the main scope of the processing is determined by law enforcement, eliminates the exclusion of the purely domestic activity. The discussion of the last exclusion that will have as an effect the application of the Police Directive is more complicated.

The Police Directive applies to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. The definition of competent authorities extends beyond law enforcement authorities as it also applies to any other body or entity entrusted by Member State law to exercise public authority and public powers.[20] We argue that the activity of individuals that collaborate with law enforcement by using the Automon app falls under the scope of the application of the Directive.

The app is designed by law enforcement to assist them in their activities. Because of the dual function of the app, as a game and as a surveillance tool, all app users operate as an extended arm of law enforcement and assist in the performance of their duties. The users of the app perform criminal investigation and detection activities, which are typical of law enforcement. As it has been clarified in the case law of the ECtHR, the rights of the individuals will be seriously endangered if the law enforcement could evade its legal obligations by making use of private agents.[21] Thus, situations in which the police may not have been directly involved, but in which they have worked with or trusted individuals to collect information also fall within the scope of law enforcement activities.[22] In our case, in order to avoid the possibility that law enforcement agencies can circumvent their legal obligations (Purtova 2018, 59) by making use of individuals that carry out law enforcement tasks via smartphone games, the Police Directive should apply

The Directive introduces a level for data protection for individuals in the framework of law enforcement activities as well as a number of obligations for data controllers and processors without referring to a cross border element. Thus, activities that are purely national also fall within the scope of the application of the Directive. To comply with the Police Directive the processing of personal data must be: lawful and fair, specified, explicit and for a legitimate purpose, adequate and not excessive, accurate and kept up to date when necessary, kept in a form which permits identification of the data subject for no longer than is necessary and, secured from unauthorised or unlawful processing.[23] While these principles seem to be generally addressed by the design of the app, other legal aspects need consideration and are discussed below.

Automon app users under the Police Directive

After establishing in the previous section that the Police Directive applies when individuals collaborate with the law enforcement, this section will discuss more specifically the roles that it attributes to law enforcement and Automon app users.

As stated in its recital 7, the Police Directive aims to ensure an equivalent level of protection of the rights and freedoms of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security in all Member States. However, it provides only for the minimum standards of protection since, in implementing it, Member States are allowed to introduce higher safeguards for the protection of the rights and freedoms of the data subject.[24]

After establishing that the data collected in the framework of the Automon app qualify as personal it is easy to establish the data subject. As it was explained by Bart Driessen, the only data that the app will collect are the number plates, leaving out all the irrelevant parts of the picture taken by the app user. Following this explanation, since on the basis of a number plate the owner of the vehicle can be identified, she/he qualifies as the data subject. In addition, also the controller and processor can be easily identified.

According to article 3(8) of the Police Directive:

> '"controller" means the competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data'. The processor is: 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'.[25]

Processing of data also includes the data collection activity. In the case of the Automon app, the law enforcement establishes and determines – quite literally – the rules of the game and the reasons for processing the collected data (see also the sub-section 'directing the surveillant gaze'). Thus, by designing the affordances of the app, thereby allowing certain and denying other actions, and supporting this by clear instructions to the users, the Dutch police clearly qualifies as the controller. The individuals that collect and process the data are the data processors.

Thus, the provisions of the Police Directive give a legal status to individuals collaborating with the law enforcement, even in the seemingly innocuous and playful context of an online game. They are not only natural persons enjoying an app but data processors that are subject to the legal rules and which have specific duties and obligations on the basis of the Police Directive.

Discussion and implications

As was shown in the previous section, the game-like façade cannot hold up to close legal scrutiny. The qualification of the activity performed with the Automon app under the Police Directive has a number of legal implication that have to be taken into consideration by law enforcement agencies that are considering using similar tools to increase the participation of the public.

Firstly, the Police Directive aims to ensure the protection of standards when law enforcement collaborates with specific processors to safeguard the rights of data subjects. Processors may only be selected by the controller if they implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Directive and will ensure the protection of the rights of the data subject.[26] This provision is clear and precise in its wording and it leaves very little

space for the Member States to manoeuvre, unless for introducing even stricter requirements. Specifically, the Dutch law implementing the Police Directive[27] introduced article 6c to the *Wet politiegegevens* (Police data law) on *verwerkers* (processors). Together with the delegated legislation[28] which added article 6:1b to the *Besluit politiegegevens* (Decision police data), it almost literally transposes the conditions laid down in the Police Directive.

