University of Groningen

Privacy and Participation in Public

Ritsema van Eck, Gerard

DOI:
[10.33612/diss.171025411](https://doi.org/10.33612/diss.171025411)

IMPORTANT NOTE: You are advised to consult the publisher's version (publisher's PDF) if you wish to cite from it. Please check the document version below.

Document Version
Publisher's PDF, also known as Version of record

Publication date:
2021

[Link to publication in University of Groningen/UMCG research database](#)

Citation for published version (APA):
Ritsema van Eck, G. (2021). *Privacy and Participation in Public: Data protection issues of crowdsourced surveillance*. [Thesis fully internal (DIV), University of Groningen]. University of Groningen.
<https://doi.org/10.33612/diss.171025411>

Copyright

Other than for strictly personal use, it is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license (like Creative Commons).

The publication may also be distributed here under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license. More information can be found on the University of Groningen website: <https://www.rug.nl/library/open-access/self-archiving-pure/taverne-amendment>.

Take-down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from the University of Groningen/UMCG research database (Pure): <http://www.rug.nl/research/portal>. For technical reasons the number of authors shown on this cover page is limited to 10 maximum.

Privacy and Participation in Public

Data protection issues of
crowdsourced surveillance

Gerard Jan Ritsema van Eck

Cover design by the author and dr. C. Slofstra

Typesetting by the author

Druk: Ridderprint, Alblasserdam

Typeset in Mercury and Operator (© Hoefler Type Foundry)

rijksuniversiteit
 groningen

Privacy and Participation in Public

Data protection issues of crowdsourced surveillance

Proefschrift

ter verkrijging van de graad van doctor aan de
Rijksuniversiteit Groningen
op gezag van de
rector magnificus prof. dr. C. Wijmenga
en volgens besluit van het College voor Promoties

De openbare verdediging zal plaatsvinden op

donderdag 16 september 2021 om 16:15 uur

door

Gerard Jan Ritsema van Eck

geboren op 8 februari 1988
te Groningen

Promotores

Prof. dr. G.P. Mifsud Bonnici

Prof. dr. P.C. Westerman

Beoordelingscommissie

Prof. dr. K. Ball

Prof. mr. dr. A.R. Lodder

Prof. mr. dr. S.H. Ranchordas

Table of Contents

1	Introduction	3
1.1	The milkman: surveillance just a lifetime ago	5
1.1.1	Research question and overview of the introduction	8
1.2	Technological developments: dataveillance and smartphones	10
1.3	Surveillant developments: participation, and crowdsourcing	13
1.4	Legal developments: Privacy and data protection rights in public spaces	17
1.4.1	A reasonable expectation: The USA	21
1.4.2	A reasonable expectation in Europe?	22
1.4.3	Data protection under the ECHR	29
1.4.4	Data protection at the EU	34
1.4.5	Taking stock: Privacy in public space	37
1.5	Outline	39
2	Emergency calls with a photo attached: The effects of urging citizens to use their smartphones for surveillance	47
2.1	Introduction	50
2.1.1	Object of the current chapter	52
2.1.2	Overview of the current chapter	53
2.1.3	A note on terminology	54
2.2	Societies of discipline	55
2.2.1	Short term effects: visibility	56
2.2.2	Long term effects: normalization	60
2.2.3	An empowerment within the panopticon?	62

2.3	Societies of control	66
2.3.1	Inclusion in databases	67
2.3.2	Loss of anonymity vis-à-vis the police	70
2.3.3	Normalization and chilling effects	72
2.3.4	The erosion of the presumption of innocence and social trust	74
2.3.5	Cumulative disadvantages resulting from simulation and prediction	76
2.4	Policy implications	78
2.5	Conclusion	81
2.5.1	Avenues for future research	83
2.6	Postscript	87
3	Mobile devices as stigmatizing security sensors: The GDPR and a future of crowdsourced ‘broken windows’	91
3.1	Introduction	93
3.2	Websites and apps	95
3.2.1	Free to be	98
3.2.2	My Safetipin	99
3.2.3	SpotCrime and Crime Maps	103
3.2.4	GeoEstrela, MeldStad, and Ir-Rahal Taghna	104
3.2.5	WayGuard	108
3.3	Potential concerns	109
3.4	Legal analysis	123
3.4.1	Personal data as ‘Resource’?	125
3.4.2	Re-identification through combination	130
3.4.3	Remedies on the basis of the new EU legislation	134

3.4.4	Groups	138
3.4.5	Preventive measures on the basis of the new EU legislation	140
3.5	Conclusion	141
4	Algorithmic Mapmaking in “Smart Cities”: Data Protection Impact Assessments as a means of Protection for Groups	151
4.1	Introduction	155
4.2	How Maps Are Made	157
4.3	Maps and (Missing) Group Rights	161
4.4	Making Group Rights Real Through DPIAs?	167
4.4.1	Opportunities	171
4.4.2	Limitations	177
4.5	Conclusion	180
5	Capturing licence plates: police participation apps from an EU data protection perspective	183
5.1	Introduction	186
5.2	The Automon app: Surveillance, game, or both?	189
5.2.1	Background	191
5.2.2	Directing the surveillant gaze	199
5.2.3	Gamification and rewards	207
5.3	Legal Analysis	209
5.3.1	Automon app data as personal data	210
5.3.2	GDPR or Law Enforcement Directive?	212
5.3.3	Automon app users under the Law Enforcement Directive	216

5.4	Discussion and implications	218
5.5	Conclusion	223
5.6	Postscript	225
6	General discussion: Private data, public spaces?	227
6.1	A look back: main conclusions so far	230
6.2	Bringing the threads together	238
6.2.1	Understanding crowdsourced surveillance	238
6.2.2	The impact of crowdsourced surveillance on public space	241
6.2.3	Re-evaluating privacy and data protection rights with regards to crowdsourced surveillance	247
6.3	A look ahead: Quo vadis, privacy in public?	251
6.3.1	Data protection impact assessments	252
6.3.2	Group data protection rights	255
6.4	Conclusion	260
7	Table of cases	263
7.1	Council of Europe	265
7.1.1	European Court of Human Rights	265
7.1.2	European Commission on Human Rights	266
7.2	European Union	266
7.3	United States of America	267
7.3.1	Supreme Court of the United States	267
7.3.2	Circuit Court	267
7.3.3	District Court	268
7.4	Germany	268

7.5	Netherlands	268
8	Table of treaties, legislation & documents	271
8.1	United Nations	273
8.1.1	Conventions	273
8.1.2	United Nations Commission on Human Rights	273
8.2	Council of Europe	273
8.2.1	Conventions	273
8.2.2	Recommendations	273
8.3	European Union	274
8.3.1	Primary Legislation	274
8.3.2	Secondary legislation	274
8.3.3	Documents	275
8.4	National legislation	276
8.4.1	Netherlands	276
8.4.2	United States of America	277
9	References	279
	Curriculum Vitea	321
	Dankwoord/Acknowledgments	325

List of Figures and Tables

Figure 1.1: Employee of the provincial inspection service takes a sample of milk	6
Table 1.1: Some major surveillance schemata compared	15
Figure 1.2: Representation of selected ECtHR case-law on the reasonable expectation of privacy	27
Figure 1.3: Venn-diagram representing various legal docu- ments of relevance to the rights to privacy and personal data protection in Europe	32
Figure 2.1: Photograph taken with an Apple iPhone	58
Figure 3.1: Screenshot of the My Safetipin website	100
Figure 3.2: Screenshot of a map of Manhattan, Queens, and Brooklyn as seen on the Trulia real estate website	102
Figure 3.3: Screenshot of a map of the city centre of Gronin- gen as seen in the Meldstad app	106
Figure 4.1: Screenshot of a Strava heatmap	154
Figure 4.2: Screenshot of the Waze map of London	160
Figure 5.1: Screenshot of the map view in Pokémon Go	190
Figure 5.2: Screenshot of the map view in Automon	202
Figure 5.3: Screenshot of the garage in Asphalt 9	206
Figure 5.4: Screenshot of the garage in Automon	206
Table 6.1: The influence of crowdsourced surveillance on public space	245

List of Abbreviations

A29WP	Article 29 Working Party
ANPR	Automatic Number Plate Recognition
CCTV	Closed Circuit Television
CFEU	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
ECHR	In text: European Convention on Human Rights
~	In case citations: Reports of Judgments and Decisions of the ECtHR
ECJ	European Court of Justice
ECR	European Court Reports
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EU	European Union
FBI	Federal Bureau of Investigation
GDPR	General Data Protection Regulation
GIS	Geographic Information Systems
GPS	Global Positioning System
GSM	Global System for Mobile communications
ICT	Internet and Communications Technologies
IoT	Internet of Things
IP	Internet Protocol
LBS	Location based services
LGBT	Lesbian, gay, bisexual, and transgender
NGO	Non-governmental organization
OJ	Official Journal of the European Union

PIA	Privacy Impact Assessment
RDW	Rijksdienst voor het Wegverkeer
SCOTUS	Supreme Court of the United States
SUV	Sports Utility Vehicle
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
TGV	Train à Grande Vitesse
UN	United Nations
UNTS	United Nations Treaty Series
US	In text: United States
~	In case citations: United States Reports
USA	United States of America

English Summary

In the last decade, what it means to be private in public has been uprooted by smartphones. When we take these machines with us, we also bring their cameras and other embedded sensors into public spaces. This has led corporations and (local) governments to ‘crowdsource’ their surveillance; a novel surveillance structure in which data is gathered by dispersed people and processed and used by central actors. Crowdsourced surveillance is a cheap and reasonably easy way to collect data on diverse phenomena, which may otherwise be difficult to quantify, including, for example, traffic congestion trends and generalized feelings of (un)security in certain neighbourhoods. People willingly engage in these surveillance networks because they see it as their civic duty, to obtain some benefit, or because they are drawn in by gamified aspects.

This puts a novel and unique pressure on public spaces: the watchful eye of single citizens is connected to powerful actors through both direct means and opaque algorithms. Despite the severe strain this puts on people and places, it is difficult to find legal protections against instances of such crowdsourced surveillance of public spaces. Not only is the legal system ill-equipped to cope with the intermeshed nature of crowdsourcing, but privacy protections are also (necessarily) weaker in public spaces: precisely where crowdsourced surveillance is at its strongest. This leads to the research question of this thesis: How can we explain the interactions and occasional mismatches between the legal frameworks for privacy and personal data protection that

arise in public space, as a result of the rise of crowdsourced surveillance? Based on the challenges identified, several promising avenues for improving legal protections will be highlighted.

The dissertation integrates findings from surveillance studies with legal analysis into data security and privacy law to answer the research question. The body of the thesis consists of four case studies in crowdsourced surveillance, each of which used as an analytical starting point. Together, they put today's technical and organizational state of play into focus and provide a structure for thinking about how tomorrow's technologies would need to be regulated. The cases include multimedia emergency reporting; crowdsourced data collection on safe and dangerous areas; numerous mapmaking efforts; and a Pokémon Go-like game by the Dutch police to find stolen vehicles.

The analysis of these case studies highlights a number of distinct and often concerning aspects of crowdsourced surveillance of public spaces. First, it may be difficult to define the applicable theoretical model of surveillance, as crowdsourcing relies on both loose networks *and* powerful central actors to punish transgressors. In practice, this combination leads to a rise of social control in public spaces, which is supercharged by the involvement of the state or large corporations. This makes public spaces less open to deviation from existing social norms; what is worse, however, is that the unrestricted involvement by anyone means that prejudice and discrimination can run rampant.

At present, European laws on privacy and data protection fail to provide sufficient guarantees for those concerned. Often, laws might simply not apply because the data collected in public spaces is not considered ‘personal.’ Furthermore, it is difficult to undo many of the effects of crowdsourced surveillance, if not impossible. Those affected need tools that are appropriate for the job, and this dissertation concludes that there are currently two legal instruments needed. First, data protection impact assessments need to be strengthened and made mandatory to avoid adverse effects altogether. Second, data protection rights should be extended to groups, as crowdsourced surveillance impacts them most. We can only guarantee the continuing quality of our streets, parks and squares with these improvements to the legal framework.

Nederlandse Samenvatting

In het afgelopen decennium hebben smartphones de betekenis van privacy in de openbare ruimte fundamenteel veranderd. Met deze draagbare telefoons in onze broekzakken, nemen we ook camera's, microfoons, en talloze andere sensoren mee de wereld in. Dit heeft het mogelijk gemaakt voor bedrijven en (lokale) overheden om hun surveillance te 'crowdsourcen': een nieuwe surveillancestructuur waarin gegevens wijdverspreid verzameld worden door vele mensen en verwerkt worden door centrale actoren. Participanten nemen deel aan dit soort surveillance omdat ze het als hun burgerplicht zien, omdat er een beloning tegenover staat, of vanwege game-achtige aspecten die het leuk maken om te doen. Crowdsourced surveillance is de laatste jaren een goedkope en redelijk eenvoudige manier geworden om gegevens te verzamelen over diverse verschijnselen, die anders wellicht moeilijk te kwantificeren zijn, zoals bijvoorbeeld verkeersopstoppen en gevoelens van (on)veiligheid in bepaalde buurten.

Dit veroorzaakt een nieuwe en unieke druk op de openbare ruimte, namelijk het waakzame oog van talloze burgers dat zowel direct als via ondoorzichtige algoritmes verknoopt is geraakt met machtige actoren. Hoewel dit een grote impact kan hebben op burgers en de openbare ruimte, is het moeilijk om juridische bescherming te vinden tegen dergelijke gecrowdsourcde surveillance. Niet alleen is het rechtssysteem slecht toegerust om het hoofd te bieden aan de verwevenheid van crowdsourcing, maar ook is privacybescherming (noodzakelijkerwijs) zwakker in de openbare

ruimte: precies daar waar de gecrowdsourcde surveillance het sterkst is. Hieruit volgt de onderzoeksvraag van dit proefschrift: Hoe verklaren we de interacties en mismatches tussen de wettelijke kaders voor privacy en bescherming van persoonsgegevens die ontstaan in de openbare ruimte door de opkomst van crowdsourced surveillance? Uitdagingen voor de wettelijke bescherming zullen worden geïdentificeerd en verschillende routes voor verbetering zullen worden uitgelicht.

Om deze onderzoeksvraag te beantwoorden worden in dit proefschrift de inzichten uit surveillancewetenschappen geïntegreerd met een juridische analyse van de geldende databeschermings- en privacywetgeving. Er worden vier casestudies van crowdsourced surveillance als analytisch uitgangspunt gebruikt. Deze cases omvatten onder andere multimediale rapportages aan noodhulpdiensten, het verzamelen van gegevens over gevoelens van veiligheid in verschillende gebieden, het gebruik van crowdsourcing om kaarten te maken en een Pokémon Go-achtig spel van de Nederlandse politie om gestolen voertuigen op te sporen. Tezamen brengen deze casestudies de huidige technische en organisatorische stand van zaken in beeld en bieden ze een framework om te onderzoeken hoe toekomstige technologieën gereguleerd zouden moeten worden.

De analyse van deze casestudies belicht verschillende, vaak zorgwekkende, aspecten van crowdsourced surveillance in de openbare ruimte. Het blijkt ingewikkeld te identificeren welke theoretisch surveillancemodel precies van

toepassing in op crowdsourced surveillance in de openbare ruimte, omdat deze gebruik maakt van zowel losse netwerk- en als krachtige centrale actoren om overtreders te bestraffen. In de praktijk leidt deze combinatie tot een toename van de sociale controle in de openbare ruimte, die door de betrokkenheid van de staat of de grote bedrijven nog verder wordt versterkt. Dit vermindert de tolerantie voor afwijkingen van bestaande sociale normen in de publieke ruimte. Bovendien biedt deze ongereguleerde betrokkenheid van vele actoren weinig bescherming tegen risico's zoals discriminatie en werkt ze deze mogelijk zelfs in de hand.

Op dit moment biedt de Europese wetgeving op het gebied van privacy en gegevensbescherming onvoldoende bescherming aan de betrokkenen. Vaak zijn deze wetten niet van toepassing omdat de gegevens die in de openbare ruimte worden verzameld, niet als “persoonlijk” worden beschouwd. Bovendien blijkt crowdsourced surveillance vele effecten te hebben op de openbare ruimte die niet eenvoudig ongedaan gemaakt kunnen worden. Dit proefschrift concludeert dat momenteel twee noodzakelijke, passende juridische instrumenten ontbreken die betrokkenen kunnen beschermen tegen crowdsourced surveillance. Hiertoe zouden ten eerste gegevensbeschermingseffectbeoordelingen aangescherpt en verplicht gesteld moeten worden. Ten tweede zouden gegevensbeschermingsrechten ook bescherming moeten bieden aan groepen, aangezien zij het meest worden getroffen door crowdsourced surveillance in de openbare ruimte.

1. Introduction

1.1 The milkman: surveillance just a lifetime ago

Figure 1.1 shows a photo of a milkman taken in Groningen in 1927, while a provincial inspector is checking his wares. This was just two years after the introduction of the first portable 35mm camera, the Leica, which made it possible to quickly snap pictures on the go.¹ The milkman warily looks into the lens of this technological disruptor, perhaps wondering why this potentially precarious moment is being photographed, or worried about the outcome of this milk-related governmental surveillance. Meanwhile, the inspector seems to already be accustomed to this mode of oversight and goes about his business undisturbed.

This photograph might very well be one of the few data trails of this milkman that still exists. His face has been digitized and is now part of the provincial archives of Groningen, a structured database maintained by the government.² However, his name and all the details of his personal life cannot be ascertained based on this one data point. No profile can be assembled from disparate data sources, and no risk score can be calculated.

- 1 See also the effect that the introduction of the portable Kodak Camera had on the development of the debate about technology and privacy in the United States of America: Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193.
- 2 Compare here *Amann v Switzerland* ECHR 2000-II 245, paras 65–67. Note, however, that the milkman in the photograph is probably no longer alive. The European Union personal data protection framework (n 75 and 76) therefore does not apply to him.

If the same man had been born a century later, his datafied life would have looked starkly different. He would not have had the chance to examine each camera in public space so warily; there are simply too many. Furthermore, the milkman would probably not even consider this, as most of

Figure 1.1: Employee of the provincial inspection service takes a sample of milk.³

3 'Graaf Adolfstraat: Medewerker Provinciale Keuringsdienst Neemt Monster van Melk Bij Melkventer' <<http://beeldbankgroningen.nl/beelden/detail/ef36d097-06d1-2038-3b71-6b3bf8a75add>> accessed 18 December 2018.

his idle moments on the street would be spent staring at the latest reviews he received on his smartphone; a camera, positioned just above the glistening screen, constantly pointed at his own face. His horse-drawn carriage might be a GPS-enabled electric delivery vehicle with a number plate that is scannable using automated number plate recognition (ANPR) and instantaneously matched to a single entry in a complete database of millions of number plates.

David Lyon defines surveillance as “the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction.”⁴ Both the milkman of a century ago and his hypothetical modern counterpart were subjected to surveillance, albeit in very diverse ways. Nowadays, for example, Bayesian statistics employed by the inspection agency will, in all likelihood, predict a low probability of our milkman selling sour milk and allocate scarce resources elsewhere. Thus, the chance of being subjected to governmental inspection might be much lower now than in 1927. However, as government surveillance fades into the algorithmic background, another type of actor appears centre stage: the watchful citizen, not content to trust food and safety standards at face value. Dissatisfied customers might leave unfavourable reviews on internet forums and, as his electric delivery vehicle zips out of the street, snap a picture to post to a local WhatsApp group. Inspection agencies

4 *Surveillance Studies: An Overview* (Polity 2007) 14. More on surveillance below in section 1.3 ‘Surveillant developments: participation, and crowdsourcing.’

can also request such input from citizens in order to optimize their operations. Then, it becomes a form of ‘crowd-sourced surveillance’ that allow organizations to outsource their surveillance without large investments: an enticing proposition for anyone looking to gather more data cheaply.

1.1.1.1 Research question and overview of the introduction

This fictitious example underscores how different contemporary surveillance is in comparison to 1927.⁵ In the current day and age, technological possibilities have enabled even single citizens to ceaselessly monitor and interpret their surroundings. The flip side of surveillance is privacy, which can only exist where the former is “gap-ridden, transparent, and incomplete.”⁶ This connection between technological developments and privacy can be traced back to Samuel D. Warren and Louis D. Brandeis’ seminal article ‘The Right

- 5 e.g. Kevin D Haggerty and Richard V Ericson, ‘The Surveillant Assemblage’ (2000) 51 *British Journal of Sociology* 605; Bart Simon, ‘The Return of Panopticism: Supervision, Subjection and the New Surveillance’ (2005) 3 *Surveillance & Society* 1; Maša Galič, Tjerk Timan and Bert-Jaap Koops, ‘Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation’ (2017) 30 *Philosophy & Technology* 9; Kurt Iveson and Sophia Maalsen, ‘Social Control in the Networked City: Datafied Dividuals, Disciplined Individuals and Powers of Assembly’ (2019) 37 *Environment and Planning D: Society and Space* 331. Furthermore, see chapter 3 of this thesis.
- 6 Julie E Cohen, ‘What Privacy Is For’ (2013) 126 *Harvard Law Review* 1904, 1930.

to Privacy.⁷ Since the publication of that article in 1890, the right to privacy has evolved and changed dramatically.

In recent decades, the right to personal data protection developed as a reaction to the rise of data based surveillance as described above, and for many has become a *pars pro toto* for the right to privacy. Data protection legislation is meant to protect citizens against watchful organizations. However, nowadays any single person might be a watcher. As people pervade public spaces, this puts an increased surveillance pressure on the streets, squares, and parks where one might have expected to remain relatively untracked not so long ago.

As technologies progress and possibilities for crowd-sourced surveillance proliferate, so do the privacy and data protection issues. This dissertation therefore investigates the following research question: How can we explain the interactions and occasional mismatches between the legal frameworks for privacy and personal data protection that arise in public space, as a result of the rise of crowdsourced surveillance? Based on the challenges identified, I aim to foreground a number of promising avenues for improving legal protections.

In this introduction, three important developments will be discussed which form the context of this research question. First, I will elaborate on the technological developments that enable contemporary surveillance. Second, the issue of crowdsourced surveillance will be discussed: what is it, and why is it so important for privacy in public spaces? In the

7 (n 1).

third and longest section, the legal background on privacy and data protection rights in public space will be discussed. This discussion will demonstrate that for understanding and informing the (legal) balance between surveillance and privacy, public space has become an important area of interest. Finally, the case studies, which form the four chapters comprising the body of the book, are shortly introduced.

1.2 Technological developments: dataveillance and smartphones

When considering the surveillance a modern-day milkman may be subjected to, the importance and ubiquity of networked data technologies is striking. Governments (perennially strapped for cash) and businesses (perennially looking for a financial edge over their competition) employ networked data technologies rather than expensive, clumsy, and potentially duplicitous humans to surveil populations and persons of interest. The data gathered is not only used to discipline subjects, but increasingly to algorithmically modulate their surroundings, making certain options easily available and excluding others.⁸

These fundamental changes have been engendered by the rise of dataveillance technologies and their decreasing prices.⁹ World Wide Web browsers on desktop computers

8 Gilles Deleuze, 'Postscript on the Societies of Control' (1992) 59 October 3.

9 Roger Clarke, 'Information Technology and Dataveillance' (1988) 31 Communications of the ACM 498.

are no longer the only quotidianly used internet-enabled technologies. Connected computers have become cheap, mobile, and (to varying degrees) weatherproof. They are outfitted with sensors that can record e.g. audio, video, and temperature as well as antennas that can pick up WiFi, Bluetooth, GSM, and GPS signals.

Governments have played an active role in introducing connected sensors to public spaces. They have (often locally and through opaque public-private partnerships) been installing so-called ‘Internet of Things’ (IoT) devices on lamp-posts, garbage bins, car fleets, building walls, and any other surface which seems capable of accommodating a screw. The physical spaces designed by planners are increasingly outfitted with connected sensors with the aim of becoming the next ‘smart city,’ which “is, at its very foundation, a system of surveillance.”¹⁰ As physical spaces increasingly converge with cyberspaces,¹¹ it should perhaps be no surprise that surveillance — the business model of the internet¹² — has started to spill over into the streets.

10 David Murakami Wood and Debra Mackinnon, ‘Partial Platforms and Oligoptic Surveillance in the Smart City’ (2019) 17 *Surveillance & Society* 176, 176.

11 Julie E Cohen, ‘Cyberspace as/and Space’ (2007) 107 *Columbia Law Review* 210, 245–47.

12 Bruce Schneier and Agne Pix, ‘Surveillance Is the Business Model of the Internet’ (*OpenDemocracy*, 18 July 2017) <<https://www.opendemocracy.net/en/digitaliberties/surveillance-is-business-model-of-internet/>> accessed 28 May 2019.

In addition, citizens have revolutionized public space surveillance by their use of one technology in particular. We can (and do) take it everywhere with us, from mountaintops to metro cars, from concert halls to toilets in dingy dive bars. It has weaved itself into the fabric of everyday life.¹³ It's uniquely connected through billions of broadband internet subscriptions sending reams of data around the globe. It will probably be within your reach whilst reading this dissertation: the smartphone.

Smartphones are carried into public spaces by billions of users¹⁴ because they provide unparalleled connected convenience. The ubiquity of smartphones, their constant connectedness, and the sensors (including the cameras) embedded in them make them uniquely suitable to surveillance in public.¹⁵ The useful output of these devices relies on copious amounts of input to generate it. The majority of this data does not come from the direct commands users give, but from the various sensors attached to the phone, which probe the space around them. Both within the device and in the

13 “The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.” Mark Weiser, ‘The Computer for the 21st Century’ (1991) 265 *Scientific American* 94, 94.

14 ITU Telecommunication Development Bureau, ‘ICT Facts and Figures 2017’ <<https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf>> accessed 11 October 2018.

15 See also Tjerk Timan and Anders Albrechtslund, ‘Surveillance, Self and Smartphones: Tracking Practices in the Nightlife’ (2018) 24 *Science and Engineering Ethics* 853.

metaphorical cloud¹⁶ algorithms interpret this data and then create innumerable new layers of data. In the past decade, no surveillance technology has spread through public spaces so quickly and easily as smartphones, hoovering up data wherever they go — i.e. everywhere.

1.3 Surveillant developments: participation, and crowdsourcing

The technological advances described above have changed surveillance. Together, businesses, governments, and citizens have cast a sensing net¹⁷ over public spaces, capturing themselves and each other, creating more and novel possibilities to gather and analyse data. The ongoing digitalization of almost all aspects of the human world has amplified surveillance into one of the hallmarks of our culture.¹⁸ It is, despite its cloak-and-dagger connotations, quite a mundane activity in which we all participate on a daily basis.¹⁹

To understand how the introduction of smartphones has influenced surveillance, it can be useful to think of a network that is composed of human and non-human actors.²⁰ A very

16 A.k.a. someone else's computer.

17 Term borrowed from Julie E Cohen, 'The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy' (2018) 31 *Philosophy & Technology* 213, 219–220.

18 David Lyon, *The Culture of Surveillance: Watching as a Way of Life* (Polity 2018).

19 Lyon, *Surveillance Studies* (n 4) 13.

20 Bruno Latour, *Reassembling the Social: An Introduction to Actor-Network-Theory* (Oxford University Press 2005).

simplistic network might consist of a police officer watching a citizen with the use of a CCTV camera. If any of these three actors — the officer, the camera, or the citizen — changes, this can have effects throughout the network. Consider for instance an upgrade from a fixed low-resolution camera to a high-resolution camera with extensive panning, tilting, and zooming capabilities. The new features allow the operator to more actively track a specific person, but make it more difficult for anyone caught in the gaze to simply walk out of view.

Any subject that is being watched thus ‘participates’ in surveillance; even inmates of Bentham’s panopticon participate by internalizing the fear of punishment and thereby enabling the functioning of the network.²¹ The introduction of smartphones in surveillance networks has boosted particular kinds of participation, such as lateral surveillance²² and sousveillance.²³ Both are done by individuals to, respec-

- 21 Anders Albrechtslund and Peter Lauritsen, ‘Spaces of Everyday Surveillance: Unfolding an Analytical Concept of Participation’ (2013) 49 *Geoforum* 310, 310–314; Michel Foucault, *Discipline and Punish: The Birth of the Prison* (Alan Sheridan tr, 2nd Vintage Books ed, Vintage Books 1995) 201; But also through forms or performance, see e.g. Rachel Hall, Torin Monahan and Joshua Reeves, ‘Surveillance and Performance (Editorial)’ (2016) 14 *Surveillance & Society* 153. See also subsection 2.2.2 of this thesis.
- 22 An around phenomenon, rather than top-down-and-around. Mark Andrejevic, ‘The Work of Watching One Another: Lateral Surveillance, Risk, and Governance’ (2002) 2 *Surveillance & Society* 479.
- 23 Focused on countering organizational surveillance, rather than working inside of it. Steve Mann, Jason Nolan and Barry Wellman, ‘Sousveillance: Inventing and Using Wearable Computing Devices

Surveillance schema	Data is		
	collected by	collected on	used by
Surveillance	Institution	Citizen	Institution
Sousveillance	Citizen	Institution	Citizen
Lateral	Citizen	Citizen	Citizen
Crowdsourced	Citizen	Citizen	Institution

Table 1.1: Some major surveillance schemata compared.

tively, monitor social relations or challenge actors that are more powerful. However, smartphones are also (unsurprisingly) used *by* powerful actors: they crowdsource their surveillance practices to willing participants, who take their smartphones with them into public spaces and gather data there. In such crowdsourced surveillance, the objects of surveillance (who might themselves be influenced, managed, protected, or directed) actively participate in surveillance networks that have been set up by organizations of which they are not part. The data they collect is then used in manners beyond their control. See table 1.1 for an overview of selected surveillance schemata.

Crowdsourced participation is becoming increasingly important in surveillance practices and takes many forms. On the one hand, it is being employed by businesses. Think for example of how Google Maps tracks the precise location

for Data Collection in Surveillance Environments' (2002) 1 Surveillance & Society 331.

of its users to both enhance their immediate experience and to increase the accuracy of the navigational directions in general.²⁴ Many people also track their own lives using apps or platforms provided for profit.²⁵ On the other hand, governmental agencies have discovered it as a way to responsibilize²⁶ citizens and increase their surveillance capabilities without necessarily needing to make concomitant investments. This can take extreme forms: it has even been used to watch a territorial border for potential illegal immigration.²⁷

In sum, technological developments have fuelled both the quality and quantity of surveillance in public. Crowdsourced surveillance has been added to the many schemata of surveillance, enabled by citizens who bring billions of surveillance devices into public space. The advantages of crowdsourced surveillance to governments and businesses have seen to its many and diverse uses. As a result, crowdsourced surveillance is increasingly permeating public space.

24 See further subsection 5.2.1 of this thesis.

25 Jennifer R Whitson, 'Gaming the Quantified Self' (2013) 11 *Surveillance & Society* 163.

26 Lyn Hinds and Peter Grabosky, 'Responsibilisation Revisited: From Concept to Attribution in Crime Control' (2010) 23 *Security Journal* 95.

27 Hille Koskela, "'Don't Mess with Texas!'" Texas Virtual Border Watch Program and the (Botched) Politics of Responsibilization' (2011) 7 *Crime, Media, Culture* 49.

1.4 Legal developments: Privacy and data protection rights in public spaces

The fundamental changes to the surveillance networks created by internet-enabled participation technologies pose new challenges to privacy and data protection in public space.²⁸ For one, crowdsourced surveillance does not easily map onto privacy and data protection regimes, as these primarily protect individuals against states or corporations.²⁹ Although both these actors are involved, their roles are more ambiguous as the participants (and thus data collection) lie beyond the direct control of a central institution.

Further adding to the complexity is the fact that the specific legal challenges can vary greatly between instances of crowdsourced surveillance, as operating mechanisms are manifold. The type of actors collecting which sort of data that is processed in which manner and to what end can differ per instance and may determine which rules and regulations are applicable. Data collection by police forces deserves special mention here because they have always relied on tips — a form of crowdsourced surveillance — from the public in order to carry out their tasks.

28 Defined above as “the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction.” See Lyon, *Surveillance Studies* (n 4) 14.

29 Bart van der Sloot, ‘Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation’ (2014) 4 *International Data Privacy Law* 307.

Finally, when reviewing the laws and regulations protecting privacy and data protection rights against crowdsourced surveillance, it becomes clear that the fact that crowdsourced surveillance is taking place in public space is particularly problematic. In fact, balancing surveillance and privacy under the current privacy and data protection regimes, increasingly requires an understanding and awareness of which spaces are public and which are not.

In general, the importance of place for the law is well established.³⁰ For instance, being naked in a place “for public life and not suited to unclothed recreation” is illegal in the Netherlands³¹ but taking a shower at home is not. Historically, many privacy protections are also based on the notion that ‘my home is my castle.’ The fourth amendment to the constitution of the United States of America³² stands as a classical example of this approach. In it, as in many jurisdic-

30 e.g. Nicholas K Blomley, David Delaney and Richard T Ford (eds), *The Legal Geographies Reader: Law, Power, and Space* (Blackwell Publishers 2001); Nicholas K Blomley, ‘Flowers in the Bathtub: Boundary Crossings at the Public–Private Divide’ (2005) 36 *Geoforum* 281; Andreas Osiander, ‘Sovereignty, International Relations, and the Westphalian Myth’ (2001) 55 *International Organization* 251.

31 *Wetboek van Strafrecht* (Dutch Criminal Code), art 430a, author’s translation.

32 “The right of the people to be secure in their persons, *houses*, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” (Italics added.)

tions around the world,³³ the home is conceptualized as the space where private activities take place. One goes out into public space to socialize and interact; this necessarily means that one becomes observable to others and claims to privacy should be considered null and void.³⁴

However, it is increasingly recognized by courts that privacy protections do not stop at the front door. As was already alluded to in the beginning of this introduction, this development has mostly been instigated by technological developments that have led to the capability to record and reproduce (inter)actions: As individuals have become increasingly exposed to such possibilities, so has the risk of privacy infringements taking place in public. This has revealed that the dichotomous distinction between private and public spaces in law is largely fictional. Furthermore, rather than either private (such as most toilets) or public (such as most streets and parks), many spaces are semi-public and fall somewhere in between these extremes. Take for

33 e.g. Bryce Clayton Newell, Silvia de Conca and Kirsten Thomasen, 'Surveillance and Privacy in North American Public Spaces' in Bryce Clayton Newell, Tjerk Timan and Bert-Jaap Koops (eds), *Surveillance, Privacy, and Public Space* (Routledge 2018) 223.

34 Johan Gottlieb Fichte already observed this in 1796, see 'Foundations of Natural Right' in Torin Monahan and David Murakami Wood (eds), *Surveillance studies: A reader* (Oxford University Press 2018) 68; See for more a thorough treatment of the subject Bert-Jaap Koops, 'Privacy Spaces' (2018) 121 *West Virginia Law Review* 611.

instance bars, supermarkets, most workspaces, and modes of (public) transport.³⁵

A final challenge is created by the constantly changing privateness and publicness of various spaces. Besides technological advances, social and legal developments have altered how individuals experience the world beyond their front door. This underlines that space is (repetitively re-) created by society.³⁶ These difficulties surrounding the definition of public space have become especially pronounced in legal privacy protections. The following subsections will elaborate upon how the publicness of space has become highly relevant to the privacy and data protection regimes concerning crowdsourced surveillance. Readers already familiar with this legal framework may wish to skip forward to section 1.4.5, where some of the quintessential implications for public space crowdsourced surveillance will be discussed.

35 See for an overview focused on privacy and data protection issues Koops (n 34); For an interesting view from the perspective of the users of such spaces, see Elaine Sedenberg, Richmond Wong and John Chuang, 'A Window into the Soul: Biosensing in Public' in Bryce Clayton Newell, Tjerk Timan and Bert-Jaap Koops (eds), *Surveillance, Privacy, and Public Space* (Routledge 2018).

36 Henri Lefebvre, *The Production of Space* (Donald Nicholson-Smith tr, Blackwell 1991).

1.4.1 A reasonable expectation: The USA
If courts are willing to recognize that a certain degree of privacy is to be protected even in spaces that are public,³⁷ they need to determine the extent of that protection. It follows that the protection of privacy requires a determination of the publicness and/or privateness of a space. This was for instance the approach taken by the Supreme Court of the United States of America (SCOTUS) when developing the influential ‘reasonable expectation test’ in *Katz v US*.³⁸ The case hinged on the question whether a phone booth could be considered a private or a public space, and thus whether the Federal Bureau of Investigation had needed a warrant for wiretapping it. The SCOTUS tried to route around the issue of space, by stating that the fourth amendment “protects people, not places”³⁹ and by developing a test that asks whether a person has exhibited an actual expectation of privacy, and whether society is prepared to recognize that expectation as reasonable.⁴⁰

The second part of the test re-introduces exactly the question of space that the court had tried to evade: whether society will recognize certain expectations as reasonable (or not) is largely determined by *where* a person was and how public that space was. The SCOTUS has thus opted for incorporating the social norm into the legal norm. Such an ap-

37 Meant here in the dichotomous legal sense.

38 389 US 347 (1967).

39 *ibid*, 351.

40 *ibid*, (JM Harling, concurring), 361.

proach has drawbacks and (as always in the area of privacy) it should be no surprise that one such drawback stems from technological advances. As new technologies become widely available, new social norms develop around them.⁴¹ This has forced and continues to force the federal courts to constantly reconsider which expectations society is prepared to recognize as reasonable. Some recent technologies that courts have considered include infrared cameras,⁴² Global Position System (GPS) trackers,⁴³ cell phone location data,⁴⁴ and data held on a smartphone.⁴⁵

1.4.2 A reasonable expectation in Europe?

In Europe, the protection of privacy does not stem from a constitution, but from the European Convention on Human Rights (ECHR) which entered into force in 1953 and to which all the member states of the Council of Europe are party. Article 8.1 of the Convention states that: “Everyone has the right to respect for his private and family life, his *home* and his correspondence” (*italics added*). The subsequent article

41 “We shape our tools and thereafter they shape us.” John M Culkin, ‘A Schoolman’s Guide to Marshall McLuhan’ *The Saturday Review* (18 March 1967) 51.

42 *Danny Kyllo v United States* 533 US 27 (2001).

43 *United States v Antoine Jones* 565 US 400 (2012).

44 *United States v Quartavious [sic] Davis* 785 F3d 498 (11th Cir 2015); *Timothy Ivory Carpenter v United States* 585 US ____ (2018).

45 *David Leon Riley v California*; *United States v Brima Wurie* 573 US 373 (2014).

8.2 provides an exhaustive list of instances in which interferences with this right are allowed, given that they have a basis in a law that is both accessible and foreseeable in its effects.⁴⁶ An interference is justifiable when it is “in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

Note that in article 8.1 of the Convention we find a notion of ‘home’ similar to the previously mentioned fourth amendment to the constitution of the USA. This, again, implies a strict separation between the space of home, which is deemed private, and any space outside of the home, which is consequently not private. It was thus inevitable that the European Court of Human Rights (ECtHR, the Court established by the Convention to adjudicate on it), would run into the same problems as the SCOTUS in dealing with cases where some privacy might be found in spaces outside the home *stricto sensu*. As similar problems beget similar solutions, a watered down version of the *Katz*-test also appears in Europe.⁴⁷

46 See e.g. *S and Marper v United Kingdom* ECHR 2008–V 167, para 95; and *Kennedy v United Kingdom* App no 26839/05 (ECtHR, 18 May 2010), para 151.

47 Although inspiration from across the Atlantic has not been explicitly acknowledged by the ECtHR in any judgements, it was recognized in two separate opinions. See *Polanco Torres et Movilla Polanco v Spain* App no 34147/06 (ECtHR, 21 September 2010, dissenting opinion of BM Zupacnčič) and *Benedik v Slovenia* App no 62357/14 (ECtHR, 24

This happened in the case of *PG and JH*, two men who were convicted of attempting to raid a Securicor cash-collection van. Listening devices planted in the flat of a third accomplice had recorded them planning the heist. However, after their arrest, the police could not prove that the recorded voices belonged to the defendants as they refused to speak whenever a tape was running. The police was thus not able to compare the voices recorded in the flat with those of the arrestees. Therefore, police officers engaged them in conversations, including about football, whilst wearing a hidden recording device. This allowed the police to match their voices to those taped previously.⁴⁸ All three men were convicted to lengthy prison sentences.

The ECtHR was subsequently faced with the question whether a violation of article 8 ECHR on the right to privacy outside a home had taken place. In paragraph 56 of the judgement, it extensively lists previous case law to support the notion that “private life is not a term susceptible to ex-

April 2018, concurring opinion of G Yudkivska joined by M Bošnjak). For recent political-economy perspective on the expectation of privacy in public at both the US and European federal courts see Perry Keller, ‘The Reconstruction of Privacy through Law: A Strategy of Diminishing Expectations’ (2019) 9 International Data Privacy Law 132. Note further that the literal words ‘reasonable expectation of privacy’ first appeared in *Halford v United Kingdom* ECHR 1997–III, para 43. It was mentioned in that case by the UK, however, the judges in that case dismissed the notion without deeming it worthy of explication.

48 *PG and JH v United Kingdom* ECHR 2001–IX 195, paras 8–18.

haustive definition.” Although this semantic formula was at the time not new for the Court, at the end of the paragraph it added a new conclusion to it: “There is therefore a zone of interaction of a person with others, even in a public context, which may fall within the scope of ‘private life’.” In paragraph 57, the Court continues by discussing how it can be established whether an interference with the right to privacy has indeed occurred in public:

There are a number of elements relevant to a consideration of whether a person’s private life is concerned by measures effected outside a person’s home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person’s reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain.⁴⁹

49 *ibid*, para 57.

In this paragraph, the Court pays significant attention to the importance of social spaces for privacy expectations and engages explicitly with the fundamental tension between public spaces and the right to privacy. It states, much in line with the SCOTUS but somewhat less stringently, that “a person’s reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor” in determining whether private life considerations arise.

After these initial two cases, a body of case law has developed dealing with the question whether an infringement of the right to privacy had taken place outside a home. A selection of this case law is presented in Figure 1.2 with arrows representing explicit references made by the Court itself. The importance of semi-public spaces is clearly noticeable in these cases at the ECtHR. A large portion of the case law on privacy in public deals with semi-public places such as workplaces in *Köpke v Germany*⁵⁰ and *Bărbulescu v Romania*.⁵¹ Even in the judgement in *PG and JH* quoted at some length above, the court already expanded the notion of ‘home’ found in article 8.1 ECHR to ‘home or private premises.’ It seems that the proper amount of privacy that may be expected in those spaces is likely to cause friction.

50 App no 420/07 (ECtHR, 5 October 2010).

51 App no 61496/08 (ECtHR, 5 September 2017), para 73.

Figure 1.2: A graphical representation of selected case-law of the European Court of Human Rights on the reasonable expectation of privacy, with arrows indicating references made by the Court in/to the paragraphs indicated. Note that not all cases in the figure are mentioned in the main text. Full references to those cases are given on the reverse.

Figure 2.1 (continued). *Von Hannover I*⁵² & *II*,⁵³ “*ICI PARIS*”,⁵⁴ *Leempoel*,⁵⁵ *Standard Verlags*,⁵⁶ *Peck*,⁵⁷ *Perry*,⁵⁸ and *Axel Springer*⁵⁹ are not mentioned in the main text, but included in the figure on the previous page.

52 *Von Hannover v Germany I* ECHR 2004–VI 41. In *Von Hannover I*, the court started using ‘legitimate’ for public figures, whereas ‘reasonable’ was consistently used for others. The exact distinction remains unclear[†] as do its consequences, and the court’s jurisprudence on this point has recently received a scathing treatment from Kirsty Hughes.[‡]

† Jens Kremer, ‘The End of Freedom in Public Places? Privacy Problems Arising from Surveillance of the European Public Space’ (PhD thesis, University of Helsinki 2017) 160–61.

‡ ‘The Public Figure Doctrine and the Right to Privacy’ (2019) 78 Cambridge Law Journal 70.

53 ECHR 2012–I 399, para 97.

54 *Hachette Filipacchi Associes (“ICI PARIS”) v France* App no 12268/03 (ECtHR, 23 July 2009).

55 *Leempoel & SA ED Cine Revue v Belgium* App no 64772/01 (ECtHR, 9 November 2006).

56 *Standard Verlags v Austria II* App no 21277/05 (ECtHR, 4 June 2009).

57 *Peck v United Kingdom* ECHR 2003–I 123.

58 *Perry v United Kingdom* ECHR 2003–IX 141.

59 *Axel Springer AG v Germany* App no 39954/08 (ECtHR, 7 February 2012).

