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

Gerard Jan Ritsema van Eck[1]

Accepted for publication in Bryce Clayton Newell, Tjerk Timan, and Bert-Jaap Koops (eds) *Surveillance, Privacy and Public Space* (Routledge 2018), part of the Routledge Studies in Surveillance series, edited by Kirstie Ball, William Webster and Charles Raab

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.

1 Security, Technology, and *e*-Privacy (ST*e*P) research group, University of Groningen, the Netherlands. g.j.ritsema.van.eck@step-rug.nl. Gerard Jan Ritsema van Eck MA is a PhD researcher at the Security, Technology, and e-Privacy (STeP) research group at the University of Groningen. His research focuses on the use of smartphones for participatory surveillance and its impact on the free enjoyment of human rights in public spaces.

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 centers are geared towards receiving phone calls, not photos and videos, from the public.[2] 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 (e.g. RapidSOS 2016), 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 are a push to make the 911 emergency response system in the 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" (The National 911 Program 2016); and an effort within the EU Horizon2020 research programme to create "a solution including a new smartphone app and on-line portal which are capable of being deployed in any European city" (Community Research and Development Information Service 2015a).[3] 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 emergency situations (Nederlandse Omroep Stichting 2016).

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 (Lauer 2012; de Certeau 1984). Interestingly, the smartphone enters the academic debate on surveillance mostly as an object which can be surveilled by (state) authorities or as a tool for sousveillance (e.g., Reilly 2015; Timan and Albrechtslund 2015, 4; Leistert 2013). 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" (Timan and Albrechtslund

2 See for a typical example of the predominance of voice calls for emergency situations the Dutch Politie app (the official app of the Dutch police) which redirects the user to calling 112 when s/he tries to report an emergency (Nationale Politie 2015).

3 For related projects see also (Community Research and Development Information Service 2016b; Community Research and Development Information Service 2016c; Community Research and Development Information Service 2016d).

2015, 16). This silence comes despite a wide range of possibilities that the ubiquity of smartphones presents to policy makers looking for new surveillance tools.[4]

The object of this chapter is, therefore, 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.

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 which focus on thorough applications and refinements of the theories developed in the previous two phases (Galič, Timan, and Koops 2016). 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 analyze 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.

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:

i. a person acting in a private capacity uses a mobile computing or communication device (which is usually a smartphone); to
ii. communicate to a police control room data other than (only) voice or text data; about
iii. a current or very recent situation; for which
iv. 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 moving[5]), 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

4 See for an artist's rendition of such possibilities for instance Nolan's *The Dark Knight* (2008) which features a botnet which turns all smartphones in the fictional Gotham City into echolocation devices.

5 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.

take place in other software environments—for example, e-mail or instant messaging apps. The term instant police reporting apps is used to cover all such scenarios to ensure consistency.

SOCIETIES OF DISCIPLINE

Michel Foucault (1995a) was the first to describe the panopticon as a schema for the functioning of power was. He based much of his analysis on Jeremy Bentham's infamous prison plans. In the short term, panoptic architectures endeavor 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 behaviors 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 (Foucault 1995a, 209).

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) systems[6] because they share a central working 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 more suitable metaphors (Koskela 2003; especially page 293, where she gives a more detailed treatment of some of the critiques). The central question in this section is, therefore, if 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 subsections. The first subsection 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 studies the long term effects. In the final subsection, attention will turn to a possible empowerment of the users of instant police reporting applications in the panoptical diagram.

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 control 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

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

Image 1. Photograph taken with an Apple iPhone 6 smartphone in London on 17 September 2015 by Benjamin Welle. Available at https://flic.kr/p/A81u4w under the Creative Commons Attribution-NonCommercial 2.0 Generic license available at http://creativecommons.org/licenses/by-nc/2.0/

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 figure in Image 1 (left), a photograph taken with a smartphone in the center of London. A fairly 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 would be circulated to police officers patrolling in the vicinity of where the photo was taken,[7] 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.

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 (see Welsh and Farrington 2002). 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,[8] the monotony of the images leads them to engage in unproductive behaviors (le Goff, Malochet, and Jagu 2011, 45). One strategy to alleviate these shortcomings are so-called “smart” CCTV systems, which incorporate algorithms that automatically alert operators to disruptions of a normal state of affairs.

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

8 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.

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

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 (Foucault 1995a, 201). 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 behavior.

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 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 calls[9]), 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 behavior frequently, or because they have a strongly developed sense of civic duty[10] combined with a strict set of (moral, social, and/or legal) norms which are thus regularly violated.