In its current design, the Automon app does not comply with this requirement. In the Automon app, game participants carry out the collection of data on behalf of the law enforcement. It is not law enforcement, as the controller, that chooses its collaborators. They are self-selected by voluntarily downloading the app and participating in the game. They might be anybody, independent of how protected their devices are. Law enforcement can also not ensure that individuals will implement appropriate technical and organisational measures. It cannot ensure that the data will not be used for other purposes or that will not be retained by the app users for a longer period than the one established by the law. As a result, the Automon app and practices similar to it infringe the safeguards of the data protection rules.

Secondly, there is another general principle that the collaboration of the individuals with the police in ways similar to the Automon app might infringe. This is the proportionality principle that must guide decisions of law enforcement to interfere with the fundamental rights of the individuals, including their right to data protection (Milaj 2015). This principle determines the necessary and sufficient conditions for limiting a protected right (Barak 2012, 3) as well as serves to restrict the exercise of powers from the State authorities (van den Brink et al. 2007, 143).

As it was argued also in the previous section under the 'surveillant gaze', law enforcement may receive a large amount of personal data through Automon from non-qualified and non-specialised sources. Consequently, not all the data transferred to law enforcement by individuals will be relevant. This will be the case especially in those situations in which individuals by themselves have suspicions that a vehicle might be stolen and thus make pictures that they send in via the app. The problem is only exacerbated by the game-like design of Automon. As a result, law enforcement will be overloaded with personal data that, even if there is no match with a stolen car, will show the location of specific vehicles at specific points in time and thus reveal unjustifiably large amounts of personal data. It cannot be excluded that these data might be the result of various biases or incorrect information. When the Automon app is conceptualised as a game this might not be particularly problematic, but for a police surveillance tool it is deeply troublesome.

Note that Dutch police aims to reduce this effect by immediately deleting any data on number plates sent to them that do not result in a 'hit.' Furthermore, the ANPR system is integrated in the app on the smartphone, thus only the number plate data is transmitted to the police servers and not the rest of the photo that might contain more personal data. Although *prima facie* effective measures to stem the collection of unnecessary personal information, they might create a tension with article 25 of the Police Directive[29] which requires that logs are kept of the 'collection, alteration, consultation, disclosure including transfers, combination, and erasure' of personal data in automated processing systems. It goes on to specify that

> The logs of consultation and disclosure shall make it possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data.

When a no-hit occurs in the Automon system only collection and erasure take place, but no consultation and disclosure. Therefore, it would seem that as long as logs are kept, they can be devoid of any personal data. However, no logs seem to be kept at all in the current design of Automon.

Thirdly and finally, article 27 of the Police Directive requires that a Data Protection Impact Assessment (DPIA) takes place 'where a type of processing, in particular, using new technologies' is likely to result in a high risk to the rights and freedoms of natural persons. Following the guidelines of the Article 29 Data Protection Working Party's (A29WP)[30] DPIAs should be carried out as early as is practicable (2017, 25). In this manner, DPIAs can support decision makers during the design phase. At the moment, however, such an assessment has not yet taken place. Bart Driessen indicated that any data protection considerations are put on hold until a final decision has been made on the location of the field tests. By relegating these considerations to a separate part of the process to be completed at a later date, the DPIA can no longer play the supporting role in following the privacy by design principles[31] that the A29WP accords it (2017, 25).

From the above implications, it is clear that the Automon app does not comply with the European legislation on data protection. As a result, practices like the Automon app, independent of any evaluation on their usefulness or gameplay value, do not fulfil the legal requirements and thus strictly qualify as unlawful. Law enforcement could therefore be subject to fines (the amount of which is established by each Member State when implementing the Police Directive – in the Netherlands the maximum applicable fine is currently set at €830,000.00)[32] or even to judicial processes initiated by the Data Protection Authority or individuals who feel their rights have been infringed.