1.4.3 Data protection under the ECHR

Since *Von Hannover II* in 2012, the development of the reasonable expectation of privacy has come to a standstill at the European Court of Human Rights. Instead, a formidable body of data protection jurisprudence was created at the ECtHR. Rather than focusing on the question whether a privacy expectation exists in each separate case and if so, whether it was reasonable — the thorny issue which has led to such an abundance of jurisprudence at the other side of the Atlantic — the ECtHR has developed data protection as a *pars pro toto* for privacy in public spaces. This happened notwithstanding the lack of a separate right to personal data protection in the European Convention of Human Rights.

This was made possible by the adoption of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) which became effective in 1985. In it, the Council of Europe enshrined various personal data protection principles. This was done in reaction to the rapid increases in the storage and sorting capabilities of computers. Rather than establishing a new and separate right to data protection, the Council placed Convention 108 under the umbrella of the right to privacy as protected by Article 8 ECHR. A prescient move, as data processing technologies would present the largest threats to privacy in the decades to come.

In early 2000, Convention 108 found its way into two landmark cases at the ECtHR: *Rotaru v Romania*⁶⁰ and *Am-*

60 ECHR 2000–V 109, paras 45–46.

man v Switzerland.⁶¹ In them, the Court concluded that the storage of personal data by state authorities necessarily interfered with Article 8.⁶² This was the Court's logical conclusion after considering that Convention 108 broadens the right to privacy to include data protection. It did technically leave open the possibility that data storage might *not* interfere with Article 8 if the data stored do *not* concern someone's private life. However, the Court "points out in this connection that the term 'private life' must not be interpreted restrictively."⁶³ As a result, it is hard to imagine any personal data that does not concern someone's private life.

It is important to note in this context that contemporary surveillance of both public and private spaces relies heav-

- 61 (n 2), paras 65–67. For a more recent example in which this link was made explicit, see e.g. *Shimovolos v Russia* App no 30194/09 (ECtHR, 21 June 2011), para 65 in particular, which builds on *PG and JH* (n 48), *Peck* (n 57, although not with regards to the expectation of privacy), *Amann* (n 2), and *Rotaru* (n 60). Kremer (n 52) 165–98 provides a more thorough overview of these and related developments at the court.
- 62 Already in 1987, in *Leander v Sweden*, neither party contested that the processing of personal data amounted to an interference with article 8. However, the facts in that case had taken place before Convention 108 came into force. Series A no 116, para 48.
- 63 *Amman* (n 2), para 65. Similarly, in para 66 of *S and Marper* (n 46) the Court uses its other stock phrase in this regard: "The Court notes that the concept of 'private life' is a broad term not susceptible to exhaustive definition."

ily on data technologies.⁶⁴ Since well nigh any surveillance technology focuses on the storage of personal data, these thus interfere with article 8.1 ECHR similarly to *Rotaru* and *Amman*. Because the interference with the right to privacy is relatively straightforward to establish, the focus of many cases shifts to whether the interference can be justified on the basis of article 8.2. This point may be illustrated especially well by looking at the 2010 case of *Uzun v Germany* that concerned the application of a GPS tracker to a car.⁶⁵ When explicating the general principles applicable to the case, the Court gives a thorough treatment of the question whether interferences to the right to privacy are possible outside the home.⁶⁶ However, these principles are not applied to the case, as the ECtHR can rely on personal data collection and storage alone to determine a violation.⁶⁷

The Supreme Court of the US was faced with very similar facts in *US v Jones* in 2012.⁶⁸ Not being able to rely on data protection as an integral part of the privacy protections offered by the fourth amendment, the SCOTUS had to consider the defendants' privacy expectations and their reason-

64 José Van Dijck, 'Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology' (2014) 12 *Surveillance & Society* 197.

65 ECHR 2010-VI 7.

66 *ibid*, para 44. Note that this paragraph is perhaps even more extensive than the one quoted above in *PG and JH*.

67 *ibid*, paras 49–53.

68 (n 43), and especially Justice Sonia Sotomayor's and Justice Samuel Alito's concurring opinions.

Figure 1.3, on the left: This Venn-diagram represents schematically the various legal documents of relevance to the rights to privacy and personal data protection at a European level. The Treaty on the Functioning of the EU (TFEU) explicitly gave the EU the (formerly implicit) competence to legislate on personal data protection in Article 16.⁶⁹ The Charter of Fundamental Rights of the European Union (CFEU) was adopted in 2009 to underscore the Union's commitment to human rights.⁷⁰ Note that article 8 CFEU on data protection was linked to article 8 ECHR on privacy rather than to Convention 108.⁷¹

69 [2016] OJ C202/47, 55.

70 [2016] OJ C202/393.

71 Explanations relating to the Charter of Fundamental Rights [2007] OJ C303/17, 33 read in conjunction with CFEU, art 52(7). Even before the Charter came into force AG Kokott followed this reasoning in paras 51–56 of his opinion on case C–275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* [2008] ECR I–271; and the Court followed suit in joined cases C–92/09 and C–93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen* [2010] ECR I–11063, para 52.

ableness. As in *Uzun*, it concerned a vehicle driving on public roads and thus visible to anyone. Attaching a GPS tracker had made tracing the car significantly easier for the police, but it had not been impossible before. Could Jones therefore have reasonably expected that the government would attach the gadget to his car? The varying positions in the majority and minority opinions in the case indicate that clear-cut answers are hard to come by.

1.4.4 Data protection at the EU

Data protection has started to eclipse privacy at the European Court of Human Rights in Strasbourg. If you hop on a TGV there and travel a little under two hours in a northwesterly direction, you can exit in Luxembourg at the bottom of the Kirchberg. The train ride crosses through the idyllic hills and forests of the Moselle region and, unseen to the contemporary eye, through the front lines of centuries of wars that ravaged the continent. At the top of the Kirchberg, we find the Court of Justice of the European Union (CJEU), the apex court of the European Union (EU) and its forerunners. Established with the aim of promoting peace through economic integration,⁷² they lacked the legal powers to legislate on privacy for most of their existence.

72 Robert Schuman, 'La Déclaration Schuman Du 9 Mai 1950' (*À propos de l'UE*, 24 October 2017) <https://europa.eu/european-union/about-eu/symbols/europe-day/schuman-declaration_fr> accessed 19 January 2020.

Data protection however, with its clear commercial ramifications, found its way into the *acquis communautaire* in the 1990s.⁷³ This is an essential moment for privacy in public spaces as, as was pointed out above, contemporary surveillance is predicated on large-scale data processing. More than 20 years later, updated ‘first-rate data protection rules providing for the world’s highest standard of protection’⁷⁴ were adopted to keep in step with technological advances. These self-congratulatory words of course refer to the General Data Protection Regulation⁷⁵ (GDPR) and the Law Enforcement Directive.⁷⁶

- 73 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 and Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L350/60.
- 74 Frans Timmermans, Andrus Ansip and Věra Jourová, ‘Joint Statement on the Final Adoption of the New EU Rules for Personal Data Protection’ (*European Commission Press Release Database*, 14 April 2016) <http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm> accessed 16 January 2018.
- 75 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) [2016] OJ L119/1.
- 76 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 legislation as formulated in the GDPR and the Law Enforcement Directive is further refined by The Court of Justice of the European Union. When disputes over the detailed rules laid down in these acts arise, the Court adjudicates.⁷⁷ This places the CJEU in a powerful position within this entire constellation, as its explication of any articles determines their precise meanings.⁷⁸ The extensive case law of the CJEU explaining articles in the GDPR has further demarcated what types of data are personal data and thus protected under the GDPR and the Law Enforcement Directive. In the case of surveillance technologies, its explication of articles in the GDPR can determine whether a violation of the right to privacy took place.⁷⁹ As we will see in the chapters ahead,

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 (Law Enforcement Directive) [2016] OJ L119/89.

77 Treaty on European Union [2016] OJ C202/13, art 19(3)b.

78 The *Satamedia* cases are an interesting example of the multi-layered data protection jurisprudence developing in Europe; they travelled between Finnish domestic courts, the Court of Justice of the European Union, and the European Court of Human Rights. See respectively case C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008] ECR I-9831 and *Satakunnan Markkinapörssi and Satamedia* App no 931/13 (ECtHR, 27 June 2017). As these cases focus on a derogation for journalistic practices with regards to personal data protection, they lie outside the scope of this thesis proper and they will not be dealt with in depth here.

79 In the recent *SyRi* case in the Netherlands, the general principles found in art 5 GDPR were used to establish the seriousness of an in-

this can be crucial for the protections offered to individuals and groups in public spaces.

1.4.5 Taking stock: Privacy in public space

Traditionally, privacy laws relied on spatial factors to determine where protections are warranted. At home, the quintessential private *place*, there is an overwhelming reasonable expectation that privacy is (or at least should) be protected, while in various types of public spaces such expectations may vary depending on evolving social norms and circumstances. Crowdsourced surveillance nowadays takes myriad and overlapping forms, and may have little regard for the space and privacy expectations from which data is being scraped. This may even in itself influence expectations of what may happen in a space. As legal safeguards are based around these reasonable privacy expectations, the protection of privacy in public space can be a knotty issue.

I have also discussed how the GDPR and the Law Enforcement Directive are aimed at protecting personal data in the wake of the rise of networked dataveillance. Predicated as these new technologies may be on (metaphorically ethereal) clouds, physical location remains of the essence as they have cast an unprecedented sensing net over public spaces. This presents heretofore-unforeseen challenges to the legal

interference with article 8 ECHR, further underscoring the blurring between the two legal regimes. See Rb. Den Haag 5 February 2020, ECLI:NL:RBDHA:2020:865 (*SyRi*), para 6.41.

data protection framework.⁸⁰ It is of the utmost importance to deal with these challenges, as personal data protection takes a central place in shielding citizens against contemporary dataveillance.

I have made clear that the determinants of what constitutes ‘privacy’ have become more complicated because of these new developments. Traditional considerations, based primarily on spatial factors – the home as the epitome of the private; elsewhere varying degrees of privacy and surveillance – are still valid, but are now modified by other factors. At the same time, personal data protection takes the ‘perso-

80 See further chapter 2 of this thesis. Note that in 1998 the European Commission of Human Rights declared a case involving a general complaint against public space CCTV inadmissible, as “all that can be observed is essentially public behaviour,” thereby effectively shutting down a large part of the legal debate. *Herbecq and the association “Ligue des droits de l’homme” v Belgium* (1998) 92-B DR 92. The recent rise in popularity of biometric recognition technologies seems to renewed the interest from the legal community in security cameras, however.

In the last few years, an increasing number of cross-disciplinary publications on privacy in public has appeared, making some inroads: e.g. Bryce Clayton Newell, Tjerk Timan and Bert-Jaap Koops (eds), *Surveillance, Privace and Public Space* (Routledge 2018); Tjerk Timan, Bryce Clayton Newell and Bert-Jaap Koops (eds), *Privacy in Public Space: Conceptual and Regulatory Challenges* (Edward Elgar Publishing 2017); Maša Galič, ‘Surveillance, Privacy and Public Space in the Stratumseind Living Lab: The Smart City Debate, beyond Data’ (2019) 68 *Ars Aequi* 570. Bryce Clayton Newell and Bert-Jaap Koops (eds

nalness' of data⁸¹ as the main criterion for determining what deserves protection. Yet, due the rise of crowdsourced surveillance technologies, *personal* data are now picked up on a large scale in *public* spaces. As I have shown, public spaces, personal data, and privacy protection have become intermeshed in entirely new and complex ways. It is this terra incognita that this dissertation aims to chart.

1.5 Outline

The body of this work is divided into four chapters, each of which is based on previously published work that I (co-) authored. In each of these chapters, a specific instance of crowdsourced surveillance is used as an analytical starting point. These analyses range from, and cross over between, the philosophical, geographical, sociological, and legal, depending on the nature of the case study at hand. Together, they bring into focus both the technological and organizational state of play today, and provide frameworks for thinking about how the technologies of tomorrow might need to be regulated.

First, attention will be paid to technologies that allow citizens to more easily share multimedia files and streams with law enforcement agencies. Various kinds of media and metadata, such as pictures, videos, and geo-location, can be attached to emergency reports to the police using dedicat-

81 In the words of article 4(1) of the GDPR: “relating to an identified or identifiable natural person (...); an identifiable natural person is one who can be identified, directly or indirectly.”

ed platforms, social networking sites, or general communication apps such as WhatsApp. Although potentially a very useful source of information, this also raises considerable concerns regarding surveillance and privacy in public spaces: it exhorts citizens to establish a supervisory gaze over anyone, at any time, and anywhere.

Chapter 2 analyses these concerns using theories from surveillance studies. It considers the (surprisingly high) applicability of panoptical theories by Foucault and others to the effects of increased visibility of citizens in public spaces. This analysis reveals how discriminatory tendencies might be introduced and exacerbated. Attention is then paid to Deleuze's 'societies of control' and related notions such as database surveillance, surveillance assemblages, and predictive policing. This analysis shows that the enrichment of emergency reports with media and metadata from smartphones can pressurize people into conformity, erode the presumption of innocence, and diminish societal trust. Furthermore, this process will disproportionality affect already disadvantaged groups and individuals.

Chapter 3 then looks at various smartphone apps and services which are available on the Google Play Store and encourage users to report where and when they feel they are in an unsafe or threatening environment. This user-generated content may be used to build datasets, which can show areas that are considered 'bad,' and to map out 'safe' routes through such neighbourhoods. Despite certain advantages for those who feel vulnerable in public spaces, this data in-

herently carries the danger that streets or neighbourhoods become stigmatized and already existing prejudices might be reinforced. Such stigmas might also result in negative consequences for property values and businesses, causing irreversible damage to certain parts of a municipality. Overcoming such an “evidence-based stigma” (even if based on biased, unreviewed, outdated, or inaccurate data) becomes nearly impossible and raises the question how such data should be managed.

In chapter 4, one of the possible uses of such data — mapmaking — is discussed in more depth. Maps are powerful communication tools, and mapmaking used to be a privileged affair. In recent times, this has changed as the above-mentioned “smart cities” have been outfitted with video, audio, and other kinds of “Internet of Things” sensing devices. The data-streams they generate can be combined with crowdsourced data (for instance of the kind discussed in chapter 3) to create a vast multitude of interactive maps on which individuals are constantly (re)grouped on the basis of abnormality, deviation, and desirability. Many have argued that under these circumstances personal data protection rights should be extended to groups.

However, group rights are an awkward fit for the current European data protection framework, which is heavily focused on individuals. One possible opening for better protection is offered by Data Protection Impact Assessments (DPIAs), which are mandatory to carry out when the ‘systematic monitoring of a publicly accessible area on a large

scale'⁸² necessary for mapmaking takes place. They form an opportunity to recognize the risks of e.g. discrimination at an early stage. Furthermore, by including representatives of local (disadvantaged) groups, the strong performative qualities of maps can offer occasions for groups of citizens in smart cities to proactively shape the environments in which they live. However, there are serious limitations. The inclusion of affected data subjects and their representatives is not mandatory and very costly. Establishing effective data protection for groups negatively impacted by mapmaking software thus seems nigh on impossible in lieu of substantial legislative change.

In chapter 5 we return to police–citizen interaction tools. 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 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 chapter studies the example of the Automon app and contributes to the existing debate on crowd-

82 GDPR (n 75), point (c) of art 35(3).

sourced 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 EU data protection standards.

Finally, the various insights from the chapters are combined in the conclusion, chapter 6. In it, the main findings of chapters 2–5 will be revisited and synthesized. Special attention will be paid to crowdsourced surveillance and its impact on public spaces and the rights to data protection and privacy. Urgent problems for human rights that reappeared at various points throughout the thesis will be identified. The thesis will end with suggestions for how these problems may be approached with a view to not only minimizing any infringements, but also ensuring the quality of our public spaces.

As the reader might have gathered at this point, this work encompassed and transcends many traditional academic disciplines. It covers topics familiar to law and surveillance studies, and flows seamlessly from one to the other.⁸³ Both of these disciplines come with their own methodological challenges: law can seem almost devoid of methodology,⁸⁴

83 Although the reader might recognize some points in the text where a switch between disciplines is made quite unceremoniously.

84 And if there is any, it's likely to amount to nonsense. See Felix S Cohen, 'Transcendental Nonsense and the Functional Approach' (1935) 35 Columbia Law Review 809.

and surveillance studies is itself a highly transdisciplinary effort⁸⁵ which started sociologically, but now incorporates elements from *inter alia* science and technology studies, psychology, media studies, geography, history, anthropology, gender studies, and philosophy. Combining these two fields in one thesis has led to a happy form of epistemological anarchism⁸⁶ that can challenge and inspire both authors and writes alike. Ultimately, it is hoped that the milkman from 1927, if he were to be transported to 2020, would have a better understanding of how privacy in public spaces is being transformed by crowdsourced surveillance after having read all those chapters. In his honour, might I suggest that a glass of milk might go along nicely with the chapters to come?

85 Torin Monahan and David Murakami Wood, 'Introduction: Surveillance as a Transdisciplinary Endeavor' in Torin Monahan and David Murakami Wood (eds), *Surveillance studies: A reader* (Oxford University Press 2018).

86 Term very loosely borrowed from Paul Feyerabend, *Against Method* (4th ed, Verso 2010).

**2. Emergency calls with a
photo attached: The effects of
urging citizens to use their
smartphones for surveillance**

Previously published as: Gerard Jan Ritsema van Eck, 'Emergency Calls with a Photo Attached: The Effects of Urging Citizens to Use Their Smartphones for Surveillance' in Bryce Clayton Newell, Tjerk Timan and Bert-Jaap Koops (eds), *Surveillance, Privacy, and Public Space* (Routledge 2018).⁸⁷ Some minor spelling and grammar errors have been corrected in, and a postscript has been added to this version.

87 I gratefully acknowledge the many helpful comments received from an anonymous reviewer and the editorial team of *Surveillance, Privacy and Public Space* which helped to strengthen the argument and provided various avenues for connecting the chapter to broader debates and literature. Many thanks are also due for the constructive feedback I received on early drafts of this chapter by Prof. Mifsud Bonnici. Early ideas for this chapter were presented in November 2015 at the Cyberspace '15 conference of the Masaryk University in Brno, Czech Republic, where I received several helpful comments.

Abstract

Various kinds of media and metadata, such as pictures, videos, and geo-location, can be attached to emergency reports to the police using dedicated platforms, social networking sites, or general communication apps such as WhatsApp. Although potentially a very useful source of information for law enforcement agencies, this also raises considerable concerns regarding surveillance and privacy in public spaces: It exhorts citizens to establish a supervisory gaze over anyone, at any time, and anywhere.

This chapter analyses these concerns using theories from surveillance studies. It considers the (surprisingly high) applicability of panoptical theories by Foucault and others to the effects of increased visibility of citizens in public spaces. This analysis importantly reveals how discriminatory tendencies might be introduced and exacerbated. Attention is then paid to Deleuze's 'societies of control' and related notions such as database surveillance, surveillance assemblages, and predictive policing. This analysis shows that the enrichment of emergency reports with media and metadata from smartphones can pressurize people into conformity, erode the presumption of innocence, and diminish societal trust. Furthermore, this process will disproportionality affect already disadvantaged groups and individuals. Policy makers are advised to implement enriched emergency reports carefully.

2.1 Introduction

With the rising popularity of smartphones, citizens are being offered increasingly fast mobile internet connections with exceedingly high or even non-existent data caps. At the same time, the quality of smartphone cameras is increasing rapidly. This means that, at least from a technical point of view, any citizen on the street could record high quality photographs or videos of emergencies and share them with the police instantaneously.

However, most emergency call centres are geared towards receiving phone calls, not photos and videos, from the public.⁸⁸ This means that, in situations where time is of the essence, all the capabilities that modern smartphones offer are suddenly rendered useless. To remedy this situation, various market parties, predominantly from the United States of America,⁸⁹ have recently started offering configurations that make it possible to receive and process reports based on a wider variety of media. Besides market parties developing standalone “instant police reporting applications” and the related infrastructures, federal institutions on both sides of the Atlantic are supporting similar projects. Most notable is a push to make the 911 emergency response system in the

88 See for a typical example of the predominance of voice calls for emergency situations the official app of the Dutch police which redirects the user to calling 112 when s/he tries to report an emergency: Nationale Politie, ‘Politie App’ <<https://www.politie.nl/app>> accessed 3 December 2015.

89 e.g. RapidSOS, ‘Haven’ (2016) <www.rapidsos.com> accessed 9 December 2016.

United States capable of allowing “digital information (e.g. voice, photos, videos, text messages) to flow seamlessly from the public, through the 911 network and eventually, directly to first responders;”⁹⁰ and an effort within the EU Horizon2020 research program to create “a solution including a new smartphone app and on-line portal which are capable of being deployed in any European city.”⁹¹ Finally, many police forces are exploring how they might leverage already established communication platforms, such as WhatsApp or Facebook, although doubts remain about the feasibility of using them for emergencies.⁹²

90 The National 911 Program, ‘The Future of 911’ (911.gov) <www.911.gov/futureof911.html> accessed 23 May 2016.

91 Community Research and Development Information Service, ‘Citizen Interaction Technologies Yield Community Policing (CITY-CoP)’ (CORDIS) <http://cordis.europa.eu/project/rcn/197273_en.html> accessed 12 November 2015; For related projects see also Community Research and Development Information Service, ‘Inspiring CITIZE Participation for Enhanced Community Policing AcTions (INSPEC2T)’ (CORDIS) <http://cordis.europa.eu/project/rcn/194895_en.html> accessed 18 May 2016; Community Research and Development Information Service, ‘TRusted, CITizen - LEA CoILaboratIon over SOcial Networks (TRILLION)’ (CORDIS) <http://cordis.europa.eu/project/rcn/194841_en.html> accessed 18 May 2016; Community Research and Development Information Service, ‘Unity’ (CORDIS) <http://cordis.europa.eu/project/rcn/194893_en.html> accessed 18 May 2016.

92 Nederlandse Omroep Stichting, ‘Contact Met de Politie? Stuur Een Appje!’ (NOS, 8 December 2016) <<http://nos.nl/artikel/2147234-contact-met-de-politie-stuur-een-appje.html>> accessed 9 December 2016.

2.1.1.1 Object of the current chapter

These developments should raise scholarly concern from those working in the field of surveillance studies. Each new configuration of surveillance capabilities introduces a new configuration of actors and their capabilities; opening up new strategies, new vulnerabilities and new avenues for resistance.⁹³ Interestingly, the smartphone enters the academic debate on surveillance mostly as an object that can be surveilled by (state) authorities or as a tool for sousveillance.⁹⁴ This is in line with the — until recently — minimal state efforts to engage citizens to actively use their smartphones to collect data on ongoing incidents. Additionally, those who did record such footage “did not feel a part of a surveillance network.”⁹⁵ This silence comes despite a wide range of possibilities that the ubiquity of smartphones presents to policy makers looking for new surveillance tools.⁹⁶

93 Josh Lauer, ‘Surveillance History and the History of New Media: An Evidential Paradigm’ (2012) 14 *New Media & Society* 566; Michel de Certeau, *The Practice of Everyday Life* (University of California Press 1984).

94 Paul Reilly, ‘Every Little Helps? YouTube, Sousveillance and the “anti-Tesco” Riot in Stokes Croft’ (2015) 17 *New Media & Society* 755; Timan and Albrechtslund (n 15) 856; Oliver Leistert, *From Protest to Surveillance: The Political Rationality of Mobile Media: Modalities of Neoliberalism* (PL Academic Research 2013).

95 Timan and Albrechtslund (n 15) 868.

96 For an artist’s rendition of such possibilities see for instance Christopher Nolan, *The Dark Knight* (Warner Bros 2008) which features a botnet which turns all smartphones in the fictional Gotham City into echolocation devices.

The object of this chapter, therefore, is to investigate the societal effects of instant police reporting applications for smartphones. Not only does this fill a lacuna in the current literature on surveillance and smartphones, it shows that such possibilities come at a cost: processing and storing the gathered information leads to a loss of privacy in public spaces, and exhorting citizens to act as police informants introduces discriminatory biases, pressures towards normalization, and chilling effects.

2.1.1.2 Overview of the current chapter

Theories from surveillance studies will be used to explore the societal effects of instant police reporting applications. The theoretical developments in the field of surveillance studies can be divided into three phases: panoptical, post-panoptical, and contemporary conceptualizations that focus on thorough applications and refinements of the theories developed in the previous two phases.⁹⁷ This chapter falls squarely in the latter category.

In the first section of the theoretical body of this chapter, entitled “Societies of discipline,” panoptical theories will be used to analyse the effects of instant police reporting applications. In the section entitled “Societies of control,” post-panoptical theories will be applied. Since the focus of this chapter is on societal effects, a third section is dedicated to discussing the implications for policy makers before turning to the conclusion.

97 Galič, Timan and Koops (n 5).

2.1.1.3 A note on terminology

Before engaging with the theoretical body of this chapter, it is necessary to delineate the exact phenomenon under scrutiny. Instant police reporting applications have not taken on any definitive form yet and, as such, no more than a working definition can be provided. For the purposes of this chapter, a preliminary definition of the term “instant police reporting app” (or application) will therefore be used to denote any scenario in which:

- a person acting in a private capacity uses a mobile computing or communication device (which is usually a smartphone); to
- communicate to a police control room data other than (only) voice or text data; about
- a current or very recent situation; for which
- quick police intervention is deemed necessary by said person, either to deescalate/end the situation or to apprehend any alleged transgressors (whether or not they have fled).

The data referred to in the second point could, for instance, be images (either still or moving⁹⁸), audio files, geolocation data, or combinations thereof. There may be no dedicated stand-alone mobile application involved in any step of such a scenario, as such communications might also take place in other software environments — for example, e-mail or in-

98 Note that the term “image” is used in this chapter to denote any still and/or a moving image material, i.e. both photo and video materials are covered by this term.

stant messaging apps. The term instant police reporting apps is used to cover all such scenarios to ensure consistency.

2.2 Societies of discipline

Michel Foucault was the first to describe the panopticon as a schema for the functioning of power. He based much of his analysis on Jeremy Bentham's infamous prison plans. In the short term, panoptic architectures endeavour to make their objects (be they prisoners, pupils, or the population as whole) potentially visible and thereby vulnerable to disciplinary intervention when they engage in behaviours deemed undesirable by the operators of the panopticon. In the long term, this vulnerability is internalized by the objects of the panopticon, consequently turning them into normalized "docile bodies." Foucault argued that power could function according to this efficient diagram not only in enclosed settings, but even in society at large. Such a generalized mode of social control is typical of what Foucault termed societies of discipline.⁹⁹

Foucault's ideas of the panopticon and panopticism became standard references in the field of surveillance studies. In recent scholarship, panoptical theories have been especially prevalent in studies on closed-circuit television (CCTV) systems¹⁰⁰ because they share a central working

99 Foucault (n 21) 209.

100 The term "CCTV system" is used in this chapter as a shorthand for any security camera system in a public space, as is common usage. The term is not meant to denote whether or not the circuits that

mechanism with the panopticon: a visibility to the gaze of invisible watchers. This “surprisingly similar” manner of operation suggests that the panopticon provides a valuable theoretical model for understanding visual surveillance in the contemporary city. However, various critics hold that there might be metaphors that are more suitable.¹⁰¹ The central question in this section is, therefore, whether and how the panoptical scheme can provide a deeper understanding of the working mechanisms of instant police reporting applications.

This section is divided into three sections. The first subsection 2.2.1 begins by investigating how smartphone applications for instant police reporting relate to panoptical theories in the short term and compares this to descriptions of the working mechanisms of CCTV in the academic literature. The second subsection 2.2.2 studies the long-term effects. In the final subsection 2.2.3, attention will turn to a possible empowerment of the users of instant police reporting applications in the panoptical diagram.

2.2.1 Short term effects: visibility

In a typical-use scenario of instant police reporting applications, the user would snap a photograph of a criminal act in progress, which would then be transmitted to a police con-

the security cameras are attached to are closed or (as is increasingly prevalent) interconnected to other systems.

101 Hille Koskela, “‘Cam Era’ — the Contemporary Urban Panopticon” (2003) 1 *Surveillance & Society* 292 and especially page 293 thereof where she gives a more detailed treatment of some of the critiques.

trol room and then retransmitted to officers on the street who might be able to immediately apprehend a suspect. This prompt police response is enabled by the visual nature of the material being shared: whereas a phone call to the emergency services would have resulted in the same flow of information, the nature of the information shared would be very different: rather than an image, a verbal or textual description of a suspect would be circulated.

The effectiveness of image sharing can be exemplified by considering the central person in Figure 2.1, a photograph taken with a smartphone in the centre of London. An accurate description of the central figure would be that of a male of average height with short hair, wearing a black suit and backpack, listening to white earphones. Phoning in this description to the police would probably yield very little actionable intelligence given the probable prevalence of persons fitting that description in central London. However, if the photo in question were to be circulated to police officers patrolling near where the photo was taken,¹⁰² the police might stand a much better chance at apprehending the suspect: his visibility renders him vulnerable to disciplinary intervention. What is thus most striking about the short-term effects of instant police reporting applications in relation to the workings of a panopticon is this very direct link between the visibility of the suspect and her or his vulnerability to disciplinary intervention.

102 Based on information provided by the reporter or location data appended to either the image or the report.

Figure 2.1: Photograph taken with an Apple iPhone 6 smart-phone.¹⁰³

103 Benjamin Welle, 'IMG_1264' (Flickr, 17 September 2015) <<https://flic.kr/p/A81u4w>> accessed 5 August 2019.

This mechanism is nearly identical to that of CCTV systems — perennial symbols for surveillance and the panopticon in particular. The efficacy of CCTV systems in crime reduction seems to be limited at best, however, for a number of reasons.¹⁰⁴ Although CCTV cameras watch over many public spaces, the triviality of the bulk of the collected footage means that the majority of the video streams are only ever watched by people retroactively and only if disturbances or crimes have been reported. In those cases where there are operators actively watching live camera footage at all times in the hopes of spotting a crime,¹⁰⁵ the monotony of the images leads them to engage in unproductive behaviours.¹⁰⁶ So-called “smart” CCTV systems are one strategy to alleviate these shortcomings, incorporating algorithms that automatically alert operators to disruptions of a normal state of affairs.

Although instant police reporting applications also present a filtered data stream, there are two salient differences.

104 Brandon C Welsh and David P Farrington, ‘Crime Prevention Effects of Closed Circuit Television: A Systematic Review’ (Home Office Research, Development and Statistics Directorate 2002) 252 <<http://webarchive.nationalarchives.gov.uk/20090410070401/http://www.homeoffice.gov.uk/rds/pdfs2/hors252.pdf>> accessed 20 May 2016.

105 It bears mention here that CCTV systems are often used by the police for myriad other purposes as well, such as providing a helicopter view of a developing situation and providing intel to officers on the scene. Such purposes are outside the scope of this chapter.

106 Tanguy le Goff, Virginie Malochet and Tiphaine Jagu, ‘Surveiller à Distance. Une Ethnographie Des Opérateurs Municipaux de Vidéo-surveillance’ (Institut d’aménagement et d’urbanisme 2011) 45.

First, the filter is formed by watchful citizens rather than by algorithms; this point will be returned to at length below. Second, the geographic reach of smartphones is limited only by that of their users, not by police budget constraints or bureaucratic and civic procedures regarding the placement of cameras. This means that the visibility of citizens vis-à-vis the police is heightened and geographically widened, and thereby the vulnerability to disciplinary intervention is increased.

2.2.2 Long term effects: normalization

The long-term effect of panopticism in Foucault's disciplinary societies is normalization. Over time, the knowledge that deviation is followed by punishment is internalized by the subjects and they no longer even consider deviating; the functioning of power has become independent of whether it is being exercised.¹⁰⁷ In this subsection, the focus will be whether the functioning of power through instant police reporting applications can become automatic enough to stop a potential transgressor from engaging in deviant behaviour.

A crucial first step is convincing subjects that they are always potentially visible to authorities with the ability to punish. It is trivial to convince anyone in the industrialized world that wherever others are present, smartphones are also present. However, convincing anyone that a smartphone constitutes, in terms of its abilities to summon the police, not only a potential call to an emergency number but

107 Foucault (n 21) 201.

also an image recording and streaming device might be less straightforward.

Whether such claims can be made convincingly will depend on whether widespread uptake of instant police reporting apps will take place. If regulatory pressure develops to require phone manufacturers to make such functionalities available (as is currently the case with regard to voice-based emergency calls¹⁰⁸), uptake would be nearly ubiquitous. However, regardless of such regulatory pressures, a part of the population might choose to frequently use instant police reporting apps, either because their occupations mean that they come into contact with illegal behaviour frequently, or because they have a strongly developed sense of civic duty¹⁰⁹ combined with a strict set of (moral, social, and/or legal) norms which are thus regularly violated.

108 Although no legal requirements exist in this regard, the standardization group ETSI requires emergency calls to always be possible from a mobile phone (except when it is turned off) since at least 1998, making it a de facto requirement on phone manufacturers. ETSI, 'Universal Mobile Telecommunications System (UMTS); LTE; Service Aspects; Service Principles (3GPP TS 22.101 Version 11.10.0 Release 11)' <http://www.etsi.org/deliver/etsi_ts/5C122100_122199/5C122101/5C11.10.00_60/5Cts_122101v111000p.pdf> accessed 26 January 2016.

109 Among the more intriguing examples in this category are people who fashion themselves superhero personas to fight crime. For many of them, reporting to the police is an important part of being a real-life superhero: Elaine Fishwick and Heusen Mak, 'Fighting Crime, Battling Injustice: The World of Real-Life Superheroes' (2015) 11 *Crime, Media, Culture* 335.

This suggests that the active user base will not reflect society at large, but will be made up of a subset of the population who can not only afford a smartphone with a mobile broadband subscription, but also choose to actively participate. This means that the potential long-term intensification of panoptical principles outlined above is only possible on the terms of these citizens.

2.2.3 An empowerment within the panopticon?

Rather than just an increase in the powers of the police (or, more broadly, the state security and safety apparatus), the reporting citizens are also endowed with certain powers by instant police reporting applications. This subsection will investigate how such an empowerment might take place and what the effects thereof might be.

Encouraging citizens to take an active role in panoptical schema is not a new idea. Bentham already opened the inner workings of his model prison to a scrutinizing public.¹¹⁰ Groombridge has sketched the notion of an “omnicon,” where the community, rather than a state agent, monitors the feeds from local CCTV cameras.¹¹¹ This would shield against the excesses of surveillance because it is easier to differentiate between normal and abnormal behaviour based on the con-

110 Foucault (n 21) 207.

111 Nic Groombridge, ‘Crime Control or Crime Culture TV?’ (2002) 1 *Surveillance & Society* 30, 43.

textual knowledge that neighbours have about each other.¹¹² Groombridge's preliminary sketch has been expanded by Goold with regard to how the footage from CCTV cameras in public spaces might be widely distributed and watched.¹¹³

Because these analyses predate the advent of affordable smartphone cameras and mobile broadband internet, they assume a privileged position for the state concerning the placement of cameras. Thus, their focus is on how the watching of visual surveillance material might change, rather than on the mechanisms used for collecting such material. However, it is at the stage of collection where instant police reporting applications introduce new processes that can empower citizens.

Such an empowerment within the panoptic diagram should be problematized. Compare, for instance, two studies of CCTV operators who received no training in identifying suspicious behaviour:¹¹⁴ French CCTV operators described by le Goff, Malochet and Jagu routinely engaged in discriminatory practices by concentrating disproportionately on (black) youth whose clothing and appearance signalled

112 *ibid* 42; Daniel Trottier, 'Crowdsourcing CCTV Surveillance on the Internet' (2014) 17 *Information, Communication & Society* 609, 621.

113 Benjamin J Goold, 'Open to All? Regulating Open Street CCTV and the Case for Symmetrical Surveillance' (2006) 25 *Criminal Justice Ethics* 3, 12–14.

114 These studies were selected not because training might have been a panacea for the problems presented, but because they offer examples that show some similarity with instant police reporting applications, insofar that their users will also be more-or-less untrained.

that they belonged to a “subversive” youth culture;¹¹⁵ British CCTV operators have shown similar behaviour — being male, young, black, or a combination thereof made visitors to city centres more than twice as likely to be the target of the scrutiny of operators than could be expected on the basis of their prevalence in either the general population or arrests statistics.¹¹⁶

Daniel Trottier points out that there is little reason to believe that surveillance amateurs will engage in less discriminatory behaviours, especially if they are instructed to be vigilant for suspicious activity.¹¹⁷ Consider, for example, the cases of *nextdoor.com*, a social networking site targeted towards supporting neighbourhood communication, and *Neighbors*, an app by Amazon which is tied to their Ring video doorbell. Despite their seemingly benign goals, the companies behind them have been battling accusations of facilitating racism, as many of the posts on the platforms relating to security incidents seem to involve at least a degree of racial profiling.¹¹⁸ It seems that in a politico-societal context of

115 le Goff, Malochet and Jagu (n 106) 26–29.

116 Clive Norris and Gary Armstrong, ‘CCTV and the Social Structuring of Surveillance’ (1999) 10 *Crime Prevention Studies* 157, 162–163.

117 Trottier (n 112) 622.

118 Pendarvis Harshaw, ‘Nextdoor, the Social Network for Neighbors, Is Becoming a Home for Racial Profiling’ (*Fusion*, 24 March 2015) <www.fusion.net/story/106341/nextdoor-the-social-network-for-neighbors-is-becoming-a-home-for-racial-profiling/> accessed 16 December 2016; Sam Levin, ‘What Happens When Tech Firms End up at the Center of Racism Scandals?’ (*The Guardian*, 30

responsibilizing “see something, say something” campaigns and moral governance towards personal risk reduction,¹¹⁹ ordinary citizens will rely on stereotypes when given a broad mandate to select any scene they come across for further police scrutiny. In the words of Bruce Schneier: ‘If you ask amateurs to act as front-line security personnel, you shouldn’t be surprised when you get amateur security.’¹²⁰

In conclusion, the functioning of instant police reporting can be panoptical. However, it is a panopticon that is partly run by, and on the potentially discriminatory terms of, the most frequent users.

September 2016) <www.theguardian.com/technology/2016/aug/30/tech-companies-racial-discrimination-nextdoor-airbnb> accessed 16 December 2016; Caroline Haskins, ‘Amazons Home Security Company Is Turning Everyone Into Cops’ (*Motherboard*, 7 February 2019) <https://motherboard.vice.com/en_us/article/qvyvzd/amazons-home-security-company-is-turning-everyone-into-cops> accessed 12 February 2019.

119 Sean P Hier, Kevin Walby and Josh Greenberg, ‘Supplementing the Panoptic Paradigm: Surveillance, Moral Governance and CCTV’ in David Lyon (ed), *Theorizing Surveillance: The Panopticon and Beyond* (Routledge 2006) 236; Joshua Reeves, ‘If You See Something, Say Something: Lateral Surveillance and the Uses of Responsibility’ (2012) 10 *Surveillance & Society* 235.

120 Bruce Schneier, ‘How We Won the War on Thai Chili Sauce’ (*Schneier on Security*, 1 November 2007) <https://www.schneier.com/essays/archives/2007/11/how_we_won_the_war_o.html> accessed 22 November 2018.

2.3 Societies of control

The role of databases containing troves of potentially incriminating personal data is crucial for understanding any contemporary surveillance technology, a point to which Gilles Deleuze's "Postscript on the Societies of Control" draws our attention.¹²¹ It is related to two other topics which he points out and which are of concern for this section: database entries containing information on identified or potentially identifiable individuals; and the effects that storing large numbers of (bits and pieces of) such data in rhizomatically connected, temporally open-ended, and ever-modulating databases can have on society. The central question in this section is therefore what the societal effects of storing data obtained through instant police reporting applications might comprise, and who will be targeted by these effects.

To answer this question, theories that can broadly be labelled as "postpanoptical"¹²² will be leveraged. In the first subsection 2.3.1, attention will be paid to whose data could be more likely to be included in databases as a result of instant police reporting. This question of addition to surveillance databases is fundamental; it determines who can be targeted and, conversely, who cannot be targeted by the possible societal effects to which attention will turn in the other subsections on anonymity (in 2.3.2), normalization (in 2.3.3), the presumption of innocence (in 2.3.4), and cumula-

121 (n 8).

122 Galič, Timan and Koops (n 5).

tive disadvantages resulting from simulation and prediction (in 2.3.5), respectively.

As will become clear throughout this section, the salience of post-panoptical theories depends on specific implementations and everyday uses that have not yet materialized at the time of writing. Therefore, this section needs to be more tentative than the previous section. Analogies with current surveillance practices are used where possible to infer possible future trajectories of instant police reporting applications.

2.3.1 Inclusion in databases

Surveillant assemblages, as introduced by Haggerty and Ericson and deeply influenced by Deleuze, are potentially endless multiplicities of objects and processes that form a functional unit for the purposes of surveillance. Such assemblages can be rhizomatically reassembled into ever-larger and modulating assemblages¹²³ However, a functional unit is needed which allows surveillant assemblages to be tied together: a database where the data about individuals who are deemed (at least) “of interest” are stored. In the next sections, we will discuss the centrality of such databases in determining the societal effects of instant police reporting applications.

Instant police reporting applications generate images for immediate police usage. If these images are of a certain minimum quality, they also record those “gaseous flows of

123 Haggerty and Ericson (n 5).

personal information” that bodies willingly and unwillingly emit.¹²⁴ An image of a body is thus also an image of the biometric characteristics of that body. Images therefore could facilitate the creation of (bits and pieces of) data about persons that is stored and analysed in digital databases. By making use of metadata appended to either the image or the report, location and other information could also be extracted and stored.

Ostensibly, this could happen to anyone who happens to walk by in the background of an image snapped for instant police reporting purposes: a quick glance at Figure 2.1 reveals many innocuous bystanders.¹²⁵ However, a closer investigation of two of the dynamics at play reveals that specific groups of people have a greater chance of being included in surveillance databases as a result of instant police reporting applications.

First, the influence of biases held by the reporting citizens, which was already discussed in subsection 2.2.3 on empowerment within the panopticon, has recurring salience here. Being young, dark-skinned, male, or visibly belonging to some marginalized group might increase the risk of being included in databases as a result of instant police reporting applications.

124 Gavin JD Smith, ‘Surveillance, Data and Embodiment: On the Work of Being Watched’ (2016) 22 *Body & Society* 108.

125 Since Figure 2.1 is only presented here for illustrative purposes, it should be mentioned that the central figure is probably also quite innocuous.

Second is the influence of the selection of, and by, frequent users. When someone is spotted whilst stealing from a cash register, it might be obvious that s/he needs to be reported to the police as this clearly concerns a criminal act. However, what about a drunken teenager? Should s/he be reported to the police? At what point does “drunk and disorderly” become a matter that should be brought to the attention of the police?¹²⁶ As was pointed out in subsection 2.2.2 on the long-term effects of the panopticon, the most avid users of instant police reporting applications will be those with a strong sense of civic duty combined with strict norms. Therefore, the thresholds for reporting and subsequent inclusion in databases in such ambiguous cases will be formed by the (moral, social, or legal) norms of those persons who have the lowest thresholds.

This means that those who frequently exhibit deviant behaviour in public spaces will more frequently end up in police databases, whether the behaviour in question was illegal or not. This will include those who unwittingly exhibit such transgressive behaviours: people diagnosed with mental disorders (including but not limited to, for instance, autistic or psychotic disorders), and “newcomers” to specific public spaces such as immigrants, young children, and

126 Foucault considered this an essential moment as it signals the move from illegality, which may be tolerated, towards delinquency, which should be corrected and normalized. Instant police reporting applications put this power in the hands of citizens. See Foucault (n 21) 277–78.

tourists who are not yet aware of the local mores. Because these groups are already under heightened scrutiny from various (state) authorities, the added scrutiny as a result of instant police reporting apps can exacerbate earlier harms. There are also those who wittingly exhibit transgressive behaviours: for instance, protestors — who will be discussed in subsection 2.3.3 on normalization and chilling effects.

2.3.2 Loss of anonymity vis-à-vis the police

An effect of the inclusion of data from instant police reporting applications in surveillance databases is that it might become easier for the police to identify who was doing what at a certain location, at a certain time, and with whom. This effect is presupposed in all of the other effects listed in the sections below and it is thus crucial to better understand it before moving on. In general, identification of suspects is one of the reasons for surveillance in public spaces, and the reports from instant police reporting applications form nothing more than a new source of material in this regard.

In order to facilitate identification after an instant police report has come in, readily available software can translate image data to (biometric) data, store it, and compare it to previously collected data. In this way, an operator who receives an image of a suspect can have a quick answer to the question “Has this person been photographed previously?” If no positive identification can be inferred, perhaps a link to

data collected earlier can be made, slowly but surely building a profile of an as-of-yet unnamed citizen.