This suggests that the active userbase 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.

9 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 2015, 26).

10 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 (Fishwick and Mak 2015, 347).

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 (Foucault 1995a, 207). Groombridge has sketched the notion of an "omnicon," where the community, rather than a state agent, monitors the feeds from local CCTV cameras (Groombridge 2002, 43). This would shield against the excesses of surveillance because it is easier to differentiate between normal and abnormal behavior on the basis of the contextual knowledge that neighbors have about each other (Groombridge 2002, 42; Trottier 2014, 621). Groombridge's preliminary sketch has been expanded by Goold (2006, 12–14) with regard to how the footage from CCTV cameras in public places might be widely distributed and watched.

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 behavior[11]: French CCTV operators described by le Goff, Malochet and Jagu (2011, 26–29) routinely engaged in discriminatory practices by concentrating disproportionally on (black) youth whose clothing and appearance signaled that they belonged to a "subversive" youth culture; British CCTV operators have shown similar behavior—being male, young, black, or a combination thereof made visitors to city centers 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 (Norris and Armstrong 1999, 162–63).

Daniel Trottier (2014, 622) points out that there is little reason to believe that surveillance amateurs will engage in less discriminatory behaviors, especially if they are instructed to be vigilant for suspicious activity. Consider, for example, the case of nextdoor.com, a social networking site targeted towards supporting neighborhood communication. Despite its seemingly benign goal, the company has been battling accusations of facilitating racism, as many of the posts on the platform relating to security incidents seem to involve at least a degree of racial profiling (Harshaw 2015; Levin 2016). It seems that in a politico-societal context of responsibilizing "see

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

something, say something" campaigns and moral governance towards personal risk reduction (Hier, Walby, and Greenberg 2006, 236), ordinary citizens will rely on stereotypes when given a broad mandate to select any scene they come across for further police scrutiny.

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.

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 (1992) "Postscript on the Societies of Control" draws our attention. 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 "post-panoptical" (Galič, Timan, and Koops 2016) will be leveraged. In the first subsection, 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, normalization, the presumption of innocence, and cumulative disadvantages resulting from simulation and prediction, 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.

Inclusion in databases

Surveillant assemblages, as introduced by Haggerty and Ericson (2000) 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 assemblages (Haggerty and Ericson 2000). 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 subsections, 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 personal information" that bodies willingly and unwillingly emit (Smith 2016). An image of a body is thus also an image of the biometric characteristics of that body. Images therefor could facilitate the creation of (bits and pieces of) data about persons that is stored and analyzed 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 Image 1 reveals many innocuous bystanders.[12] 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 the subsection 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.

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. But 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?13 As was pointed out in the subsection on the long-term effects of the panopticon above, 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 behavior in public places will more frequently end up in police databases, whether the behavior in question was illegal or not. This will include those who unwittingly exhibit such transgressive behaviors: 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 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

12 Since Image 1 is only presented here for illustrative purposes, it should be mentioned that the central figure is probably also quite innocuous.

13 In *Discipline and Punish* Foucault (1995a, 277–78) 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.

behaviors: for instance protestors—who will be discussed in the subsection on normalization and chilling effects.

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 subsections 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, why not also let the algorithm populate a database[14] using data extracted from smart CCTV camera images? The practice of holding on to CCTV material for a limited period of time (le Goff, Malochet, and Jagu 2011, 41) already inscribes anyone captured moving about in public spaces as inherently "of interest" for a limited period of time. Local, national (e.g., the Next Generation Identification database of the FBI), and international databases of wanted persons would also form a logical addition here, as might databases maintained by private parties (Winston 2015).

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 out in the previous subsection. Furthermore, the choice of who to add to the database is filtered by citizens on the lookout for transgressive behaviors. 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.

14 This could either be the same database, or a connected, separate database.

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 (1967, 35) prophesized that such unfettering scrutiny would mean that "most persons in society would be […] in jail." Although this might be overly pessimistic, the above does imply a normalizing pressure to not engage in petty illegal behavior 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 places 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-story 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 more casual protestors, which increases their chances of being included in a police database (See also Schneider and Trottier 2012).

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 behaviors and those suspected of committing them. However, the ubiquity of smartphones means that the minutia 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 shifts the burden of proof and dilutes the right to remain silent (Milaj and Mifsud Bonnici 2014).