Conclusion

The Automon app is developed by the Dutch Police to involve citizens in law enforcement activities and to extend the scope of action of the police without expanding its force. The app fits within a larger trend of providing the general public with automated tools that they can use to participate in police work. Such tools respond to various needs felt by both law enforcement and citizens alike by using game-like elements to direct the surveillant gaze of participants. Even when the goals of such tools are lofty and the form in which citizens can participate is decidedly ludic, these activities are subject to legal rules. Thus far, there are no specific rules on police-citizen interaction at EU level. The EU legal framework adopted in 2016, which aims to conform the activity of law enforcement to data protection rules, did not consider specifically this emerging trend. The general data protection rules applicable to law enforcement are, however, broad and, as it was analysed in this paper, cover also the individuals' participation in police investigations.

The Automon app design was initiated before the adoption of the Police Directive, when the national rules were the ones regulating the field. Today, it fails to comply with these general rules established by the Directive on three grounds. Firstly, it cannot

ensure that law enforcement makes use only of processors that demonstrate to have adopted appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Directive and ensure the protection of the rights of the data subject. Secondly, the proportionality of the interference with the private life of the individuals, as for example their location at a specific point in time (Woods 2017), cannot be ensured. Thirdly, although this should have been the case, a DPIA has not yet taken place.

As a result, we argue that using the Automon app or similar applications by law enforcement does not meet the requirements prescribed by the current legal regime. This is a clear example of the disconnection between law and technology that reflects how legal rules lag behind any technological advances. To overcome such a situation, specific rules regulating the police-citizen interaction are desirable. Since the provisions of the Police Directive on the use of external processors by law enforcement are sufficiently clear, precise and unconditional, there is no space for the national legislator to fill the gap. Therefore, any new legal intervention is to be taken at European level.

Notes

1. The Pokémon Go app was released in the summer of 2016. It utilizes the player's mobile device's GPS ability to locate, capture, battle, and train virtual creatures, called Pokémon, which appear on the screen as if they were at the same real-world location as the player.
2. Note that 'Automon' is being used as a working title. It seems likely that a possible final version will use a different name, because 'Automon' is also a company which develops case management software for probation agencies in the United States of America, see ('About Us' 2018). Furthermore, Automon is one of the main antagonists in a Power Rangers episode (Koichi 2002).
3. More specifically: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation (GDPR)) [2016] OJ L119/1; and Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities or the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Police Directive) [2016] OJ L119/89.
4. A portmanteau of 'digital' and 'vigilante' (seemingly) first coined by Ruth Martin (2007).
5. The app provides guidance on what characteristics a user might want to look out for, a point to which we will return below.
6. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L141/73, art 33.
7. In 2015 there were 3.429 billion mobile broadband subscriptions worldwide (ITU Telecommunication Development Bureau 2015). This means that Pokémon Go was installed on approximately 1 in 4.3 smartphones with internet access worldwide.
8. Beyond the two specific user bases initially targeted by the police, Automon will also be open to the general public. It can be hypothesized that their surveillant gaze will be similar to that of gamers discussed here.
9. Convention on Road Traffic (concluded 8 November 1986, entered into force 21 May 1977) 1042 UNTS 17, art 35–36.

10. GDPR, recital 26; Police Directive, recital 21.
11. Convention on Road Traffic (n 9), art 35–36.
12. Case C–582/14 *Patrick Breyer v Bundesrepublik Deutschland* EU:C:2016:339, Opinion of AG Sánchez-Bordona, paras 68–73.
13. Case C–582/14 *Breyer* (n 12), para 46.
14. Case C–582/14 *Breyer* (n 12), para 47–48.
15. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR) [2016] OJ L119/88.
16. GDPR, art 2(2)c.
17. GDPR, art 2(2)b.
18. GDPR, art 2(2)d.
19. Police Directive, art 1(1).
20. Police Directive, recital 11, art 3(7).
21. *Van Vondel v The Netherlands* App no 38258/03 (ECtHR, 25 October 2007), para 49.
22. *MM v The Netherlands* App no 39339/98 (ECtHR, 8 April 2003), para. 42; *A v France* App no 14838/89 (ECtHR, 23 November 1993), paras 38–39.
23. Police Directive, art 4(1).
24. Police Directive, art 1(3).
25. Police Directive, art 3(8).
26. Police Directive, art 22(1).
27. Wet van 17 oktober 2018 tot wijziging van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens ter implementatie van Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen, *Stb*. 2018, 401.
28. Besluit van 6 december 2018 tot wijziging van het Besluit politiegegevens, het Besluit justitiële en strafvorderlijke gegevens en het Besluit politiegegevens bijzondere opsporingsdiensten ter implementatie van Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, *Stb*. 2018, 496.
29. Implemented in Dutch law in article 32 of the *Wet Politiegegevens*.
30. These guidelines are based on the GDPR rather than the Police Directive. However, in lieu of a similar guiding document for the police context we use these guidelines to make a preliminary assessment. The guidelines have since been adopted by the European Data Protection Board.
31. Police Directive, art 20.
32. *Wet Politiegegevens,* art 35c juncto *Wetboek van Strafrecht* (Criminal Code), art 23(4).