Here the virtually endless potential for rhizomatic coupling of surveillant assemblages through the use of databases becomes apparent: if an algorithm can compile a database of (pieces of data about) individuals who may be of interest using images submitted through instant police reporting applications, a — separate but connected, or the same — database can also be populated using data from for instance smart CCTV cameras. Compare here the already long-established practice of holding on to “dumb” CCTV material for a limited period in order to be able search through them manually when a report comes in:¹²⁷ this would merely lend that process a mathematical hand. Furthermore, local, national (e.g. the Next Generation Identification database of the FBI), and international databases of wanted persons would form a logical addition here, as might databases maintained by private parties.¹²⁸

To conclude this subsection, this new source of data provided by instant police reporting applications brings not only a quantitative change (which might be rather small) but also a qualitative change: the selection of the data added could be skewed towards certain groups, as was pointed

127 le Goff, Malochet and Jagu (n 106) 41.

128 Ali Winston, ‘Los Angeles Sheriff Invests in New Tech to Expand Biometric Database’ (*Reveal*, 3 July 2015) <<https://www.revealnews.org/article/los-angeles-sheriff-invests-in-new-tech-to-expand-biometric-database/>> accessed 13 April 2016.

out in the previous subsection. Furthermore, the choice of who to add to the database is filtered by citizens on the lookout for transgressive behaviours. This might frame everyone captured in the submitted image as worthy of at least a cursory investigation, if not as a suspect then at least as a witness. Thus, having one's data included in surveillance databases as a result of instant police reporting heightens the chance of losing your anonymity vis-à-vis the police now or at a later point in time.

2.3.3 Normalization and chilling effects

An important effect of the possible addition of (potentially) identifiable data to surveillance databases as a result of instant police reporting applications is normalization. This subsection investigates what the substantive normalizing effects might be using post-panoptical theories.

The strict norms of the frequent users of instant police reporting applications might mean that acts which are illegal, but of which it is generally accepted that they go unpunished most of the time, will be reported to the authorities. Although there are probably not enough police officers to follow up on each minor infraction, this does not suggest that abundant reporting will be without consequences altogether. Primarily, data about offenders may be added to the local police database of “known offenders” that is only acted upon at a later point in time — for instance, if the number of transgressions by the same person becomes excessive. Furthermore, institutions faced with limited resources might

wish to automate the process of handing out fines for minor infractions using biometrics, in a manner similar to how many speeding tickets are currently issued using automatic number plate recognition (ANPR) software. Alan Westin predicted that such unfettering scrutiny would mean that “most persons in society would be [...] in jail.”¹²⁹ Although this might be overly pessimistic, the above does imply a normalizing pressure to not engage in petty illegal behaviour whenever others are present.

Because they engage in acts that are designed to attract substantial attention, protestors form an especially interesting category with regard to normalization. In order for them to succeed, they need to tiptoe around, and sometimes cross over, the edges of social, moral, and legal norms and do so in spaces where they are highly visible; an open invitation to instant police reporting users. Chilling effects on free speech occur when protestors are forced to consider whether their cause is more important to them than their existence (or lack thereof) in a police database: will I protest the new multi-storey parking garage, or will I remain anonymous to the police? Note that protestors have always had to consider such questions and that it might not influence the most determined amongst them. However, instant police reporting applications can also dramatically increase the visibility of

129 Alan F Westin, *Privacy and Freedom* (The Bodly Head 1967) 35.

more casual protestors, which increases their chances of being included in a police database.¹³⁰

2.3.4 The erosion of the presumption of innocence and social trust

Threats to the presumption of innocence and social trust arise when instant police reporting applications are construed as measures of mass surveillance. Such a construction may seem counter-intuitive at first: any recordings made are obviously targeted towards specific transgressive behaviours and those suspected of committing them. However, the ubiquity of smartphones means that the minutiae of everyday life can be captured and shared with the police at any moment. Coupled with the possibilities for virtually endless retention of data and the inherent biases of users, this means that for citizens (and especially those citizens in already marginalized positions) the effects of instant police reporting applications can be analogous to those of other mass surveillance measures: anyone can at any time be added to a database for the sole purpose of using the gathered data later during a possible investigation. Such a pre-emptive logic presents a threat to the principle of the presumption of innocence: data is gathered by the police without a specific suspicion, which

130 See also Christopher J Schneider and Daniel Trottier, 'The 2011 Vancouver Riot and the Role of Facebook in Crowd-Sourced Policing' (2012) 175 BC Studies 57.

shifts the burden of proof and dilutes the right to remain silent.¹³¹

Another effect of measures of mass surveillance is the corrosion of social trust in society. The co-optation of citizens in mass surveillance efforts, in particular, eats away at such interpersonal trust: citizens are asked to approach one another as possible suspects, and must take into account that they may be approached in this way by others as well.¹³² Maria Los relates such strategies explicitly to those employed by the internal security services of former communist states in Eastern Europe and points out the atomization of society which results: “[E]ach individual not only views all others as potential spies but must also be aware of being similarly viewed by others. This creates painful barriers of fear and humiliation that divide and terrorize society.”¹³³ One only needs to imagine what might happen if, during a wild night out in the city, someone in a group of friends takes out her/his phone to record a video. Tjerk Timan and Nelly Oudshoorn found that, in such situations, the primary concern of those documented was the dissemination of the materi-

131 Jonida Milaj and Jeanne Pia Mifsud Bonnici, ‘Unwitting Subjects of Surveillance and the Presumption of Innocence’ (2014) 30 Computer Law & Security Review 419.

132 Gary T Marx, ‘The Public as Partner? Technology Can Make Us Auxiliaries as Well as Vigilantes’ (2013) 11 IEEE Security & Privacy 56.

133 ‘Looking into the Future: Surveillance, Globalization and the Totalitarian Potential’ in David Lyon (ed), *Theorizing Surveillance: The Panopticon and Beyond* (Routledge 2006) 83.

al;¹³⁴ a concern which is currently mostly connected to the lack of control over privacy on social networking sites.¹³⁵ Add the police as a potential recipient and, in a society saturated with smartphones, such situations are apt to spiral out of control and lead to a loss of generalized societal trust.

2.3.5 Cumulative disadvantages resulting from simulation and prediction

All the effects pointed out so far in this section are most pronounced on those people whose data is collected in surveillance databases. As discussed above, their makeup is not neutral. This is deeply troublesome, as it means that citizens in already marginalized positions will be especially affected by the rhizomatic coupling of databases. This phenomenon is known as a cumulative disadvantage: a way in which past negative decisions tend to cluster future hardships on certain persons or groups.¹³⁶

- 134 Tjerk Timan and Nelly Oudshoorn, 'Mobile Cameras as New Technologies of Surveillance? How Citizens Experience the Use of Mobile Cameras in Public Nightscape' (2012) 10 *Surveillance & Society* 167.
- 135 Jesse Fox and Jennifer J Moreland, 'The Dark Side of Social Networking Sites: An Exploration of the Relational and Psychological Stressors Associated with Facebook Use and Affordances' (2015) 45 *Computers in Human Behavior* 168, 171–72.
- 136 Oscar HJr Gandy, 'Quixotics Unite! Engaging the Pragmatists on Rational Discrimination' in David Lyon (ed), *Theorizing Surveillance: the Panopticon and Beyond* (Routledge 2006) 319; Oscar HJr Gandy, 'Exploring Identity and Identification in Cyberspace' (2000) 14 *Notre Dame Journal of Law, Ethics & Public Policy* 1085, 1100–01.

Related to and overlapping with cumulative disadvantages are the final and perhaps most nebulous effects of the accumulation of identifiable and potentially identifiable data as a result of instant police reporting applications: the effects related to simulation and prediction. A photograph taken with a smartphone is an altogether different beast than a Polaroid, and mostly so because of the metadata embedded in the photo itself or in the message used to send the photo. These include time and location that might be important for the purposes of prediction; they are two of the three data points used by PredPol,¹³⁷ one of the most widespread commercial software packages that police forces can use to guestimate when and where crimes might take place and thus where police presence is needed.

However, inputting data obtained from instant police reporting applications into such predictive algorithms runs the risk of reifying user biases. Such software influences the surveillance discretion of the police, e.g., when and where they will be looking for crime.¹³⁸ If users consistently send in reports from certain areas, the police will, given enough prods by the algorithm, inevitably find crime there. This retroactively justifies the many reports, and will in turn lead to

137 The final data point being the type of crime. 'How Predictive Policing Works: We Provide Guidance on Where and When to Patrol' (*PredPol*, 2015) <<http://www.predpol.com/how-predictive-policing-works/>> accessed 9 May 2016.

138 Elizabeth E Joh, 'The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing' (2016) 10 *Harvard Law & Policy Review* 15.

even more patrolling and more biased data being fed into the algorithms.¹³⁹ As a result, the individuals and communities living in neighbourhoods where a relatively high number of reports are being filed will suffer from a further amplification of the surveillance tax — the chilling effects and negative social stigma that results from increased crime and police scrutiny.¹⁴⁰

2.4 Policy implications

This chapter has a clear focus towards the future: instant police reporting applications (at the time of writing) are not yet a widespread phenomenon. Throughout the theoretical body of this chapter, formed by the previous two sections, various strands of ideas and arguments surfaced which may critically shape the future of citizen involvement in crime fighting using smartphones. Three implications follow from this chapter for policy makers who wish to gain from instant police reporting applications the highest possible reduction

139 Such loops might very well negate the possible advantage which predictive algorithms present for creating a more equitable distribution of surveillance discretion. Elizabeth E Joh, 'Discretionless Policing: Technology and the Fourth Amendment' (2007) 95 California Law Review 199; Elizabeth E Joh, 'Policing by Numbers: Big Data and the Fourth Amendment' (2014) 89 Washington Law Review 35, 58.

140 Joh, 'The New Surveillance Discretion' (n 138) 32; Alessandro Mantelero, 'Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection' (2016) 32 Computer Law & Security Review 238, 240.

in criminality combined with the highest level of human rights protection possible.

A first implication, which follows from the panoptical diagram, is that the widespread uptake of instant police reporting applications will be critical in determining whether possible transgressors will modify their behaviour. Lobbying standard-setting organizations to grant instant police reporting functionalities the same status as emergency calls seems to be the most effective option here. Another important actor in the promotion of instant police reporting applications might be the mass media in the broadest sense possible. They provide the narratives through which people make sense of surveillance¹⁴¹ and, as such, can directly and indirectly affect potential transgressors. If potential transgressors are confronted with stories in which a criminal has been caught on the basis of smartphone reporting – and attach some value to these stories¹⁴² – they might decide not to proceed. The media can also influence possible transgressors indirectly, by presenting smartphone apps for instant police reporting to the general public as an essential tool for personal safety and thus contributing to their widespread uptake.

141 Dietmar Kammerer, 'Surveillance in Literature, Film and Television' in Kirstie Ball, Kevin D Haggerty and David Lyon (eds), *Routledge Handbook of Surveillance Studies* (Routledge 2012) 99.

142 Aaron Doyle, 'Revisiting the Synopticon: Reconsidering Mathiesen's "The Viewer Society" in the Age of Web 2.0' (2011) 15 *Theoretical Criminology* 283.

Second, many of the negative effects outlined in section 2.3 ‘Societies of control’ above are a result of overzealous reporting. These effects can be dampened if the police employs its discretionary power once a report has been filed not just to decide if officers on the ground are dispatched, but also to decide how the personal data from the report will be handled.¹⁴³ Operators receiving reports (whether emergency call-takers or specialized operators) should select individuals from images for addition to databases, rather than outsourcing this process to an algorithm that might add anyone. Although more costly in the short term, this can ensure the privacy of bystanders and somewhat dampen the cumulative disadvantage which results from the discriminatory biases of app users. In the long run, this will heighten the acceptance of instant police reporting applications, resulting in more and more valuable usage of the apps. Here, the role of the media must again be emphasized: instant police reporting applications should be promoted as tools only to be employed in life-or-death situations similar to emergency telephone numbers in order to prevent overzealous reporting.

Finally and most importantly, continued and careful attention to vulnerable groups is warranted throughout the operation of instant police reporting applications. Especially the re-use of the data obtained through instant police reporting applications should be approached with extreme caution. In the section above, only one potential effect of the use of data from instant police reporting applications

¹⁴³ Compare here also note 126.

for the purposes of prediction has been discussed, but the possibilities for re-use are manifold. However, any dataset (even partly) based on instant police reporting should be considered biased from the outset, which invariably taints the results from any subsequent analyses. Basing policies on such results is ill advised, and risks instituting discriminatory procedures.

2.5 Conclusion

This chapter set out to investigate the societal effects of instant police reporting applications for smartphones using theories from surveillance studies. The chapter was split in two following Deleuze's claim that the societies of discipline as described by Foucault have been superseded by societies of control.¹⁴⁴ His analysis is often taken to mean that any theoretical study of contemporary surveillance using panoptical schemas is essentially flawed. However, this may be too simplistic:¹⁴⁵ this chapter has shown that the combination of both panoptic and post-panoptic theoretical frameworks can, if applied critically and carefully, enhance and broaden our understanding of a surveillance phenomenon.

At the time of writing, instant police reporting applications are an emerging phenomenon. It might be that instant police reporting applications will lead a life lingering in the depths of various app repositories to be installed from time to time but rarely used. However, that law enforcement

144 Deleuze (n 8) 3.

145 Simon (n 5) 2.

agencies will have increasing amounts of visual recordings of suspicious behaviours made available to them — whether through dedicated platforms, social networking sites, or email — by the general public and that the possibilities for analysis and storage of such materials are growing seems evident. The results from this chapter therefore have broader relevance.

Instant police reporting applications request that we trust fellow citizens to judge whose anonymity may be sacrificed to facilitate the work of the police — holders of the exclusive right to intra-territorial violence in order to maintain social order. The section 2.2 ‘Societies of discipline’ has demonstrated the power that potential users of such apps wield. However, with great power there must also come great responsibility.¹⁴⁶ The extent of this responsibility was established in section 2.3 ‘Societies of control’ where the societal effects of the loss of anonymity were discussed: pressures towards conformity, the chilling of free speech, the erosion of social trust and the presumption of innocence, and how these might disproportionately affect already disadvantaged individuals and groups. An essential question, which can and should not be answered in an academic publication, but in the public debate, thus remains: how great is the power and responsibility that we are willing to grant the public in supporting the police in the execution of their tasks?

146 Stan Lee, ‘Spider-Man!’, *Amazing Fantasy #15* (Marvel Comics 1962).

2.5.1 Avenues for future research

There are certain questions that do belong in the academic debate. This chapter has sketched out what the societal effects of instant police reporting applications might be in the very near future, and there is abundant room for more in-depth research. This subsection lists, non-exhaustively, various avenues for future research in multiple academic fields, but much interdisciplinary work also remains. Independent of the field of research, a special sensitivity towards possible discriminatory tendencies is warranted.

What is needed first and foremost is continuing scrutiny to document how instant police reporting applications, or more generally, the ways in which citizens make visual recordings available to the police, will advance in the coming years. Especially interesting will be a Science and Technology Studies approach focused on specific implementations to study how the developments described in this chapter will play out on the streets, and how the user base of such apps will develop. The sensitivity of Science and Technology Studies to non-use¹⁴⁷ is also interesting from a policy perspective: what are prohibiting and facilitating factors for citizens and police officers in the context of the use of instant police reporting applications? Will users engage in acts of trolling, for instance by flooding the system with meaningless pictures, and how will police forces respond to such behaviour?

147 Lynsey Dubbeld, 'Telemonitoring of Cardiac Patients: User-Centred Research as Input for Surveillance Theories' in David Lyon (ed), *Theorizing Surveillance: The panopticon and beyond* (2006) 192.

Related to this question is the perhaps more criminological concern: are there certain transgressions that lend themselves especially well to reporting using smartphones? If there are, how does that influence the execution of police tasks and the distribution of police resources? Think here for instance of the obvious discrepancies in visibility between public intoxication and white-collar fraud: will differences in visibility between various crimes shift police resources in ways which favour or disfavour certain groups? Moreover, could citizens turn this process on its head to give more visibility to crimes they deem important, for instance through collective actions?

Another topic that will merit assiduous dissection in the years to come is the role of the private sector in the development and ongoing support of instant police reporting applications. This chapter has focused on the relationship between the police and citizens as their respective roles are, to a certain degree, foreseeable. However, any part of the analysis presented here could be deeply influenced by the involvement of the private sector, which is already taking a lead in related technologies. For example, Vigilant Solutions maintains a database of over 2 billion ANPR readings,¹⁴⁸ and Taser International provides a hosting solution for the videos made with their popular Axon police body-worn camer-

148 Vigilant Solutions, 'LPR Data' <www.vigilantsolutions.com/wp-content/uploads/2014/08/LPR_Data_AUG2014_LFS.pdf> accessed 15 December 2016.

as.¹⁴⁹ It thus seems likely that these or similar companies will also play an important role in instant police reporting applications. However, this raises profound questions: what are the judicial and democratic controls on them? What will the bargaining position of states and local police departments be, both during initial negotiations and once a system has been deployed? Furthermore, do companies stand to gain from incentivizing use, financially or otherwise, and how will this influence the effects instant police reporting applications have on society? Thorough analysis using the surveillant assemblage theoretical framework seems especially suited for investigation of these highly relevant and under-researched questions.

This chapter has analysed possible societal consequences of instant police reporting apps using theories on surveillance and social control. Although perhaps only a small shift, an analysis focused on privacy rather than surveillance might highlight how instant police reporting apps impact other processes including, for instance, identity building.¹⁵⁰ Such an analysis is especially salient with regard to teenagers who engage in complex privacy behaviours vis-à-vis authority figures and institutions¹⁵¹ but who are largely de-

149 David Gelles, 'Taser International Dominates the Police Body Camera Market' (*The New York Times*, 12 July 2016) <www.nytimes.com/2016/07/13/business/taser-international-dominates-the-police-body-camera-market.html> accessed 15 December 2016.

150 Cohen, 'What Privacy Is For' (n 6).

151 danah boyd and Alice E Marwick, 'Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies', *A Decade in Internet*

pendent on public spaces to escape the gaze of parents and educational institutions.¹⁵² They may feel that their spaces for identity formation are being threatened by technophilic police forces in cahoots with overzealous citizens, but more considerate scrutiny is needed. Attention to the rhizomatic tying of surveillance assemblages is needed in this context as such linkages may lead to “context collapse,” in which the carefully separated private spaces of teenagers start meshing.¹⁵³ The role that social networking and sharing platforms play in the lives of teenagers and young adults deserves special attention in this regard.¹⁵⁴

Instant police reporting applications also offer an impetus for further research by cultural geographers who address the role of popular mobile communication and computation technologies in the experience of spaces.¹⁵⁵ Their perspective on the implications of the active involvement of state actors (and specifically those state actors with a claim to force) in such intimate and quotidian technologies could

Time: Symposium on the Dynamics of the Internet and Society (2011)
 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128> accessed 23 March 2016.

152 Carissa Véliz, ‘In the Privacy of Our Streets’ in Bryce Clayton Newell, Tjerk Timan and Bert-Jaap Koops (eds), *Surveillance, Privacy, and Public Space* (Routledge 2017) 18.

153 boyd and Marwick (n 151).

154 Schneider and Trottier (n 130); Timan and Albrechtslund (n 15).

155 For a more general call for increased attention to popular mobile technologies in cultural geography see Samuel Kinsley, ‘Vulgar Geographies? Popular Cultural Geographies and Technology’ (2016) 17 *Social & Cultural Geography* 793.

enhance our understandings of contemporary cities, saturated as they are with smartphones and security concerns. Particularly interesting might be a study of how the erosion of social trust is spatially distributed: is it more prevalent in, e.g., public transport, where “see something, say something” campaigns are already widespread, or are such effects larger in spaces that are traditionally less associated with security threats?

Finally, legal scholars might consider the impact of instant police reporting applications on data protection frameworks. The meshing of citizen and police roles problematizes the often strict separation between data collecting and processing regimes for private persons and law enforcement agencies. Concepts such as notification and consent, which are central to data protection frameworks for non-governmental purposes around the globe, seem inept to deal with the dual pressures of technology and security:¹⁵⁶ should users of instant police reporting applications literally shout across the street to inquire if criminals consent to being filmed?

2.6 Postscript

Generals always prepare for previous wars, and scholars always study outdated technologies. The original ideas for this chapter were formed at the end of 2015, and the first draft

156 Kevin D Haggerty, ‘What’s Wrong with Privacy Protections? Provocations from a Fifth Columnist’ in Austin Sarat (ed), *A World without Privacy: What Law Can and Should do* (Cambridge University Press 2015).

was completed during the summer of 2016. In March 2019, the Dutch emergency call centres adopted Advanced Mobile Location, which establishes and shares the precise location of a caller based on either WiFi or Global Positioning System signals.¹⁵⁷ At the same time, experiments are ongoing to include live video feeds into the workflow of these centres.¹⁵⁸ Thus, there appears to be a trend towards integrating functionalities like those described in this chapter into the existing emergency response framework rather than providing a separate application.

157 Nederlandse Omroep Stichting, 'Politie kan 112-beller met Android-telefoon beter lokaliseren' (*NOS*) <<https://nos.nl/1/2275680>> accessed 15 March 2019.

158 Charlotte Van den Berg, 'Videobellen Naar 112?' (*JenV Magazine*, December 2018) <<https://magazines.rijksoverheid.nl/jenv/jenvmagazine/2018/04/dit-is-nu>> accessed 15 March 2019.

**3. Mobile devices as
stigmatizing security sensors:
The GDPR and a future of
crowdsourced 'broken windows'**

Previously published as: Oskar Josef Gstrein and Gerard Jan Ritsema van Eck, ‘Mobile devices as stigmatizing security sensors: the GDPR and a future of crowdsourced ‘broken windows’ (2018) 8(1) International Data Privacy Law 69 (doi: 10.1093/idpl/ipx024).¹⁵⁹ Some minor updates have been made to reflect recent judgements by the CJEU.

159 The authors contributed equally to this work. The authors gratefully acknowledge the assistance of various colleagues who helped by pointing us to and providing additional information about the various apps mentioned in this chapter: at the University of Groningen Prof. Mifsud Bonnici and Frank Pace; and at the University of Malta Dr. Iain Reid. They also Thank Zoe Condcliffe of Plan Australia for providing them with additional information about the Free to Be app. The authors also wish to thank Karen P. Mohan for her careful language check.

Abstract

Various smartphone apps and services are available that encourage users to report where and when they feel they are in an unsafe or threatening environment. This user-generated content may be used to build datasets, which can show areas that are considered ‘bad,’ and to map out ‘safe’ routes through such neighbourhoods. Despite certain advantages, this data inherently carries the danger that streets or neighbourhoods become stigmatized and already existing prejudices might be reinforced. Such stigmas might also result in negative consequences for property values and businesses, causing irreversible damage to certain parts of a municipality. Overcoming such an ‘evidence-based stigma’ — even if based on biased, unreviewed, outdated, or inaccurate data — becomes nearly impossible and raises the question how such data should be managed.

3.1 Introduction

Nobody wants to live in a bad neighbourhood but, alas, some of us do. It is inevitable: where there are ‘better’ neighbourhoods, there must also be neighbourhoods that are deemed poor, unsafe, or even dangerous. However, such perceptions can change over time: some neighbourhoods ‘improve’ through the efforts of city councils, investors, and inhabitants whereas others slowly become dilapidated for various reasons.

It is generally very difficult to assess the quality of a neighbourhood. Such ‘verdicts’ are mostly based on one or

several personal opinion(s). However, what if socially constructed views are aggregated into datasets that are immune from the wear and tear of time? On the one hand, there could be a more accurate, evidence-based view on local conditions. On the other hand, inhabitants and local businesses could become trapped in stigmas based on datasets outside of their control. Does such data merely reflect a social situation in a public space, or does it amount to personal data? This question merits attention as companies and local governments are starting to collect, store, analyse, and publicize such data, specifically related to feelings of fear and insecurity.

The authors of this chapter aim to investigate how sets of such geo-tagged user-generated content might negatively impact neighbourhoods and the communities and individuals living within them, especially when data is misinterpreted, becomes ‘out-dated’, inaccurate or irrelevant over time. This chapter will discuss whether possible legal remedies to such problems can be found in the new European Data Protection Framework¹⁶⁰, which will gain binding force in the member states of the European Union (EU) in May 2018.

The authors will argue that the free development of personality needs to be taken into consideration carefully when using such data. It is necessary to observe whether effective safeguards and remedies are in place to protect individuals who are indirectly subject to such technologies. Under certain circumstances, data-based statements about

160 Consisting of the General Data Protection Regulation (GDPR) (n 75); and the Law Enforcement Directive (n 76).

a neighbourhood might easily be used or abused to describe an individual once s/he has been connected with the area concerned. In addition to individual privacy concerns, the chapter also ties in to broader debates concerning the protection of privacy for groups—specifically the communities living in neighbourhoods.

This chapter will make observations on this subject by investigating several websites and smartphone applications (apps) which encourage their users to report where and when they feel that they are in an insecure or threatening public space. Such crowdsourced content may be used to build datasets that can show streets and neighbourhoods that are considered ‘bad’.

In the following section 3.2 various websites and apps in this field will be described. Then, ethical and other consequences of their use will be discussed in section 3.3. In the penultimate section 3.4 it will be analysed whether there are legal remedies in the new EU Data Protection Framework for those who are negatively impacted by evidence-based stigmas. Finally, the conclusion in section 3.5 will provide an overview and deliver some final thoughts on ways forward.

3.2 Websites and apps

Numerous websites and apps¹⁶¹ ask users to share geotagged reports describing (inter alia) feelings of fear. The apps pre-

161 Note that the distinction between websites and apps is blurred at times: some apps function as overlays for websites, and many of the websites described are ‘responsive’ ie are easily accessible and navi-

sented in this section have been chosen because of the diversity of actors that have initiated and supported them, and the multiplicity of purposes for which the data has been gathered. The geographical origins of each app have not been considered in the selection process, although the section 3.4 ‘Legal analysis’ is targeted towards EU Data Protection law (for reasons noted there). As most of the apps are available for take-up around the globe, including in the EU, they — or apps very similar to them — could potentially influence public spaces everywhere. Because a small number of apps are discussed in some detail, the specific sociotechnical affordances¹⁶² of the apps have served as a selection criterion, rather than their geographical origins. In other words, by not limiting the examples to the EU, the authors hope to be able to provide a richer palette of examples.

The apps presented below form interesting case studies because they invite users to specifically share feelings of fear and unsafety. However, they are not the only services on which such feelings are actively being shared and from which they can thus be harvested by interested parties. Currently,

gable using a browser on either a smartphone or a desktop computer. Furthermore, many systems offer different functionalities on smartphones (either browser-based or in apps) than on desktop computers, but utilize the same underlying infrastructure and databases.

162 Affordances are ‘the perceived and actual properties of the thing, primarily those fundamental properties that determine just how the thing could possibly be used’ and ‘provide strong clues to the operations of things’. Donald A Norman, *The Design of Everyday Things* (Basic Books 2002) 3.

there is a growing academic and industry interest in using geo-tagged posts to social media sites such as Twitter and Facebook to establish ‘hot spots’ where crimes might occur in the (near) future.¹⁶³ This is sometimes also referred to as an innovative form of collecting open source intelligence.¹⁶⁴ Williams, Burnap and Sloan even propose to consider Twitter users as ‘sensors’ that can track criminal activities and inform law enforcement about minor public offences such as ‘broken windows’.¹⁶⁵ This usage of data from social networking sites generates largely analogous challenges to the ones discussed in this chapter.

Note that the purpose of this section is not to provide a definitive overview of the most popular (or even all) apps

163 Johannes Bendler and others, ‘Investigating Crime-to-Twitter Relationships in Urban Environments—Facilitating a Virtual Neighbourhood Watch’, *Proceedings of the European Conference on Information Systems (ECIS)* (2014); Matthew S Gerber, ‘Predicting Crime Using Twitter and Kernel Density Estimation’ (2014) 61 *Decision Support Systems* 115; Nick Malleson and Martin A Andresen, ‘The Impact of Using Social Media Data in Crime Rate Calculations: Shifting Hot Spots and Changing Spatial Patterns’ (2015) 42 *Cartography and Geographic Information Science* 112; Matthew L Williams, Pete Burnap and Luke Sloan, ‘Crime Sensing with Big Data: The Affordances and Limitations of Using Open Source Communications to Estimate Crime Patterns’ [2016] *British Journal of Criminology* 320.

164 Kim Miller, ‘How to Collect Open Source Intelligence’ (*In Homeland Security*) <<http://inlandsecurity.com/how-to-collect-open-sourceintelligence>> accessed 17 August 2017.

165 Williams, Burnap and Sloan (n 163) 321.

currently available in this field.¹⁶⁶ Furthermore, the authors cover the essential features, but do not endeavour to create a detailed analysis of each app. Finally, the authors do not intend to present any of these services as worthy or insufficient offers; nor do they recommend or not recommend their use for further development.

3.2.1 Free to be

The 'Free to Be' project, which ran from 13 October to 31 December 2016, collected geotagged data describing where young women in Melbourne, Australia, felt safe or unsafe. The project was initiated and paid for by Plan Australia, which is part of Plan International, an NGO most well known for its longstanding 'Sponsor a child' programme. The company Crowdspot,¹⁶⁷ that specializes in crowdsourcing of geospatial information, provided the app and other technical infrastructure based on OpenStreetMap data.¹⁶⁸

166 For an overview of apps aimed at rape prevention see Rena Bivens and Amy Adele Hasinoff, 'Rape: Is There an App for That? An Empirical Analysis of the Features of Anti-Rape Apps' (2018) 21 *Information, Communication & Society* 1050

; For an overview of how mobile phones mediate feelings of fear in public see Kathleen M Cumiskey and Kendra Brewster, 'Mobile Phones or Pepper Spray?: Imagined Mobile Intimacy as a Weapon of Self-Defense for Women' (2012) 12 *Feminist Media Studies* 590.

167 CrowdSpot, 'Featured Projects' (*CrowdSpot*) <<http://crowdspot.com.au/>> accessed 22 February 2017.

168 OpenStreetMap Foundation, 'OpenStreetMap' (*OpenStreetMap*) <<https://www.openstreetmap.org/>> accessed 22 February 2017.

Users could add a ‘happy spot’ or a ‘sad spot’ on a map of Melbourne, and attach a description of an incident or a photograph of the area.¹⁶⁹ During the data collection (and for a short while afterwards) a map showing all happy and sad spots was publicly available through the app and through a web browser. Besides warning other users of spaces that may be ‘dodgy’ and pointing out which routes might be safer, the collected data will also be shared with local stakeholders in the hopes of inspiring them to make changes to the physical environment.¹⁷⁰ Furthermore, the data is being shared with the Monash University in Melbourne in order to analyse the data.¹⁷¹

3.2.2 My Safetipin

This project was founded with the aim of enabling vulnerable persons (especially young women) to be able to understand security risks in their neighbourhoods better, and collects data to this end (Figure 3.1). Although the app was

169 Lauren Day, ‘Free To Be Online Map Shows Where Women Feel Unsafe in Melbourne’ (*ABC News*, 8 December 2016) <<http://www.abc.net.au/news/2016-12-08/free-to-be-online-map-shows-where-women-in-melbourne-feel-unsafe/8103410>> accessed 3 February 2017.

170 Olivia Lambert, ‘New Map Reveals Dangerous Areas for Women after Dark’ (*News.Com.Au*, 27 October 2016) <<http://www.news.com.au/lifestyle/real-life/news-life/new-map-reveals-dangerous-areas-for-women-after-dark/news-story/ac74124366927004dd09838cd278a-ba8>> accessed 3 February 2017.

171 Email from Zoe Condliffe of Plan Australia to authors (8 February 2017).

works, or passes through regularly). For these circles, the user frequently receives updates on the security situation.

The app presents information about lighting and visibility (to determine if others can see the user when s/he crosses an area) and rates openness (to determine if the user can see around). It rates the diversity (presence of women and children), how crowded, and how close a place is to public transport. Finally, it shows the position of law enforcement agencies and allows users to share how safe they feel. Additionally, users can share their location with trusted contacts. Users can also react to submissions of others by confirming or contesting the accuracy or relevance of reports.¹⁷²

Particularly interesting about this app is its attempt to shape the behaviour of both its users and policymakers. Users receive suggestions for safe walking routes, and are alerted when they enter an 'unsafe' area in order to allow them to modify their behaviour accordingly. Policymakers are targeted by putting the issue of safety (particularly safety for women when they use public transport or walk somewhere after office hours) in the public spotlight and by providing crowdsourced data to them.¹⁷³

172 For more information see 'My Safetipin: Personal Safety' (Google Play, 7 April 2017) <<https://play.google.com/store/apps/details?id=com.safetipin.mysafetipin>> accessed 29 May 2017. The app is also available for iOS devices.

173 'Safetipin' (*Apps that keep you safe*) <<http://safetipin.com/>> accessed 29 May 2017. Aggregated data on the 'safety score' of neighbourhoods is also available through this website.

Figure 3.2: Screenshot by the authors of a map of Manhattan, Queens, and Brooklyn as seen on the Trulia real estate website. The map has been overlaid with crime data from SpotCrime and various ‘for sale’ properties.¹⁷⁴

174 Trulia, ‘Queens and Viewable Map Area Homes For Sale & Real Estate’ (NY Real Estate & Homes for Sale) <https://www.trulia.com/for_sale/40.632112163148,40.829316775872,-74.026498761825,-73.762826886825_xy/12_zm/#map-crime> accessed 22 July 2017.

3.2.3 SpotCrime and Crime Maps

SpotCrime is a predominantly USA focused website which publicizes data on crimes. The data is supplied by local law enforcement agencies, collected from news sources, and the public can submit tips through crimetip.us.¹⁷⁵ It publishes this data on CrimeSpot.com, where users can look up the 50 most recent crimes in a given area on a map¹⁷⁶ and set e-mail alerts for crimes reported in a 5-mile radius of an address. The information provided by SpotCrime is limited to the location, time, type, and sometimes a short description of the crime, and shown overlaid on Google Maps.¹⁷⁷

Notably, the data from SpotCrime is used by the Trulia real estate website, on which each listing is accompanied by a ‘Crime score’ ranging from lowest to highest, which can be clicked in order to get historic data about the most recent 2500 crimes in the area (Figure 3.2).¹⁷⁸

175 SpotCrime, ‘Crime Tips’ (*Submit a crime tip*) <<https://crimetip.us/>> accessed 15 February 2017.

176 Email from costumer representative “Michelle” of SpotCrime to authors (15 February 2017).

177 Google Inc., ‘Google Maps’ (*Google Maps*) <<https://www.google.nl/maps>> accessed 22 February 2017.

178 Trulia, ‘Trulia Launches Crime Maps to Add Insights and More Complete Data to American Neighborhoods’ (*News Room*, 2 June 2011) <<http://info.trulia.com/press-releases?item=106144>> accessed 14 February 2017.

A very similar app that is targeted to Brazil is Crime Maps.¹⁷⁹ Since most of the features mirror the ones just presented, this app will not be discussed individually.

3.2.4 GeoEstrela, MeldStad, and Ir-Raħal Tagħna

Various municipalities are starting to offer their citizens ways to report rubbish and damaged street furniture through mobile and desktop interfaces, usually accompanied by promises that reports will be quickly — or at least quicker than before the system was launched — dealt with. Even though such systems lie somewhat outside the focus of this chapter, which is apps that can be used to report fear, they merit inclusion for at least four reasons: primarily because the harms to the reputation of a specific area are similar, although perhaps less serious; because the number of such systems seems to be growing; because the involvement of municipalities might lend the reports extra credibility; and because within community surveillance efforts aimed at increasing safety, improving the quality of life using such apps is often seen as an integral part of the programme, rather than something which serves a distinct function.¹⁸⁰

179 For more information visit ‘Crime Maps’ (*Google Play*, 21 September 2016) <<https://play.google.com/store/apps/details?id=com.rdr.map-scrimes.lite>> accessed 29 May 2017.

180 Anaïk Purenne and Grégoire Palierse, ‘Towards Cities of Informers? Community-Based Surveillance in France and Canada’ (2017) 15 *Surveillance & Society* 79, 82–5.

In this subsection, three such systems will be introduced: the *GeoEstrela* system from Lisbon in Portugal, the *MeldStad* system from Groningen in the Netherlands, and the *Ir-Raħal Tagħna* system from Malta.

In the civil parish of Estrela in Lisbon of about 20,000 inhabitants, citizens can report issues such as broken street furniture, loose cobblestones, weed, faded road markings, rubbish and dog faeces through the *GeoEstrela* website.¹⁸¹ The geotagged reports are shown overlaid on Google Maps on a publicly available website and stored (seemingly) indefinitely. Citizens can attach up to three photos to their report, and the civil parish services attaches a photo once the situation has been cleaned or repaired, which the reporting user is notified of through e-mail. The system, which was launched in late 2014, had at the time of writing received over 5000 reports, of which more than 70 per cent had been resolved.¹⁸²

A similar service exists in the city of Groningen, the Netherlands: *MeldStad*, although the sort of information that can be submitted is broader: not only broken street furniture or dog faeces can be reported, but also dangerous road crossings and spots where speeding occurs regularly (Figure

181 Note that there is no separate *GeoEstrela* app, but that the website is optimized for reporting when accessed using a smartphone.

182 Junta de Freguesia da Estrela, 'GeoEstrela' (*GeoEstrela*) <<https://www.jf-estrela.pt/caap/app/gso/>> accessed 13 February 2017.

Figure 3.3: Screenshot taken using an Android smartphone by the authors of a map of the city centre of Groningen, The Netherlands, as seen in the *Meldstad* app. Outstanding reports can be seen overlaid as pushpins.

3.3).¹⁸³ Finally, requests for items such as playgrounds can also be submitted through MeldStad. Citizens can send their reports through a website, dedicated iOS and Android apps, or a WhatsApp number. All outstanding reports are visible on a proprietary map that is publicly available, but disappear once the report has been dealt with.¹⁸⁴

A similar app that aims at improving the communication between public administration and the population has just been rolled out in the EU's smallest member state, Malta. The *Ir-Raġal Tagħna* (or 'Our Kind of Town') app is set 'to make it easier for citizens to report any problem from any spot, without the need to go personally to their respective local council'.¹⁸⁵ At the time of writing, it had been rolled out in the area of St. Paul's Bay and was available on the Google Play Store.

183 Note that some time after the original publication of this chapter, the municipality stopped using the Meldstad app. It has been replaced by the *Slim Melden Groningen* app, developed and maintained by the external company Civity. The app also has bespoke versions used in Utrecht, Velsen, Deventer, Zaanstad, and Monnickendam.

184 Gemeente Groningen, 'Gebreken in Uw Buurt Melden' (*Gemeente Groningen*) <<https://gemeente.groningen.nl/gebreken-en-overlast-melden>> accessed 13 February 2017; Gemeente Groningen, 'Meldingen Groningen' (*MeldStad*) <<http://fleximap.groningen.nl/gnmaps/meldingen/>> accessed 13 February 2017.

185 Nikita Kozlov as quoted in 'Our Kind of Town' (*Times of Malta*, 26 February 2017) <<http://www.timesofmalta.com/articles/view/20170226/technology/Our-kind-of-town.640852>> accessed 13 March 2017.

3.2.5 WayGuard

This app is available for iOS and Android. It was launched in 2016 by the German subsidiary of the insurance corporation AXA and designed in cooperation with the local police of Cologne, Germany.¹⁸⁶

Once installed, a user gets the opportunity to share the current location of the device with the ‘WayGuard Team’ and persons of trust like family members, partners, or friends. The app enables communication to persons of trust via a call or a chat function. Users can also be notified when a target, like someone’s home, has been reached. Finally, should an emergency occur, an emergency call can be made easily through a dedicated function of the app. The WayGuard Team will then know the precise location of the user and notify the police.

Furthermore, the app provides information how to behave when walking or cycling to a destination or when using public transport. This content is provided in cooperation with the police of Cologne. The app has won an award for ‘best security app’ in the year 2016 awarded by a German magazine.¹⁸⁷

186 AXA Konzern AG, ‘WayGuard: Begleit-App Für Ein Gutes Gefühl Unterwegs’ (Wayguard, 2016) <<https://www.wayguard.de/>> accessed 6 February 2017.

187 ‘Die Besten Apps Des Jahres 2016 – Teil 1/7’ (Androidmag, 2 November 2016) <<http://androidmag.de/app-reviews/die-besten-apps-des-jahres-2016-teil-1/>> accessed 27 February 2017.

3.3 Potential concerns

At the start of this section it must be stated that the services presented above have different purposes, feature different designs, and are being operated in different cultural and societal circumstances. This is important to bear in mind, as contextual factors such as time, space, place, economy, and technology are crucial when it comes to the fundamental human right to privacy.¹⁸⁸

However, there are also numerous parallel characteristics that are interesting to observe: first, all of these services have in common that they address issues of safety and fear in public spaces. Secondly, they represent innovative configurations — or: assemblages¹⁸⁹ — of smartphones and internet-based services. Thirdly, there is a tendency of combining several sources of data with each other to get a more complete picture of the situation in an environment, community or a neighbourhood. These sources include user inputs, news reports, law enforcement data like crime statistics, and others. Fourthly, major aspects of the assessment of a situation are based on individual perceptions of people in specific situations. Finally, most of these services are used on experimental or semi-experimental bases. None of them had be-

188 Joseph A Cannataci, 'Report of the Special Rapporteur on the Right to Privacy' (31st Human Rights Council, 3 August 2016) <<http://www.ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc>> accessed 27 February 2017; Helen Fay Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 *Washington Law Review* 119.

189 Haggerty and Ericson (n 5).

come well-established services with a large commercial or publicly highly relevant impact at the time of writing.

Despite the diversity of the examples presented in the previous section 3.2, their parallel characteristics mean that their usage might lead to similar, and sometimes serious, problems. We build upon the apps presented above to discuss six salient scenarios.

First, data of pseudo- or anonymous users obtained through such apps might be aggregated and combined with other records and datasets. Sometimes those might be publicly available, such as reports published by law enforcement agencies on crime statistics in the case of CrimeSpot. Potentially, non-public sources could also be used, if they are available for purchase, compromised – e.g. hacked – or available to a state authority that is legally entitled to access them even if they were originally created for other purposes. This is concerning because it cannot be guaranteed that an individual remains unidentifiable if she/he wishes to.¹⁹⁰

190 In order to present a clearer conclusion on the state of arts in this area the UN Special Rapporteur on the right to Privacy, Joseph A Cannataci, intends to work on a Thematic Action Stream entitled ‘Big Data and Open Data’. For more information see Joseph A Cannataci, ‘Parallel Streams of Action (TAS) for the Mandate of the UN Special Rapporteur for Privacy and the First Set of Priorities’ (*Privacy and Personality: a forum exploring perspectives on privacy and other fundamental rights*, 3 June 2016) <<https://www.privacyandpersonality.org/2016/06/privacy-and-personality-blog-3-parallel-streams-of-action-tas-for-the-mandate-of-the-un-special-rapporteur-for-privacy-and-the-first-set-of-priorities/>> accessed 8 March 2017.

Research with medical records and studies with credit card information have shown that it is surprisingly easy to single out individuals from large and (seemingly) pseudonymized or anonymized sets of data.¹⁹¹

Additionally, there seems to be significant interest and resources to improve data analytic techniques. Hence, it might be the case that a method for pseudo or anonymization works for the moment, but not in the future. This is very worrying for users who report feeling vulnerable and at risk of victimization.

As will be discussed in the legal analysis in more detail, the new EU Data Protection Framework provides safeguards for data once it qualifies as “personal” in line with the legal definition. However, what seems concerning are those instances in which data that doesn’t fit the legal definition of personal data does allow for the extraction of general behavioural patterns or conclusions regarding situational circumstances once it is combined with data from other sources. Although data analytic techniques marketed as “big data”, “open data”, “artificial intelligence” and “deep learning” are rapidly evolving to make this ever easier, the legal frameworks largely fail to address these potential concerns.

191 For the medical sector see the work of Latanya Sweeney. For example ‘Only You, Your Doctor, and Many Others May Know’ [2015] Technology Science <<http://techscience.org/a/2015092903>>. For the medical sector see the work of Latanya Sweeney. For example ‘Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata’ (2015) 347 Science 536.

This is particularly worrisome if decisions are based on the combination of data sources in the absence of societal experience or legitimate knowledge on how to combine such sources to actually predict human behaviour.¹⁹² The discussion on implicit or ‘baked-in’ discrimination when employing smart or autonomous decision-making is currently just beginning to take shape on a broad interdisciplinary level¹⁹³

192 This problem has also been discussed in connection with the use of proprietary software (‘COMPAS’) in the United States of America. In order to help judges make decisions on probation conditions of individuals the software suggested a probability score which should reflect how likely a person would commit another crime in the future. After a critical investigation of the results of the software there were claims that it discriminates against black defendants. The claim was denied by the development company. The score was based on a questionnaire which did not include questions on race, but there was also not sufficient testing if the questions would result in biased scores. More discussion can be found at Julia Angwin and others, ‘Machine Bias’ (*ProPublica*, 23 May 2016) <<https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>> accessed 17 August 2017; Oskar Josef Gstrein, ‘How to Approach Technology, Human Rights and Personality in the Digital Age? – A Few Thoughts’ (*Privacy and Personality*, 24 October 2016) <<https://www.privacyandpersonality.org/2016/10/how-to-approach-technology-human-rights-and-personality-in-the-digital-age-a-few-thoughts/>> accessed 17 August 2017.

193 In Germany for example, a Civil Society Organization with the title ‘Algorithm Watch’ has been founded recently. To read more about the initiative see Matthias Spielkamp, ‘Inspecting Algorithms for Bias’ (*MIT Technology Review*, 12 June 2017) <<https://www.technologyreview.com/s/607955/inspecting-algorithms-for-bias/>> accessed 18 August 2017. In the USA the ‘AI NOW initiative’ strives to

and will be discussed further below. Nevertheless, there seems to be an overwhelming economical and political desire to roll out these technologies on an unprecedented scale as fast as possible in order to reap the economic gains.

Secondly, any technology we use makes us increasingly traceable by state or corporate actors through the burgeoning surveillant assemblage operating in public spaces, especially in areas saturated with high-tech infrastructure.¹⁹⁴ The re-identification, already pointed to above, of either the user of the app or others might also facilitate further tracking, behavioural profiling, and monitoring.¹⁹⁵ This decreases

contribute to develop a better understanding of the social impacts of Artificial Intelligence. It also issues annual reports with recommendations 'AI NOW' (AI Now Institute, New York University) <<https://ainowinstitute.org/>> accessed 8 November 2017. One of the authors of this chapter has presented on the issue at a Special Workshop of IVR 2017 World Congress in Lisbon entitled 'New Technology and (Non-)Human Agency: Risks, Responsibilities and Regulation'.

194 See for citizens' perspectives and scenarios Linnet Taylor and others, 'Customers, Users or Citizens? Inclusion, Spatial Data and Governance in the Smart City' (Maps4Society Final Project Report 2016) <<http://ssrn.com/abstract=2792565>> accessed 23 March 2017.

195 Online tracking might be associated mainly with cookies and IP addresses. However, it is also possible to use other methods such as the combination of certain characteristics of a device (operating system, screen resolution, web browser and version number, etc.). Steven Englehardt and Arvind Narayanan, 'Online Tracking: A 1-Million-Site Measurement and Analysis' (2016) <http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf> accessed 23 March 2017. For a (currently patched) example of how aspects that one might not consider can make one trace-

the options for staying private in public both quantitatively (i.e. the amount of public spaces in which privacy is possible) and qualitatively (i.e. the extent to which privacy can be achieved in those spaces). Easily accessible spaces of privacy where personal development is possible under less societal restraints are essential,¹⁹⁶ as is the availability of a modicum of privacy in public.¹⁹⁷

However, this seems currently threatened more than ever due to technological and societal developments.¹⁹⁸ Most people carry electronic sensors permanently in their pockets or on their wrists in the forms of smartphones, watches, or other wearables that can track their wearers and those around them.¹⁹⁹ This creates environments in which surveillance is so ubiquitous as to become ambient.²⁰⁰ This leads to a hollowed out expectation of privacy in public.²⁰¹ The apps

able see Lukasz Olejnik and others, 'The Leaking Battery: A Privacy Analysis of the HTML5 Battery Status API' [2015] International Association for Cryptologic Research (e-Print archive) <<https://eprint.iacr.org/2015/616.pdf>> accessed 22 February 2017.

196 boyd and Marwick (n 151); Cohen, 'What Privacy Is For' (n 6).

197 Nissenbaum (n 189) 139; Westin (n 129) 35.

198 Newell, Timan and Koops (n 80); Marja Beckers, 'Absender Unbekannt' [2017] *Hohe Luft* 54.

199 Ivo Flammer, 'Genteel Wearables: Bystander-Centered Design' (2016) 14 *IEEE Security & Privacy* 73.

200 For a similar argument in the online world, see Joel R Reidenberg, 'The Transparent Citizen' (2015) 47 *Loyola University Chicago Law Journal* 437.

201 Joel R Reidenberg, 'Privacy in Public' (2014) 69 *University of Miami Law Review* 141.

under scrutiny form an especially interesting category of artefacts, as they encourage citizens to actively use these sensors and upload data on safety and fear. This raises the stakes for anyone captured in the shared (meta-)data.²⁰²

This phenomenon could be referred to as ‘technological gentrification’. Similar to areas in communities which see a steep rise in rents and real estate prices because there is a rapid growth in investment capital, ubiquitously deployed surveillance infrastructure deprives the large majority of individuals of the opportunity to develop freely and equally. Hence, community areas that are ‘technologically gentrified’ will solidify social structures up to a level where the potential of individual and collective development will be drastically reduced.

Thirdly, a potential concern in the use of such technologies is how they might lead to prejudices against communities by presenting (aggregated) individual feelings or sentiments. Although this makes them seem ‘evidence-based’, they are based on incomplete and biased datasets. There is the danger that the sample of users of an app like ‘WayGuard’, for example, is too small to be used as a basis for a verdict. Furthermore, not only the amount of data might be concerning, but also the portion of society (e.g. mostly

202 Gerard Jan Ritsema van Eck, ‘Emergency Calls with a Photo Attached: The Effects of Urging Citizens to Use Their Smartphones for Surveillance’ in Bryce Clayton Newell, Tjerk Timan and Bert-Jaap Koops (eds), *Surveillance, Privacy, and Public Space* (Routledge 2018). Republished in this thesis as chapter 2.

young, female or male, techsavvy etc.) which contributes to the dataset might be concerning.²⁰³ Ultimately, there is the issue of discrimination in the data collection: when prodded to watch for suspicious behaviour, people disproportionately rely on stereotypes²⁰⁴ to decide whom and what is ‘out of the ordinary’; which is decidedly different from the legally prescribed category of suspicion.²⁰⁵ Thus, areas with more young, black males²⁰⁶ might receive more negative reviews than warranted. Also, note here that low-income and ethnically diverse neighbourhoods tend to participate less in on-line platforms like *GeoEstrela*, thus skewing the data even further.²⁰⁷ The picture that emerges from crowd-generated content is thus not an objective photograph, but rather an impressionistic painting.²⁰⁸

203 For a broader discussion and empirical examples on the basis of Twitter usage, see Luc Anselin and Sarah Williams, ‘Digital Neighborhoods’ (2016) 9 *Journal of Urbanism* 305, 305; Eszter Hargittai, ‘Potential Biases in Big Data: Omitted Voices on Social Media’ (2020) 38 *Social Science Computer Review* 10.

204 Norris and Armstrong (n 116).

205 Sebastian Larsson, ‘A First Line of Defence? Vigilant Surveillance, Participatory Policing, and the Reporting of “Suspicious” Activity’ (2017) 15 *Surveillance & Society* 94.

206 Norris and Armstrong (n 116) 162–3.

207 Burak Pak, Alvin Chua and Andrew Vande Moere, ‘FixMyStreet Brussels: Socio-Demographic Inequality in Crowdsourced Civic Participation’ (2017) 24 *Journal of Urban Technology* 65.

208 AT Crooks and others, ‘User-Generated Big Data and Urban Morphology’ (2016) 42 *Built Environment* 396.

In general, it is questionable if subjective feelings should serve as a basis to come to a verdict about (parts of) communities. The neighbourhood that one person finds inspiring and important, sometimes is unsafe and unsound for another. In that context, it might be interesting to remember that quarters like Montmartre in Paris or Friedrichshain in Berlin, which are ‘established’ or ‘hip’ at the moment, have both had a reputation for being less fancy and at times very unsafe. With the passing of time, both of them have managed to increase their reputation and became quarters that are sought after and even famous. Hence, the question arises whether it is favourable to collect and disseminate data that marks areas for being very dangerous or unsafe. Can such stigmas still be overcome if they are backed up by widely available data?²⁰⁹

Fourthly, there is the issue of repurposing of data. Data created by such services may be sold or resold by corporations and become subject to business models that can lead to negative and potentially illegitimate effects affecting the dignity of persons living or working in any area covered by the app in question. Less dramatic might be repurposing of the data that is in line with the legal framework, but still questionable.

Concerned individuals are often unaware of the practices and existence of data brokers, which sell or re-sell data to support marketing efforts, mitigate risks, or facilitate the

209 Lefebvre (n 36), especially page 165 thereof.

search for people.²¹⁰ One example that is frequently reported is credit scoring, which is sometimes heavily based on the postal code a person is registered under.²¹¹ In the USA, where this type of business is very developed, some authors call for legislative measures that increase transparency and accountability. The ultimate goal is to give individuals — who are typically consumers — more control over data that relates to them.²¹² In Europe, the Commission of the EU has set new initiatives at the beginning of 2017 to assess the impact and potential of commercial exploitation of nonpersonal data that is not covered by the new Data Protection Framework. These ‘next steps towards a European data economy’ include an assessment of the activities of data brokers.²¹³ Both of these initiatives remain nationally or regionally limited and tied to economic regulation.

The question remains what happens when some of this data is traded or transferred across global regions. Trans-border data flows regulation should generally be considered

210 Stephen Beake (ed), *Data Brokers and the Need for Transparency and Accountability* (Nova Publishers 2014).

211 This is a problem in connection with the larger issue of trading personal data; Barbara Wimmer, ‘Adresshandel: Das Geschäft Mit Unseren Persönlichen Daten’ (*futerezone*, 1 December 2015) <<https://futurezone.at/netzpolitik/adresshandel-das-geschaef-mit-unseren-persoেনlichen-daten/100.371.363>> accessed 27 February 2017.

212 Beake (n 211) 56.

213 European Commission, ‘Commission outlines next steps towards a European data economy’ (2017) IP/17/5.

from a perspective of legal pluralism.²¹⁴ However, the lack of a specific legally binding international framework for the sale and re-sale of data makes it likely that regional and international human rights frameworks will remain the starting points to address concerns arising from cross-regional transfer or commercial exploitation of such data.

Efforts to build cross-regional bridges based on mutual legal assistance and reciprocity, such as the EU–US ‘Safe Harbour’ and ‘Privacy Shield’ regimes, have their difficulties in withstanding the temptations of extraterritorial application of specific laws of the respective partners.²¹⁵ Hence, it

214 Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013).

215 The EU–US Safe Harbour regime (Decision 2000/520/EC) was declared void by a judgment of the CJEU in case C–362/14 *Maximilian Schrems v Data Protection Commissioner* EU:C:2015:650 (*Schrems I*). It was then replaced with the Privacy Shield ((EU) 2016/1250). However, there remained severe scepticism on the European level whether Privacy Shield lives up to its promises. The influential Article 29 Working Party issued a statement on 13 June 2017 in which it requests more evidence that the guarantees are actually kept: ‘Preparation of the Privacy Shield Annual Joint Review’ <http://ec.europa.eu/newsroom/document.cfm?doc_id=45272> accessed 18 August 2017. Some courts in the US require international corporations such as Google to hand over personal data to US authorities regardless where they are stored, see e.g. *Matter of Search of Content Stored at Premises Controlled by Google Inc*, No 16-MC-80263-RS, 2017 WL 3478809 (ND Cal Aug 14 2017). See also Daniel R Stoller, ‘Google Must Turn Over Data Stored Abroad Sought Under U.S. Warrant’ (*Bloomberg Law: Privacy and Data Security*, 15 August 2017) <<https://www.bna.com/google-turn-data-n73014463160/>> accessed 18 August 2017. While

remains to be seen how much needed international standards and rules will evolve.

Additionally, if data remains in the public domain for an indefinite amount of time it is questionable how it will be used by different governmental actors. This is becoming increasingly topical considering the vast amount of data created for various purposes. There exist drastic historic examples of how this had negative effects on parts of societies in the past.²¹⁶

For example, the Netherlands had a very comprehensive population registration system before they were invaded by Nazi Germany in 1939. After the regime change, the specific and precise data was abused to enable many Jewish deaths.²¹⁷ Looking at the kind of data being gathered by apps such as those described in the previous section 3.2, one could imagine it being used to justify repressive policies against certain neighbourhoods and the communities living in them.²¹⁸

Google will most likely attempt to bring this issue in front of the US Supreme Court it is not unlikely that similar decisions will be made by courts in the future. After publication of the article on which this chapter is based, the Privacy Shield decision was indeed declared invalid by the CJEU in Case C-311/18 *Data Protection Commissioner v Facebook Ireland and Maximilian Schrems* EU:C:2020:559 (*Schrems II*).

216 William Seltzer and Margo Anderson, 'The Dark Side of Numbers: The Role of Population Data Systems in Human Rights Abuses' (2001) 68 *Social Research* 481.

217 *ibid* 486–8.

218 For a poignant example of how repressive regimes can present poor neighbourhoods and the communities living in them as creating so-

Fifthly, there might be various financial harms. Real estate owners might be facing decreasing property values if potential buyers are scared away by high levels of reported fear in certain areas. Trullia, the second most popular real estate website in the USA,²¹⁹ already provides such a score for each property listed based on SpotCrime data. Furthermore, shops and other businesses operating in a certain area might face a slinking away of their patronage.

A sixth point of concern emerges if besides potential homebuyers, law enforcement agencies also start using user-generated data to inform their decisions and deploy resources. It is easily imaginable that ‘predictive policing’ — which has law enforcement agencies using software to simulate the needs of a community for policing and which uses factors like past crime statistics, weather predictions, etc. — might also include the data from services like WayGuard.²²⁰

In a positive light, this could be seen as responding to citizens’ needs. However, there might also be downsides. First, such patrolling might create a self-fulfilling prophecy:

cietal injustices, rather than being the result of them, see Mustafa Dikeç, ‘Police, Politics, and the Right to the City’ (2002) 58 *GeoJournal* 91.

219 ‘Top Sites by Category: Regional/North America/United States/Business and Economy/Real Estate’ (*Alexa*) <http://www.alexa.com/topsites/category/Regional/North_America/United_States/Business_and_Economy/Real_Estate> accessed 29 March 2017.

220 ‘How Predictive Policing Works: We Provide Guidance on Where and When to Patrol’ (n 137).

there will be more arrests in areas with a higher police presence,²²¹ which consequently justifies the negative reports and increased surveillance,²²² which in turn further damages the reputation of a certain area without targeting the root causes of crime.²²³ However, even if no arrests are made, increased police surveillance can by itself already inhibit free expression, movement, and unconventional behaviour, especially in already marginalized communities with strained relations to law enforcement agencies.²²⁴ We will not come back to this point as a European framework concerning the use of police data for predictive policing is currently lacking.²²⁵ However, the need for a public debate and awareness of the use of such data seems evident.

221 For a similar argument in the data of big context analytics, see Joh, ‘Policing by Numbers’ (n 139).

222 Julia van Heek, Katrin Arning and Martina Ziefle, ‘The Surveillance Society: Which Factors Form Public Acceptance of Surveillance Technologies?’ in Markus Helfert and others (eds), *Smart Cities, Green Technologies, and Intelligent Transport Systems* (Springer International Publishing 2017).

223 Taylor Shelton, ‘The Urban Geographical Imagination in the Age of Big Data’ (2017) 4 *Big Data & Society* 205395171666512.

224 Joh, ‘The New Surveillance Discretion’ (n 138) 31–2; Mantelero, ‘Personal Data for Decisional Purposes in the Age of Analytics’ (n 140) 240.

225 Francesca Bosco and others have detailed, as an example of the lack of harmonization, the opaque framework of ‘hardly comprehensible’ rules regulating the myriad German police databases: ‘Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities’ in Serge Gutwirth, Ronald Leenes and Paul de Hert (eds), *Reforming*

3.4 Legal analysis

After flagging some concerns regarding the apps and services the authors presented in the previous section, this section will aim at providing a legal analysis of the situation. However, this cannot be done without putting such an effort in context.

As a reference framework, the revised European Union Data Protection Framework²²⁶ will be used, which is about to become legally binding in May 2018. The choice of this framework is useful because the situation in Europe will be more strongly harmonized than at the time of writing of this document. This will result in a situation with less national differences in regulation between European countries. Additionally, at its core this text is an international text that

European Data Protection Law, vol 20 (Springer Netherlands 2015) 14–5. The courts in both Luxembourg and Strasbourg have not had ample opportunity yet to develop case law on the subject, see Rosamunde van Brakel and Paul de Hert, ‘Policing, Surveillance and Law in a Pre-Crime Society: Understanding the Consequences of Technology Based Strategies’ (2011) 20 *Cahiers Politicistudies* 163, 185. Finally, see Orla Lynskey, ‘Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing’ (2019) 15 *International Journal of Law in Context* 162. The closest to a legal framework comes the non-binding Council of Europe Recommendation CM/Rec(2010) 13 of the Committee of Ministers to member states on the protection of individuals with regard to the automatic processing of personal data in the context of profiling <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId1409000016805cdd00> accessed 11 August 2017.

226 See footnote 160.

seems useful when considering potential general problems arising from the use of apps that relate to security and fear. Furthermore, the new legal texts might be considered as benchmarks when it comes to the achievements of legislative activity in the area that might also be interesting for other regions of the global community.²²⁷ Another formal argument for choosing the European Union Data Protection Framework as a reference framework is Article 3 of the General Data Protection Regulation (GDPR), which results in an exceptionally broad territorial scope. According to Article 3 paragraph 2 lit b, a controller or processor of personal data is subject to the regulation if it is operating outside of the EU, but the handling of personal data relates to a data subject whose behaviour takes place within the Union. Ultimately, since the texts of GDPR and the Law Enforcement Directive have been adopted recently in April 2016,²²⁸ one would hope that the issues presented by the current state of technological development are addressed entirely or at least sufficiently.

Because the data gathered by the operators of the apps and services can be used by private and public authorities (particularly law enforcement agencies; LEAs) the GDPR and Directive (EU) 2016/680 of the European Parliament

227 European Commission, 'Joint Statement on the Final Adoption of the New EU Rules for Personal Data Protection' <http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm> accessed 24 March 2017.

228 *ibid*; GDPR, art 99; Law Enforcement Directive, art 65.

and of the Council of 27 April 2016 (Law Enforcement Directive) will be considered. However, before going into specific legislation, it is useful to look at the bigger legal picture.

3.4.1 Personal data as ‘Resource’?

In order to motivate her nation to be more dynamic in the area and leave the old paradigm of ‘purpose limitation’ behind, German Chancellor, Angela Merkel, has been referring to data as ‘the resource of the 21st century’.²²⁹ Indeed, corporations like Alphabet Inc., the parent company of Google, Facebook, and others²³⁰ have created economic imperia based on the creation, storage, analysis, and commercialization of personal data.²³¹ Furthermore, public administrations are under increasing pressure to become more cost effective, efficient, and responsive. One of the possible strategies to achieve this is the automation and standardization of internal and external communication. In short: the private and public sector are increasingly using automated personal data processing to improve their performance.

229 ‘Merkel: Daten Sind Rohstoffe Des 21. Jahrhunderts’ (*heise online*, 11 February 2015) <<http://www.heise.de/newsticker/meldung/Merkel-Daten-sind-Rohstoffe-des-21-Jahrhunderts-2867735.html>> accessed 6 March 2017.

230 ‘G Is for Google’ (*Alphabet*) <<https://abc.xyz/>> accessed 6 March 2017; ‘Facebook – Log In or Sign Up’ (*Facebook*) <<https://www.facebook.com>> accessed 22 August 2017.

231 ‘The World’s Most Valuable Resource Is No Longer Oil, but Data’ (*The Economist*, 6 May 2017) <<http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-anti-trust-rules-worlds-most-valuable-resource>> accessed 29 May 2017.

This raises challenges for the fundamental human rights framework developed to safeguard privacy and the use of personal data. This framework traditionally addresses primarily the state and its authorities;²³² however, both the general framework and privacy in particular have changed significantly over time and with the transition to the digital age.²³³ While ‘being left alone’ can be linked to a ‘liberal’ or first-generational human rights tradition which emphasizes the protection of the individual with inalienable rights against the threats posed by state authorities not controlled by the rule of law, second and third generational human rights concern the composition of society.²³⁴ In other words: the question is no longer only how to protect an individual from an illegitimate (historically physical) interference by a state, but now also compromises of spheres of personal autonomy (closer to the German tradition of ‘informational self-determination’) and the regulation of access to those

232 This is based on the fact that states were the first ones with the interest and ability to process large amounts of personal data for administrative purposes. See for instance van der Sloot (n 29).

233 Remember the introduction to the famous article of Warren and Brandeis on the right to privacy in this context: (n 1) 193–96.

234 The division of human rights into three generations goes back to the end of the 1970s and is accredited to Karel Vasak who refers to liberal or negative rights, social rights, and rights of solidarity: ‘A 30-Year Struggle’ (1977) 30 UNESCO Courier 28, 29.

spheres of personal development by the State and other members of society such as corporations.²³⁵

For reasons of enforcement and sovereignty concerns, the human rights framework still emphasizes the obligations of the state towards the people living on its territory and largely sticks to the first-generation pattern. Additionally, an obligation is added for the State to create an environment which respects and promotes rights such as privacy which transforms privacy from a 'right to be let alone' to a second-generational 'social right'. At this stage, regulation of private corporations by states and regional bodies (which draw their legitimacy from states who pass their sovereignty onto them in specific areas) such as the EU come into play. The activities of corporations that affect large groups of people are mostly addressed in laws referring to (or 'protecting') consumers. All other relationships are, from a legal perspective, subject to private law and contractual freedom. The latter comes with the assumption that parties have (more or less) equal power and tools at their disposal to defend their interests.

However, the use of data as a 'resource' challenges this setup significantly and provokes the question whether the current legal system is able to adequately address the chal-

235 This idea still dates back to the famous census judgment of the German Federal Constitutional court from 15 December 1983. The judgment itself is focused on the actions of state authorities and not private parties. BverfG, judgement of the First Senate of 15 December 1983, 1 BvR 209, 269, 362, 420, 440, 484/83.

lenges of the digital age. Specifically, the apps and services described in this chapter partly pose questions that resemble situations in which ‘collective rights’ or third-generational human rights concerns appear.

Often individual users and small businesses face much bigger corporations when personal data has been captured, and this is no different if the data capture has taken place in a public space as a result of an action by another user or ambient sensor.²³⁶ Many corporations operate internationally and are thus hard to regulate for individual states. It is questionable if their tools and methods are as powerful as the ones of their counterparts, which is the assumption that the legal order is based on.²³⁷

The only common denominator to protect humans from the negative consequences of data processing is thus dignity, or human rights in legal terms. However, it remains disputed to which these are binding for large, international corpo-

236 Lilian Edwards, ‘Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective’ (2016) 2 European Data Protection Law Review 28, 38–9.

237 Lisa M Austin, ‘Enough about Me: Why Privacy Is about Power, Not Consent (or Harm)’ in Austin Sarat (ed), *A World without Privacy: What Law Can and Should Do?* (Cambridge University Press 2015) 161; Alessandro Mantelero, ‘From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era’ in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of data technologies* (Springer 2017) 149.

rations such as the ones who collect and process the lion's share of personal data in the digital age.

Recently there is a tendency within the United Nations to place more responsibility on large technological corporations, which includes the responsibility to act as promoter and guardians of human rights like privacy.²³⁸ However, states themselves remain primarily responsible for the protection of such rights and the creation of an environment that is beneficial for human rights.²³⁹ One crucial aspect in that regard, is to guarantee human rights regardless of whether a person is a citizen of a specific country or not.²⁴⁰

238 UNCHR, 'The right to privacy in the digital age' (2017) UN Doc A/HRC/34/L.7/Rev.1,3: 'Recalling that business enterprises have a responsibility to respect human rights as set out in the Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, and that the obligation and the primary responsibility to promote and protect human rights and fundamental freedoms lie with the State [...]'

239 *ibid.*

240 UNCHR 'Report of the Special Rapporteur on the right to privacy, Joseph A Cannataci' (2017) UN Doc A/HRC/34/60, para 44: 'Who deserves the right to privacy: everybody, everywhere. Recommendation: States should prepare themselves to ensure that both domestically and internationally, Privacy be respected as a truly universal right — and, especially when it comes to surveillance carried out on the Internet, privacy should not be a right that depends on the passport in your pocket.'

3.4.2 Re-identification through combination

Fundamental Human Rights are not only protected in constitutions or documents like the Charter of Fundamental Rights of the European Union (CFEU).²⁴¹ They are also—and with greater precision—enshrined in acts based on them, such as the GDPR, which covers the handling of private data by corporations, and the Law Enforcement Directive, which focuses on personal data that is used for purposes to ensure public security by competent authorities.²⁴²

When considering their applicability, however, one must keep in mind the exceptions of their material scope: anything that falls outside the general scope of EU law is not covered, as well as anything within the scope of the specific provisions on the common foreign and security policy of the EU, and personal data processed in the context of household uses.²⁴³

Further limiting their applicability is the seemingly uncontroversial definition of ‘personal data’ in both the GDPR²⁴⁴ and the Law Enforcement Directive,²⁴⁵ which both state identically:

‘Personal data’ means any information relating to an identified or identifiable natural person

241 (n 69).

242 Law Enforcement Directive, art 1(2)a; GDPR, art 1(2).

243 GDPR, art 2(2).

244 GDPR, art 4(1).

245 Law Enforcement Directive, art 3(1).

(‘data subject’); an identifiable natural person is one 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.

This definition seems comprehensive at first glance.

However, it is not helpful when resolving an old dogmatic conflict between legal scholars about the meaning of ‘personal’ in the combination ‘personal data’.²⁴⁶ There is an abstract theory (or ‘objective criterion’) which says that personal data is data that can be tied to a person in view of all the knowledge that exists about it, regardless of the circumstances or the situation or the actors handling it (in legal

246 This conflict seems particularly present in the legal discourse in Germany (‘relative oder absolute Bestimmbarkeit’). Judith Nink and Jan Pole, ‘Die Bestimmbarkeit Des Personenbezugs - Von Der IP-Adresse Zum Anwendungsbereich Der Datenschutzgesetze’ [2015] *Multimedia und Recht* 563; Matthias Bergt, ‘Die Bestimmbarkeit Als Grundproblem Des Datenschutzrechts - Überblick Über Den Theorienstreit Und Lösungsvorschlag’ [2015] *Zeitschrift für Datenschutz* 365; Wolfgang Ziebarth, ‘Perspektive Der Bestimmbarkeit’ in Ger- not Sydow (ed), *Europäische Datenschutzgrundverordnung: Der neue Praktiker-Kommentar zur Datenschutz-Grundverordnung* (Nomos 2017), mn 33–40. See also para 25 of Case C–582/14 *Patrick Breyer v Bundesrepublik Deutschland* EU:C:2016:779, in which the CJEU mentions this conflict.

terms the processor or controller). The concrete theory (or ‘relative criterion’) however, focuses on the specific knowledge and means a processor or controller of the data has and only considers data to be personal if an actor is able to tie data to a person in the known circumstances. The difference is that under the abstract theory, more data has to be protected and less data is exploitable for economical or other causes.²⁴⁷

The definition of personal data in the EU does not clearly indicate whether it is based on the abstract or concrete theory. As already referred to above, the GDPR²⁴⁸ and the Law Enforcement Directive²⁴⁹ both refer identically to ‘an identifiable natural person [...] who can be identified, directly or indirectly [...]’. Recently, in the case of *Breyer v Germany* on the question of whether dynamic Internet Protocol (IP) addresses are personal data, the Court of Justice of the European Union (CJEU) appeared to suggest that it is developing a tendency towards the abstract theory.²⁵⁰ It held that (dynamic) IP addresses collected by the German government to prevent attacks on governmental websites constitute personal data, because the users of those addresses could be identified with the help of Internet Service Providers.²⁵¹ This

247 See Case C-582/14 *Patrick Breyer* (ibid), para 25.

248 GDPR, art 4(1).

249 Law Enforcement Directive, art 3(1).

250 Case C-582/14 *Patrick Breyer* (n 247).

251 ibid, para 49.

could suggest that the CJEU has finally acknowledged that the abstract theory has prevailed.

However, on closer scrutiny, the arguments of the judges reveal that this decision can hardly be generalized. The court itself opens several venues to the legality of such a collection of data: if consent of the user was sought;²⁵² if legal safeguards would be introduced which prohibit the identification process; and — most saliently for the abstract/concrete discussion — if the requirements in time, cost, and manpower would be so disproportionate ‘that the risk of identification appears in reality to be insignificant’.²⁵³ Hence, it is submitted that it is not possible to interpret this judgment as a categorical decision by the CJEU to stick to either the abstract or the concrete theory. In effect, the judgment only adds one more nuance to this complex problem.

Think about this distinction in the light of the considerations raised in the above section: although it might not be possible to tie certain specific data points to a person by using just one database, it might become possible by combining one (maybe closed) database with other (maybe openly available) databases. For example, the data gathered by an app like My Safetipin might not be considered personal data per se in legal terms, but combined with other databases (such as OpenStreetMaps, newspaper articles, police re-

252 *ibid*, para 64. The whole second question in the judgment revolves around the subject of consent or the lack thereof.

253 *ibid*, para 45–49.

ports, etc.) it might be possible to identify some users of the app.

This raises the question if a potential gap in the definition exists that appears when the combination of two (or more) datasets that do not contain personal data actually produces personal data. The safeguards enshrined in the Law Enforcement Directive and GDPR that prohibit the re-use of data for incompatible purposes do not apply to indirectly personally identifiable data as presented above,²⁵⁴ and consider each source of data on a case-by-case basis.

3.4.3 Remedies on the basis of the new EU legislation

Generally, protection of the law can exist for legal persons, such as corporations, foundations, or public authorities, and natural persons. Focusing first on legal persons, their ability to have their interests covered by fundamental rights is limited and varies from country to country, even within the EU.²⁵⁵ This means, for example, that entrepreneurs who run businesses in areas that are perceived to be prone to crimes like robbery and murder according to services like Spot-

254 GDPR, art 5(1)b; Law Enforcement Directive, art 4(1)b.

255 For some guidance on the issue see Dirk Ehlers and Ulrich Becker (eds), *European Fundamental Rights and Freedoms* (de Gruyter Recht 2007) 385–6; PHPHMC van Kempen, ‘Human Rights and Criminal Justice Applied to Legal Persons. Protection and Liability of Private and Public Juristic Entities under the ICCPR, ECHR, ACHR and Af-ChHPR’ (2010) 14 *Electronic Journal of Comparative Law* 1, 29–32.

Crime are not entitled to remedies under either the GDPR or the Law Enforcement Directive.²⁵⁶

The CFEU might entitle the owners of businesses or assets like apartments or houses to some sort of remedy if they can prove that their right to property in Article 17 is being infringed in a personal capacity. However, paragraph 1 of this provision is clearly directed towards the state and not other private parties. Here civil law might be useful in cases where it is possible to prove an actual loss that is directly caused by running the service. It is very unlikely that this will be possible to prove, for example for a shop-owner who says one specific client did not buy one specific item because of bad ratings. Devaluation of buildings or assets is also hardly covered in these scenarios, since it will be hard to prove that the service is the only reason for the change in the value.

Focusing on natural persons, there is a wide range of remedies available at their disposal if the data collected about them is considered personal (following the logic of the above subsection 3.4.2), although the structure of enforcement might differ for the GDPR and the Law Enforcement Directive. Leaving general procedural considerations aside and assuming the lawfulness of processing (consent has been given, there is legitimate reason for the collection and

256 Sentence 2 of recital 14 of the GDPR states in this regard: ‘This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.’

processing, etc.),²⁵⁷ the relevant rights of the data subject are knowledge about the information processed or held,²⁵⁸ right of access,²⁵⁹ and the right of rectification and/or erasure.²⁶⁰ The GDPR contains furthermore a ‘right to be forgotten’,²⁶¹ a right to restrict the processing,²⁶² and a right to object data processing in cases of automated decision making (for profiling or credit scoring for example).²⁶³

Most of these remedies, like the right to know which data is processed or the rights to alter (have the actual situation reflected in the data) or delete it, are not innovative and stem from times when concerns about data processing related mainly to government use of data.

When it comes to the seemingly more innovative and broadly discussed ‘right to be forgotten’, it should be considered in detail what it actually entails. While one might derive from the actual wording of Article 17 of the GDPR that an individual is entitled to have a specific piece of personal data deleted completely and everywhere,²⁶⁴ the current situation is more complex. One needs to differentiate a ‘right to

257 GDPR, art 6; Law Enforcement Directive, art 8.

258 GDPR, art 14, Law Enforcement Directive, art 13.

259 GDPR, art 15; Law Enforcement Directive, art 14.

260 GDPR, art 16, 17; Law Enforcement Directive, art 16.

261 GDPR, art 17.

262 *ibid*, art 18.

263 *ibid*, art 21.

264 Oskar Josef Gstrein, *Das Recht Auf Vergessenwerden Als Menschenrecht: Hat Menschenwürde Im Informationszeitalter Zukunft?* (Nomos 2016) 198–200.

delist’ information from the index of a search engine according to the Google Spain judgment of the CJEU²⁶⁵ and a right which is best understood as a more complete right to erasure enshrined in Article 17 paragraph 2 GDPR.²⁶⁶ In summary, while the term ‘right to be forgotten’ suggests protection of data subjects in hindsight, for example when they become identifiable against their will through one of the apps or services that was presented above or while suffering other negative consequences, the actual legal remedies do not hold up to this expectation.

Based on the quality and quantity of legal tools available, it seems that a natural person is fairly protected against the negative consequences of services such as those described in section 3.2 ‘Websites and apps’, particularly if the party responsible for processing or controlling the data is a private entity. This protection as described in legal texts, however, can sometimes be extremely difficult to ensure in real world scenarios.²⁶⁷

265 Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* EU:C:2014:317.

266 Oskar Josef Gstrein, ‘The Right to Be Forgotten in the General Data Protection Regulation and the Aftermath of the *Google Spain* Judgment (C-131/12)’ (2017) 5 *Privacy in Germany, Datenschutz und Compliance* 9, 11–15.

267 This seems especially true of access rights, which are necessary enablers for many other data protection rights. See for instance Clive Norris and others (eds), *The Unaccountable State of Surveillance: Exercising Access Rights in Europe* (Springer 2016); Robert Rothmann, ‘Video Surveillance and the Right of Access: The Empirical Proof of

If the party controlling the data is a competent authority working on public security — e.g. a police force or a city council — the remedies seem to be more limited in quantity. However, this is also a field where procedural safeguards might be applicable that are part of (more nationally diverse) administrative or criminal law. Hence, it is difficult to conclude that the protection of an individual is more limited in such scenarios in the EU in general.

3.4.4 Groups

Although the remedies presented above might, at least in theory, provide a fair level of protection against negative consequences for individuals, many of the negative effects outlined in the previous section do not, or not necessarily, occur at the individual level. The reification of prejudices about certain areas for instance does not target any specific individual, and no personal data needs to be included in any part of the analytic procedures leading up to it. The communities—composed of individual, natural persons—living in those areas will be on the receiving end of the negative consequences such as increased police surveillance.

This points to a further potential problem with the definition of personal data in the GDPR and the Law En-

Panoptical Asymmetries' (2017) 15 *Surveillance & Society* 222; Jef Ausloos and Pierre Dewitte, 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice' (2018) 8 *International Data Privacy Law* 4; René LP Mahieu, Hadi Asghari and Michel van Eeten, 'Collectively Exercising the Right of Access: Individual Effort, Societal Effect' (2018) 7 *Internet Policy Review*.

forcement Directive: it does not cover data which identifies groups of individuals (either formally recognized as a legal person or not), rather than single natural persons. However, the data from apps such as those described above will often refer to specific spots, streets, or neighbourhoods, and consequently the communities living there. If such descriptions do not identify anyone—and why would they?—the entire data protection framework is not applicable.

This is not unique to the case study at hand, but fits into a larger emerging problem area within data protection and privacy legislation in the context of big data analytics. Such analyses are interested in the individual mostly as a member of (myriad) groups, many of which are created by the analyses themselves, unstable in membership and not self-aware.²⁶⁸ Even if we were to accept that groups should be able to defend their data protection and privacy rights, the question remains how such rights might be protected, especially without negatively influencing the already established level of individual protection.²⁶⁹ The preventive solutions we

268 Linnet Taylor, Bart van der Sloot and Luciano Floridi, ‘Conclusion: What Do We Know About Group Privacy?’ in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy* (Springer 2017) 227.

269 Ugo Pagallo, ‘The Group, the Private, and the Individual: A New Level of Data Protection?’ in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of data technologies* (Springer 2017) 167.

discuss in the next subsection might provide some relief in this regard as well.²⁷⁰

3.4.5 Preventive measures on the basis of the new EU legislation

The remedies presented so far are exactly that: remedies for when negative consequences have already materialized. When looking at the previous section, however, this does not provide a satisfactory solution for all potential harms: e.g. increased traceability and a generalized loss of privacy in public cannot be retroactively repaired. Interestingly, with the introduction of the GDPR two possibly preventive measures have also been introduced: data protection by design and Data Protection Impact Assessments (DPIAs). Article 25 requires data controllers to ‘implement appropriate technical and organisational measures [...] which are designed to implement data-protection principles [...] in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects’.²⁷¹ Furthermore, Article 35 of the GDPR requires a DPIA when ‘a high risk to the rights and freedoms of natural persons’ are foreseen.²⁷²

In the context of the apps discussed, technical measures could for instance include strong and properly implemented

270 Mantelero, ‘From Group Privacy to Collective Privacy’ (n 238) 150–54.

271 GDPR, art 25(1).

272 *ibid*, art 35.

encryption where feasible.²⁷³ In addition, human–computer interaction design measures could help users to meaningfully exercise their right to be forgotten in the contexts within which the apps are being used.²⁷⁴ For now, it remains to be seen though how these articles can be given meaning beyond their good intentions, and how to deal with cases in which system developers do not follow preventive guidelines. Although the GDPR does provide for administrative fines of up to 10 million Euros or 2 percent of annual global turnover if Article 25 (on data protection by design) has been infringed,²⁷⁵ specific tests still need to be developed in order to be able to adjudicate exactly when this will be the case. Furthermore, it seems unlikely that companies will spontaneously share their design and development processes with outside scrutinizers.

3.5 Conclusion

As the legal analysis in the above section revealed, the potential problems stemming from services that document fear

273 As proposed by a group of researchers at the Berkman Klein Center of Harvard University: Mat Ollsen, Bruce Schneier and Jonathan Zittrain, ‘Dont Panic, Making Progress on the “Going Dark” Debate’ (2016) <https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf> accessed 24 March 2017.

274 Lachlan Urquhart and Tom Rodden, ‘New Directions in Information Technology Law: Learning from Human–Computer Interaction’ (2017) 31 *International Review of Law, Computers & Technology* 150, 155–58.

275 GDPR, art 83(4)a.

and reveal ‘dangerous’ areas lie not in the remedies which are legally available within the EU. This seems true, at least, if the data produced is considered personal data.

However, this leaves the consideration aside that such remedies must be easy to use for the persons concerned and must be effective. The lessons learned from cases such as *Schrems I & II*²⁷⁶ on Safe Harbor and the Privacy Shield or *Google Spain v AEPD and Mario Costeja Gonzalez*²⁷⁷ on the ‘right to be forgotten’ seem to suggest that the practical application of rights needs to be facilitated significantly. Furthermore, the interpretation of the jurisprudence in the *Google Spain* case raises three key concerns: in the administration of requests, the transparency of decision-making processes, and the geographical scope of the right. Nevertheless, at least the setup of the framework seems to be appropriate to tackle the challenges.

A lack of safeguards and remedies results from possible gaps of the definition of ‘personal data’ in texts such as GDPR or the Law Enforcement Directive. There is a risk that several sources of data will be combined and make individual persons identifiable, even if none of the sources is considered to be personal data itself, e.g. because it only contains certain pieces of information or has been pseudo- or anonymized using state of the art technology. It should be carefully investigated whether such a ‘release-and-complete-freedom’

276 (n 215).

277 Case C-131/12 *Google Spain* (n 266). See also Norris and others (n 268); Rothmann (n 268).

model²⁷⁸ is appropriate in regard to datasets that contain information about, for instance, neighbourhoods.

Caution with respect to the release of anonymized data is warranted, as it seems unlikely that personal data that has once been de-identified with state of the art technologies will remain risk-free forever. There are incidents which suggest increased caution and consideration: in Australia, a dataset containing seemingly de-identified health records of patients was successfully re-connected with the persons concerned after being published by the government delivering on its commitment to ‘open data’. Even though the government reacted and promptly removed the dataset after notification, it is not unlikely such data will end up on some vending platform in the ‘darknet’.²⁷⁹ Highly sensitive data will always contain a certain risk and the question should not be whether the risk can be removed forever and in all circumstances, but rather how it should be managed each time the data is being put to use. Possibly, the tendency to publish data aggressively should be countered with a legal requirement that foresees a privacy impact assessment each

278 Sophie Stalla-Bourdillon and Alison Knight, ‘Anonymous Data v. Personal Data—a False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data’ (2016) 34 *Wisconsin International Law Journal* 284, 322.

279 Paul Farrell, ‘The Medicare Machine: Patient Details of “Any Australian” for Sale on Darknet’ (*The Guardian*, 3 July 2017) <<https://www.theguardian.com/australia-news/2017/jul/04/the-medicare-machine-patient-details-of-any-australian-for-sale-on-darknet>> accessed 29 August 2017.

time the purpose of data processing changes. The UN Special Rapporteur on the right to privacy has also included this topic as one of his main areas of concern for upcoming reports.²⁸⁰

Furthermore, data about groups of people and local communities is also not covered by the current legal framework. The importance and aspects of group privacy and spaces to develop freely must be studied further in that regard. It is increasingly visible that the deployment of high-tech infrastructure needed to operate ‘smart cities’ or to guarantee increased safety in public through the use of technologies such as CCTV comes with the consequence that spaces for free development of ideas and movements disappear.

The authors would like to coin the term ‘technological gentrification’ in this context. It describes the slow-down (and perhaps ultimate death) of societal development as a result of the endeavour to provide increased security and predictability in public spaces as a consequence of the inappropriate mass use of invasive technologies such as (smart) CCTV or mobile devices as stigmatizing security sensors. The chilling effects resulting from this situation — the permanent observation of public behaviour — set the stage for a world of continuous ex ante compliance. This means that

280 The report on dangers of Big Data & Open Data is expected to be presented to the General Assembly in 2017. United Nations, Office of the High Commissioner of Human Rights, ‘Planned Thematic Reports and Call for Consultations’ <<http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/ThematicReports.aspx>> accessed 29 August 2017.

certain areas of cities or entire communities will lose their potential to re-develop by experimenting with new forms of societal interaction.

There is a growing and interesting body of literature in this context on the development of smart cities and the impact of technologies like CCTV.²⁸¹ However, it remains questionable whether such mostly theoretical knowledge will see a sufficient transfer to the broader ranks of society, which are subjected to highly sophisticated technologies without being completely aware of its basic functioning and the consequences of its use.

It is important to remember at this stage that secondary law, such as the GDPR and the Law Enforcement Directive, is based on primary EU law such as the CFEU. The wording of Article 8 CFEU and the fact that it is a right different from Respect for private and family life (Article 7 CFEU) suggests that in the EU the term ‘personal data’ has to be interpreted broadly since it is not necessarily tied to the context of the use of data or traditional privacy rights.²⁸² Hence, it might

281 For a comprehensive overview on topics relating to Smart Cities see Houbing Song and others, *Smart Cities: Foundations, Principles, and Applications* (John Wiley & Sons 2017). For CCTV see Demetrius Klitou, ‘Public Space CCTV Microphones and Loudspeakers: The Ears and Mouth of “Big Brother”’ in Demetrius Klitou, *Privacy Invading Technologies and Privacy by Design* (Springer 2014) 116.

282 CFEU, art 8 (on the protection of personal data) states in para 1: ‘Everyone has the right to the protection of personal data concerning him or her.’ This also would support the argument by the CJEU that art 8 is a different fundamental right than CFEU, art 7 (on pri-

perhaps be possible to interpret the definition of personal data to include datasets that are the result of apps and services such as those discussed in this chapter.