Acknowledgements

The authors would like to thank Bart Driessen of the Dutch Police for answering our many questions about the Automon-app and providing us with the screenshots. Furthermore, we thank Carola Onderdelinden for her help in the early stages of our research.

Disclosure statement

No potential conflict of interest was reported by the authors.

ORCID

Gerard Jan Ritsema van Eck http://orcid.org/0000-0003-2009-2320

References

"About Us". 2018. *AutoMon: Innovative Solutions for Community-based Corrections*. https://automon.com/about/.

Albrechtslund, Anders, and Peter Lauritsen. 2013. "Spaces of Everyday Surveillance: Unfolding an Analytical Concept of Participation." *Geoforum; Journal of Physical, Human, and Regional Geosciences* 49: 310–316. doi:10.1016/j.geoforum.2013.04.016.

Al-Sharieh, Saleh, and Jeanne Mifsud Bonnici. 2018. "From the Persuasion of Theory to the Certainty of Law: A Multi-Jurisdictional Analysis of the Law of Community Policing in Europe." *European Journal of Comparative Law and Governance* 5 (2): 179–202. doi:10.1163/22134514-00502005.

Anselin, Luc, and Sarah Williams. 2016. "Digital Neighborhoods." *Journal of Urbanism* 9 (4): 305–328. doi:10.1080/17549175.2015.1080752.

Article 29 Data Protection Working Party. 2017. "Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679 (WP 248 Rev.01)." ec.europa.eu/newsroom/document.cfm?doc_id=47711.

Barak, Aharon. 2012. *Proportionality: Constitutional Rights and Their Limitations*. Cambridge: Cambridge Studies in Constitutional Law, Cambridge University Press.

Cardullo, Paolo, and Rob Kitchin. 2018. "Being a "Citizen" in the Smart City: Up and Down the Scaffold of Smart Citizen Participation in Dublin, Ireland." *GeoJournal*. doi:10.1007/s10708-018-9845-8.

Cassa, Christopher, Rumi Chunara, Kenneth Mandl, and John S Brownstein. 2013. "Twitter as a Sentinel in Emergency Situations: Lessons From the Boston Marathon Explosions." *PLoS Currents: Disasters*, doi:10.1371/currents.dis.ad70cd1c8bc585e9470046cde334ee4b.

Cohen, Julie E. 2016. "The Surveillance-industrial Complex: The Irony of the Participatory Turn." In *The Participatory Condition in the Digital Age*, edited by Darin Barney, Gabriella Coleman, Christine Ross, Jonathan Sterne, and Tamar Tembeck, 207–226. Minneapolis: University of Minnesota Press.

Curry, Micheal R. 2004. "The Profiler's Question and the Treacherous Traveler: Narratives of Belonging in Commercial Aviation." *Surveillance & Society* 1 (4): 475–499. doi:10.24908/ss.v1i4.3332.

Davis, Edward F. III, Alejandro A. Alves, and David Alan Sklansky. 2014. "Social Media and Police Leadership: Lessons from Boston." *New Perspectives in Policing*, 1–20.

Foucault, Michel. 1995. *Discipline and Punish: The Birth of the Prison*. Translated by Alan Sheridan. 2nd Vintage Books ed. New York: Vintage Books.

Gandy, Oscar H. 2000. "Exploring Identity and Identification in Cyberspace." *Notre Dame Journal of Law, Ethics & Public Policy* 14 (2): 1085–1111.

Gandy, Oscar H. 2006. "Quixotics Unite! Engaging the Pragmatists on Rational Discrimination." In *Theorizing Surveillance: The Panopticon and Beyond*, edited by David Lyon, 318–336. Abingdon: Routledge.

Ganti, Raghu, Fan Ye, and Hui Lei. 2011. "Mobile Crowdsensing: Current State and Future Challenges." *IEEE Communications Magazine* 49 (11): 32–39. doi:10.1109/MCOM.2011.6069707.