At the moment though, it seems that the EU legal framework alone will not suffice as a solution for all the potential problems presented. What is thus clear is that — especially because it remains largely an open matter how services which describe neighbourhoods or deal with the perception of fear may impact certain area and people — various issues will deserve continuing scrutiny in order to hopefully be able to develop workable solutions to emerging problems early on.

First, the legal analysis has focused solely on EU data protection framework. Nevertheless, the legal context with regards to privacy, data protection and informational

vacy) as stated prominently in Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* EU:C:2016:970, para 129, last sentence. The question arises because the jurisprudence of the European Court of Human Rights seems currently, at least for practical purposes, equivalent in terms of the scope of protection applicants are being granted. Note here also that art 8 of the European Convention on Human Rights is very similar to art 7 CFEU. Additionally, art 53 CFEU guarantees that the level of protection offered is at least equivalent to the European Convention on Human Rights and ties the substantial privacy protection of both treaties even closer. Hence, the question remains what the added value of art 8 CFEU would be. Although the added value might not be apparent at this point in time, it might become clearer in the future as a result of technological developments and changing uses of personal data.

self-determination diverges widely around the world and it is being discussed whether these rights are the same or different.²⁸³ The concerns and apps discussed, however, do not neatly follow jurisdictional lines. Most apps are available for download by interested users in repositories such as the Google Play store and the Apple app store without geographic restrictions; and where they are targeted at specific issues in specific locations — such as the Free to Be app in Melbourne — copies for other locations can be produced at relatively low economic costs. The authors hope to have sketched out some legal challenges and ways forward that will also be applicable in other jurisdictional contexts, but much work clearly remains in this regard.

Secondly, such systems might become the basis for ‘evidence based’ prejudices and discrimination. Data in itself can only suggest certain conclusions, even if it is already analysed and processed using complex algorithms and substantive computing power. Humans must understand the criteria on which such suggestions are based and not look at them naively, or worse, base decisions on them that might negatively affect individuals.

283 For example, the UN Special Rapporteur on the right to privacy has launched a conference series with the title ‘Privacy, Personality and Flows of Information’ which is envisaged to result in a report on the subject in October 2020. For more information visit <<http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/ThematicReports.aspx>> (n 281).

Thirdly, terms like ‘safe’, ‘unsafe’, ‘good’, and ‘bad’ are very difficult to rate on simple scales. A neighbourhood that is stimulating and interesting for one person might be scary and terrifying for another. Breaking down such notions in quantifiable categories leads to a loss of descriptive richness. This problem is amplified when the judgments or impressions of a group of people are aggregated to single conclusions. Will reviews of neighbourhoods indeed affect dwellers, real estate owners, and local businesses in the way user generated reviews can drive restaurants out of business?²⁸⁴ Moreover, what will the potential for abuse of such services be if certain individuals find ways to discredit areas through fake reviews or reports?

Finally, and connected to the previous issue, yet another techno-social system has been added to the surveillance assemblage operating in urban environments. It contributes to a pervasive remaking of how we experience privacy in public spaces, and curtails the free development of personalities and communities. With some modifications, many of the problems and solutions discussed in this chapter might be applicable to many similar systems which (enable users to) track, log, trace, analyse, and rate whatever takes place in public. The question arises when enough is enough: which technology is the straw that breaks the camel’s back?

284 Michael Luca, ‘Reviews, Reputation, and Revenue: The Case of Yelp. Com’ [2016] Harvard Business School working paper 12-016.

**4. Algorithmic Mapmaking in
“Smart Cities”: Data Protection
Impact Assessments as a means
of Protection for Groups**

Previously published as: Gerard Jan Ritsema van Eck, ‘Algorithmic Mapmaking in “Smart Cities”: Data Protection Impact Assessments as a means of Protection for Groups’ in Angela Daly, Kate S Devitt and Monique Mann (eds), *Good data* (Institute of Network Cultures 2019).²⁸⁵ Some minor spelling and grammar errors have been corrected in this version.

285 An early version of this chapter was presented to my colleagues at the department of Transboundary Legal Studies in Groningen. I thank them for the frank comments which helped to sharpen the argument. I thank Prof. Jeanne Mifsud Bonnici for her many comments on various early drafts. Thanks are due to Lauren Elrick for her careful language check. Finally, I would like to thank the participants of the Surveillance Studies Network 8th Biennial Conference at Aarhus University, Denmark, who provided valuable feedback and inspiration.

Abstract

Maps are powerful communication tools, and mapmaking used to be a privileged affair. In recent times, this has changed as “smart cities” have been outfitted with video, audio, and other kinds of “Internet of Things” sensing devices. The data-streams they generate can be combined with volunteered data to create a vast multitude of interactive maps on which individuals are constantly (re)grouped based on abnormality, deviation, and desirability. Many have argued that under these circumstances personal data protection rights should be extended to groups.

However, group rights are an awkward fit for the current European data protection framework that is heavily focused on individuals. One possible opening for better protection is offered by Data Protection Impact Assessments (DPIAs), which are mandatory to carry out when the ‘systematic monitoring of a publicly accessible area on a large scale’²⁸⁶ necessary for mapmaking takes place. They form an opportunity to recognize the risks of e.g. discrimination at an early stage. Furthermore, by including representatives of local (disadvantaged) groups, the strong performative qualities of maps can offer occasions for groups of citizens in smart cities to proactively shape the environments in which they live.

There are serious limitations. Although DPIAs are mandatory, the inclusion of affected data subjects and their representatives is not. This undermines many of the possible advantages. Finally, the high costs associated with the pro-

286 GDPR (n 75), art 35(3)c.

cess might mean many companies engage with it only superficially and temporarily. Establishing effective data protection for groups negatively impacted by mapmaking software through DPIAs thus seems nigh on impossible in lieu of substantial legislative change.

Figure 4.1: Screenshot taken by the author of a Strava heatmap.²⁸⁷ Shown is the Stadspark in Groningen, the Netherlands. The clearly visible small semi-circle in the bottom is a 400-meter running track whereas the larger oval above it goes around a pond and measures almost exactly one kilometre; it therefore constitutes a popular running route.

²⁸⁷ Strava Inc, 'Strava Global Heatmap' (Strava) <<https://labs.strava.com/heatmaps>> accessed 2 February 2018.

4.1 Introduction

In late 2017, Strava revealed its “global heatmap” which shows popular running and cycling routes around the world. Although first reported as a ‘striking visualization of over one billion activities’,²⁸⁸ the tone of the reporting quickly changed when it was discovered that secret (military) locations could also be located using the heatmap.²⁸⁹ The Stratumseind, a popular nightlife area in the Dutch city of Eindhoven received similarly negative press when it was turned into a “Living Lab” ‘where massive amounts of data about people’s activities will be used [...] to study which factors contribute to violence and discomfort.’²⁹⁰ This data is overlaid on a map of the area, and the police can quickly intervene when and where suspicious patterns emerge. One reporter dubbed it ‘Having a beer with Big Brother’.²⁹¹

Clearly, the usage of large amounts of data to draw maps raises concerns. The practice, however, seems to be booming

288 ‘Strava: A Global Heatmap of Athletic Activity’ *The Guardian* (2 November 2017) <<https://www.theguardian.com/lifeandstyle/the-running-blog/gallery/2017/nov/02/strava-a-global-heatmap-of-athletic-activity>> accessed 8 February 2018.

289 Alex Hern, ‘Fitness Tracking App Strava Gives Away Location of Secret US Army Bases’ *The Guardian* (28 January 2018) <<https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases>> accessed 8 February 2018.

290 ‘Eindhoven Living Lab’ (*European Network of Living Labs*) <<http://www.openlivinglabs.eu/livinglab/eindhoven-living-lab>> accessed 22 March 2018.

291 Author’s translation. Peter de Graaf, ‘Een Biertje Met Big Brother Erbij’ *De Volkskrant* (23 November 2015) 11.

rather than decreasing. “Smart” and dumb cities alike are increasingly being outfitted with video, audio, and various other “Internet of Things” (IoT) sensing devices in order to gather ever more data,²⁹² and an even more potent, and often cheaper, stream of data can be crowdsourced or scraped from (the smartphones of) city dwellers. Once generated, the data needs to go somewhere, and often they end up in maps.

This chapter will consider these developments by combining insights from critical geography and data protection law, particularly the General Data Protection Regulation (GDPR) that recently came into force in the European Union. Specifically, the chapter will begin by investigating the relationship between data and maps, and why they are such salient artefacts. In the next section, the issue of maps is problematized and the lack of legal protections for affected groups is discussed. Then, Data Protection Impact Assessments (DPIAs), a tool that has received renewed interest because of the introduction of the GDPR, are introduced as a possible solution in the absence of strong legislation. However, are they really a panacea that can provide meaningful safeguards, or an expensive Band-Aid that will be avoided, ignored, and brushed aside?

292 Privacy International, ‘Smart Cities: Utopian Vision, Dystopian Reality’ <<https://privacyinternational.org/node/638>> accessed 4 May 2018.

4.2 How Maps Are Made

Drawing a map is a powerful act. Who draws a map, decides what is shown on it: physical features of the landscape, roads, settlements, or claims to certain territories by various (imagined) groups.²⁹³ Maps provide a representation of a certain geographical area that, even if not fully objective, at least is claimed to represent the truth.²⁹⁴ Map drawing has historically been a privileged affair that is only undertaken by those with the means and motivation to do so: ‘scientists, planners, urbanists, technocratic subdividers and social engineers’.²⁹⁵ However, over the past two decades, the global north has seen a dizzying multiplication of geotagged databases visually overlaid on maps, each of which comprises a new map in itself.²⁹⁶ Such ‘Geographic Information Systems’, or simply GIS as they are referred to in the technocratic jargon,

293 For an interesting example of how the national map of Indonesia/the former Dutch East Indies was used in this way, see Benedict R Anderson, *Imagined Communities: Reflections on the Origin and Spread of Nationalism* (2nd edn, Verso 2006) 175 and further; For a contrasting example of the same phenomenon, see Jeremy W Crampton, ‘Bordering on Bosnia’ (1996) 39 *GeoJournal* 353, 353–61.

294 Camilo Arturo Leslie, ‘Territoriality, Map-Mindedness, and the Politics of Place’ (2016) 45 *Theory and Society* 169, especially 172–73 thereof.

295 Lefebvre (n 36) 38.

296 Note that from hereon, the term ‘map’ in this chapter will be used to describe any visual representation of geographic or georeferenced data that claims to describe some spatial territory, i.e. maps in paper atlases as well as interactive Geographic Information Systems such as Waze.

are often not carefully constructed by single authors but are based on aggregations of data from a multiplicity of sources, each of which might have been collected differently.²⁹⁷

Outfitting an environment with enough IoT sensors to collect the critical mass of geotagged data needed to feed a GIS can be prohibitively expensive for all but the most well-funded smart cities. A cheap and therefore popular alternative, or addition, is crowdsourcing. Roughly, organizations that crowdsource the collection of georeferenced data in order to make maps have three options. One option is that data is collected purposefully by participants that have knowledge of (and perhaps an interest in) how it will be processed further. This is the approach taken by, for example, OpenStreetMap that is ‘built by a community of mappers that contribute and maintain data about roads, trails, cafés, railway stations, and much more’.²⁹⁸ Another option is to scrape together the various geotagged data trails that smartphone users leave behind,²⁹⁹ as is done by the Living

297 For some examples of differing input arrangements in this context, see Oskar Josef Gstrein and Gerard Jan Ritsema van Eck, ‘Mobile Devices as Stigmatizing Security Sensors: The GDPR and a Future of Crowdsourced “Broken Windows”’ (2018) 8 International Data Privacy Law 69, 70–74. The referenced article has been republished in this thesis as chapter 3.

298 OpenStreetMap Foundation, ‘About’ (*OpenStreetMap*) <<https://www.openstreetmap.org/about>> accessed 11 April 2018.

299 Smith (n 124) 108.

Lab in Eindhoven and various others.³⁰⁰ The third option is to combine these two strategies. This model is successfully employed by the navigation app Waze, which takes into account the current traffic situation to calculate the fastest routes. To be able to do so, it scrapes data on the speed and location of its users and combines this with data on for instance road closures that users are encouraged to add using a gamified system of badges and achievements. Furthermore, in various cities such as Rio de Janeiro, New York City, and Ghent, Waze receives data on upcoming road closures from local governments through its Connected Citizens Programme — in exchange, the local governments gain access to information on accidents and other traffic disruptions.³⁰¹ As Gekker and Hind point out, this makes it ‘not necessarily easy to make a clean split between those who “produce” the map, those who “edit” the map and those who “consume” the map.’³⁰²

Once collected, the manner in which crowdsourced georeferenced data is presented further blurs the lines between producers, editors, and consumers. Georeferenced datasets are visualized as cartographic imagery in interactive envi-

300 e.g. Federico Botta, Helen Susannah Moat and Tobias Preis, ‘Quantifying Crowd Size with Mobile Phone and Twitter Data’ (2015) 2 Royal Society Open Science 150162.

301 ‘Connected Citizen’s Programme’ (Waze) <<https://www.waze.com/ccp>> accessed 2 February 2018.

302 Alex Gekker and Sam Hind, “‘Outsmarting Traffic, Together’: Driving as Social Navigation’ in Clancy Wilmott and others (eds), *Playful Mapping in the Digital Age* (Institute of Network Cultures 2016) 83.

ronments overlaid on Google Maps or similar services like OpenStreetMaps or Bing Maps,³⁰³ engaging the user in acts

303 Which itself also provides a seamless transition between multiple ‘views’ of the same area, such as ‘map,’ ‘terrain,’ ‘traffic,’ and ‘satellite.’

Figure 4.2: Screenshot taken by the author of the Waze live map of part of the centre of London, England.³⁰⁴ The three data sources are clearly visible: the coloration of the streets is based on scraped movement data, the balloons are based on user submitted reports, and the map data comes from Google maps.

304 Waze Mobile Ltd., ‘Live Map’ (Free driving directions, traffic reports & GPS navigation app by Waze) <<https://www.waze.com/livemap>> accessed 5 February 2018.

of active sense making.³⁰⁵ This makes *prima facie* sense, as the public is accustomed to engaging with large data sets visually.³⁰⁶

Interestingly, something else is also gained when crowdsourced georeferenced data is offered as a map. This mode of presentation immediately embeds the data within what Leslie calls ‘the “system of maps,” the full panoply of mutually-reinforcing, mutually referential map images that subjects are exposed to [...], a system ultimately grounded in a generalized awareness of cartography’s scientism.’³⁰⁷ Thus, by becoming maps, crowdsourced georeferenced data sets also gain the performative power that comes with the claim to truth-correspondence of maps. Put differently: Because people tend to take maps at face value, any data overlaid is also taken at face value, whether it purports to show a crime hotspot or a traffic jam.

4.3 Maps and (Missing) Group Rights

The role of many modern algorithms is to render “big data” actionable based on hyper complex probalistics.³⁰⁸ They do this by categorizing people into groups: for example, those

305 Jeremy W Crampton, ‘Maps as Social Constructions: Power, Communication, and Visualization’ (2001) 25 Progress in Human Geography 235.

306 Helen Kennedy and others, ‘Engaging with (Big) Data Visualizations: Factors That Affect Engagement and Resulting New Definitions of Effectiveness’ (2016) 21 First Monday.

307 Leslie (n 294) 172.

308 Louise Amoore, ‘Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times’ (2011) 28 Theory, Culture & Society 24.

who should be shown a certain advertisement, those who should not be let into an airplane without an extra security check, or those who should receive special police attention because they know a victim of a recent shooting.³⁰⁹

In public spaces, the push to make cities smart by outfitting them with a multitude of sensors also increases the influence of grouping algorithms.³¹⁰ Take, for example, those who are unwittingly part of a suspicious pattern in the Stratumseind Living Lab in Eindhoven. Once identified, the location of the pattern is shown on a map that, as outlined above, forms an effective communication method for the end-result of such algorithms: it embeds the abstract (and perhaps highly contestable³¹¹) output of the algorithm in the ‘panoply of maps.’³¹² Private security personnel can then be deployed to re-establish order. The Strava example mentioned before shows that an environment does not need to be highly saturated with IoT sensors for such groupings to have an effect:

309 Ali Winston, ‘Palantir Has Secretly Been Using New Orleans to Test Its Predictive Policing Technology’ (*The Verge*, 27 February 2018) <<https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd>> accessed 7 March 2018; David Lyon (ed), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (Routledge 2003).

310 Edwards (n 236).

311 e.g. Williams, Burnap and Sloan (n 163), who found that the same Twitter data can reveal juxtaposed phenomena in areas with either high or low levels of crime.

312 Leslie (n 294) 172.

only a few smartphones in the Syrian desert were enough to give away the locations of various secret military bases.

The most problematic side product of map-making algorithms can be geographical biases. Although they do not directly affect individuals, they can deeply impact local communities³¹³ through, for instance, increased police surveillance.³¹⁴ This can be caused, *inter alia*, by a skew in the collection of crowdsourced geographic data, in which marginalized communities tend to be underrepresented,³¹⁵ or conversely, their overrepresentation in historical data.³¹⁶ After the collection phase, bias can also creep in during analysis. At this stage though, it may be harder to detect any biases³¹⁷ because the inner workings of many algorithms can be difficult to understand for non-experts and, in the case of self-learning algorithms, for the developers of the algo-

313 Mantelero, 'Personal Data for Decisional Purposes in the Age of Analytics' (n 140) 240.

314 Joh, 'The New Surveillance Discretion' (n 138) 31–32; Note in this context that Andrew D. Selbst recently proposed an impact assessment framework specifically for predictive policing solutions, see 'Disparate Impact in Big Data Policing' (2018) 52 Georgia Law Review 109.

315 Pak, Chua and Moere (n 207); Monica M Brannon, 'Datafied and Divided: Techno-Dimensions of Inequality in American Cities' (2017) 16 City & Community 20.

316 Selbst (n 314) 133; Joh, 'Policing by Numbers' (n 139) 58; Delbert S Elliot, 'Lies, Damn Lies and Arrest Statistics' (Center for the Study and Prevention of Violence 1995).

317 Brent Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics' (2017) 30 Philosophy & Technology 475, 479 and 490.

rithm itself.³¹⁸ Such biases can easily turn into disparate impacts and discrimination when the output of an algorithm is taken at face value. This is especially salient for mapmaking algorithms because, as was discussed above, representing abstract outputs on maps increases their performativity.

The enigmatical nature of refined data processing means that even if strong anti-discrimination legislation exists, it might not provide much protection.³¹⁹ This follows from the simple fact that, in order to bring a claim, for instance in a class action setting, claimants need to be aware that they belong to a group that has been negatively impacted. In the context of algorithmic grouping, where groups are constantly being made, re-made, and deleted based on hyper complex probabilistics, this awareness is usually lacking.³²⁰

Furthermore, relying on the current EU data protection framework often falls short. Consider for instance the idea of consent, a cornerstone in individual data protection law.³²¹ It seems questionable whether the (often heavily in-

318 Joh, 'The New Surveillance Discretion' (n 138) 21; Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).

319 Mantelero, 'Personal Data for Decisional Purposes in the Age of Analytics' (n 140) 248; Bryce Goodman, 'Discrimination, Data Sanitisation and Auditing in the European Union's General Data Protection Regulation' (2016) 2 European Data Protection Law Review 493, 502 on the GDPR, and specifically art 9 juncto art 22(4).

320 Mittelstadt (n 317) 487–88; Alessandro Mantelero, 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment' (2018) 34 Computer Law & Security Review 754, 764.

321 GDPR, art 6(1)a.

toxicated) visitors to the Stratumseind gave informed consent to use their personal data for research purposes. And what about their rights to receive access to the data kept on them, in order to see if it is correct³²² or whether so-called ‘special categories’ of data such as their ethnicity or sexual orientation — easily guessed by observing e.g. the entrance to an LGBT nightclub — have been processed?³²³ Both questions are, from a legal perspective, moot because the Living Lab and Strava anonymize all data before analysis. The latter even gives users an opt-out to making their anonymized data available.³²⁴ The individual focus of the human rights framework means that the analysis of anonymous data, which by definition cannot be traced back to any individual, can never infringe any data protection rights. However, it is clear that groups can suffer the consequences of the processing of data that does not identify anyone in the group, for instance when a map clearly indicates where extra police presence might be needed or where antagonists can strike secret military bases.

Many have argued that under these circumstances it no longer makes sense to only defend the personal data protection rights of individuals.³²⁵ Rather, we should be protecting group rights, which are rights ‘possessed by a group qua

322 *ibid*, art 15.

323 *ibid*, art 9.

324 Drew Robb, ‘The Global Heatmap, Now 6x Hotter’ (*Medium*, 1 November 2017) <<https://medium.com/strava-engineering/the-global-heatmap-now-6x-hotter-23fc01d301de>> accessed 7 February 2018.

325 e.g. Mantelero, ‘Personal Data for Decisional Purposes in the Age of Analytics’ (n 140) 241; Mittelstadt (n 317); Linnet Taylor, Luciano

group rather than by its members severally³²⁶ and more specifically, the data protection rights of groups created by classification algorithms.³²⁷

However, group rights are an awkward fit for the current European data protection framework, which is heavily focused on individuals.³²⁸ Combined with the recent adoption of the GDPR and the associated legislative fatigue,

Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies* (Springer 2017) 2.

326 Peter Jones, 'Group Rights' (*Stanford Encyclopedia of Philosophy*, 29 March 2016) <<http://plato.stanford.edu/archives/sum2016/entries/rights-group/>> accessed 5 March 2018.

327 Supra (n 325).

328 Bart van der Sloot, 'Do Groups Have a Right to Protect Their Group Interest in Privacy and Should They? Peeling the Onion of Rights and Interests Protected under Article 8 ECHR' in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of data technologies* (Springer 2017); Lilian Edwards and Michael Veale, 'Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"?' (2018) 16 *IEEE Security & Privacy* 46, 47. Note that the existence of group (or collective) rights in general has long been a topic of debate within legal and political philosophy scholarship. There is not sufficient room within the current chapter to provide an overview that would do justice to this debate, but the interested reader may, for both pro and contra perspectives, refer to inter alia Peter Jones, 'Human Rights, Group Rights, and Peoples' Rights' (1999) 21 *Human Rights Quarterly* 80; Miodrag A Jovanović, *Collective Rights: A Legal Theory* (Cambridge University Press 2012); Tamir Yeal, 'Against Collective Rights' in Christian Joppke and Steven Lukes (eds), *Multicultural Questions* (Oxford University Press 1999); David Miller, 'Group Rights, Human Rights and Citizenship' (2002) 10 *European Journal of Philosophy* 178; Neus Torbisco Casals

which prevents any major innovations in data protection rights in the near future, it seems unlikely that group data protection rights will become a staple of data protection law in Europe anytime soon.³²⁹ This section has accentuated why this might be problematic. Therefore, the next section will introduce DPIAs, which might provide a workable solution that can be implemented without completely overhauling the legislative framework.

4.4 Making Group Rights Real through DPIAs?

DPIAs have been around for several decades,³³⁰ but the GDPR has renewed interest in them. The GDPR became directly applicable in the member states of the European Union (EU) on 25 May 2018.³³¹ It aims to create ‘first-rate data protection rules providing for the world’s highest standard of protection.’³³² Some of the central tools the GDPR employs in order to ensure this high standard are preventative measures, such

(ed), *Group Rights as Human Rights: A Liberal Approach to Multiculturalism* (Springer 2006).

329 Taylor, Floridi and van der Sloot (n 325) 233.

330 Although they already existed in a primordial form in the 1970s, their development really took flight after the mid 1990s. Roger Clarke, ‘Privacy Impact Assessment: Its Origins and Development’ (2009) 25 Computer Law & Security Review 123.

331 GDPR, art 99(2).

332 European Commission (n 227).

as storage limitations,³³³ codes of conduct,³³⁴ certification,³³⁵ data protection by design and by default,³³⁶ and rules on the security of personal data.³³⁷ This approach aimed at reducing risks seems fitting for personal data protection, as it can be difficult to predict harms³³⁸ and it might be even more complicated to reverse them.

DPIAs are a central instrument in this toolbox, and required if the processing of personal data is ‘likely to result in a high risk to the rights and freedoms of natural persons.’³³⁹ In cases where it is unclear whether high risks will materialize, the Article 29 Working Party recommends that a DPIA be carried out nonetheless in order to minimize risks and ensure compliance.³⁴⁰ ‘A DPIA is a process designed to describe the processing, assess its necessity and proportionality and

333 GDPR, art 5(1)e.

334 *ibid*, art 40.

335 *ibid*, art 42.

336 *ibid*, art 25.

337 *ibid*, art 32.

338 Arvind Narayanan, Joanna Huey and Edward W Felten, ‘A Precautionary Approach to Big Data Privacy’ in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, vol 24 (Springer Netherlands 2016) 358.

339 GDPR, art 35(1).

340 Article 29 Data Protection Working Party, ‘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)’ 8 <ec.europa.eu/newsroom/document.cfm?doc_id=47711> accessed 2 February 2018.

help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data.’³⁴¹ This process can take many forms depending on, *inter alia*, the type of personal data processing being assessed³⁴² but its minimum requirements are: a description of the processing; an assessment of the proportionality and necessity of the processing (i.e. can the same aim be achieved with less personal data processing); measures to minimize risks to data subjects; and an active involvement of those data subjects.³⁴³

Crowdsourced maps are usually of publicly accessible areas such as streets, neighbourhoods and parks, if only because it would be hard to find a crowd in an area that is *not* publicly accessible.³⁴⁴ In particular, the GDPR requires DPIAs if ‘systematic monitoring of a publicly accessible area on a large scale’ takes place.³⁴⁵ The Article 29 Working Party points out that such data collection can be especially problematic because data subjects might not be aware of the data processing. Furthermore, they might not be able to prevent their data from being collected without avoiding the public area in question, rendering the public place less public and

341 *ibid* 31. Note that the Article 29 Working Party has been renamed to the European Data Protection Board (EDPB) when the GDPR came into force. GDPR, art 68–76.

342 Article 29 Data Protection Working Party, ‘Guidelines on DPIA’ (n 340), annex 1.

343 *ibid*, annex 2.

344 Although not completely impossible if one for instance invites a crowd of people to their private castle or estate.

345 GDPR, art 35(3)c.

any form of consent meaningless.³⁴⁶ Therefore, safeguards to gauge and minimize risks are certainly needed, and it seems it will be nigh on impossible to avoid doing a DPIA when gathering crowdsourced data for making maps.

As DPIAs are thus a necessary step in the development of crowdsourced maps, they might form a promising avenue to address the problems identified in the previous section. As we have seen however, trying to deal with group data protection rights within the EU data protection framework achieves unsatisfactory results. So why should Data Protection Impact Assessments be better suited to deal with map-making algorithms that analyse crowdsourced data if they are a part of that same framework? In the next two subsections, only those aspects that are pertinent to this specific question will be dealt with. Many others have already written extensively on DPIAs and proposed various models and frameworks.³⁴⁷ The object here is not to duplicate their work

346 Article 29 Data Protection Working Party, 'Guidelines on DPIA' (n 340) 9.

347 See, among many others, e.g. the interactive software released by the French Data Protection Authority, the Commission Nationale de l'Informatique et des Libertés, 'The Open Source PIA Software Helps to Carry out Data Protection Impact Assessment' (CNIL, 31 May 2018) <<https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment>> accessed 28 August 2018; Commission Nationale de l'Informatique et des Libertés, 'Privacy Impact Assessment (PIA) Templates' <<https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf>> accessed 28 August 2018; Information Commissioner's office, 'Sample DPIA Template' <<https://ico.org.uk/media/for-organisations/>

or add yet another model, but to suggest how, within existing models, a small extension could yield significant results.

4.4.1 Opportunities

Counter-intuitively, the embeddedness of DPIAs provides an opportunity to enhance the protection of group data protection rights *within* the current legal framework. Many other proposals exist to include various ethical, social, and human rights considerations in a plethora of impact assessment tools.³⁴⁸ These can serve as important inspirations and templates in the context of crowdsourced map-making initiatives. However, they form an additional financial and administrative burden that data controllers are called upon to voluntarily shoulder. By adding group rights to an already

documents/2258857/dpia-template-v1.docx> accessed 28 August 2018; The 'Guidelines on DPIA' (n 340) by the Article 29 Working Party could be read in this light; Mantelero, 'AI and Big Data' (n 320); See also various contributions to the edited volume by David Wright and Paul de Hert (eds), *Privacy Impact Assessment* (Springer 2012).

- 348 e.g. Nora Götzmann and others, 'Human Rights Impact Assessment Guidance and Toolbox (Road-Testing Version)' <https://www.humanrights.dk/sites/humanrights.dk/files/media/dokumenter/business/hria_toolbox/hria_guidance_and_toolbox_final_may22016.pdf.223795_1_1.pdf> accessed 24 August 2018; David Wright and Michael Friedewald, 'Integrating Privacy and Ethical Impact Assessments' (2013) 40 *Science and Public Policy* 755; David Wright and Emilio Mordini, 'Privacy and Ethical Impact Assessment' in David Wright and Paul De Hert (eds), *Privacy Impact Assessment* (Springer Netherlands 2012); Barbara Skorupinski and Konrad Ott, 'Technology Assessment and Ethics: Determining a Relationship in Theory and Practice' (2002) 1 *Poiesis & Praxis* 95.

existing requirement, these costs could be significantly decreased.

The most straightforward way in which group data protection rights for crowdsourced mapmaking initiatives can be safeguarded is the same way in which personal data protection rights are safeguarded: by ‘assessing [risks] and determining the measures to address them.’³⁴⁹ Many already established personal data protection principles could be applied to address any identified risks for groups. Consider, for example, how the data minimization principle could also be applied to anonymous data. In the Strava example mentioned above this simple procedure could have prevented the company great reputational loss, not to mention the unknown costs to military operations.

This example also shows how important the proactive nature of DPIAs is in making group rights real. DPIAs should be engaged in ‘as early as is practicable’³⁵⁰ in order to prevent risks from materializing. As was discussed in the section ‘Maps and (Missing) Group Rights,’ it can be difficult to reliably reconstruct what has happened once an algorithm has grouped individuals. Therefore, it is preferable to set limits and objectives beforehand³⁵¹ by, for instance auditing algorithms for disparate impacts using simulated data.³⁵²

349 Article 29 Data Protection Working Party, ‘Guidelines on DPIA’ (n 340) 4.

350 *ibid* 14.

351 Mittelstadt (n 317) 489.

352 Goodman (n 319) 503.

Besides these more general opportunities for the inclusion of group data protection rights within DPIAs, the GDPR contains a clause with specific relevance for crowdsourced mapmaking initiatives: ‘where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing.’³⁵³ At its most basic, this clause allows data controllers to seek these views and perhaps include them in the final report of the DPIA, but then essentially discount them. However, if properly engaged with, it also allows data subjects to co-produce the environments in which they live.³⁵⁴

This opportunity is created by the considerable performative power of maps, as discussed in section 4.2 ‘How Maps are Made.’ By affording local groups access to the development process, they gain ownership³⁵⁵ over the production of the map and thus their surroundings. For instance, they can have a voice in what maps will and will not show, in which way, and to whom³⁵⁶. This ability to contribute to the meaning of spaces makes DPIAs for crowdsourced maps especial-

353 GDPR, art 35(9).

354 Henri Lefebvre, ‘Right to the City’ in Eleonore Kofman and Elizabeth Lebas (eds), *Writings on Cities* (Blackwell 1996) 79.

355 To be understood in the manner that e.g. Michiel de Lange and Martijn de Waal use to the term; ‘Owning the City: New Media and Citizen Engagement in Urban Design’ (2013) 18 *First Monday* <<http://journals.uic.edu/ojs/index.php/fm/article/view/4954>>.

356 Adam Greenfield and Mark Shepard, *Urban Computing and Its Discontents* (The Architectural League of New York 2007) 44.

ly well suited for empowering residents;³⁵⁷ it allows them to change their environment from a space that they happen to live in and that others map, to a space that is mapped and co-produced by them.³⁵⁸

Such a co-production can be modelled after consent, one of the pillars of personal data protection law. Consent should always be given beforehand³⁵⁹ and by the affected data subject itself. Consent is only valid if, *inter alia*, it meets the connected requirements that it is informed, granular, and specific.³⁶⁰ By integrating these requirements into DPI-As, groups are given a way to meaningfully co-produce the crowdsourced maps and the GIS software – and thus their

357 For a parallel argument, see Simon Walker, *The Future of Human Rights Impact Assessments of Trade Agreements* (Intersentia 2009) 41 <<https://dspace.library.uu.nl/bitstream/handle/1874/36620/walker.pdf>> accessed 24 August 2018.

358 Lefebvre (n 354) 79; For a similar argument from the disciplines of human geography and urban studies, see Paolo Cardullo and Rob Kitchin, ‘Being a “Citizen” in the Smart City: Up and down the Scaffold of Smart Citizen Participation in Dublin, Ireland’ (2019) 84 *Geo-Journal* 1; and the seminal work by Sherry R Arnstein, ‘A Ladder Of Citizen Participation’ (1969) 35 *Journal of the American Institute of Planners* 216.

359 Although consent can also be withdrawn at any time (GDPR, art 7(3)); this can be difficult in this context as will be discussed below.

360 Article 29 Data Protection Working Party, ‘Guidelines on Consent under Regulation 2016/679’ 11–15 <http://ec.europa.eu/newsroom/document.cfm?doc_id=48849> accessed 3 April 2018.

living environments — at a stage when some of the processing operations are still unknown.³⁶¹

Delegates from local³⁶² communities should be included to directly speak for those affected and in turn, affect the mapmaking process and the spaces they inhabit. In addition, they alone can meaningfully and actively co-produce their environment on behalf of its inhabitants. The inclusion of representatives from disadvantaged groups can help in trying to avoid bias and discrimination. As was pointed out above, georeferenced data gathering tends to underrepresent already disadvantaged groups³⁶³ and if data is collected on these groups, it usually further stigmatizes them.³⁶⁴ The inclusion of these groups should draw the attention of map-makers to their specific concerns at an early stage.³⁶⁵

The benefit of including digital rights associations is that they can represent groups of which the existence is not yet known and can contribute expert knowledge.³⁶⁶ As was pointed out in section 4.3 ‘Maps and (Missing) Group

361 Article 29 Data Protection Working Party, ‘Guidelines on DPIA’ (n 340) 14.

362 The exact scale of ‘local’ is not defined here, as it will depend on the mapmaking effort in question. When making a global map, ‘local’ might thus very well include the world population.

363 Pak, Chua and Moere (n 207).

364 Brannon (n 315).

365 Wright and Mordini (n 348) 402.

366 Mantelero, ‘Personal Data for Decisional Purposes in the Age of Analytics’ (n 140) 252; Mantelero, ‘From Group Privacy to Collective Privacy’ (n 237) 153.

Rights’ it can be impossible to predict, or even reconstruct after the fact, which groups the algorithms constantly (re) generate. This would mean that any unforeseen groups are automatically excluded from the DPIA. In order to prevent this, digital rights associations may represent them. Note that it would seem appropriate for representatives of such associations to be cautious beyond this specific remit.

The selection of representatives is a difficult task,³⁶⁷ but the GDPR gives a hint at who might be welcome at the table regardless. Article 80 outlines how individual data subjects can mandate a ‘not-for-profit body, organisation or association which [...] has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects’ rights and freedoms with regard to the protection of their personal data’³⁶⁸ to represent them when lodging a complaint with a DPA³⁶⁹ or when seeking a judicial remedy against a DPA, data controller, or processor.³⁷⁰ This list could be expanded – either informally by data controllers currently executing a DPIA, or eventually by the European legislator – to include the representation of data subjects during DPIAs in the sense of article 35(9) of the GDPR.

367 See also the next subsection 4.4.2.

368 GDPR, art 80(1).

369 *ibid*, art 77.

370 *ibid*, art 78 and 79.

4.4.2 Limitations

Although the EU legislator pays lip service to the ethical and social issues that result from large scale data processing and have an impact beyond the individual, these are included neither in article 35 of the GDPR which describes Data Protection Impact Assessments, nor in the various DPIA models provided by the Data Protection Authorities (DPA) of the member states.³⁷¹ As a result, despite the many opportunities listed above, a number of important limitations to DPIAs as a tool for enhancing group data protection rights in the context of crowdsourced mapmaking needs to be considered.

A fundamental limitation to the possibility of using DPIAs as embedded in the GDPR is formed by the voluntary nature of the inclusion of groups and their representatives in the process. Article 35(9) is qualified as follows: ‘*Where appropriate*, the controller shall seek the views of data subjects or their representatives on the intended processing [...]’ (emphasis added). It remains unclear, at least for the moment, where this would and would not be appropriate; a situation that the Article 29 Working Party failed to remedy in its opinion on DPIAs.³⁷² It seems improbable that companies

371 Mantelero, ‘AI and Big Data’ (n 320) 756; GDPR, recital 75. See also footnote 347.

372 Raphaël Gellert, ‘The Article 29 Working Party’s Provisional Guidelines on Data Protection Impact Assessment’ (2017) 3 European Data Protection Law Review 212, 215; Atanas Yordanov, ‘Nature and Ideal Steps of the Data Protection Impact Assessment Under the General Data Protection Regulation’ (2017) 3 European Data Protection Law Review 486, 493; Dariusz Kloza and others, ‘Data Protection Impact

will interpret this provision widely and be eager to engage in the time-consuming, costly, and potentially politically laden process³⁷³ if it can easily be avoided. As seen above, however, it would be exactly this inclusion that engenders many opportunities.

If we assume that companies do engage in DPIAs and include affected data subjects and representatives of local (disadvantaged) groups, many limitations still remain. First of all, when we compare the data protection rights of groups that can be protected through DPIAs to the rights that individuals have over their personal data, it seems that it is chiefly the prohibition on the processing of special categories of data that can be somewhat enhanced through engaging in DPIAs. Left by the wayside are many other principles, such as for example accuracy, accountability, confidentiality, or a lawful basis for processing such as informed and freely given consent.³⁷⁴ For now, these data protection principles seem out of reach for groups.

The selection of groups to be represented would also present a data controller eager to conduct a DPIA with major difficulties. As was discussed in section 4.2 ‘How Maps are Made’ it is impossible to pinpoint exactly who produces,

Assessments in the European Union: Complementing the New Legal Framework towards a More Robust Protection of Individuals’
3 <https://cris.vub.be/files/32009890/dpialab_pb2017_1_final.pdf>
accessed 17 August 2018.

373 Mantelero, ‘AI and Big Data’ (n 320) 755.

374 See GDPR, art 5 for a more comprehensive set of data processing principles.

edits, or consumes a contemporary map; we could add to this confusion those who are impacted by a map. Even if it would be possible to neatly separate these roles and find suitable representatives for each affected group, the composition of all the groups that will (or might) be formed by an algorithm cannot always be known beforehand. Furthermore, many distinct local communities are not neatly divided in classical neighbourhoods³⁷⁵ and the involvement of neighbourhood associations, which may be easy to access for data controllers, might not lead to accurate representation. Finally, assuming that a somewhat complete overview of groups to be represented has been established, it is extremely difficult to decide who can speak on behalf of each group.³⁷⁶ As the success of a DPIA hinges on the accurate composition of the groups and involvement of their representatives, careful consideration for each separate DPIA is warranted.³⁷⁷

Finally, even if companies do engage in the process initially and include as many views as possible, for a DPIA to be truly successful it should be a circular process that is reg-

375 Alan Harding and Talja Blokland-Potters, *Urban Theory: A Critical Introduction to Power, Cities and Urbanism in the 21st Century* (Sage 2014) 179.

376 Mantelero, 'Personal Data for Decisional Purposes in the Age of Analytics' (n 140) 254; Mantelero, 'From Group Privacy to Collective Privacy' (n 237) 150.

377 The permanent ad-hoc committees proposed by Mantelero might provide some solace for specific data controllers, although it remains unclear who would be responsible for solving the underlying problem: 'AI and Big Data' (n 320) 771.

ularly repeated. This is even more important if self-learning algorithms are employed as their outcomes can show unexpected changes over time. This can include changes in the groups targeted, thus necessitating a constant updating of the composition of representatives. The costs necessary to continually assess the possible negative impacts of crowd-sourced mapmaking software that has already been written and released might not, in the view of profit maximizing companies, be justified by the possible results.

4.5 Conclusion

The question asked at the beginning of the chapter was whether DPIAs could form a panacea or a Band-Aid when protecting group data protection rights in crowdsourced mapmaking initiatives. It laid out the strong performative power of maps and how crowdsourced data is used to make them. Then, it introduced how this practice interacts with the current personal data protection framework in the European Union, leaving undesirable gaps in the safeguarding of group rights. Finally, it introduced Data Protection Impact Assessments and discussed how they could help in alleviating these problems without overhauling the current legislative framework in the EU.

When taking stock of both the opportunities and limitations that DPIAs offer for group data protection rights in crowdsourced mapmaking initiatives it seems that they could easily be circumvented, their effect would be limited at best, that the proper representation of groups is high im-

possible, and that their long-term impact is uncertain in the face of self-learning algorithms. Still, companies interested in retaining consumer trust — and gaining a competitive advantage when dealing with responsible customers and partners — would be well-advised to make the investment. This goes doubly so for governmental bodies and institutions: DPIAs form an opportunity to use group rights to put the performative power of maps in the hands of those being mapped. Despite the many gaps and pitfalls, DPIAs for map-making initiatives that utilize crowdsourced georeferenced data should be performed, and they should include as many views as possible; Public space should belong to the public, not to companies writing mapping software.

It is up to the EU legislature — and in the meantime: the European Data Protection Board, formerly known as the Article 29 Working Party, whose importance ‘for the EU data protection cannot be overstated’³⁷⁸ — to ensure that group data protection rights can be properly incorporated within the European Data Protection framework. This is the only way to ensure that the uncomfortable Band-Aid proposed in this chapter becomes unnecessary and can be ripped off.

378 Paul de Hert and Vagelis Papakonstantinou, ‘The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?’ (2016) 32 Computer Law & Security Review 179, 193.

**5. Capturing licence
plates: police participation
apps from an EU data
protection perspective**

Previously published as: Jonida Milaj and Gerard Jan Ritsema van Eck, 'Capturing Licence Plates: Police-Citizen Interaction Apps from an EU Data Protection Perspective' (2020) 34(1) *International Review of Law, Computers & Technology* 1 (doi: 10.1080/13600869.2019.1600335).³⁷⁹ Some minor spelling and grammar errors have been corrected in, and a postscript has been added to this version.

379 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.

Abstract

In October 2017 a Pokémon Go-like smartphone app called ‘Automon’ was revealed 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 in case a vehicle is indeed stolen they might qualify for a financial reward. In addition, when someone reports that a vehicle has recently been stolen, game participants that are in the vicinity receive a push notification and are tasked to search for that specific vehicle and license plate.

This chapter 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 the involvement of individuals in law enforcement activities and confronts them for the first time with the data protection standards of the European Union (EU). It is concluded that the Automon app design fails to comply with the new legal standards at EU level.

5.1 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

In October 2017 the Dutch police chief Erik Akerboom revealed several new initiatives to increase the public's contribution and engagement in investigation activities.³⁸⁰ One of these initiatives is the development of a Pokémon Go-like³⁸¹ smartphone app called 'Automon'³⁸². Automon is designed in the form of a game that instigates participants to photograph

380 John van den Heuvel and Mick van Wely, 'Politiepokémon op komst: Burgers kunnen met app gestolen auto's opsporen' (*De Telegraaf*, 7 October 2017) <<https://www.telegraaf.nl/nieuws/552919/politie-pokemon-op-komst>> accessed 15 May 2018; Arnout de Vries, 'App: Automon' (*Social Media DNA*, 18 October 2017) <<http://socialmediadna.nl/automon/>> accessed 15 May 2018.

381 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.

382 Note that 'Automon' was used as a working title only, and that it is also the name of a company which develops case management software for probation agencies in the United States of America, see 'About Us' (*AutoMon: innovative solutions for Community-Based Corrections*, 2018) <<https://automon.com/about/>> accessed 14 May 2018. Furthermore, Automon is one of the main antagonists in a Power Rangers episode, see Sakamoto Koichi, 'Forever Red' (*Power Rangers: Wild Force*, 5 October 2002).

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 qualify for a financial reward. In addition, when someone reports that a car has recently been stolen, 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 surveillance³⁸³ and the involvement of individuals in police activities is not a new phenomenon. Distributing the labour between the law enforcement and individuals is considered fruitful since it relies on a multitude of watchers and it has the benefit of achieving a particular goal that might otherwise be difficult to achieve due to the limited resources that law enforcement has at its disposition. 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 with 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 the

383 Albrechtslund and Lauritsen (n 21) 314.

law enforcement personal data of others. The simple participation in a game with the scope to assist the law enforcement in their activities might turn individuals in joint data controllers or processors and place upon them the rights and obligations prescribed by the applicable laws and regulations.

This chapter 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).³⁸⁴

The case study of the Automon app is analysed in light of the applicable EU legislation and case law. 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 5.2 provides background information on the role of technologies in the involvement of citizens in police activities, crowdsourced surveillance, and digilantism³⁸⁵. Section 5.3 analyses the

384 More specifically the GDPR (n 75) and the Law Enforcement Directive (n 76).

385 A portmanteau of 'digital' and 'vigilante' (seemingly) first coined by Ruth Martin 'Digilante Justice: Citizenship in Cy-

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, in section 5.4 are discussed the legal implications of the findings of the previous sections.

5.2 The Automon app: Surveillance, game, or both?

Lots of people, elderly, but also youngsters were running on the street looking after Pokémons [sic]. So we said: Hey, if they are looking after Pokémons [sic], can they go after stolen cars?

— Bart Driessen

This section introduces the Automon app under scrutiny in this chapter. 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.

Note that the description of the Automon app in this chapter is primarily based on a telephone interview conducted in June 2018 with Police Commissioner Bart Dries-

berspace' (2007) 16 *The New Atlantis* 124.

Figure 5.1: 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.

sen, 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 chapter 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 5.2.2 the importance of the selection of users and how they are instructed is considered. In the final subsection 5.2.3 attention is paid to how they are enticed to keep using the app.

5.2.1 Background

A typical scenario of use of the Automon app might start with the user spotting a suspicious vehicle.³⁸⁶ 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

386 The app provides guidance on what characteristics a user might want to look out for, a point to which we will return below.

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 her/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 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.³⁸⁷ 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 depend 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 does not have the tools to recognize stolen cars: “If you don’t tell the public

387 Deborah Lupton, ‘Apps as Artefacts: Towards a Critical Perspective on Mobile Health and Medical Apps’ (2014) 4 *Societies* 606.

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.³⁸⁸ 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

388 Schneider and Trottier (n 130).

fears of vigilantism and other forms of ‘cowboy-ish’ behaviours when citizens are actively involved in neighbourhood watch groups.³⁸⁹ Therefore, the police prefer 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.³⁹⁰

An interesting counter-example to the Vancouver riots that 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.³⁹¹ However, several people were wrong-

389 Jason Pridmore and others, ‘Keeping an Eye on the Neighbours: Police, Citizens, and Communication within Mobile Neighbourhood Crime Prevention Groups’ (2019) 92 *The Police Journal: Theory, Practice and Principles* 97, 110.

390 *ibid* 108–112; Keith Spiller and Xavier L’Hoiry, ‘Watch Groups, Surveillance, and Doing It for Themselves’ (2019) 17 *Surveillance & Society* 288; Anouk Mols and Jason Pridmore, ‘When Citizens Are “Actually Doing Police Work”: The Blurring of Boundaries in WhatsApp Neighbourhood Crime Prevention Groups in The Netherlands’ (2019) 17 *Surveillance & Society* 272.

391 Edward F III Davis, Alejandro A Alves and David Alan Sklansky, ‘Social Media and Police Leadership: Lessons From Boston’ [2014] *New Perspectives in Policing* 1; Christopher Cassa and others, ‘Twitter as a Sentinel in Emergency Situations: Lessons from the Boston Marathon Explosions’ [2013] *PLoS Currents: Disasters* <<http://currents.plos.org/disasters/?p=8687>> accessed 2 May 2018; Kate Starbird and others, ‘Rumors, False Flags, and Digital Vigilantes: Misinformation on Twitter after the 2013 Boston Marathon Bombing’,

ly 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.³⁹² 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 stolen SUV, the remaining suspect was arrested.

Similarly, during the aftermath of the terrorist attacks in Paris in November 2015 the Brussels police had to ask the

iConference 2014 Proceedings (iSchools 2014) <<http://hdl.handle.net/2142/47257>> accessed 24 March 2016; Dave Lee, 'Boston Bombing: How Internet Detectives Got It Very Wrong' *BBC News* (19 April 2013) <<http://www.bbc.com/news/technology-22214511>> accessed 16 February 2016.

- 392 David Montgomery, Sari Horwitz and Marc Fisher, 'Police, Citizens and Technology Factor into Boston Bombing Probe' *The Washington Post* (21 April 2013) <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> accessed 14 September 2018; David Montgomery, Marc Fisher and William Branigin, 'FBI Releases Images of Two Suspects in Boston Marathon Bombings' *Washington Post* (18 April 2013) <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> accessed 14 September 2018.

users of Twitter to remain silent because tweets might give away movements of the police in real time — to which the public dutifully responded by flooding related hashtags with pictures of cats.³⁹³ 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.³⁹⁴ However, seen from a more critical perspective the Automon app also fits in an ongoing trend of using networked computing technologies to responsabilize citizens for government tasks.³⁹⁵ Mantello poignantly called such forms of

393 Kevin Rawlison, 'National Emergency? Belgians Respond to Terror Raids with Cats' (*The Guardian*, 22 November 2015) <<http://www.theguardian.com/world/2015/nov/22/national-emergency-belgians-respond-with-cats>> accessed 8 February 2016.

394 e.g. Timan and Albrechtslund (n 15) 855.

395 e.g. van Brakel and de Hert (n 225); Cardullo and Kitchin (n 358); Koskela, "Don't Mess with Texas" (n 27); Larsson (n 205); Peter Mantello, 'The Machine That Ate Bad People: The Ontopolitics of the Precrime Assemblage' (2016) 3 *Big Data & Society* 1; Marx (n 132); Pridmore and others (n 389); Purenne and Palierse (n 180); Antonio Vera and Oliver Salge Torsten, 'Crowdsourcing and Policing: Opportunities for Research and Practice' [2017] *European Police Science and Research Bulletin* 143; Trottier (n 112); Andrew Millie, 'Citizens

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-centred, pro-active, net-worked and, at times, and [sic] gamified versions of automated governance”³⁹⁶ (italics in original). On this view, the app mostly exists to offload what should be police tasks to an untrained and unpaid work force of volunteers who cannot — but perhaps should, as we shall see in the next section 5.3 — be held accountable.

Such responsabilization 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 Lui.³⁹⁷ Crowdsensing is especially well suited for collecting data from public spaces as people often carry their smartphones with them wherever they go. Crowdsensing application can be anything from fully participatory to ful-

in Policing: The Lived Reality of Being a Police Support Volunteer’ (2019) 29 Policing and Society 407; Mols and Pridmore (n 390).

396 Mantello (n 395) 2.

397 ‘Mobile Crowdsensing: Current State and Future Challenges’ (2011) 49 IEEE Communications Magazine 32.

ly opportunistic.³⁹⁸ 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.’³⁹⁹ 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 subsections). On the other hand, the police receive the location of stolen vehicles and consequently the possibility

398 *ibid* 32.

399 Haosheng Huang and others, ‘Location Based Services: Ongoing Evolution and Research Agenda’ (2018) 12 *Journal of Location Based Services* 63, 1.

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 that, as will be discussed in the legal analysis below, also has important legal repercussions under the new personal data protection regime of the EU.

5.2.2 Directing the surveillant gaze

When citizens are enrolled in surveillance practices, they must learn how to apply a “surveillant gaze”⁴⁰⁰ 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.⁴⁰¹ 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:⁴⁰²

400 Gary T Marx, *Undercover: Police Surveillance in America* (University of California Press 1988); Foucault (n 21).

401 Larsson (n 205) 97; Micheal R Curry, ‘The Profiler’s Question and the Treacherous Traveler: Narratives of Belonging in Commercial Aviation’ (2004) 1 *Surveillance & Society* 475.

402 See also Larsson (n 205) 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 practice⁴⁰³ 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

403 See also Lyon, *The Culture of Surveillance* (n 18).

than actual rules.⁴⁰⁴ Users are free — and even encouraged (see the next subsection 5.2.3) — 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.⁴⁰⁵ 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 utilize 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 them⁴⁰⁶ and the

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

405 Larsson (n 205) 98; Ritsema van Eck (n 202) 163–64.

406 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

Figure 5.2: A screenshot of the map view in a prototype of the Automon app. Notice how it uses a stylized map in a similar manner to Pokémon Go (see Figure 5.1), albeit with a cooler colour scheme. Screenshot provided by the Dutch Police.

ANPR-capabilities of the app might be a timesaving way of ensuring compliance. On the other hand, businesses might choose not to jeopardize 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.⁴⁰⁷

The second group to which the app will be marketed are gamers. In this manner, the police hope to benefit from the popularity of Pokémon Go and other mobile games. However, it is not clear how this will be done and several questions might be raised. If the police aim 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?

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.

407 Latour (n 20) 181.

The label of ‘gamer’ hardly discriminates in today’s world. Pokémon Go, which was downloaded over 800 million times worldwide,⁴⁰⁸ itself is a demonstration that especially casual mobile gaming has become a mainstream activity.⁴⁰⁹ 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 aim to approach gamers indirectly, then the call must be sent to the 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 gamers⁴¹⁰ might use their surveillant gaze: First, if they try to score points in Automon, they might

408 Iain Harris, ‘Pokemon Go Captures 800 Million Downloads’ (*pocketgamer.biz*, 30 May 2018) <<http://www.pocketgamer.biz/news/68209/pokemon-go-captures-800-million-downloads/>> accessed 11 October 2018.

409 In 2015 there were 3.429 billion mobile broadband subscriptions worldwide ITU Telecommunication Development Bureau, ‘ICT Facts and Figures 2015’ <<https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf>> accessed 11 October 2018. This means that Pokémon Go was installed on approximately 1 in 4.3 smartphones with internet access worldwide.

410 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.

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 experienced 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.⁴¹¹ This could lead to more police resources being spent on those areas compared to low-income areas.⁴¹² 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 found that such tools are used to keep those who are ‘others’ out of homogenous areas.⁴¹³ 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

411 Anselin and Williams (n 203) 318.

412 Joh, ‘Policing by Numbers’ (n 139); Joh, ‘The New Surveillance Discretion’ (n 138).

413 (n 180) 88.

Figure 5.3: 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 October 19, 2018.

Figure 5.4: A screenshot of the garage view in a prototype of the Automon app, showing a car that can be upgraded, or “pimped,” using in-game currency. Screenshot provided by the Dutch Police.

are part of a disadvantaged group find their number plates will be scanned more often.⁴¹⁴ After all, can ‘someone like that’ really afford a ‘car like that’?

5.2.3 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 Figure 5.3 and Figure 5.4. 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 5.4). 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

414 Gandy, ‘Exploring Identity and Identification in Cyberspace’ (n 136); Gandy, ‘Quixotics Unite!’ (n 136); Ritsema van Eck (n 202) 168–69.

milestones, such as scanning fifty number plates, might earn the player bonus in-game points.

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 utilize (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 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.⁴¹⁵ Whereas play is ‘quite consciously outside “ordinary” life as being “not serious,”’⁴¹⁶ 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.’⁴¹⁷ There

415 Julie E Cohen, ‘The Surveillance-Industrial Complex: The Irony of the Participatory Turn’ in Darin Barney and others (eds), *The Participatory Condition in the Digital Age* (University of Minnesota Press 2016) 210–11.

416 Johan Huizinga, *Homo Ludens: A Study of the Play-Element in Culture* (Routledge & Kegan Paul 1980) 13.

417 *ibid.*

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 want 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 aspire 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 have chosen a whimsical, game-like form. Because of these divergences, the Automon app is neither a dedicated surveillance app, nor a dedicated game.

5.3 Legal Analysis

Having discussed 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 Law Enforcement 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 subsection 5.2.1 ‘Background’ above will probably lead to a multitude of similar initiatives by police forces throughout Europe.

5.3.1 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 Law Enforcement 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.⁴¹⁸ 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.*”⁴¹⁹ In the case of number plates, the obvious means of identification are the vehicle registration databases that each Member State is required to maintain.⁴²⁰ 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 5.3.3 ‘Automon app users under the Law Enforcement 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.⁴²¹ The Court of Justice followed this line of reasoning in its decision.⁴²² Whether the police actually use this authority either in general or in specific cases does

418 Convention on Road Traffic (concluded 8 November 1986, entered into force 21 May 1977) 1042 UNTS 17, art 35–36.

419 GDPR, recital 26; Law Enforcement Directive, recital 21.

420 Convention on Road Traffic (n 418), art 35–36.

421 Case C–582/14 *Breyer* (n 246), Opinion of AG Sánchez-Bordona, paras 68–73.

422 Case C–582/14 *Breyer* (n 246), para 46.

not matter.⁴²³ 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. This goes even stronger for the number plates of stolen vehicles, as the police will have files on any those vehicles, which make direct identification possible. Thus, number plates qualify as personal data: The strict European personal data protection framework should be applied to what might seem an amusing diversion.

5.3.2 GDPR or Law Enforcement 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.⁴²⁴ 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 that regulate the collaboration between law enforcement

423 *ibid*, para 47–8.

424 Gstrein and Ritsema van Eck (n 297) 79.

and citizens, the data protection legislation is very broad and accommodates such situations. In their work on community policing in EU law, Al-Sharieh and Mifsud Bonnici find the legal bases for such an activity broadly in the rule of law and the crime prevention framework.⁴²⁵

Generally, the GDPR applies when individuals process personal data of their fellow citizens. 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,⁴²⁶ processing of data that falls in the area of Common Foreign and Security Policy,⁴²⁷ and processing for law enforcement activities for the scope of prevention, detection, investigation, and prosecution of crime.⁴²⁸ In the latest case, the Law Enforcement Directive applies.⁴²⁹

There are no indications that the Automon app collects and processes data for the purpose of foreign, security and defence policy. The exception of the purely personal and household activities would have been valid if the app had only one function, the gaming one. However, the double function of

425 Saleh Al-Sharieh and Jeanne Mifsud Bonnici, 'From the Persuasion of Theory to the Certainty of Law: A Multi-Jurisdictional Analysis of the Law of Community Policing in Europe' (2018) 5 *European Journal of Comparative Law and Governance* 179, 182.

426 GDPR, art 2(2)c.

427 GDPR, art 2(2)b.

428 GDPR, art 2(2)d.

429 Law Enforcement Directive, art 1(1).

the app as a game and as a surveillance tool makes the situation different. The fact that the data are sent to the RDW 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 Law Enforcement Directive is more complicated.

The Law Enforcement 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.⁴³⁰ 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 app users in this case carry out the crime investigation and detection activity 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 en-

430 Law Enforcement Directive, recital 11, art 3(7).

forcement could evade its legal obligations by making use of private agents.⁴³¹ Thus, situations in which the police may have not been involved in directly, but in which it has collaborated with or trusted on individuals to collect information, also fall under the field of the law enforcement activities.⁴³² In our case, in order to avoid the possibility that law enforcement agencies can circumvent their legal obligations⁴³³ by making use of individuals that carry on law enforcement tasks via smartphone games, the Law Enforcement 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 Law Enforcement 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

431 *Van Vondel v The Netherlands* App no 38258/03 (ECtHR, 25 October 2007), para 49.

432 *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.

433 Nadezhda Purtova, ‘Between the GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public–Private Partnerships’ (2018) 8 *International Data Privacy Law* 52, 59.

and, secured from unauthorized or unlawful processing.⁴³⁴ While these principles seem to be generally addressed by the design of the app, other legal aspects need consideration and are discussed below.

5.3.3. Automon app users under the Law Enforcement Directive

After establishing in the previous section that the Law Enforcement 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 Law Enforcement 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.⁴³⁵

After establishing that the data collected in the framework of the Automon app qualify as personal it is easy to es-

434 Law Enforcement Directive, art 4(1).

435 Law Enforcement Directive, art 1(3).

tablish 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 based on 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 Law Enforcement 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.”⁴³⁶

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 subsection 5.2.2 ‘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.

436 Law Enforcement Directive, art 3(8).

Thus, the provisions of the Law Enforcement 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 Law Enforcement Directive.

5.4 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 Law Enforcement 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 Law Enforcement 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.⁴³⁷ 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

⁴³⁷ Law Enforcement Directive, art 22(1).

implementing the Law Enforcement Directive⁴³⁸ introduced article 6c to the *Wet politiegegevens* (Police data law) on *verwerkers* (processors). Together with the delegated legislation⁴³⁹ which added article 6:1b to the *Besluit politiegegevens* (Decision police data), it almost literally transposes the conditions laid down in the Law Enforcement Directive.

In its current design, the Automon app does not comply with this requirement. In the Automon app, participants to the game 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

438 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.

439 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.

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.⁴⁴⁰ This principle determines the necessary and sufficient conditions for limiting a protected right⁴⁴¹ as well as serves to restrict the exercise of powers from the State authorities.⁴⁴²

As it was argued also in subsection 5.2.2 ‘directing the surveillant gaze’, law enforcement may receive a large amount of personal data from non-qualified and non-specialized sources through Automon. As a result, not all the data transferred by the individuals to law enforcement 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

440 Jonida Milaj, ‘Invalidation of the Data Retention Directive: Extending the Proportionality Test’ (2015) 31 Computer Law & Security Review 604.

441 Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* (Cambridge University Press 2012) 3.

442 Jacobine van den Brink and others, ‘General Principles of Law’ in Jan H Jans, Sacha Prechal and Rob Widdershoven (eds), *Europeanisation of public law* (Europa Law Publishing 2007) 143.

the game-like design of Automon. As a result, law enforcement will be overloaded with personal data that, even if do not match 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 conceptualized 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 Law Enforcement Directive⁴⁴³ 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 Auto-

443 Implemented in Dutch law in article 32 of the *Wet Politiegegevens*.

mon system, only collection and erasure take place, but no consultation and disclosure. Therefore, it would seem that as long as logs are kept, they could 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 Law Enforcement 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 Article 29 Data Protection Working Party’s (A29WP) Guidelines,⁴⁴⁴ DPIAs should be carried out as early as is practicable.⁴⁴⁵ In this manner, DPIAs can support decision makers during the design phase. However, at the moment such an assessment has not yet taken place. Bart Driessen indicated that any data protection considerations have been put on hold until a final decision is taken on where the field tests would be held. By relegating these considerations to a separate part of the process to be completed later, the DPIA can now no longer

444 These guidelines are based on the GDPR rather than the Law Enforcement 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.

445 Article 29 Data Protection Working Party, ‘Guidelines on DPIA’ (n 340) 25.

play the supportive role in following privacy by design principles⁴⁴⁶ that the A29WP accords it.⁴⁴⁷

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 Law Enforcement Directive – in the Netherlands the maximum applicable fine is currently set at € 830,000.00)⁴⁴⁸ or even to judicial processes initiated by the Data Protection Authority or individuals who feel their rights have been infringed.

5.5 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.

446 Law Enforcement Directive, art 20. For a discussion of the role of Privacy by Design in community policing ICT systems, see Saleh Al-Sharieh and others, ‘Securing the Person and Protecting the Data: The Requirement and Implementation of Privacy by Design in Law Enforcement ICT Systems’ in Jeanne Pia Mifsud Bonnici and Joseph Cannataci (eds), *Changing communities, changing policing* (Neuer Wissenschaftlicher Verlag 2018).

447 Article 29 Data Protection Working Party, ‘Guidelines on DPIA’ (n 340) 25.

448 *Wet Politiegegevens*, art 35(c) juncto *Wetboek van Strafrecht* (Criminal Code), art 23(4).

The app fits within a larger trend of providing the 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 chapter, cover also the individuals' participation in police investigations.

The Automon app design was initiated before the adoption of the Law Enforcement 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,⁴⁴⁹ cannot be ensured. Thirdly, a DPIA has not taken place even though this should have been the case.

As a result, we argue that in the current legal regime the making use of the Automon app or of similar ones by law enforcement does not fulfil the requirements prescribed by law. 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 Law Enforcement 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.

5.6 Postscript

In the weeks following the publication of the article on which this chapter is based, the Dutch national police force decided to cancel further development of the Automon app. The reasons cited for this decision were the lack of solutions for unspecified privacy problems. The cost of the project remains unclear.⁴⁵⁰

449 Lorna Woods, 'Automated Number Plate Recognition: Data Retention and the Protection of Privacy in Public Places' (2017) 2 *Journal of Information Rights, Policy and Practice*.

450 Wilmer Heck, 'Pokémon-App van de Politie Komt Er Niet' *NRC Handelsblad* (9 November 2019) 13.

6. General discussion: Private data, public spaces?

This thesis opened with a picture of a milkman taken in 1927. Almost a century ago, he looked wearily into the eye of a camera during a routine inspection of his wares. His time has gone, but surveillance has stayed and technological possibilities for data collection have flourished. The object of this thesis has been to better understand the legal balance between surveillance on the one hand and privacy on the other. The focus was on crowdsourced surveillance, a novel schema in which data is gathered by scattered citizens and analysed and used by central actors. In a series of case studies, various technologies were investigated to answer the research question: How can we explain the interactions and occasional mismatches between the legal frameworks for privacy and personal data protection that arise in public space, as a result of the rise of crowdsourced surveillance? Now it is time to take stock of the status quo and look forward, examining possibilities to better protect the milk sellers of 2027.

This discussion is divided in three main sections in which the findings of the previous four chapters will be discussed and synthesized. In the first section, the main conclusions of the body of this thesis shall be revisited. Special attention will be given to the finding that innovative surveillance technologies in public space influence the publicness of space and, subsequently, the rights to privacy and data protection in these spaces. In the second section, insights from the preceding chapters will be combined to highlight crosscutting concerns. An overarching view will be taken

to evaluate crowdsourced surveillance, its impact on public space, and finally, to re-evaluate privacy and data protection rights with regards to crowdsourced surveillance. The third section considers challenges and solutions for the future. It describes two options for policy makers and legislators, based on the analyses of the impacts that crowdsourced surveillance has on privacy in public spaces. Finally, the thesis will conclude with a summary of the core findings.

6.1 A look back: main conclusions so far

In chapter 2, *Emergency calls with a photo attached: the effects of urging citizens to use their smartphones for surveillance*, the possibility to send the police pictures using direct messaging was discussed. The first draft of the chapter was written in 2015, when various emergency call centres were researching how they could take advantage of the growing popularity of sharing visual media with smartphones.⁴⁵¹ The logic was simple: If a citizen could send an image along with their emergency call, this could potentially be very informative since a picture may be worth a thousand words. However, this would also create the possibility to send the police pictures of potentially any privacy sensitive situation without oversight. Therefore, the societal effects of instant police reporting apps were investigated in this first case study.

451 Although it might be tempting to think that sending an image to first responders should be easy-peasy half a decade later, the infrastructure is still not available beyond sporadic testing.

The chapter approached this question by merging and transforming the two main schemata in surveillance studies: the panopticon and surveillant assemblages. The panopticon as a schema for the functioning of power was popularized by Michel Foucault.⁴⁵² He describes how (possible) visibility in combination with the prospect of being punished provided an impetus for the inmates of the eponymous prison to accept the norm imposed on them. Importantly, Foucault showed that power could function in this manner throughout society: in schools, in hospitals, and even in public spaces. From my analysis of crowdsourced surveillance in public space using this schema, it becomes clear that it can be understood as a disciplining measure.

In the early 1990s, Gilles Deleuze argued that a shift had taken place from discipline to control as a primary mode of governance,⁴⁵³ made possible by surveillant assemblages.⁴⁵⁴ With the advent of magnificent computing power, it had become possible to modulate the environment of people. They are no longer disciplined to behave a certain way, but controlled by the constant opening and closing of options. Loosely translated, Gilles Deleuze argues that technological innovations have increased the possibilities to modulate behaviours long before they become delinquent, i.e. to prevent rather than punish. This modulation, or personalisation, of interventions is made possible by surveillant assemblages as

452 Foucault (n 21).

453 Deleuze (n 8).

454 Haggerty and Ericson (n 5).

introduced by Kevin Haggerty and Richard Ericson.⁴⁵⁵ They argue that computerized surveillance operates through databases, and more specifically, through the continuous (re) configuration of databases into assemblages, which provides ever more complete accounts of who we are. Their quality as loosely tangled webs earned surveillant assemblages the adjective rhizomatic, like plants whose root structure is essential to their spread and survival but obscured from view. Using this surveillance assemblages schema, I show how crowdsourced surveillance can be viewed as a powerful tool to pressurize citizens into conformity.

My combination of the two schemata — panoptica and surveillant assemblages — elucidates the societal impact of this crowdsourced surveillance technology in novel ways. The possibility of attaching a photo to an emergency call clearly contributes to a police panopticon by heightening the visibility of everyone in public space. However, this is a panopticon partly run by citizens and on their terms. No legal oversight exists to control for, for instance, discriminatory tendencies in the public at large. This becomes doubly relevant when considering surveillant assemblages. By sharing pictures with the police, inclusion therein happens at the discretion of anyone willing to go through the trouble of pressing the send button. To prevent ending up in a database, the standard of the strictest citizens must therefore be complied with. This loss of privacy in public has clear chill-

455 *ibid.*

ing effects, and implementation of this technology should be done under strict conditions only.

In chapter 3, *Mobile devices as stigmatizing security sensors: The GDPR and a future of crowdsourced “broken windows”*, a different mode of crowdsourced surveillance was investigated. It analyses apps and websites with which users can review streets and neighbourhoods with regard to how safe they feel there. These user-generated reviews are often combined with data released by governmental agencies, such as crime statistics. The products of these apps are various scores and map overlays which explicitly qualify public spaces as “good” or “bad” areas. The influence of such scores on property values is an obvious concern. Moreover, the stigmas these technologies apply to areas may be equally damaging in the long run. The appearance of objectivity provided by the seemingly neutral underlying data makes these stigmas nigh impossible to remove. As a result, neighbourhoods and the communities living in them are being brandished by every one-star review. The investigation of these technologies thus underscores how crowdsourced surveillance shapes public space and impacts its users.

In the second half of the chapter, the possible safeguards that the GDPR offers against these harms were analysed. This seems intuitive, as the apps rely on the processing of large amounts of data. Its applicability would mean that affected people can rely on the elaborate set of rights contained therein. However, my investigations have made clear that the most important data points — the verdicts on the

character of an area — are by definition not personal data, i.e. they do not refer to any singular person, and therefore the GDPR is not applicable.⁴⁵⁶ Rather, the apps describe areas and thus indirectly the communities living within them. As data protection rules focus on protecting single natural persons, they are wholly inept to protect even the smallest groups of persons. In the chapter, it was shortly considered whether data protection rights should be extended to groups in order to fill this gap. Finally, an important argument was put forward on how Data Protection Impact Assessments may have a significant role to play in preventing the harms caused by these apps.

In chapter 4, *Algorithmic mapmaking in “smart cities”*: *Data protection impact assessments as a means of protection for groups*, the arguments set out in the preceding chapter are elaborated upon and refined in the context of mapmaking. With the advent of mapping and navigation apps such as Google Maps, the drawing of maps evolved from a privileged affair to something that many of us engage in routinely, albeit often unknowingly. However, while a map might have been drawn by either a silent cartographer or a drunken crowd, it always appears to portray the world objectively as it is.⁴⁵⁷ Their seeming truth-correspondence means they can sig-

456 GDPR, art1(1) read in conjunction with 4(1).

457 Or, for that matter, an artist with a little red cart. See Simon Weckert, ‘Google Maps Hacks: Performance and Installation’ (*Simon Weckert*, 2020) <<http://www.simonweckert.com/googlemapshacks.html>> accessed 4 February 2020.

nificantly affect the lives of the people living in any mapped area with subjective data. I have revealed, again, a problematic gap, as the data describes groups of people rather than any identifiable person. Therefore, the GDPR is, again, not applicable and affected people are left without a remedy.

The second half of the chapter investigates how a possible solution could be implemented relatively swiftly. Rather than advocating for sweeping legislative change, it is suggested that group rights should be included in DPIAs. At the moment, data controllers are already obliged to carry out DPIAs when engaging in certain types of data processing as a preventative measure.⁴⁵⁸ This provides an early opportunity to include (representatives of) groups in the design phase of mapping apps, and identify and resolve any potential problems. It might even allow groups to gain a more proactive role in how their environments are being mapped and shaped. However, there are also serious limitations. Although DPIAs provide an ex-ante avenue for protection, ex-post remedies are still out of reach for groups. Furthermore, a representative selection of group delegates to participate in a DPIA would be crucial, but almost unworkable in practice.

In chapter 5, *Capturing license plates: Police participation apps from an EU data protection perspective*, a crowd-sourced police surveillance app was scrutinized. The app in question was called ‘Automon’ and was announced by the Dutch police in 2017. With the app, citizens could scan li-

458 GDPR, art 35.

cense plates — i.e. take a photograph of a car to be read by built in ANPR software — to determine whether a vehicle is stolen. The Automon app would furthermore contain a gaming aspect in which users could score points by scanning as many number plates as possible and completing missions such as photographing a specific number of cars with a certain colour. Finally, if a scanned vehicle would indeed be stolen, the player could qualify for a monetary reward from an insurance company. *Prima facie*, the Automon app seems an amusing diversion with which citizens could support the police in the fight against car theft. Nevertheless, the legal ramifications of the app could have been major.

In order to establish the legality of the app, I first determined whether the EU data protection framework is applicable. To do so, it was established whether licence plates are personal data. In contrast to the two previous chapters, it was concluded that they indeed are; the police can easily use them to identify people. Interestingly — and surprisingly for a game — the GDPR is not applicable. As the investigation and detection of criminal activities is a law enforcement task, the Law Enforcement Directive is applicable. The Law Enforcement Directive was adopted at the same time as the GDPR and lays down the rules for the processing of personal data by the police and for policing ends.⁴⁵⁹

As such, it is obvious that the Law Enforcement Directive applies to the police and how they manage Automon. More

459 See section 1.4.4 of this thesis for a short overview of the data protection framework of the EU.

surprisingly, this also applies to the citizens who download the game. This is the result of various rulings of the European Court of Human Rights in which it stressed that law enforcement agencies cannot evade their legal obligations by outsourcing their tasks to private individuals or companies. In order to safeguard human rights, any obligations on the police must also apply to any external agents who act on behalf of the police. This means that the Automon app should not be regarded as a game, but approached only as the state surveillance tool that it is.

This creates a number of problems. First, the police are bound by the principle of proportionality in its personal data collection: collect only what you need in order to achieve your goals. However, the design as a game nudges players to catch ‘em all.⁴⁶⁰ Second, the police should ensure that anyone who processes data on their behalf employs proper security; the police cannot just outsource their responsibilities to whoever downloads an app. Third and irrespective of the status of the players, the police should have done a DPIA in which it could have foreseen part of these problems. These concerns were not just academic: Shortly after publication of the article on which the chapter is based, the Automon project was cancelled by the police. This underscores the important lessons that should be drawn from my analysis

460 Phrase borrowed from Jason Paige and John Loeffler, *Pokémon Theme* (Robbins Entertainment 1999). The Automon app was partly inspired by the success of the *Pokémon Go* mobile game.

of the potential impact of police-led crowdsourced surveillance in public space.

6.2 Bringing the threads together

In the previous section, the chapters that make up the body of this thesis were discussed in the order in which they appeared, as were the conclusions following from these chapters. In this section, it will be examined how these case studies contribute to the understanding of crowdsourced surveillance technologies, their impacts on public space, and the pressure they put on current privacy and data protection rights. Furthermore, a number of important issues that resurfaced in several chapters will be discussed.

6.2.1 Understanding crowdsourced surveillance

In the introduction of this thesis, I described how technological developments have increased the ubiquity of surveillance. Next, the analyses of crowdsourced surveillance apps in *chapters 2–5* have demonstrated that technological developments have not only altered the quantity, but also the quality of surveillance technologies. I have shown that with regards to crowdsourced surveillance, the two theoretical frameworks with which surveillance is traditionally analysed no longer fully apply: neither panopticism (and the associated discipline) nor surveillant assemblages (and the associated control) can satisfactorily explain their workings

and effects.⁴⁶¹ With regards to panopticism, it can be noted that crowdsourced surveillance apps all empower users to see and share discretionarily.⁴⁶² The gaze is broad, but filtered by participants rather than central controllers.⁴⁶³ This muddles the classical notions of a state (aiming at) panoptically seeing all public places in order to provide internal security and maintaining order. In other words, rather than big brother watching you, the entire family is watching something.⁴⁶⁴

At the same time, the surveillant assemblage also fails as an appropriate model for the developments investigated: it is, after all, the state — and especially police forces and their monopoly on internal violence — which stands out as an

461 See sections 2.2 ‘Societies of discipline’ and 2.3 ‘Societies of control’ for more on these analytical frames in the specific context of instant police reporting apps. For a general treatment of the theoretical developments in the field of surveillance studies see Galič, Timan and Koops (n 5).

462 See section 2.2.3 ‘An empowerment within the panopticon?’

463 See also David Murakami Wood and Kirstie Ball, ‘Brandscapes of Control? Surveillance, Marketing and the Co-Construction of Subjectivity and Space in Neo-Liberal Capitalism’ (2013) 13 *Marketing Theory* 47, 60–61.

464 Compare here Burkhard Schafer: “in the world of crowdsourced surveillance, Big Brother is us” in ‘Crowdsourcing and Cloudsourcing CCTV Surveillance’ (2013) 37 *Datenschutz und Datensicherheit* 434, 434. Schafer was writing about crowdsourcing CCTV material, similarly to Groombridge (n 111); Goold (n 113); and Trottier (n 112). See section 2.2.3 ‘An empowerment within the panopticon?’ for a comparison of such technologies and the apps investigated in this thesis.

end-user of the data streams described. Their power to discipline transgressors makes many of the issues noted in this thesis so problematic. The modulations and data streams⁴⁶⁵ typical of surveillant assemblages can at any moment be used to single out any individual, and suddenly reveal the disciplinary power, which lay dormant and hidden in the networked hypercomplexities.⁴⁶⁶ Metaphorically speaking: although the entire family is watching, only big brother may ultimately decide to interfere.

Thus, as private users and LEAs use crowdsourced surveillance apps to make visible certain places and people, the effects are both disciplinary *and* modulatory. The network is as much hierarchically structured and intentionally knowable, as it is rhizomatic, liquid,⁴⁶⁷ and in a constant state of re-assembly. Smartphones are opening up possibilities for new configurations of watchers, watched, and other actors. With the current rapid advancements in carry-on and IoT tech, there is no reason to suppose these developments will slow down. Furthermore, nothing indicates that the police will let go of its position at the apex of public space surveillance.

465 Or in the jargon of smart city advocates: efficiencies.

466 Iveson and Maalsen (n 5) 354–55.

467 Zygmunt Bauman and David Lyon, *Liquid Surveillance: A Conversation* (Polity Press 2013).

6.2.2 The impact of crowdsourced surveillance on public space

The case studies in this thesis demonstrate that the impact of crowdsourced surveillance apps on privacy goes hand in hand with changes in public space.⁴⁶⁸ These changes are produced by what we feel in and think about these spaces,⁴⁶⁹ and in turn they influence our behaviours and expectations. In this sub-section, I will discuss what drives these changes, and what they mean for the public spaces affected.

First, crowdsourced surveillance apps can change how we feel about certain spaces. For instance, the apps described in *chapters 3 and 4* encourage reporting subjective feelings of safety in public spaces. These crowdsourced data are then mapped and layered over cities, creating neighbourhoods that feel “dangerous.” However, due to the voluntary nature of crowdsourced surveillance programs, only a select portion of the population will take them up.⁴⁷⁰ These partic-

468 For a similar argument in the context of CCTV-surveillance, see Hille Koskela, “‘The Gaze without Eyes’: Video-Surveillance and the Changing Nature of Urban Space’ (2000) 24 *Progress in Human Geography* 243.

469 Loosely based on two of the three forces of spatial production as identified by Henri Lefebvre; respectively representational space and representations of space. See also the text box ‘Space, the legal, and Henri Lefebvre’ in the introduction where representations of space were already shortly discussed and Lefebvre (n 36) 38–42. The third spatial production force, spatial practices, is of little relevance here.

470 See primarily sections 2.2.3 ‘An empowerment within the Panopticon?’ and 5.2.2 ‘Directing the surveillant gaze.’

ipants probably have a threshold for transgressive behaviour that is below average,⁴⁷¹ resulting in normalizing pressures and skews in the type and locations of the submitted reports. Any outcomes – whether it be online interactive maps and/or decisions on where police officers will be deployed – (partially) based on such data will be skewed as well.⁴⁷² The stigmas thus created are hard to overcome as they have a veneer of data-based reliability. The result is a process of congealment: The focus on subjective experiences of fear of these apps not only amplifies the production of spaces that feel unsafe, but also solidifies it.

Furthermore, crowdsourced surveillance influences the ways in which we (try to) coherently reason about space. This rational approach to space can be very powerful when applied by infrastructure designers, city planners, urbanists, and architects.⁴⁷³ Crowdsourced datasets providing geo-tagged information on feelings of safety, for example, may seem to provide valuable input for their thought processes, but their application can be deeply problematic.⁴⁷⁴ Investors, including homebuyers, will shy away from areas labelled as dangerous. Consider also how public actors could use such

471 See section 2.3.3 ‘Normalization and chilling effects.’

472 See further sections 2.3.5 ‘Cumulative disadvantages resulting from simulation and prediction’ and 4.3 ‘Maps and (missing) group rights.’

473 Lefebvre (n 36) 38–39.

474 See further e.g. Gandy, ‘Quixotics Unite!’ (n 136); and more generally Lyon, *Surveillance as Social Sorting* (n 309); and Geoffrey C Bowker and Susan Leigh Star, *Sorting Things out: Classification and Its Consequences* (MIT Press 1999).

skewed data, for example in predictive policing. This will result in increasing the visibility of already overexposed areas and groups to the police.⁴⁷⁵ Thus, rather than objectively describing certain spaces, crowdsourced surveillance technologies may serve to redefine these spaces.

Now that it is clear that crowdsourced surveillance apps impact public spaces, let us turn to the question what that impact is. We can understand this by borrowing from an ongoing debate in the social sciences,⁴⁷⁶ and in human geography in particular, on what makes a space *more* public or *more* private.⁴⁷⁷ Lyn H. Lofland proposes that the predictability of who will be in a space determines how private or public a space is.⁴⁷⁸ If the variety in people and the variety in the be-

475 See sections 2.2.1 ‘Short term effects: visibility,’ 2.3.2 ‘Loss of anonymity vis-à-vis the police,’ 2.3.5 ‘Cumulative disadvantages resulting from simulation and prediction,’ and Joh, ‘The New Surveillance Discretion’ (n 138).

476 See for an overview of the debate Junxi Qian, ‘Geographies of Public Space: Variegated Publicness, Variegated Epistemologies’ (2018) 44 *Progress in Human Geography* 77.

477 Harding and Blokland-Potters (n 375) 186.

478 Lyn H Lofland, *The Public Realm: Exploring the City’s Quintessential Social Territory* (de Gruyter 1998). The second factor Lofland identified is closely related to the first and concerns access control. This approach to defining publicness borrows heavily from the economic concepts of excludability and rivalry. If a good is neither exclusive nor rivalrous, it is considered to be public. (See Karsten Mause, ‘A Political-Economic Perspective on Privacy in Public Spaces’ in Tjerk Timan, Bryce Clayton Newell and Bert-Jaap Koops (eds), *Privacy in Public Space: Conceptual and Regulatory Challenges* [Edward Elgar 2017].) No one can be excluded from public spaces, and one person’s

haviours of people one can expect to encounter increases, so does the publicness of a space. In other words, if you can expect the unexpected, you are in a public space.⁴⁷⁹ Due to the normalizing pressures imposed by crowdsourced surveillance apps as discussed above, the variety in people and behaviours could very well decrease, resulting in spaces that are less public.

Note that less public does not necessarily mean more private. Rather than merely distinguishing private from public space, Lyn H. Lofland proposes three ideal types of spaces: fully public spaces, fully private places, and parochial spaces.⁴⁸⁰ In fully public spaces one can expect to meet total strangers and in fully private spaces one can expect to meet only certain specific people, such as housemates. Besides these two extremes, there are also parochial spaces. These are spaces that are accessible to the public at large, but where a strong sense of commonality exists between ha-

consumption of public spaces does not diminish their availability to others. With regards to access controls, the case studies have underlined that crowdsourced surveillance tools do not put access controls into the hands of users. At most, they allow reports to be sent to the police on the basis of which someone might be retro-actively removed. See, in general, chapter 2 of this thesis.

479 Lefebvre also touched upon this theme, pointing out that encounters – both expected and unexpected – are an essential part of urban public spaces. See (n 354) 129.

480 Although she uses the term ‘realm’ rather than ‘space.’ See also Mark Gottdiener, ‘Review of *The Public Realm: Exploring the City’s Quintessential Social Territory* by Lyn H. Lofland’ (1999) 105 *American Journal of Sociology* 544.

	Private	Parochial	Public
Encounters	Completely predictable	Mostly predictable	Unpredictable
Social control	None from outsiders, complete from insiders	High	Low
Privacy expectations	Extreme	Low	High
Influence of crowd-sourced surveillance

Table 6.1: The influence of crowdsourced surveillance on public/parochial space, visualized using the ideal types from Lofland’s work.

bitual users of a space. Examples include bars with frequent visitors and streets where neighbours know each other well. In such spaces, social control tends to be high, as social norms need to be constantly reinforced.

Therefore, that public spaces are becoming less public because of crowdsourced surveillance does emphatically *not* mean that public spaces are becoming more private.⁴⁸¹ Rather, a process of parochialization seems to be taking place. Anyone who does not conform to a norm of commonality is caught in the crowdsourced surveillance assemblage and pressurized into normality.⁴⁸² This process slowly but surely erodes the expectation of privacy from public spaces.⁴⁸³

481 As we will see in the next sub-section, this also holds for the legal notion of privacy. The idea of an increase in the privateness of public spaces is doubly counterintuitive if we consider the growing body of academic work on how the built environment itself ceaselessly tracks, records, and analyses public spaces. See e.g. Tali Hatuka and Eran Toch, 'Being Visible in Public Space: The Normalisation of Asymmetrical Visibility' (2017) 54 *Urban Studies* 984; Daniel Trotter, 'Digital Vigilantism as Weaponisation of Visibility' (2017) 30 *Philosophy & Technology* 55; Many of the chapters from Newell, Timan and Koops (n 80); Paolo Cardullo, Cesare Di Felicianantonio and Rob Kitchen (eds), *The Right to the Smart City* (Emerald Insight 2019); Alex Gekker and Sam Hind, 'Infrastructural Surveillance' [2019] *New Media & Society*.

482 For similar effects of social networking apps in general, see Lee Humphreys, 'Mobile Social Networks and Urban Public Space' (2010) 12 *New Media & Society* 763.

483 See also Joh, 'Policing by Numbers' (n 139) on 61: "The very quality of public life may be different when government watches everyone — surreptitiously — and stores all the resulting information".

Given that privacy rights and regulations hinge on these expectations of privacy, crowdsourced surveillance apps kick-start a downward cycle of reduced expectations of privacy, increasing surveillance, and reduced protection of privacy rights.

6.2.3 Re-evaluating privacy and data protection rights with regards to crowdsourced surveillance

The previous section has described how crowdsourced surveillance technologies erode the publicness of public space. It was pointed out that in Lofland's terms, this did not entail a rise in their privateness. In this sub-section, I will turn my attention to the legal interpretation of privateness: the rights to privacy and data protection. Especially when we look back at the (appropriately titled) *sections* 3.4 'Legal analysis' and 5.3 'Legal analysis,' a worrying picture emerges in this regard.

Both of these sections start with a discussion of whether the data processed is personal data⁴⁸⁴ at all, and thus whether the EU data protection framework applies.⁴⁸⁵ The first of these two sections focused on websites and apps operated by municipalities and businesses on which users can report feelings of (un)safety; the second section focused on the 'Au-

484 In the sense of GDPR art 4(1) and Law Enforcement Directive art 3(1): "any information relating to an identified or identifiable natural person."

485 GDPR, art 2(1).

tomon' app, which the Dutch police prototyped, on which users could check number plates against a database of stolen cars. This discussion is highly important for data gathered in public space, as identification might often not be a necessary step for data controllers⁴⁸⁶ to achieve their goals. Still, it could be argued that privacy rights (rather than data protection rights) are being infringed, and that therefore the data protection framework should offer some safeguards. Thus, narrowing down privacy rights to *personal* data protection rights results in insufficient legal protection against the impact of crowdsourced surveillance technologies.