Gstrein, Oskar Josef, and Gerard Jan Ritsema van Eck. 2018. "Mobile Devices as Stigmatizing Security Sensors: The GDPR and a Future of Crowdsourced "Broken Windows"." *International Data Privacy Law* 8 (1): 69–85. doi:10.1093/idpl/ipx024.

Harris, Iain. 2018. "Pokemon Go Captures 800 Million Downloads." *Pocketgamer.Biz*, May 30. http://www.pocketgamer.biz/news/68209/pokemon-go-captures-800-million-downloads/.

Huang, Haosheng, Georg Gartner, Jukka M. Krisp, Martin Raubal, and Nico Van de Weghe. 2018. "Location Based Services: Ongoing Evolution and Research Agenda." *Journal of Location Based Services*, 1–31. doi:10.1080/17489725.2018.1508763.

Huizinga, Johan. 1980. *Homo Ludens: A Study of the Play-Element in Culture*. London: Routledge & Kegan Paul.

ITU Telecommunication Development Bureau. 2015. "ICT Facts and Figures: The World in 2015." International Telecommunications Union. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.

Joh, Elizabeth E. 2014. "Policing by Numbers: Big Data and the Fourth Amendment." *Washington Law Review* 89 (1): 35–68.

Joh, Elizabeth E. 2016. "The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing." *Harvard Law & Policy Review* 10 (1): 15–42.
Koichi, Sakamoto. 2002. "Forever Red." Power Rangers: Wild Force, October 5.
Koskela, Hille. 2011. "'Don't Mess with Texas!' Texas Virtual Border Watch Program and the (Botched) Politics of Responsibilization." *Crime, Media, Culture* 7 (1): 49–65. doi:10.1177/1741659010369957.
Larsson, Sebastian. 2017. "A First Line of Defence? Vigilant Surveillance, Participatory Policing, and the Reporting of 'Suspicious' Activity." *Surveillance & Society* 15 (1): 94–107. doi:10.24908/ss.v15i1.5342.
Latour, Bruno. 2005. *Reassembling the Social: An Introduction to Actor-network-theory*. Clarendon Lectures in Management Studies. New York: Oxford University Press.
Lee, Dave. 2013. "Boston Bombing: How Internet Detectives Got It Very Wrong." *BBC News*, April 19, sec. Technology. http://www.bbc.com/news/technology-22214511.
Lupton, Deborah. 2014. "Apps as Artefacts: Towards a Critical Perspective on Mobile Health and Medical Apps." *Societies* 4 (4): 606–622. doi:10.3390/soc4040606.
Lyon, David. 2018. *The Culture of Surveillance: Watching as a Way of Life*. Cambridge: Polity.
Mantello, Peter. 2016. "The Machine That Ate Bad People: The Ontopolitics of the Precrime Assemblage." *Big Data & Society* 3 (2): 1–11. doi:10.1177/2053951716682538.
Martin, Ruth. 2007. "Digilante Justice: Citizenship in Cyberspace." *The New Atlantis* 16: 124–127.
Marx, Gary T. 1988. *Undercover: Police Surveillance in America*. Berkeley: University of California Press.
Marx, Gary T. 2013. "The Public as Partner? Technology Can Make Us Auxiliaries as Well as Vigilantes." *IEEE Security & Privacy* 11 (5): 56–61. doi:10.1109/MSP.2013.126.
Milaj, Jonida. 2015. "Invalidation of the Data Retention Directive: Extending the Proportionality Test." *Computer Law & Security Review* 31 (5): 604–617. doi:10.1016/j.clsr.2015.07.004.
Millie, Andrew. 2018. "Citizens in Policing: The Lived Reality of Being a Police Support Volunteer." *Policing and Society*, 1–13. doi:10.1080/10439463.2018.1451529.
Montgomery, David, Marc Fisher, and William Branigin. 2013. "FBI Releases Images of Two Suspects in Boston Marathon Bombings." *Washington Post*, April 18. https://www.washingtonpost.com/world/national-security/investigators-focus-on-video-of-two-men-at-scene-of-boston-marathon-bombings/2013/04/18/6dadfcfa-a833-11e2-8302-3c7e0ea97057_story.html.
Montgomery, David, Sari Horwitz, and Marc Fisher. 2013. "Police, Citizens and Technology Factor into Boston Bombing Probe." *The Washington Post*, April 21. https://www.washingtonpost.com/world/national-security/inside-the-investigation-of-the-boston-marathon-bombing/2013/04/20/19d8c322-a8ff-11e2-b029-8fb7e977ef71_print.html.
Pridmore, Jason, Anouk Mols, Yijing Wang, and Frank Holleman. 2018. "Keeping an Eye on the Neighbours: Police, Citizens, and Communication Within Mobile Neighbourhood Crime Prevention Groups." *The Police Journal: Theory, Practice and Principles*. doi:10.1177/0032258X18768397.
Purenne, Anaïk, and Grégoire Palierse. 2017. "Towards Cities of Informers? Community-based Surveillance in France and Canada." *Surveillance & Society* 15 (1): 79–93. doi:10.24908/ss.v15i1.5619.
Purtova, Nadezhda. 2018. "Between the GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public–Private Partnerships." *International Data Privacy Law* 8 (1): 52–68. doi:10.1093/idpl/ipx021.
Rawlison, Kevin. 2015. "National Emergency? Belgians Respond to Terror Raids with Cats." *The Guardian*, November 22. http://www.theguardian.com/world/2015/nov/22/national-emergency-belgians-respond-with-cats.
Ritsema van Eck, Gerard Jan. 2018. "Emergency Calls with a Photo Attached: The Effects of Urging Citizens to Use Their Smartphones for Surveillance." In *Surveillance, Privacy, and Public Space*. Studies in Surveillance 2, edited by Bryce Clayton Newell, Tjerk Timan, and Bert-Jaap Koops, 157–178. Abingdon: Routledge.
Schneider, Christopher J., and Daniel Trottier. 2012. "The 2011 Vancouver Riot and the Role of Facebook in Crowd-Sourced Policing." *BC Studies* 175: 57–72.
Spiller, Keith, and Xavier L'Hoiry. 2018. "Watch Groups, Surveillance, and Doing It for Themselves." Presented at the Surveillance Studies Network Conference, Aarhus, June 8.