Another important topic of discussion concerning how data protection rights in public spaces are impacted by crowdsourced surveillance apps lies in the distinction between the General Data Protection Regulation and the Law Enforcement Directive (the two legal instruments that make up the EU data protection framework).⁴⁸⁷ In subsection 5.3.2 'GDPR or Law Enforcement Directive?' it was investigated which of these two applied to the Automon app, and after careful examination it was determined that the Law En-

486 GDPR, art 4(7).

487 For completeness' sake, it should be mentioned that a third legal instrument finalizes the framework: Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L295/39, but this piece of legislation falls outside of the scope of this research.

forcement Directive should apply in order for citizens to be able to enjoy the full protection that the law offers them.

The primary reason for the applicability of the Law Enforcement Directive can be found in ECtHR case law, which stipulates that LEAs may not circumvent their legal obligations by outsourcing policing activities. However, this line of argument becomes less straightforward when we consider the apps discussed in *chapters 3 and 4*. Even though they are not designed by any police force (or even any public authority), they may be used⁴⁸⁸ or even promoted⁴⁸⁹ by them. The information from such apps can be very relevant for e.g. crime prevention purposes, and there seems to be a willingness to form various sorts of partnerships between private platforms and public LEAs.⁴⁹⁰ In these cases, the vague de-

488 Mols and Pridmore (n 390); Pridmore and others (n 389).

489 e.g. Kitty van Muiswinkel, ‘Gemeente, politie én buurtpreventie in Hendrik Ido Ambacht op Nextdoor voor communicatie met bewoners’ (*Nextdoor Blog*, 7 March 2017) <<https://blog.nextdoor.nl/2017/03/07/gemeente-politie-en-buurtpreventie-in-hendrik-ido-ambacht-op-nextdoor-voor-communicatie-met-bewoners/>> accessed 24 October 2019; ‘Politie Den Haag’ (*Nextdoor*) <<https://nextdoor.nl/agency-detail/zh/den-haag/politie-den-haag/>> accessed 24 October 2019.

490 See also Murakami Wood and Mackinnon (n 10); See for a similar development in the context of smart cities in which another public body shared data with the police without proper authorization Kristel van Teeffelen, ‘Politie Amsterdam loerde onterecht in data van milieucamera’s’ *Trouw* (16 October 2019) <<https://www.trouw.nl/gsbba1398a>> accessed 24 October 2019.

marcation between the two instruments⁴⁹¹ (the General Data Protection Regulation and the Law Enforcement Directive) thus becomes even more problematic. Further research is clearly needed to clarify how the fluidity of such digital datastreams interacts with this legal framework.

Finally, my investigation has revealed that the *Katz*-test and its ‘reasonable expectation’ counterpart at the ECtHR are problematic instruments for deciding whether an infringement on the right of privacy has taken place for two reasons. First, the publicness of space is better understood as a complex continuum than as a simple dichotomy. To adjudicate a case, however, judges need to operationalize this continuum into a — subjective — cut-off point. Second, the surveillance technologies under scrutiny themselves affect the publicness of spaces and subsequently expectations on privacy. This is particularly true for crowdsourced surveillance in public spaces, which is characterized by the active participation of citizens. As a result, each time a surveillance measure is introduced, it is reasonable to expect a little less privacy. This problem was foreseeable: any measuring device that is continually recalibrated by its object of measurement is inherently unreliable. In other words: as surveillance in public spaces increases, legal protections against that surveillance automatically decrease.

491 See in general also Purtova (n 433).

6.3 A look ahead: *Quo vadis*, privacy in public?

Having considered the impact that crowdsourced surveillance can have on public spaces, privacy and data protection rights, a look ahead is warranted, to gauge which measures could mitigate (some of) the negative effects. Inspiration for possible solutions is not scarce: both in- and outside of the academic literature, a plethora of examples can be found. They suggest how various societal actors, from individual citizens to federal governments and multinational corporations, can do better — or at least: less harm — with data from surveillance platforms.⁴⁹² In the following two subsections, I hope to point out two legal developments that show great promise specifically for crowdsourced surveillance: Data

492 See for an interesting example e.g. Agnieszka Leszczynski's proposal to look at the glitches (the errors and subsequent corrections) of platform urbanism as moments where tactical resistance can take place: 'Glitchy Vignettes of Platform Urbanism' [2019] *Environment and Planning D: Society and Space* 1; Note the echo of de Certeau (n 93) in her work. Also worth mentioning is the edited volume in which chapter 4 'Algorithmic mapmaking in "smart cities": Data Protection Impact Assessments as a means of protection for groups' of this thesis was originally published: Angela Daly, S Kate Devitt and Monique Mann (eds), *Good Data* (Institute of Network Cultures 2019). Outside of the academic ivory tower, we could for instance look at the Tada — a non-accidental anagram of data — City alliance spearheaded by the City of Amsterdam, which has set up a manifesto with six simple and laudable data principles for local governments to adhere to when implementing smart city solutions, see 'Home' (*Tada.city*) <<https://tada.city/>> accessed 28 October 2019.

Protection Impact Assessments (DPIAs) and group data protection rights.

6.3.1 Data protection impact assessments

A DPIA is a process that can be used before implementation of a project to identify and minimize potential risks.⁴⁹³ They have made repeated appearances in this thesis, for instance in (sub)sections 3.4.3 ‘Preventive measures on the basis of the new EU legislation,’ 4.4 ‘Making Group Rights Real through DPIAs?,’ and 5.4 ‘Discussion and implications.’ There are three main reasons why DPIAs in their current form can contribute to data protection and privacy rights. First as a preventative rather than corrective measures, they show great promise for minimizing the impact that future crowdsourced public space surveillance will have. Second, as was specifically pointed out in section 4.4.1 ‘Opportunities,’ DPIAs can open up the design phase for potentially affected data subjects.⁴⁹⁴ Third and finally, their embeddedness within the current legal framework means that they are a tool that can be used right now. This obviates the need to, for example, overhaul administrative law in order to implement similar preventative measures.

Furthermore, there is still untapped potential for DPIAs. For instance, Froomkin alerts us to the important way in

493 As enshrined in article 35 of the GDPR and article 27 of the Law Enforcement Directive.

494 Which may in turn also help to comply with article 25 of the GDPR on data protection by design and by default.

which they might diminish the information asymmetry that plagues privacy in public spaces.⁴⁹⁵ Information asymmetry refers to the potentially problematic situation in which some actors (surveillers) have much more information than others (who are potentially even unaware that they are being surveilled). However, this presupposes that DPIAs are made fully public, for instance as a prerequisite in a certification scheme. At the moment, however, the GDPR does not require any form of publication, and the Article 29 Working Party⁴⁹⁶ considers publication just a ‘particularly good practice [...] where members of the public are affected by the processing operation.’⁴⁹⁷ The problem with particularly good practices, though, is that they tend to cost money while the benefits might not be immediately clear to the organization footing the bill. Thus, the already considerable role DPIAs have in data protection and privacy should be expanded even further.

495 He argues that in comparison with EU data protection rules his proposal for a US variant of DPIAs (which would be somewhat akin to US Environmental Impact Statements) would still be “weak tea” as a result of the legislative landscape. A Michael Froomkin, ‘Privacy Impact Notices to Address the Privacy Pollution of Mass Surveillance’ in Tjerk Timan, Bryce Clayton Newell and Bert-Jaap Koops (eds), *Privacy in Public Space: Conceptual and regulatory challenges* (Edward Elgar 2017) 196.

496 Now the European Data Protection Board.

497 Article 29 Data Protection Working Party, ‘Guidelines on DPIA’ (n 340) 18.

Therefore, the inclusion of Data Protection Impact Assessments in the GDPR is a promising first step. This has made it enforceable to think through more privacy-friendly options before engaging in high-risk personal data processing operations. The potential benefit of carrying out a DPIA was recently illustrated in the *Manfield* case, in which a Dutch shoe store used fingerprints to enable store personnel to log into cash registers. Although the judge agreed that management might have had good reasons to choose this system, a violation of the GDPR was still found; there was no evidence that less privacy-invasive (and thus more proportional) systems were considered.⁴⁹⁸ A DPIA could have saved Manfield the costly hassle of having to replace all cash registers.

This case, in which personnel protested the use of their fingerprints, by contrast also poignantly illustrates a problem with ex-post judicial control of public space surveillance. Challenging the latter on the basis of missing or incomplete Data Protection Impact Assessments in court will namely be harder than in the relatively straightforward case of *Manfield*. The information asymmetry alluded to before is relevant again here: how could anyone bring a case without knowing that personal data processing is even happening?⁴⁹⁹

498 Rb. Amsterdam 12 august 2019, ECLI:NL:RBAMS:2019:6005 (*Manfield*).

499 In the context of administrative law, freedom of information laws might provide some relief. However, the same basic problem largely undercuts their effectiveness: if you don't know there are documents to be made public, how can you ask for them? Thus, only pro-active publication policies will be effective in this regard.

In sum, the potential benefits of carrying out DPIAs for crowdsourced surveillance technologies in public space are frustrated by its costs, its voluntary nature and the fact that it is unclear who in the group of affected individuals may challenge the implementation of these technologies. This brings us to the following section on group versus individual rights.

6.3.2 Group data protection rights

The conceptualisation of human rights as fundamentally individual rights⁵⁰⁰ severely limits the opportunities to litigate against public space surveillance measures which are, firstly, interested in groups of persons rather than persons, and which, secondly, operate based on algorithms that analyse group traits. Under these circumstances, then, the question is whether the current framework for protecting data rights is fit for the job. More broadly, there is currently a lively debate in the academic literature about whether rights should only be guarded at an individual level or should sometimes also be given a group (or: collective) dimension.⁵⁰¹ This debate has special importance in the context of data protection

500 See for a much more in-depth treatment of the subject than is room for here Jones (n 326).

501 See, in general, the various notes in section 4.3 of this thesis, but recently also Catherine Warin, 'Individual Rights and Collective Interests in EU Law: Three Approaches to a Still Volatile Relationship' (2019) 56 Common Market Law Review 463, in which she explores three areas of EU law (environmental law, consumer law, and access to documents) which reveal three different approaches to collective interests.

rights, as the means by which infringements often take place – i.e. automated means or algorithms – are aimed at groups rather than persons.⁵⁰² Group rights to data protection, then, would be those rights that are not reducible to the rights individual group members may have to data protection.⁵⁰³

The processing of data gathered in public spaces adds an extra layer of relevance to this question, as – almost by definition – people appear there in groups. Furthermore, the (groups of) people living in an area may be affected by e.g. the stigmas produced by the apps discussed in *chapter 3* and the maps discussed in *chapter 4*.⁵⁰⁴ Assigning rights to such groups could allow them to curtail processing which currently slips through the cracks of the data protection framework, but which does cause deeply troubling effects. Furthermore, if data protection is seen through the lens of

502 Consider here that the material scopes of the GDPR and the Law Enforcement Directive are limited to the processing of personal data by automated means or which forms part of a filing system (ex art 2(2) and art 2(1) respectively); Neither makes much sense if there isn't some sort of multiplicity of data subjects.

503 See *inter alia* Michele Loi and Markus Christen, 'Two Concepts of Group Privacy' (2020) 33 *Philosophy & Technology* 34; Taylor, van der Sloot and Floridi (n 268); Luciano Floridi, 'Open Data, Data Protection, and Group Privacy' (2014) 27 *Philosophy & Technology* 1; Paola Mavriki and Maria Karyda, 'Automated Data-Driven Profiling: Threats for Group Privacy' (2019) 28 *Information & Computer Security* 183; and more generally Jones (n 326).

504 The specific role of group rights in this regard was discussed respectively in subsection 3.4.4 'Groups' and section 4.4 'Maps and missing group rights.'

informational self-determination,⁵⁰⁵ then the groups using public spaces should have a right to collective informational self-determination as well. This will allow them (rather than obscure public-private partnerships) to decide on what to share about their streets and neighbourhoods, and for which purposes.⁵⁰⁶ In sum, surveillance technologies in public space highlight the need for group rights to privacy or data protection.

The implementation of group rights to data protection would require a major overhaul of the current EU data protection framework, which would come shortly after the implementation of the GDPR. Furthermore, group rights would need to be properly implemented into judicial procedures. Although not impossible,⁵⁰⁷ it seems that, especially in comparison with Data Protection Impact Assessments, their protection is currently closer to a pipe dream than to

505 The discussion on this promising principle is ongoing, but it has already made some appearances in the jurisprudence of the ECtHR. See *Breyer v Germany* App no 50001/12 (ECtHR, 30 January 2020), para 75; and *Satakunnan Markkinapörssi and Satamedia* App no 931/13 (ECtHR, 27 June 2017), para 137: “Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged.”

506 See analogously Lefebvre (n 354).

507 See again Warin (n 501) on various ways in which at least the protection of collective interests (oft on the basis of individual rights) can and has been implemented in various fields of EU law.

reality.⁵⁰⁸ In the meanwhile however, there are some minor developments with regards to group data protection rights, such as a form of collective redress that is foreseen in article 80 of the GDPR.⁵⁰⁹ In light of the relevance of group rights, these developments and their proper implementation into the judicial systems of the Member states should be encouraged.

In lieu of substantial legislative change, Sandra Wachter proposes the interesting interim route of invoking protections against indirect discrimination by association.⁵¹⁰ Her reasoning is based primarily on the ECJ cases *Coleman*⁵¹¹ and *Chez*.⁵¹² She argues that if data protection law fails in safeguarding certain rights, we should perhaps turn to anti-discrimination law.⁵¹³ Although she situates her argument within the sphere of online behavioural advertising, especially *Chez* suggests that discrimination prohibitions might

508 Taylor, van der Sloot and Floridi (n 268) 233; van der Sloot (n 328). See also sections 3.4.4 and 4.3. Footnote 328 gives a little more background on this debate.

509 See further Laima Jančiūtė, ‘Data Protection and the Construction of Collective Redress in Europe: Exploring Challenges and Opportunities’ (2019) 9 International Data Privacy Law 2.

510 ‘Affinity Profiling and Discrimination by Association in Online Behavioural Advertising’ (2020) 35 Berkeley Technology Law Journal (forthcoming).

511 Case C-303/06 *S Coleman v Attridge Law and Steve Law* [2008] ECR I-5603.

512 Case C-83/14 *CHEZ Razpredelenie Bulgaria AD v Komisia za zashtita ot diskriminatsi* EU:C:2015:480.

513 Wachter (n 510) 14.

provide a useful strategy for dealing with group privacy in public spaces as well. In that case, a non-Roma was found to be able to rely on Directive 2000/43⁵¹⁴ to challenge a measure which affected her, even though the measure was only indirectly targeted at the predominantly Roma neighbourhood in which she ran a grocer's shop.⁵¹⁵ Thus, through discrimination prohibitions, neutral provisions and practices that do in effect particularly disadvantage persons of a minority racial or ethnic origin can indeed be challenged by anyone affected.

As certain public spaces may be more commonly frequented by people of a racial or ethnic origin, this route is especially interesting for some of the issues described in this thesis. Such disparities between spaces might result, for instance, from housing and income gaps or from historical government policies.⁵¹⁶ As was discussed in subsection 2.3.5 'Cumulative disadvantages resulting from simulation and prediction,' the surveillance burden is felt most heavily in already disadvantaged neighbourhoods, and Wachter's reasoning might provide precisely those communities with the tool they need to bring their grievances before a court of law. Even though this would probably only cover a very

514 Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin [2000] OJ L180/22.

515 Case C-83/14 *Chez* (n 512), in particular paras 56, 60, 109, and 129 thereof.

516 Mark Duursma and Wilmer Heck, 'Nog 45 Gemeenten Hebben Aparte Molukse Wijk' *NRC Handelsblad* (19 May 2017) 2.

limited subset of all the problems described in this thesis, it does provide an opening for NGOs to start strategic litigation against some of the most egregious cases.

6.4 Conclusion

The crowdsourced surveillance in and of public spaces is eroding from the streets and squares of our cities their publicness. The data hunger of surveillant assemblages turns them into parochial spaces, where ‘normality’ is valued above all else. This process puts new pressures on the rights to privacy and personal data protection whilst increasing pre-existing pressures. As a result, a citizen that has entered public space cannot choose to participate in public life on her own terms. Instead, she is like a player that has entered a game and if she accepts the rules — as she must — she can play along. The other players, however, are always keeping score.

Legal and political action is called for to protect individuals, groups, and society against these impacts of crowdsourced surveillance. In the short term, Data Protection Impact Assessments may provide some relief, but the proper protection of privacy and data rights requires a radical rethinking of how these rights operate when confronted with extreme asymmetries and algorithmic opaqueness. If the ‘public’ in ‘public space’ is not to become an anachronism, the aegis of data protection must be extended beyond single citizens to also provide shelter to those actually affected: groups. They should be provided with the tools for the job

and, at this juncture in time, those tools must include data protection rights.

Groningen
October 2020

7. Table of Cases

7.1 Council of Europe

7.1.1 European Court of Human Rights

A v France App no 14838/89 (ECtHR, 23 November 1993)

Amann v Switzerland ECHR 2000–II 245

Axel Springer AG v Germany App no 39954/08 (ECtHR, 7 February 2012)

Bărbulescu v Romania App no 61496/08 (ECtHR, 5 September 2017)

Benedik v Slovenia App no 62357/14 (ECtHR, 24 April 2018)

Breyer v Germany App no 50001/12 (ECtHR, 30 January 2020)

Hachette Filipacchi Associes (“ICI PARIS”) v France App no 12268/03 (ECtHR, 23 July 2009)

Halford v United Kingdom ECHR 1997–III

Kennedy v United Kingdom App no 26839/05 (ECtHR, 18 May 2010)

Köpke v Germany App no 420/07 (ECtHR, 5 October 2010)

Leander v Sweden (1987) Series A no 116

Leempoel & SA ED Cine Revue v Belgium App no 64772/01 (ECtHR, 9 November 2006)

MM v The Netherlands App no 39339/98 (ECtHR, 8 April 2003)

Peck v United Kingdom ECHR 2003–I 123

Perry v United Kingdom ECHR 2003–IX 141

PG and JH v United Kingdom ECHR 2001–IX 195

Polanco Torres et Movilla Polanco v Spain App no 34147/06 (ECtHR, 21 September 2010)

Rotaru v Romania ECHR 2000–V 109
S and Marper v United Kingdom ECHR 2008–V 167
Satakunnan Markkinapörssi and Satamedia App no 931/13
 (ECtHR, 27 June 2017)
Shimovolos v Russia App no 30194/09 (ECtHR, 21 June 2011)
Standard Verlags v Austria II App no 21277/05 (ECtHR, 4
 June 2009)
Uzun v Germany ECHR 2010–VI 7
Van Vondel v The Netherlands App no 38258/03 (ECtHR, 25
 October 2007)
Von Hannover v Germany I ECHR 2004–VI 41
Von Hannover v Germany II ECHR 2012–I 399

7.1.2 European Commission on Human Rights

*Herbecq and the association “Ligue des droits de l’homme” v
Belgium* (1998) 92-B DR 92

7.2 European Union

Breyer, Patrick v Bundesrepublik Deutschland (C–582/14)
 EU:C:2016:779
*CHEZ Razpredelenie Bulgaria AD v Komisia za zashtita ot
diskriminatsi* (C–83/14) EU:C:2015:480
Coleman, S v Attridge Law and Steve Law (C–303/06) [2008]
 ECR I–5603
*Data Protection Commissioner v Facebook Ireland and Max-
imilian Schrems (Schrems II)* (C–311/18) EU:C:2020:559

Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (C-131/12) EU:C:2014:317

Productores de Música de España (Promusicae) v Telefónica de España SAU (C-275/06) [2008] ECR I-271

Schrems, Maximillian v Data Protection Commissioner (Schrems I) (C-362/14) EU:C:2015:650

Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others (C-698/15) EU:C:2016:970

Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy (C-73/07) [2008] ECR I-9831

Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen (C-92/09 and C-93/09) [2010] ECR I-11063

7.3 United States of America

7.3.1 Supreme Court of the United States
Carpenter, Timothy Ivory v United States 585 US ____ (2018)

Katz, Charles v United States 389 US 347 (1967)

Kyllo, Danny v United States 533 US 27 (2001)

Riley, David Leon v California; United States v Brima Wurie
573 US 373 (2014)

United States v Antoine Jones 565 US 400 (2012)

7.3.2 Circuit Court

United States v Quartavious [sic] Davis 785 F3d 498 (11th Cir 2015)

7.3.3 District Court

Matter of Search of Content Stored at Premises Controlled by Google Inc No 16-MC-80263-RS, 2017 WL 3478809 (ND Cal Aug 14 2017)

7.4 Germany

BverfG, judgement of the First Senate of 15 December 1983, 1 BvR 209, 269, 362, 420, 440, 484/83

7.5 Netherlands

SyRi Rb Den Haag 5 February 2020 NL:RBDHA:2020:865

Manfield Rb Amsterdam 12 august 2019 NL:RBAMS:2019:6005

8. Table of treaties, legislation & documents

8.1 United Nations

8.1.1 Conventions

Convention on Road Traffic (concluded 8 November 1986, entered into force 21 May 1977) 1042 UNTS 17

8.1.2 United Nations Commission on Human Rights

UNCHR ‘Report of the Special Rapporteur on the right to privacy, Joseph A Cannataci’ (2017) UN Doc A/HRC/34/60
UNCHR, ‘The right to privacy in the digital age’ (2017) UN Doc A/HRC/34/L.7/Rev.1,3

8.2 Council of Europe

8.2.1 Conventions

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)

European Convention on Human Rights

8.2.2 Recommendations

Council of Europe Recommendation CM/Rec(2010) 13 of the Committee of Ministers to member states on the protection of individuals with regard to the automatic processing of personal data in the context of profiling
<https://search.coe.int/cm/Pages/result_details.aspx?ObjectId1409000016805cdd00> accessed 11 August 2017

8.3 European Union

8.3.1 Primary Legislation

Charter of Fundamental Rights of the EU [2016] OJ C202/393

Treaty on European Union [2016] OJ C202/13

Treaty on the Functioning of the European Union [2016] OJ C202/47

8.3.2 Secondary legislation

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31

Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin [2000] OJ L180/22

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L350/60

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

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) [2016] OJ L119/1

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 (Law Enforcement Directive) [2016] OJ L119/89

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L295/39

8.3.3 Documents

Article 29 Data Protection Working Party, ‘Guidelines on Consent under Regulation 2016/679’ 11–15 <http://ec.europa.eu/newsroom/document.cfm?doc_id=48849> accessed 3 April 2018

Article 29 Data Protection Working Party, ‘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)’ 8 <ec.europa.eu/newsroom/document.cfm?doc_id=47711> accessed 2 February 2018

Explanations relating to the Charter of Fundamental Rights [2007] OJ C303/17

European Commission, ‘Joint Statement on the Final Adoption of the New EU Rules for Personal Data Protection’ <http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm> accessed 24 March 2017

8.4 National legislation

8.4.1 Netherlands

Besluit Politiegegevens (Dutch Police Data Decision)

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

Wetboek van Strafrecht (Dutch Criminal Code)

Wet Politiegegevens (Dutch Police Data Law)

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

8.4.2 United States of America

Fourth amendment to the constitution

9. References

- ‘About Us’ (*AutoMon: innovative solutions for Community-Based Corrections*, 2018) <<https://automon.com/about/>> accessed 14 May 2018
- ‘AI NOW’ (*AI Now Institute, New York University*) <<https://ainowinstitute.org/>> accessed 8 November 2017
- Albrechtslund A and Lauritsen P, ‘Spaces of Everyday Surveillance: Unfolding an Analytical Concept of Participation’ (2013) 49 *Geoforum* 310
- Al-Sharieh S and others, ‘Securing the Person and Protecting the Data: The Requirement and Implementation of Privacy by Design in Law Enforcement ICT Systems’ in Jeanne Pia Mifsud Bonnici and Joseph Cannataci (eds), *Changing communities, changing policing* (Neuer Wissenschaftlicher Verlag 2018)
- Al-Sharieh S and Mifsud Bonnici J, ‘From the Persuasion of Theory to the Certainty of Law: A Multi-Jurisdictional Analysis of the Law of Community Policing in Europe’ (2018) 5 *European Journal of Comparative Law and Governance* 179
- Amoore L, ‘Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times’ (2011) 28 *Theory, Culture & Society* 24
- Anderson BR, *Imagined Communities: Reflections on the Origin and Spread of Nationalism* (2nd edn, Verso 2006)
- Andrejevic M, ‘The Work of Watching One Another: Lateral Surveillance, Risk, and Governance’ (2002) 2 *Surveillance & Society* 479
- Angwin J and others, ‘Machine Bias’ (*ProPublica*, 23

- May 2016) <<https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>> accessed 17 August 2017
- Anselin L and Williams S, 'Digital Neighborhoods' (2016) 9 *Journal of Urbanism* 305
- Arnstein SR, 'A Ladder Of Citizen Participation' (1969) 35 *Journal of the American Institute of Planners* 216
- Article 29 Data Protection Working Party, 'Preparation of the Privacy Shield Annual Joint Review' <http://ec.europa.eu/newsroom/document.cfm?doc_id=45272> accessed 18 August 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> accessed 2 February 2018
- , 'Guidelines on Consent under Regulation 2016/679' <http://ec.europa.eu/newsroom/document.cfm?doc_id=48849> accessed 3 April 2018
- Ausloos J and Dewitte P, 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice' (2018) 8 *International Data Privacy Law* 4
- Austin LM, 'Enough about Me: Why Privacy Is about Power, Not Consent (or Harm)' in Austin Sarat (ed), *A World without Privacy: What Law Can and Should Do?* (Cambridge University Press 2015)
- AXA Konzern AG, 'WayGuard: Begleit-App Für Ein Gutes Gefühl Unterwegs' (*Wayguard*, 2016) <<https://www.wa->

yguard.de/> accessed 6 February 2017

Barak A, *Proportionality: Constitutional Rights and Their Limitations* (Cambridge University Press 2012)

Bauman Z and Lyon D, *Liquid Surveillance: A Conversation* (Polity Press 2013)

Beake S (ed), *Data Brokers and the Need for Transparency and Accountability* (Nova Publishers 2014)

Beckers M, 'Absender Unbekannt' [2017] Hohe Luft 54

Bendler J and others, 'Investigating Crime-to-Twitter Relationships in Urban Environments—Facilitating a Virtual Neighbourhood Watch', *Proceedings of the European Conference on Information Systems (ECIS)* (2014)

Berg C van den, 'Videobellen Naar 112?' (*JenV Magazine*, December 2018) <<https://magazines.rijksoverheid.nl/jenv/jenvmagazine/2018/04/dit-is-nu>> accessed 15 March 2019

Bergt M, 'Die Bestimmbarkeit Als Grundproblem Des Datenschutzes — Überblick Über Den Theorienstreit Und Lösungsvorschlag' [2015] *Zeitschrift für Datenschutz* 365

Bivens R and Hasinoff AA, 'Rape: Is There an App for That? An Empirical Analysis of the Features of Anti-Rape Apps' (2018) 21 *Information, Communication & Society* 1050

Blomley NK, 'Flowers in the Bathtub: Boundary Crossings at the Public–Private Divide' (2005) 36 *Geoforum* 281

Blomley NK, Delaney D and Ford RT (eds), *The Legal Geographies Reader: Law, Power, and Space* (Blackwell Pub-

lishers 2001)

Bosco F and others, 'Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities' in Serge Gutwirth, Ronald Leenes and Paul de Hert (eds), *Reforming European Data Protection Law*, vol 20 (Springer Netherlands 2015)

Botta F, Moat HS and Preis T, 'Quantifying Crowd Size with Mobile Phone and Twitter Data' (2015) 2 Royal Society Open Science 150162

Bowker GC and Star SL, *Sorting Things out: Classification and Its Consequences* (MIT Press 1999)

boyd d and Marwick AE, 'Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies', *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society* (2011) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128> accessed 23 March 2016

Brakel R van and de Hert P, 'Policing, Surveillance and Law in a Pre-Crime Society: Understanding the Consequences of Technology Based Strategies' (2011) 20 Cahiers Politiestudies 163

Brannon MM, 'Datafied and Divided: Techno-Dimensions of Inequality in American Cities' (2017) 16 City & Community 20

Brink J van den and others, 'General Principles of Law' in Jan H Jans, Sacha Prechal and Rob Widdershoven (eds), *Europeanisation of public law* (Europa Law Publishing

2007)

- Cannataci JA, 'Parallel Streams of Action (TAS) for the Mandate of the UN Special Rapporteur for Privacy and the First Set of Priorities' (*Privacy and Personality: a forum exploring perspectives on privacy and other fundamental rights*, 3 June 2016) <<https://www.privacyandpersonality.org/2016/06/privacy-and-personality-blog-3-parallel-streams-of-action-tas-for-the-mandate-of-the-un-special-rapporteur-for-privacy-and-the-first-set-of-priorities/>> accessed 8 March 2017
- , 'Report of the Special Rapporteur on the Right to Privacy' (31st Human Rights Council, 3 August 2016) <<http://www.ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc>> accessed 27 February 2017
- Cardullo P, Di Feliciano C and Kitchin R (eds), *The Right to the Smart City* (Emerald Insight 2019)
- Cardullo P and Kitchin R, 'Being a "Citizen" in the Smart City: Up and down the Scaffold of Smart Citizen Participation in Dublin, Ireland' (2019) 84 *GeoJournal* 1
- Casals NT (ed), *Group Rights as Human Rights: A Liberal Approach to Multiculturalism* (Springer 2006)
- Cassa C and others, 'Twitter as a Sentinel in Emergency Situations: Lessons from the Boston Marathon Explosions' [2013] *PLoS Currents: Disasters* <<http://currents.plos.org/disasters/?p=8687>> accessed 2 May 2018
- Certeau M de, *The Practice of Everyday Life* (University of California Press 1984)

- Clarke R, 'Information Technology and Dataveillance' (1988) 31 Communications of the ACM 498
- , 'Privacy Impact Assessment: Its Origins and Development' (2009) 25 Computer Law & Security Review 123
- Cohen FS, 'Transcendental Nonsense and the Functional Approach' (1935) 35 Columbia Law Review 809
- Cohen JE, 'Cyberspace as/and Space' (2007) 107 Columbia Law Review 210
- , 'What Privacy Is For' (2013) 126 Harvard Law Review 1904
- , 'The Surveillance-Industrial Complex: The Irony of the Participatory Turn' in Darin Barney and others (eds), *The Participatory Condition in the Digital Age* (University of Minnesota Press 2016)
- , 'The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy' (2018) 31 Philosophy & Technology 213
- Commission Nationale de l'Informatique et des Libertés, 'Privacy Impact Assessment (PIA) Templates' <<https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf>> accessed 28 August 2018
- , 'The Open Source PIA Software Helps to Carry out Data Protection Impact Assessment' (*CNIL*, 31 May 2018) <<https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment>> accessed 28 August 2018
- Community Research and Development Information Service, 'Citizen Interaction Technologies Yield Communi-

- ty Policing (CITYCoP)' (*CORDIS*) <http://cordis.europa.eu/project/rcn/197273_en.html> accessed 12 November 2015
- , 'Inspiring CitizeNS Participation for Enhanced Community PoliCing AcTions (INSPEC2T)' (*CORDIS*) <http://cordis.europa.eu/project/rcn/194895_en.html> accessed 18 May 2016
- , 'TRusted, CITizen - LEA CoILaboratIon over SOcial Networks (TRILLION)' (*CORDIS*) <http://cordis.europa.eu/project/rcn/194841_en.html> accessed 18 May 2016
- , 'Unity' (*CORDIS*) <http://cordis.europa.eu/project/rcn/194893_en.html> accessed 18 May 2016
- 'Connected Citizen's Programme' (*Waze*) <<https://www.waze.com/ccp>> accessed 2 February 2018
- Crampton JW, 'Bordering on Bosnia' (1996) 39 *GeoJournal* 353
- , 'Maps as Social Constructions: Power, Communication, and Visualization' (2001) 25 *Progress in Human Geography* 235
- 'Crime Maps' (*Google Play*, 21 September 2016) <<https://play.google.com/store/apps/details?id=com.rdr.map-scrimes.lite>> accessed 29 May 2017
- Crooks AT and others, 'User-Generated Big Data and Urban Morphology' (2016) 42 *Built Environment* 396
- CrowdSpot, 'Featured Projects' (*CrowdSpot*) <<http://crowdspot.com.au/>> accessed 22 February 2017
- Culkin JM, 'A Schoolman's Guide to Marshall McLuhan' *The*

- Saturday Review* (18 March 1967) 51
- Cumiskey KM and Brewster K, 'Mobile Phones or Pepper Spray?: Imagined Mobile Intimacy as a Weapon of Self-Defense for Women' (2012) 12 *Feminist Media Studies* 590
- Curry MR, 'The Profiler's Question and the Treacherous Traveler: Narratives of Belonging in Commercial Aviation' (2004) 1 *Surveillance & Society* 475
- Daly A, Devitt SK and Mann M (eds), *Good Data* (Institute of Network Cultures 2019)
- Davis EFI, Alves AA and Sklansky DA, 'Social Media and Police Leadership: Lessons From Boston' [2014] *New Perspectives in Policing* 1
- Day L, 'Free To Be Online Map Shows Where Women Feel Unsafe in Melbourne' (*ABC News*, 8 December 2016) <<http://www.abc.net.au/news/2016-12-08/free-to-be-online-map-shows-where-women-in-melbourne-feel-unsafe/8103410>> accessed 3 February 2017
- Deleuze G, 'Postscript on the Societies of Control' (1992) 59 *October* 3
- 'Die Besten Apps Des Jahres 2016 – Teil 1/7' (*Androidmag*, 2 November 2016) <<http://androidmag.de/app-reviews/die-besten-apps-des-jahres-2016-teil-1/>> accessed 27 February 2017
- Dijk J van, 'Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology' (2014) 12 *Surveillance & Society* 197
- Dikeç M, 'Police, Politics, and the Right to the City' (2002)

- Doyle A, 'Revisiting the Synopticon: Reconsidering Mathiesen's "The Viewer Society" in the Age of Web 2.0' (2011) 15 *Theoretical Criminology* 283
- Dubbeld L, 'Telemonitoring of Cardiac Patients: User-Centred Research as Input for Surveillance Theories' in David Lyon (ed), *Theorizing Surveillance: The panopticon and beyond* (2006)
- Duursma M and Heck W, 'Nog 45 Gemeenten Hebben Aparte Molukse Wijk' *NRC Handelsblad* (19 May 2017) 2
- Edwards L, 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective' (2016) 2 *European Data Protection Law Review* 28
- Edwards L and Veale M, 'Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"?' (2018) 16 *IEEE Security & Privacy* 46
- Ehlers D and Becker U (eds), *European Fundamental Rights and Freedoms* (de Gruyter Recht 2007)
- 'Eindhoven Living Lab' (*European Network of Living Labs*) <<http://www.openlivinglabs.eu/livinglab/eindhoven-living-lab>> accessed 22 March 2018
- Elliot DS, 'Lies, Damn Lies and Arrest Statistics' (Center for the Study and Prevention of Violence 1995)
- Englehardt S and Narayanan A, 'Online Tracking: A 1-Million-Site Measurement and Analysis' (2016) <http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf> accessed 23 March 2017

- ETSI, 'Universal Mobile Telecommunications System (UMTS); LTE; Service Aspects; Service Principles (3GPP TS 22.101 Version 11.10.0 Release 11)' <http://www.etsi.org/deliver/etsi_ts%5C122100_122199%5C122101%5C11.10.00_60%5Cts_122101v111000p.pdf> accessed 26 January 2016
- European Commission, 'Joint Statement on the Final Adoption of the New EU Rules for Personal Data Protection' <http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm> accessed 24 March 2017
- 'Facebook – Log In or Sign Up' (*Facebook*) <<https://www.facebook.com>> accessed 22 August 2017
- Farrell P, 'The Medicare Machine: Patient Details of "Any Australian" for Sale on Darknet' (*The Guardian*, 3 July 2017) <<https://www.theguardian.com/australia-news/2017/jul/04/the-medicare-machine-patient-details-of-any-australian-for-sale-on-darknet>> accessed 29 August 2017
- Feyerabend P, *Against Method* (4th ed, Verso 2010)
- Fichte JG, 'Foundations of Natural Right' in Torin Monahan and David Murakami Wood (eds), *Surveillance studies: A reader* (Oxford University Press 2018)
- Fishwick E and Mak H, 'Fighting Crime, Battling Injustice: The World of Real-Life Superheroes' (2015) 11 *Crime, Media, Culture* 335
- Flammer I, 'Genteel Wearables: Bystander-Centered Design' (2016) 14 *IEEE Security & Privacy* 73
- Floridi L, 'Open Data, Data Protection, and Group Privacy'

(2014) 27 *Philosophy & Technology* 1

Foucault M, *Discipline and Punish: The Birth of the Prison* (Alan Sheridan tr, 2nd Vintage Books ed, Vintage Books 1995)

Fox J and Moreland JJ, 'The Dark Side of Social Networking Sites: An Exploration of the Relational and Psychological Stressors Associated with Facebook Use and Affordances' (2015) 45 *Computers in Human Behavior* 168

Froomkin AM, 'Privacy Impact Notices to Address the Privacy Pollution of Mass Surveillance' in Tjerk Timan, Bryce Clayton Newell and Bert-Jaap Koops (eds), *Privacy in Public Space: Conceptual and regulatory challenges* (Edward Elgar 2017)

'G Is for Google' (*Alphabet*) <<https://abc.xyz/>> accessed 6 March 2017

Galič M, 'Surveillance, Privacy and Public Space in the Stratumseind Living Lab: The Smart City Debate, beyond Data' (2019) 68 *Ars Aequi* 570

Galič M, Timan T and Koops B-J, 'Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation' (2017) 30 *Philosophy & Technology* 9

Gandy OHJr, 'Exploring Identity and Identification in Cyberspace' (2000) 14 *Notre Dame Journal of Law, Ethics & Public Policy* 1085

—, 'Quixotics Unite! Engaging the Pragmatists on Rational Discrimination' in David Lyon (ed), *Theorizing Surveillance: the Panopticon and Beyond* (Routledge 2006)

- Ganti R, Ye F and Lei H, 'Mobile Crowdsensing: Current State and Future Challenges' (2011) 49 IEEE Communications Magazine 32
- Gekker A and Hind S, "'Outsmarting Traffic, Together": Driving as Social Navigation' in Clancy Wilmott and others (eds), *Playful Mapping in the Digital Age* (Institute of Network Cultures 2016)
- , 'Infrastructural Surveillance' [2019] New Media & Society
- Gellert R, 'The Article 29 Working Party's Provisional Guidelines on Data Protection Impact Assessment' (2017) 3 European Data Protection Law Review 212
- Gelles D, 'Taser International Dominates the Police Body Camera Market' (*The New York Times*, 12 July 2016) <www.nytimes.com/2016/07/13/business/taser-international-dominates-the-police-body-camera-market.html> accessed 15 December 2016
- Gemeente Groningen, 'Gebreken in Uw Buurt Melden' (*Gemeente Groningen*) <<https://gemeente.groningen.nl/gebreken-en-overlast-melden>> accessed 13 February 2017
- , 'Meldingen Groningen' (*MeldStad*) <<http://fleximap.groningen.nl/gnmaps/meldingen/>> accessed 13 February 2017
- Gerber MS, 'Predicting Crime Using Twitter and Kernel Density Estimation' (2014) 61 Decision Support Systems 115
- Goff T le, Malochet V and Jagu T, 'Surveiller à Distance. Une Ethnographie Des Opérateurs Municipaux de Vidéosur-

- veillance' (Institut d'aménagement et d'urbanisme 2011)
- Goodman B, 'Discrimination, Data Sanitisation and Auditing in the European Union's General Data Protection Regulation' (2016) 2 European Data Protection Law Review 493
- Google Inc., 'Google Maps' (*Google Maps*) <<https://www.google.nl/maps>> accessed 22 February 2017
- Goold BJ, 'Open to All? Regulating Open Street CCTV and the Case for Symmetrical Surveillance' (2006) 25 Criminal Justice Ethics 3
- Gottdiener M, 'Review of The Public Realm: Exploring the City's Quintessential Social Territory by Lyn H. Lofland' (1999) 105 American Journal of Sociology 544
- Götzmann N and others, 'Human Rights Impact Assessment Guidance and Toolbox (Road-Testing Version)' <https://www.humanrights.dk/sites/humanrights.dk/files/media/dokumenter/business/hria_toolbox/hria_guidance_and_toolbox_final_may22016.pdf_223795_1_1.pdf> accessed 24 August 2018
- 'Graaf Adolfstraat: Medewerker Provinciale Keuringsdienst Neemt Monster van Melk Bij Melkventer' <<http://beeldbankgroningen.nl/beelden/detail/ef36d097-06d1-2038-3b71-6b3bf8a75add>> accessed 18 December 2018
- Graaf P de, 'Een Biertje Met Big Brother Erbij' *De Volkskrant* (23 November 2015) 11
- Greenfield A and Shepard M, *Urban Computing and Its Discontents* (The Architectural League of New York 2007)
- Groombridge N, 'Crime Control or Crime Culture TV?'

- (2002) 1 *Surveillance & Society* 30
- Gstrein OJ, *Das Recht Auf Vergessenwerden Als Menschenrecht: Hat Menschenwürde Im Informationszeitalter Zukunft?* (Nomos 2016)
- , ‘How to Approach Technology, Human Rights and Personality in the Digital Age? – A Few Thoughts’ (*Privacy and Personality*, 24 October 2016) <<https://www.privacyandpersonality.org/2016/10/how-to-approach-technology-human-rights-and-personality-in-the-digital-age-a-few-thoughts/>> accessed 17 August 2017
- , ‘The Right to Be Forgotten in the General Data Protection Regulation and the Aftermath of the *Google Spain* Judgment (C-131/12)’ (2017) 5 *Privacy in Germany, Datenschutz und Compliance* 9
- Gstrein OJ and Ritsema van Eck GJ, ‘Mobile Devices as Stigmatizing Security Sensors: The GDPR and a Future of Crowdsourced “Broken Windows”’ (2018) 8 *International Data Privacy Law* 69
- Haggerty KD, ‘What’s Wrong with Privacy Protections? Provocations from a Fifth Columnist’ in Austin Sarat (ed), *A World without Privacy: What Law Can and Should do* (Cambridge University Press 2015)
- Haggerty KD and Ericson RV, ‘The Surveillant Assemblage’ (2000) 51 *British Journal of Sociology* 605
- Hall R, Monahan T and Reeves J, ‘Surveillance and Performance (Editorial)’ (2016) 14 *Surveillance & Society* 153
- Harding A and Blokland-Potters T, *Urban Theory: A Critical Introduction to Power, Cities and Urbanism in the 21st*

Century (Sage 2014)

- Hargittai E, 'Potential Biases in Big Data: Omitted Voices on Social Media' (2020) 38 *Social Science Computer Review* 10
- Harris I, 'Pokemon Go Captures 800 Million Downloads' (*pocketgamer.biz*, 30 May 2018) <<http://www.pocketgamer.biz/news/68209/pokemon-go-captures-800-million-downloads/>> accessed 11 October 2018
- Harshaw P, 'Nextdoor, the Social Network for Neighbors, Is Becoming a Home for Racial Profiling' (*Fusion*, 24 March 2015) <www.fusion.net/story/106341/next-door-the-social-network-for-neighbors-is-becoming-a-home-for-racial-profiling/> accessed 16 December 2016
- Haskins C, 'Amazons Home Security Company Is Turning Everyone Into Cops' (*Motherboard*, 7 February 2019) <https://motherboard.vice.com/en_us/article/qvyvzd/amazons-home-security-company-is-turning-everyone-into-cops> accessed 12 February 2019
- Hatuka T and Toch E, 'Being Visible in Public Space: The Normalisation of Asymmetrical Visibility' (2017) 54 *Urban Studies* 984
- Heck W, 'Pokémon-App van de Politie Komt Er Niet' *NRC Handelsblad* (9 November 2019) 13
- Heek J van, Arning K and Ziefle M, 'The Surveillance Society: Which Factors Form Public Acceptance of Surveillance Technologies?' in Markus Helfert and others (eds), *Smart Cities, Green Technologies, and Intelligent Transport Systems* (Springer International Publishing

2017)

- Hern A, 'Fitness Tracking App Strava Gives Away Location of Secret US Army Bases' *The Guardian* (28 January 2018) <<https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases>> accessed 8 February 2018
- Hert P de and Papakonstantinou V, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 *Computer Law & Security Review* 179
- Heuvel J van den and van Wely M, 'Politiepokémon op komst: Burgers kunnen met app gestolen auto's opsporen' (*De Telegraaf*, 7 October 2017) <<https://www.telegraaf.nl/nieuws/552919/politiepokemon-op-komst>> accessed 15 May 2018
- Hier SP, Walby K and Greenberg J, 'Supplementing the Panoptic Paradigm: Surveillance, Moral Governance and CCTV' in David Lyon (ed), *Theorizing Surveillance: The Panopticon and Beyond* (Routledge 2006)
- Hinds L and Grabosky P, 'Responsibilisation Revisited: From Concept to Attribution in Crime Control' (2010) 23 *Security Journal* 95
- 'Home' (*Tada.city*) <<https://tada.city/>> accessed 28 October 2019
- 'How Predictive Policing Works: We Provide Guidance on Where and When to Patrol' (*PredPol*, 2015) <<http://www.predpol.com/how-predictive-policing-works/>> accessed 9 May 2016

- Huang H and others, 'Location Based Services: Ongoing Evolution and Research Agenda' (2018) 12 Journal of Location Based Services 63
- Hughes K, 'The Public Figure Doctrine and the Right to Privacy' (2019) 78 Cambridge Law Journal 70
- Huizinga J, *Homo Ludens: A Study of the Play-Element in Culture* (Routledge & Kegan Paul 1980)
- Humphreys L, 'Mobile Social Networks and Urban Public Space' (2010) 12 New Media & Society 763
- Information Commissioner's office, 'Sample DPIA Template' <<https://ico.org.uk/media/for-organisations/documents/2258857/dpia-template-v1.docx>> accessed 28 August 2018
- ITU Telecommunication Development Bureau, 'ICT Facts and Figures 2015' <<https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf>> accessed 11 October 2018
- , 'ICT Facts and Figures 2017' <<https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf>> accessed 11 October 2018
- Iveson K and Maalsen S, 'Social Control in the Networked City: Datafied Dividuals, Disciplined Individuals and Powers of Assembly' (2019) 37 Environment and Planning D: Society and Space 331
- Jančiūtė L, 'Data Protection and the Construction of Collective Redress in Europe: Exploring Challenges and Opportunities' (2019) 9 International Data Privacy Law 2
- Joh EE, 'Discretionless Policing: Technology and the Fourth

- Amendment' (2007) 95 California Law Review 199
- , 'Policing by Numbers: Big Data and the Fourth Amendment' (2014) 89 Washington Law Review 35
- , 'The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing' (2016) 10 Harvard Law & Policy Review 15
- Jones P, 'Human Rights, Group Rights, and Peoples' Rights' (1999) 21 Human Rights Quarterly 80
- , 'Group Rights' (*Stanford Encyclopedia of Philosophy*, 29 March 2016) <<http://plato.stanford.edu/archives/sum2016/entries/rights-group/>> accessed 5 March 2018
- Jovanović MA, *Collective Rights: A Legal Theory* (Cambridge University Press 2012)
- Junta de Freguesia da Estrela, 'GeoEstrela' (*GeoEstrela*) <<https://www.jf-estrela.pt/caap/app/gso/>> accessed 13 February 2017
- Kammerer D, 'Surveillance in Literature, Film and Television' in Kirstie Ball, Kevin D Haggerty and David Lyon (eds), *Routledge Handbook of Surveillance Studies* (Routledge 2012)
- Keller P, 'The Reconstruction of Privacy through Law: A Strategy of Diminishing Expectations' (2019) 9 International Data Privacy Law 132
- Kempen PHPHMC van, 'Human Rights and Criminal Justice Applied to Legal Persons. Protection and Liability of Private and Public Juristic Entities under the ICCPR, ECHR, ACHR and AfChHPR' (2010) 14 Electronic Journal of Comparative Law 1

- Kennedy H and others, 'Engaging with (Big) Data Visualizations: Factors That Affect Engagement and Resulting New Definitions of Effectiveness' (2016) 21 First Monday
- Kinsley S, 'Vulgar Geographies? Popular Cultural Geographies and Technology' (2016) 17 Social & Cultural Geography 793
- Klitou D, 'Public Space CCTV Microphones and Loudspeakers: The Ears and Mouth of "Big Brother"' in Demetrius Klitou, *Privacy Invading Technologies and Privacy by Design* (Springer 2014)
- Kloza D and others, 'Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework towards a More Robust Protection of Individuals' <https://cris.vub.be/files/32009890/dpialab_pb2017_1_final.pdf> accessed 17 August 2018
- Koichi S, 'Forever Red' (*Power Rangers: Wild Force*, 5 October 2002)
- Koops B-J, 'Privacy Spaces' (2018) 121 West Virginia Law Review 611
- Koskela H, "'The Gaze without Eyes": Video-Surveillance and the Changing Nature of Urban Space' (2000) 24 Progress in Human Geography 243
- , "'Cam Era" — the Contemporary Urban Panopticon' (2003) 1 Surveillance & Society 292
- , "'Don't Mess with Texas!" Texas Virtual Border Watch Program and the (Botched) Politics of Responsibilization' (2011) 7 Crime, Media, Culture 49

- Kremer J, 'The End of Freedom in Public Places? Privacy Problems Arising from Surveillance of the European Public Space' (PhD thesis, University of Helsinki 2017)
- Kuner C, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013)
- Kushner T, *Angels in America: Millennium Approaches* (Theatre Communications Group 1992)
- Lambert O, 'New Map Reveals Dangerous Areas for Women after Dark' (*News.Com.Au*, 27 October 2016) <<http://www.news.com.au/lifestyle/real-life/news-life/new-map-reveals-dangerous-areas-for-women-after-dark/news-story/ac74124366927004dd09838cd278aba8>> accessed 3 February 2017
- Lange M de and de Waal M, 'Owning the City: New Media and Citizen Engagement in Urban Design' (2013) 18 *First Monday* <<http://journals.uic.edu/ojs/index.php/fm/article/view/4954>>
- Larsson S, 'A First Line of Defence? Vigilant Surveillance, Participatory Policing, and the Reporting of "Suspicious" Activity' (2017) 15 *Surveillance & Society* 94
- Latour B, *Reassembling the Social: An Introduction to Actor-Network-Theory* (Oxford University Press 2005)
- Lauer J, 'Surveillance History and the History of New Media: An Evidential Paradigm' (2012) 14 *New Media & Society* 566
- Lee D, 'Boston Bombing: How Internet Detectives Got It Very Wrong' *BBC News* (19 April 2013) <<http://www.bbc.com/news/technology-22214511>> accessed 16 Feb-

ruary 2016

- Lee S, 'Spider-Man!', *Amazing Fantasy #15* (Marvel Comics 1962)
- Lefebvre H, *The Production of Space* (Donald Nicholson-Smith tr, Blackwell 1991)
- , 'Right to the City' in Eleonore Kofman and Elizabeth Lebas (eds), *Writings on Cities* (Blackwell 1996)
- Leistert O, *From Protest to Surveillance: The Political Rationality of Mobile Media: Modalities of Neoliberalism* (PL Academic Research 2013)
- Leslie CA, 'Territoriality, Map-Mindedness, and the Politics of Place' (2016) 45 *Theory and Society* 169
- Leszczynski A, 'Glitchy Vignettes of Platform Urbanism' [2019] *Environment and Planning D: Society and Space* 1
- Levin S, 'What Happens When Tech Firms End up at the Center of Racism Scandals?' (*The Guardian*, 30 September 2016) <www.theguardian.com/technology/2016/aug/30/tech-companies-racial-discrimination-next-door-airbnb> accessed 16 December 2016
- Lofland LH, *The Public Realm: Exploring the City's Quintessential Social Territory* (de Gruyter 1998)
- Loi M and Christen M, 'Two Concepts of Group Privacy' (2020) 33 *Philosophy & Technology* 207b
- Los M, 'Looking into the Future: Surveillance, Globalization and the Totalitarian Potential' in David Lyon (ed), *Theorizing Surveillance: The Panopticon and Beyond* (Routledge 2006)
- Luca M, 'Reviews, Reputation, and Revenue: The Case of

- Yelp.Com' [2016] Harvard Business School working paper 12-016
- Lupton D, 'Apps as Artefacts: Towards a Critical Perspective on Mobile Health and Medical Apps' (2014) 4 *Societies* 606
- Lynskey O, 'Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing' (2019) 15 *International Journal of Law in Context* 162
- Lyon D (ed), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (Routledge 2003)
- , *Surveillance Studies: An Overview* (Polity 2007)
- , *The Culture of Surveillance: Watching as a Way of Life* (Polity 2018)
- Mahieu RLP, Asghari H and van Eeten M, 'Collectively Exercising the Right of Access: Individual Effort, Societal Effect' (2018) 7 *Internet Policy Review*
- Malleson N and Andresen MA, 'The Impact of Using Social Media Data in Crime Rate Calculations: Shifting Hot Spots and Changing Spatial Patterns' (2015) 42 *Cartography and Geographic Information Science* 112
- Mamet D, *Race* (Theatre Communications Group 2010).
- Mann S, Nolan J and Wellman B, 'Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments' (2002) 1 *Surveillance & Society* 331
- Mantelero A, 'Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Di-

- mension of Data Protection' (2016) 32 Computer Law & Security Review 238
- , 'From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era' in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of data technologies* (Springer 2017)
- , 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment' (2018) 34 Computer Law & Security Review 754
- Mantello P, 'The Machine That Ate Bad People: The On-topolitics of the Precrime Assemblage' (2016) 3 Big Data & Society 1
- Martin R, 'Digilante Justice: Citizenship in Cyberspace' (2007) 16 The New Atlantis 124
- Marx GT, *Undercover: Police Surveillance in America* (University of California Press 1988)
- , 'The Public as Partner? Technology Can Make Us Auxiliaries as Well as Vigilantes' (2013) 11 IEEE Security & Privacy 56
- Mause K, 'A Political-Economic Perspective on Privacy in Public Spaces' in Tjerk Timan, Bryce Clayton Newell and Bert-Jaap Koops (eds), *Privacy in Public Space: Conceptual and Regulatory Challenges* (Edward Elgar 2017)
- Mavriki P and Karyda M, 'Automated Data-Driven Profiling: Threats for Group Privacy' (2019) 28 Information & Computer Security 183
- 'Merkel: Daten Sind Rohstoffe Des 21. Jahrhunderts' (*heise*

- online, 11 February 2015) <<http://www.heise.de/newsticker/meldung/Merkel-Daten-sind-Rohstoffe-des-21-Jahrhunderts-2867735.html>> accessed 6 March 2017
- Milaj J, 'Invalidation of the Data Retention Directive: Extending the Proportionality Test' (2015) 31 *Computer Law & Security Review* 604
- Milaj J and Mifsud Bonnici JP, 'Unwitting Subjects of Surveillance and the Presumption of Innocence' (2014) 30 *Computer Law & Security Review* 419
- Miller D, 'Group Rights, Human Rights and Citizenship' (2002) 10 *European Journal of Philosophy* 178
- Miller K, 'How to Collect Open Source Intelligence' (*In Homeland Security*) <<http://inhomelandsecurity.com/how-to-collect-open-sourceintelligence>> accessed 17 August 2017
- Millie A, 'Citizens in Policing: The Lived Reality of Being a Police Support Volunteer' (2019) 29 *Policing and Society* 407
- Mittelstadt B, 'From Individual to Group Privacy in Big Data Analytics' (2017) 30 *Philosophy & Technology* 475
- Mols A and Pridmore J, 'When Citizens Are "Actually Doing Police Work": The Blurring of Boundaries in WhatsApp Neighbourhood Crime Prevention Groups in The Netherlands' (2019) 17 *Surveillance & Society* 272
- Monahan T and Murakami Wood D, 'Introduction: Surveillance as a Transdisciplinary Endeavor' in Torin Monahan and David Murakami Wood (eds), *Surveillance studies: A reader* (Oxford University Press 2018)

- Montgomery D, Fisher M and Branigin W, 'FBI Releases Images of Two Suspects in Boston Marathon Bombings' *Washington Post* (18 April 2013) <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> accessed 14 September 2018
- Montgomery D, Horwitz S and Fisher M, 'Police, Citizens and Technology Factor into Boston Bombing Probe' *The Washington Post* (21 April 2013) <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> accessed 14 September 2018
- Montjoye Y-A de and others, 'Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata' (2015) 347 *Science* 536
- Muiswinkel K van, 'Gemeente, politie én buurtpreventie in Hendrik Ido Ambacht op Nextdoor voor communicatie met bewoners' (*Nextdoor Blog*, 7 March 2017) <<https://blog.nextdoor.nl/2017/03/07/gemeente-politie-en-buurtpreventie-in-hendrik-ido-ambacht-op-nextdoor-voor-communicatie-met-bewoners/>> accessed 24 October 2019
- Murakami Wood D and Ball K, 'Brandscapes of Control? Surveillance, Marketing and the Co-Construction of Subjectivity and Space in Neo-Liberal Capitalism' (2013) 13

- Murakami Wood D and Mackinnon D, 'Partial Platforms and Oligoptic Surveillance in the Smart City' (2019) 17 *Surveillance & Society* 176
- 'My Safetipin: Personal Safety' (*Google Play*, 7 April 2017) <<https://play.google.com/store/apps/details?id=com.safetipin.mysafetipin>> accessed 29 May 2017
- Narayanan A, Huey J and Felten EW, 'A Precautionary Approach to Big Data Privacy' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, vol 24 (Springer Netherlands 2016)
- Nationale Politie, 'Politie App' <<https://www.politie.nl/app>> accessed 3 December 2015
- Nederlandse Omroep Stichting, 'Contact Met de Politie? Stuur Een Appje!' (*NOS*, 8 December 2016) <<http://nos.nl/artikel/2147234-contact-met-de-politie-stuur-een-appje.html>> accessed 9 December 2016
- , 'Politie kan 112-beller met Android-telefoon beter lokaliseren' (*NOS*) <<https://nos.nl/l/2275680>> accessed 15 March 2019
- Newell BC, de Conca S and Thomasen K, 'Surveillance and Privacy in North American Public Spaces' in Bryce Clayton Newell, Tjerk Timan and Bert-Jaap Koops (eds), *Surveillance, Privacy, and Public Space* (Routledge 2018)
- Newell BC, Timan T and Koops B-J (eds), *Surveillance, Privacy and Public Space* (Routledge 2018)
- Nink J and Pole J, 'Die Bestimmbarkeit Des Personenbez-

- ugs - Von Der IP-Adresse Zum Anwendungsbereich Der Datenschutzgesetze' [2015] Multimedia und Recht 563
- Nissenbaum HF, 'Privacy as Contextual Integrity' (2004) 79 Washington Law Review 119
- Nolan C, *The Dark Knight* (Warner Bros 2008)
- Norman DA, *The Design of Everyday Things* (Basic Books 2002)
- Norris C and others (eds), *The Unaccountable State of Surveillance: Exercising Access Rights in Europe* (Springer 2016)
- Norris C and Armstrong G, 'CCTV and the Social Structuring of Surveillance' (1999) 10 Crime Prevention Studies 157
- Olejnik L and others, 'The Leaking Battery: A Privacy Analysis of the HTML5 Battery Status API' [2015] International Association for Cryptologic Research (e-Print archive) <<https://eprint.iacr.org/2015/616.pdf>> accessed 22 February 2017
- Olsen M, Schneier B and Zittrain J, 'Dont Panic, Making Progress on the "Going Dark" Debate' (2016) <https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf> accessed 24 March 2017
- OpenStreetMap Foundation, 'About' (*OpenStreetMap*) <<https://www.openstreetmap.org/about>> accessed 11 April 2018
- , 'OpenStreetMap' (*OpenStreetMap*) <<https://www.openstreetmap.org/>> accessed 22 February 2017
- Osiander A, 'Sovereignty, International Relations, and the

- Westphalian Myth' (2001) 55 International Organization 251
- 'Our Kind of Town' (*Times of Malta*, 26 February 2017) <<http://www.timesofmalta.com/articles/view/20170226/technology/Our-kind-of-town.640852>> accessed 13 March 2017
- Pagallo U, 'The Group, the Private, and the Individual: A New Level of Data Protection?' in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of data technologies* (Springer 2017)
- Paige J and Loeffler J, *Pokémon Theme* (Robbins Entertainment 1999)
- Pak B, Chua A and Moere AV, 'FixMyStreet Brussels: Socio-Demographic Inequality in Crowdsourced Civic Participation' (2017) 24 Journal of Urban Technology 65
- Pasquale F, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015)
- 'Politie Den Haag' (*Nextdoor*) <<https://nextdoor.nl/agency-detail/zh/den-haag/politie-den-haag/>> accessed 24 October 2019
- Pridmore J and others, 'Keeping an Eye on the Neighbours: Police, Citizens, and Communication within Mobile Neighbourhood Crime Prevention Groups' (2019) 92 The Police Journal: Theory, Practice and Principles 97
- Privacy International, 'Smart Cities: Utopian Vision, Dystopian Reality' <<https://privacyinternational.org/node/638>> accessed 4 May 2018

- Purenne A and Palierse G, 'Towards Cities of Informers? Community-Based Surveillance in France and Canada' (2017) 15 *Surveillance & Society* 79
- Purtova N, 'Between the GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public-Private Partnerships' (2018) 8 *International Data Privacy Law* 52
- Qian J, 'Geographies of Public Space: Variegated Publicness, Variegated Epistemologies' (2018) 44 *Progress in Human Geography* 77
- RapidSOS, 'Haven' (2016) <www.rapidsos.com> accessed 9 December 2016
- Rawlison K, 'National Emergency? Belgians Respond to Terror Raids with Cats' (*The Guardian*, 22 November 2015) <<http://www.theguardian.com/world/2015/nov/22/national-emergency-belgians-respond-with-cats>> accessed 8 February 2016
- Reeves J, 'If You See Something, Say Something: Lateral Surveillance and the Uses of Responsibility' (2012) 10 *Surveillance & Society* 235
- Reidenberg JR, 'Privacy in Public' (2014) 69 *University of Miami Law Review* 141
- , 'The Transparent Citizen' (2015) 47 *Loyola University Chicago Law Journal* 437
- Reilly P, 'Every Little Helps? YouTube, Sousveillance and the "anti-Tesco" Riot in Stokes Croft' (2015) 17 *New Media & Society* 755
- Ritsema van Eck GJ, 'Emergency Calls with a Photo At-

- tached: The Effects of Urging Citizens to Use Their Smartphones for Surveillance' in Bryce Clayton Newell, Tjerk Timan and Bert-Jaap Koops (eds), *Surveillance, Privacy, and Public Space* (Routledge 2018)
- Robb D, 'The Global Heatmap, Now 6x Hotter' (*Medium*, 1 November 2017) <<https://medium.com/strava-engineering/the-global-heatmap-now-6x-hotter-23fc01d-301de>> accessed 7 February 2018
- Rothmann R, 'Video Surveillance and the Right of Access: The Empirical Proof of Panoptical Asymmetries' (2017) 15 *Surveillance & Society* 222
- 'Safetipin' (*Apps that keep you safe*) <<http://safetipin.com/>> accessed 29 May 2017
- Schafer B, 'Crowdsourcing and Cloudsourcing CCTV Surveillance' (2013) 37 *Datenschutz und Datensicherheit* 434
- Schneider CJ and Trottier D, 'The 2011 Vancouver Riot and the Role of Facebook in Crowd-Sourced Policing' (2012) 175 *BC Studies* 57
- Schneier B, 'How We Won the War on Thai Chili Sauce' (*Schneier on Security*, 1 November 2007) <https://www.schneier.com/essays/archives/2007/11/how_we_won_the_war_o.html> accessed 22 November 2018
- Schneier B and Pix A, 'Surveillance Is the Business Model of the Internet' (*OpenDemocracy*, 18 July 2017) <<https://www.opendemocracy.net/en/digitaliberties/surveillance-is-business-model-of-internet/>> accessed 28 May 2019

- Schuman R, 'La Déclaration Schuman Du 9 Mai 1950' (*À propos de l'UE*, 24 October 2017) <https://europa.eu/european-union/about-eu/symbols/europe-day/schuman-declaration_fr> accessed 19 January 2020
- Sedenberg E, Wong R and Chuang J, 'A Window into the Soul: Biosensing in Public' in Bryce Clayton Newell, Tjerk Timan and Bert-Jaap Koops (eds), *Surveillance, Privacy, and Public Space* (Routledge 2018)
- Selbst AD, 'Disparate Impact in Big Data Policing' (2018) 52 *Georgia Law Review* 109
- Seltzer W and Anderson M, 'The Dark Side of Numbers: The Role of Population Data Systems in Human Rights Abuses' (2001) 68 *Social Research* 481
- Shelton T, 'The Urban Geographical Imagination in the Age of Big Data' (2017) 4 *Big Data & Society* 205395171666512
- Simon B, 'The Return of Panopticism: Supervision, Subjection and the New Surveillance' (2005) 3 *Surveillance & Society* 1
- Skorupinski B and Ott K, 'Technology Assessment and Ethics: Determining a Relationship in Theory and Practice' (2002) 1 *Poiesis & Praxis* 95
- Sloot B van der, 'Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation' (2014) 4 *International Data Privacy Law* 307
- , 'Do Groups Have a Right to Protect Their Group Interest in Privacy and Should They? Peeling the Onion of Rights and Interests Protected under Article 8 ECHR'

- in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of data technologies* (Springer 2017)
- Smith GJD, 'Surveillance, Data and Embodiment: On the Work of Being Watched' (2016) 22 *Body & Society* 108
- Song H and others, *Smart Cities: Foundations, Principles, and Applications* (John Wiley & Sons 2017)
- Spielkamp M, 'Inspecting Algorithms for Bias' (*MIT Technology Review*, 12 June 2017) <<https://www.technology-review.com/s/607955/inspecting-algorithms-for-bias/>> accessed 18 August 2017
- Spiller K and L'Hoiry X, 'Watch Groups, Surveillance, and Doing It for Themselves' (2019) 17 *Surveillance & Society* 288
- SpotCrime, 'Crime Tips' (*Submit a crime tip*) <<https://crimetip.us/>> accessed 15 February 2017
- Stalla-Bourdillon S and Knight A, 'Anonymous Data v. Personal Data—a False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data' (2016) 34 *Wisconsin International Law Journal* 284
- Starbird K and others, 'Rumors, False Flags, and Digital Vigilantes: Misinformation on Twitter after the 2013 Boston Marathon Bombing', *iConference 2014 Proceedings* (iSchools 2014) <<http://hdl.handle.net/2142/47257>> accessed 24 March 2016
- Stoller DR, 'Google Must Turn Over Data Stored Abroad Sought Under U.S. Warrant' (*Bloomberg Law: Privacy and Data Security*, 15 August 2017) <<https://www.bna>

com/google-turn-data-n73014463160/> accessed 18 August 2017

‘Strava: A Global Heatmap of Athletic Activity’ *The Guardian* (2 November 2017) <<https://www.theguardian.com/lifeandstyle/the-running-blog/gallery/2017/nov/02/strava-a-global-heatmap-of-athletic-activity>> accessed 8 February 2018

Strava Inc, ‘Strava Global Heatmap’ (Strava) <<https://labs.strava.com/heatmaps>>

Sweeney L, ‘Only You, Your Doctor, and Many Others May Know’ [2015] *Technology Science* <<http://techscience.org/a/2015092903>>

Swift T and Little J, ‘Miss Americana and the Heartbreak Prince’ on Taylor Swift (red), *Lover* (Republic Records 2019)

Taylor L and others, ‘Customers, Users or Citizens? Inclusion, Spatial Data and Governance in the Smart City’ (Maps4Society Final Project Report 2016) <<http://ssrn.com/abstract=2792565>> accessed 23 March 2017

Taylor L, Floridi L and van der Sloot B (eds), *Group Privacy: New Challenges of Data Technologies* (Springer 2017)

Taylor L, van der Sloot B and Floridi L, ‘Conclusion: What Do We Know About Group Privacy?’ in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy* (Springer 2017)

Teeffelen K van, ‘Politie Amsterdam loerde onterecht in data van milieucamera’s’ *Trouw* (16 October 2019) <<https://www.trouw.nl/gs-bba1398a>> accessed 24 October 2019

- The National 911 Program, 'The Future of 911' (911.gov) <www.911.gov/futureof911.html> accessed 23 May 2016
- 'The World's Most Valuable Resource Is No Longer Oil, but Data' (*The Economist*, 6 May 2017) <<http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource>> accessed 29 May 2017
- Timan T and Albrechtslund A, 'Surveillance, Self and Smartphones: Tracking Practices in the Nightlife' (2018) 24 *Science and Engineering Ethics* 853
- Timan T, Newell BC and Koops B-J (eds), *Privacy in Public Space: Conceptual and Regulatory Challenges* (Edward Elgar Publishing 2017)
- Timan T and Oudshoorn N, 'Mobile Cameras as New Technologies of Surveillance? How Citizens Experience the Use of Mobile Cameras in Public Nightscape' (2012) 10 *Surveillance & Society* 167
- Timmermans F, Ansip A and Jourová V, 'Joint Statement on the Final Adoption of the New EU Rules for Personal Data Protection' (*European Commission Press Release Database*, 14 April 2016) <http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm> accessed 16 January 2018
- 'Top Sites by Category: Regional/North America/United States/Business and Economy/Real Estate' (*Alexa*) <http://www.alexa.com/topsites/category/Regional/North_America/United_States/Business_and_Economy/Real_Estate> accessed 29 March 2017

- Trottier D, 'Crowdsourcing CCTV Surveillance on the Internet' (2014) 17 *Information, Communication & Society* 609
- , 'Digital Vigilantism as Weaponisation of Visibility' (2017) 30 *Philosophy & Technology* 55
- Trulia, 'Trulia Launches Crime Maps to Add Insights and More Complete Data to American Neighborhoods' (*News Room*, 2 June 2011) <<http://info.trulia.com/press-releases?item=106144>> accessed 14 February 2017
- Trulia, 'Queens and Viewable Map Area Homes For Sale & Real Estate' (NY Real Estate & Homes for Sale) <https://www.trulia.com/for_sale/40.632112163148,40.829316775872,-74.026498761825,-73.762826886825_xy/12_zm/#m-ap-crime> accessed 22 July 2017
- United Nations, Office of the High Commissioner of Human Rights, 'Planned Thematic Reports and Call for Consultations' <<http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/ThematicReports.aspx>> accessed 29 August 2017
- Urquhart L and Rodden T, 'New Directions in Information Technology Law: Learning from Human-Computer Interaction' (2017) 31 *International Review of Law, Computers & Technology* 150
- Vasak K, 'A 30-Year Struggle' (1977) 30 *UNESCO Courier* 28
- Véliz C, 'In the Privacy of Our Streets' in Bryce Clayton Newell, Tjerk Timan and Bert-Jaap Koops (eds), *Surveillance, Privacy, and Public Space* (Routledge 2017)
- Vera A and Torsten OS, 'Crowdsourcing and Policing: Op-

- portunities for Research and Practice' [2017] European Police Science and Research Bulletin 143
- Verbinski G, *Pirates of the Caribbean: The Curse of the Black Pearl* (Walt Disney Pictures 2003)
- Vigilant Solutions, 'LPR Data' <www.vigilantsolutions.com/wp-content/uploads/2014/08/LPR_Data_AUG2014_LFS.pdf> accessed 15 December 2016
- Vries A de, 'App: Automon' (*Social Media DNA*, 18 October 2017) <<http://socialmediadna.nl/automon/>> accessed 15 May 2018
- Wachter S, 'Affinity Profiling and Discrimination by Association in Online Behavioural Advertising' (2020) 35 Berkeley Technology Law Journal (forthcoming)
- Walker S, *The Future of Human Rights Impact Assessments of Trade Agreements* (Intersentia 2009) <<https://dspace.library.uu.nl/bitstream/handle/1874/36620/walker.pdf>> accessed 24 August 2018
- Warin C, 'Individual Rights and Collective Interests in EU Law: Three Approaches to a Still Volatile Relationship' (2019) 56 Common Market Law Review 463
- Warren SD and Brandeis LD, 'The Right to Privacy' (1890) 4 Harvard Law Review 193
- Waze Mobile Ltd., 'Live Map' (Free driving directions, traffic reports & GPS navigation app by Waze) <<https://www.waze.com/livemap>> accessed 5 February 2018
- Weckert S, 'Google Maps Hacks: Performance and Installation' (*Simon Weckert*, 2020) <<http://www.simonweckert.com/googlemapshacks.html>> accessed 4 February

2020

- Weiser M, 'The Computer for the 21st Century' (1991) 265
Scientific American 94
- Welle B, 'IMG_1264' (Flickr, 17 September 2015) <<https://flic.kr/p/A81u4w>> accessed 5 August 2019
- Welsh BC and Farrington DP, 'Crime Prevention Effects of Closed Circuit Television: A Systematic Review' (Home Office Research, Development and Statistics Directorate 2002) 252 <<http://webarchive.nationalarchives.gov.uk/20090410070401/http://www.homeoffice.gov.uk/rds/pdfs2/hors252.pdf>> accessed 20 May 2016
- Westin AF, *Privacy and Freedom* (The Bodly Head 1967)
- Whitson JR, 'Gaming the Quantified Self' (2013) 11 Surveillance & Society 163
- Wijk N van der, *Drie Dagen Geluk* (FlauweCult 2013)
- Williams ML, Burnap P and Sloan L, 'Crime Sensing with Big Data: The Affordances and Limitations of Using Open Source Communications to Estimate Crime Patterns' [2016] British Journal of Criminology 320
- Wimmer B, 'Adresshandel: Das Geschäft Mit Unseren Persönlichen Daten' (*futurezone*, 1 December 2015) <<https://futurezone.at/netzpolitik/adresshandel-das-geschaeft-mit-unseren-persoenlichen-daten/100.371.363>> accessed 27 February 2017
- Winston A, 'Los Angeles Sheriff Invests in New Tech to Expand Biometric Database' (*Reveal*, 3 July 2015) <<https://www.revealnews.org/article/los-angeles-sheriff-invests-in-new-tech-to-expand-biometric-database/>> ac-

cessed 13 April 2016

- , ‘Palantir Has Secretly Been Using New Orleans to Test Its Predictive Policing Technology’ (*The Verge*, 27 February 2018) <<https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd>> accessed 7 March 2018
- Woods L, ‘Automated Number Plate Recognition: Data Retention and the Protection of Privacy in Public Places’ (2017) 2 *Journal of Information Rights, Policy and Practice*
- Wright D and Friedewald M, ‘Integrating Privacy and Ethical Impact Assessments’ (2013) 40 *Science and Public Policy* 755
- Wright D and Hert P de (eds), *Privacy Impact Assessment* (Springer 2012)
- Wright D and Mordini E, ‘Privacy and Ethical Impact Assessment’ in David Wright and Paul De Hert (eds), *Privacy Impact Assessment* (Springer Netherlands 2012)
- Yeal T, ‘Against Collective Rights’ in Christian Joppke and Steven Lukes (eds), *Multicultural Questions* (Oxford University Press 1999)
- Yordanov A, ‘Nature and Ideal Steps of the Data Protection Impact Assessment Under the General Data Protection Regulation’ (2017) 3 *European Data Protection Law Review* 486
- Ziebarth W, ‘Perspektive Der Bestimmbarkeit’ in Gernot Sydow (ed), *Europäische Datenschutzgrundverordnung: Der neue Praktiker-Kommentar zur Datenschutz-Grund-*

verordnung (Nomos 2017)

Curriculum Vitae

Gerard Jan Ritsema van Eck's academic career started at the Goeman Borgesius primary school in Aduard, the Netherlands, where he was awarded the *Gouden Griffel* for his short poems. At the Praedinius Gymnasium in Groningen, the Netherlands, he received equally glowing feedback on his coursework: 'Very well written. Pity though you don't seem to have anything to say.' After one year at the Roosevelt Academy – Utrecht University's liberal arts honours college in Middelburg, The Netherlands – he returned to Groningen.

Back in his hometown, Gerard completed a bachelor of arts in International Relations at the local Rijksuniversiteit. He went on to obtain a double master of arts degree in Euroculture⁵¹⁷ at both the Rijksuniversiteit Groningen and the Georg-August-Universität Göttingen. Gerard stuck around the Harmonie building and landed a job as a research assistant for Prof. Mifsud Bonnici. Things got wildly out of control, and the results of that are in your hands. Gerard Jan Ritsema van Eck currently works as an assistant professor at the IT-law department of the University of Groningen, where he specializes in privacy and data protection law.

517 Since everyone always asks: 'Euroculture is a two-year, 120 ECTS, English-taught multi-university Master programme focused on the study of modern European society, culture and politics in a global context.' Note, however, that it was 90 ECTS in the good old days. 'About' (*Erasmus Mundus Master of Arts Euroculture*) <<https://www.euroculturemaster.eu/about>> accessed 8 January 2021.

Dankwoord/Acknowledgments

Writing a PhD-thesis entails more than simply entering the office each day at 9 am, firing up that word processor and typing away until 5 pm.⁵¹⁸ I am grateful to all the people around me who have helped me on this journey, inspired me, given me feedback, but above all have kept me sane. Without them, this book would not exist. A word of gratitude to all of them: Thank you.

Somewhat more specifically, I would like to thank my primary PhD supervisor, professor Jeanne Pia Mifsud Bonnici. I distinctly remember walking into your office more than seven years ago, desperate for work in an economy which was not particularly friendly to recent graduates whose degrees focused on ‘identity issues in contemporary Europe’ — whatever that means. Not only did I get a job, I also found a place where I could explore ideas, and more importantly I stumbled in upon a set of great colleagues who you have gathered (and continue to gather) around you. I already look forward to all the amazing people you will hopefully introduce me to in the future!

Als tweede wil ik mijn tweede promotor, professor Pauline Westerman, bedanken. Hoewel je pas laat in het traject kwam, hebben we gelukkig nog genoeg momenten gehad waarbij we de verbazing over onze juridische adoptiefamilie konden delen. Veel dank ook voor het blijven aanmoedigen als ik er weer eens doorheen zat met de inleiding en de conclusie.

518 Although it certainly does help, as I have learned the hard way over the last year, something something pandemic.

I am also very grateful to the reading committee who perused the manuscript for this thesis thoroughly, and thus opened the way for the last step in the academic journey of my PhD: professors Kirstie Ball, Arno Lodder, and Sofia Ranchordas. I take all of your excellent suggestions with me as I continue onwards researching the wonders of data protection and surveillance, even if not all of them made it into the present thesis.⁵¹⁹

Nynke en Peter, dank jullie wel dat jullie mijn paranimfen willen zijn, en (letterlijk) naast me staan vandaag. De afgelopen jaren heeft jullie doorzettingsvermogen diepe indruk op mij gemaakt. Ik heb dan ook alle vertrouwen erin dat jullie mij hier ook wel doorheen slepen,⁵²⁰ hoe deze dag er dan ook uit is komen te zien.

A very pro-active thanks to the members of the opposition committee, who I will hopefully face either virtually or in person on March 15, 2021. Although the committee has not been formed yet, if you are reading this, you probably have agreed to a request to ask me a question, and I would like to thank you for your efforts in that respect. Whether or not I shall also be grateful for the actual questions, of course, remains to be seen.

Saleh and Oskar, thank you for relentlessly and politely grilling all my ideas, and for sharpening my mind in the process. Hans, dank voor het delen van jouw (soms wat minder

519 *ibid*, something something pandemic.

520 Eventueel met een epi-pen in m'n bovenbeen.

beleefde) kritiek op de wereld in het algemeen, en mededingingsrechtuitspraken in het bijzonder.

A big thanks to all the PhD students and other assorted “junior” staff of the STeP team and the European Law department. May the summers be smouldering in the tin tube without air conditioning: Adi, Aukje,⁵²¹ Catherine, Carolin, Daniel, Esra, Hugo, Ida, Janey, Jonida, Justin, Karen, Lauren, Martin, Matthijs,⁵²² Mel, Nynke,⁵²³ Renske, Styliana, Peter,⁵²⁴ Pieter, and Xingyu. Having lunch with you guys kept me from getting too focused; surely a great contribution. I’m blessed to count many of you among my friends.⁵²⁵

De afgelopen twee jaar heb ik een langzame beweging door het Harmoniegebouw gemaakt, van een tinnen opbouw naar een oude zolder. Daar heb ik een nieuwe, uitstekende omgeving gevonden om studenten lastig te vallen met gegevensbeschermingseffectbeoordelingen: de vakgroep IT-recht. Dank voor het vertrouwen dat ook iemand zonder meesterstitel dat best kan. In het bijzonder wil ik Tim en Evert bedanken, die toevalligerwijs het meest op mijn pad kwamen; wat mij betreft een gelukkig toeval.

521 Festival-vrijdag 4evah!

522 Dank ook namens Christien voor de (helaas kansloze) pogingen om mij vet te mesten.

523 Zie in zijn algemeenheid o.a. Rb. Midden-Nederland 13 april 1997, ECLI:NL:RBMNE:1997:1820 (*Rotonde*).

524 Assorted origami animals included.

525 And even fellow adventurers, exploring the icy north.

Door het Harmoniegebouw loop ik ondertussen al weer meer dan tien jaar⁵²⁶ rond, en dat had niet gekund zonder de portiers en de schoonmakers. Veel dank dat jullie er, zo goed en zo kwaad als het gaat, voor zorgen dat het gebouw niet uit elkaar dondert van ellende. Wat mij betreft een grootse prestatie.

I want to thank the academic surveillance studies community as a whole for making me feel welcome⁵²⁷ in your midst. I look forward to a time when we can nerdily chitchat about various forms of veillance at conferences again. In particular, I would like to thank dr. Daniel Trottier, professor Kirstie Ball, dr. Tjerk Timan, and dr. Bryce Clayton Newell for the various forms of encouragement I have received from you over the last years.

Gelukkig kon ik soms ontsnappen aan de universiteit, en het beste escapisme maak je zelf, in een muf repetitiezaaltje, op een toneel, of voor een camera. Maar ja, in je eentje is ook maar zo alleen, dus veel dank aan Albert, Annegeerte, Bart-Jan, Belinda, Benne, Bianca, Daphne, Eliza,⁵²⁸ Fardouw, Frances, Gerro, Gioa, Heike, Heleen, Hennie, Ibbe, Jan, Jelle, Johannes, Jojanneke,⁵²⁹ Joske, Joyce, Laura, Laurens, Leonie, Lotte, Mariët, Melle, Merel, Monique, Moyra, Olivia,

526 Ik voel hier niet meteen de behoefte om veel preciezer te worden.

527 I also thank the communitiy for not making me feel particularly weird for working on data protection law and surveillance without ever having had any previous formal training in these disciplines.

528 In levende en/of dode vorm.

529 Shout out to klassenvertegenwoordiger Benny.

Piet, René, Rob, Robbert, Robina, Rolien, Ron, Ronald, Samuel, Sanne, Shailaja,⁵³⁰ Suzanne, Thereza,⁵³¹ Tim, Trudy, Wies, and Wim dat ook jullie steeds weer alle schaamte overboord kieperden. Acteurs en actreutels zijn natuurlijk niets zonder regisseurs: Dank dus ook aan Aike, Annemiek, Ben, Brugt, Fenna, Nico, en TJ voor de goede en broodnodige leiding. Over bezielende toneelleiding gesproken, er is natuurlijk maar één mevrouw de voorzitter: Jojanneke met onder haar het FlauweCult-bestuur waarin door de jaren heen Frances, Joyce, Karin, Meintsje, en Tom gezeten hebben. Dank voor de koekjes, thee, en eindeloze stromen bonnetjes.

Alle drukte zou niet mogelijk zijn geweest zonder John, de held, die met de magische John-doekjes ons huis⁵³² nog een beetje op orde en fris houdt, waarvoor mijn (en Christens) dank, elke week weer. En natuurlijk de opvang, Naranja, waar Mark liefdevol en professioneel opgevangen wordt als ik het weer eens belangrijker vond om te schrijven aan één of ander boekje.

Als ik me dan eens noch met privacy noch met toneel bezighoud, zijn er gelukkig vele vrienden die mij op het rechte pad en van de straat houden. Wat ooit begon als een onsamenvattend plan van een paar puistige pubers om een LAN-party te houden in een onverwarmde schuur,⁵³³ heeft zich ontwikkeld in de meest politiek correcte groep poli-

530 Voor zover je opkwam, in ieder geval.

531 Op het oude Europa!

532 En het afgelopen jaar dus ook het kantoor.

533 Sowieso een goed plan, zeker als Joren koffiezet.

tiel incorrecte witte mannen. Arjan, Anne, dr. Elwin, Joren, Joris, Marc, Peter, en Sietse: dank voor de eindeloze stroom berichten. Ik vrees dat er in al die jaren weinigen zo diep in mijn ziel gekeken hebben als jullie.

Joris en Eva, dank voor de heerlijke vrijdagavonden, en eindeloos bij elkaar kunnen klagen over de staat van de wereld en alle mensen, dieren, en planten daarin. Daarna valt het toch altijd weer een beetje mee. Hylke en dr. Anne Marthe, jullie zouden natuurlijk vooral mij dankbaar moeten zijn voor mijn uitstekende verjaardagsfeestjes, al zeg ik het zelf.⁵³⁴ Wouter, dank voor de vele koppen koffie en koek, zonder welke een lunch natuurlijk niet genuttigd kan worden. Albert, Hylke, Johannes,⁵³⁵ Nico, en Thereza ben ik dankbaar voor het uitbreiden van mijn filmkennis. Naast alle klassiekers die ik had nooit zou hebben gezien zonder jullie, had ik natuurlijk vooral heel veel context gemist.⁵³⁶

Esther en Bouke, natuurlijk primair heel veel dank voor het opvoeden van de beste mens, jullie zullen toch met me eens zijn dat die prestatie eigenlijk niet te overtreffen is. Katalijn (inclusief verzamelde familieleden), bedankt voor de goede gesprekken en de oppasweekenden.⁵³⁷

534 Beter blijven jullie trouwens nog even in leven.

535 Bijzondere vermelding voor de pasta putanesca.

536 And I don't wanna miss a thing!

537 Waar de gesprekken vaak ook zeer heel diepgravend waren

Lieve oma,⁵³⁸ dank voor de vele decennia aan gezelligheid en geborgenheid als mater familias. Dr. Tante Pee,⁵³⁹ haar paranimf, kinderen, en bijbehorende aanhang verdienen hier een bijzondere vermelding voor de bijdragen aan de decembermaand: het einde van het jaar zou zonder jullie een stuk donkerder zijn. Veel dank voor de liefdevolle betrokkenheid door de jaren heen.

Dr. Marianne, liebe Schwester, dank voor het mij behoeden voor een Kipling-brugpieper-tas⁵⁴⁰ en het kritisch doorzagen van mijn papers.⁵⁴¹ Wat zou het leven saai zijn zonder broeder-zusterlijke lachstuipen en op z'n tijd keihard meeblèren met *Eternal Flame*.⁵⁴² Cum laude op het zijn van een grote zus!

Lieve Heleen, lieve moeder, alleen al de gedachte dat jij op een gegeven moment elk stuk van mij zou lezen en feilloos de zwakke plekken in de redenering eruit zou pikken, heeft de kwaliteit van deze dissertatie naar grote hoogte⁵⁴³ gestuwd. Zo veel dank voor alles wat je door de jaren heen voor mij betekend hebt, steeds opnieuw, altijd weer. Zonder jou zou ik de basisschool nog niet gered hebben.

538 En opa in herinnering.

539 Nu zegt u iets zinnigs.

540 Zowel letterlijk als vaak in figuurlijke zin door de jaren heen.

541 "Ik heb ook meteen even wat opmerkingen over de structuur gemaakt terwijl ik naar het Engels aan het kijken was" is een zinnetje waar dit proefschrift veel aan te danken heeft.

542 Tom Kelly, Susanna Hoffs, and Billy Steinberg, 'Eternal Flame' on *The Bangles* (red) *Everything* (Columbia 1989).

543 Of nou ja, in ieder geval omhoog.

Dr. Christien, grote liefde, door jou is niet alleen dit boekje in elk opzicht heel veel beter geworden, dat geldt voor alles. Wat hebben wij toch ontzettend geboft!

If, at this point, I still have not thanked you, I have probably simply forgotten.⁵⁴⁴ In that case: my sincerest apologies. Perhaps, however, there may have been excellent reasons for the omission too. I leave it up to the dear reader to ponder which situation might apply to herself/himself.

Lieve Mark en Esther Anna, ten eerste: dat zowel mama als papa gepromoveerd zijn, betekent niet dat jullie dat dus ook moeten, hè? Mama en papa zijn een beetje gek, vandaar. Ten tweede: jullie hebben echt niets aan dit boekje bijgedragen. Eindeloos Papa Gerard afleiden met jullie schattigheid telt niet mee, helaas. Maar aangezien dit de laatste woorden van mijn proefschrift zijn, kan ik nu wel ein-de-lijk weer komen voorlezen. Da's veel beter dan dank.

544 This section was mostly written with a very active two-year old running around my feet, so my level of concentration may have lapsed here and there. See further n 518 and n 519.