Starbird, Kate, Jim Maddock, Mania Orand, Peg Achterman, and Robert M. Mason. 2014. "Rumors, False Flags, and Digital Vigilantes: Misinformation on Twitter after the 2013 Boston Marathon Bombing." In *IConference 2014 Proceedings*. iSchools. doi:10.9776/14308.

Timan, Tjerk, and Anders Albrechtslund. 2018. "Surveillance, Self and Smartphones: Tracking Practices in the Nightlife." *Science and Engineering Ethics* 24 (3): 853–870. doi:10.1007/s11948-015-9691-8.

Trottier, Daniel. 2014. "Crowdsourcing CCTV Surveillance on the Internet." *Information, Communication & Society* 17 (5): 609–626. doi:10.1080/1369118X.2013.808359.

van Brakel, Rosamunde, and Paul de Hert. 2011. "Policing, Surveillance and Law in a Pre-Crime Society: Understanding the Consequences of Technology Based Strategies." *Cahiers Politiestudies* 20 (3): 163–192.

van den Brink, Jacobine, Willemien den Ouden, Sacha Prechal, Rob Widdershoven, and Jan H. Jans. 2007. "General Principles of Law." In *Europeanisation of Public Law*, edited by Jan H. Jans, Sacha Prechal, and Rob Widdershoven, 137–266. Groningen: Europa Law Publishing.

van den Heuvel, John, and Mick van Wely. 2017. "Politiepokémon op komst: Burgers kunnen met app gestolen auto's opsporen." *De Telegraaf*, October 7. https://www.telegraaf.nl/nieuws/552919/politiepokemon-op-komst.

Vera, Antonio, and Oliver Salge Torsten. 2017. "Crowdsourcing and Policing: Opportunities for Research and Practice." *European Police Science and Research Bulletin* 16: 143–154.

Verbinski, Gore. 2003. *Pirates of the Caribbean: The Curse of the Black Pearl*. Walt Disney Pictures.

Vries, Arnout. 2017. "App: Automon." Social Media DNA. October 18. http://socialmediadna.nl/automon/.

Woods, Lorna. 2017. "Automated Number Plate Recognition: Data Retention and the Protection of Privacy in Public Places." *Journal of Information Rights, Policy and Practice* 2 (1). doi:10.21039/irpandp.v2i1.35.