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 (Marx 2013). Maria Los (2006) 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" (2006, 83). 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. Timan and Oudshoorn (2012) found that, in such situations, the primary concern of those documented was the dissemination of the material; a concern which is currently mostly connected to the lack of control over privacy on social networking sites (Fox and Moreland 2015, 171–72). 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.

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 (Gandy 2006, 319; Gandy 2000, 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 smartphones 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 which might be important for the purposes of prediction; they are two of the three data points used by PredPol,[15] one of the most widespread commercial software packages which 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 (Joh 2016).

15 The final data point being the type of crime (PredPol 2015).

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 even more patrolling and more biased data being fed into the algorithms.[16] As a result, the individuals and communities living in neighborhoods 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 (Joh 2016, 32; Mantelero 2016, 240).

POLICY IMPLICATIONS

This chapter has a clear focus towards the future: instant police reporting applications are (at the time of writing) 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 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 behavior. 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 surveillance (Kammerer 2012, 99) and, as such, can directly and indirectly impact 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 stories (Doyle 2011)—they might decide not to proceed. The media can also impact 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.

Second, many of the negative effects outlined in the section entitled “Societies of control” 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.[17] 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

16 Such loops might very well negate the possible advantage which predictive algorithms present for creating a more equitable distribution of surveillance discretion (Joh 2007; Joh 2014, 58).

17 Compare here also footnote 13.

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 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.

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 (1992, 3) claim that the societies of discipline as described by Foucault have been superseded by societies of control. 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 (Simon 2005, 2): 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 agencies will have increasing amounts of visual recordings of suspicious behaviors made available to them—whether through dedicated platforms, social networking sites, or e-mail—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 "societies of discipline" has demonstrated the power that potential users of such apps wield. However, with great power there must also come great responsibility (Lee 1962). The extent of this responsibility was established in the section "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 disproportionally 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?

Avenues for future research

There are certain questions which 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-use (Dubbeld 2006, 192) 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 behavior?

Related to this question is the perhaps more criminological concern: are there certain transgressions which lend themselves especially well to reporting using smartphones? If there are, how does that impact 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 favor or disfavor certain groups? And could citizens turn this process on its head to give more visibility to crimes they deem important, for instance through collective actions?

Another topic which 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 (2014) maintains a database of over 2 billion ANPR readings, and Taser International provides a hosting solution for the videos made with their popular Axon police body-worn cameras (Gelles 2016). 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 analyses using the surveillant assemblage theoretical framework seems especially suited for investigation of these highly relevant and under-researched questions.

This chapter has analyzed 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 (Cohen 2013). Such an analysis is especially salient with regard to teenagers who engage in complex privacy behaviors vis-a-vis authority figures and institutions (boyd and Marwick 2011) but who are largely dependent on public spaces to escape the gaze of parents and educational institutions.[18] They may feel that their spaces for identity formation are being threatened by technophiliac 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 (boyd and Marwick 2011) start meshing together. The role that social networking and sharing platforms play in the lives of teenagers and young adults deserves special attention in this regard (e.g. Schneider and Trottier 2012; Timan and Albrechtslund 2015).

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.[19] 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 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 which 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 (Haggerty 2015): should users of instant police

18 See Carissa Véliz's (2017) contribution *In the Privacy of Our Streets* in this volume for a wider consideration of those who rely on public space for privacy.

19 See for a more general call for increased attention to popular mobile technologies in cultural geography Kinsley (2016).

reporting applications literally shout across the street to inquire if criminals consent to being filmed?

AUTHOR'S NOTE

I gratefully acknowledge the many helpful comments received from an anonymous reviewer and the editorial team 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.

DECLARATION OF CONFLICTING INTERESTS

The author pursues a PhD which is being supervised by prof. Mifsud Bonnici of the University of Groningen, who also leads the Horizon2020 CITYCoP (Citizen Interaction Technologies Yield Community Policing) project, which is funded by the European Commission under grant agreement no. 653811. One of the main projected results of CITYCoP is a smartphone application aimed at increasing community policing efforts which might include instant police reporting possibilities. The views expressed in this chapter are those of the author alone and are in no way intended to reflect those of the European Commission and/or the CITYCoP consortium.

REFERENCES

boyd, danah, and Alice E. Marwick. 2011. "Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies." In *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128.

Certeau, Michel de. 1984. *The Practice of Everyday Life*. Berkeley: University of California Press.

Cohen, Julie E. 2013. "What Privacy is for." *Harvard Law Review* 126: 1904–33.

Community Research and Development Information Service. 2015a. "Citizen Interaction Technologies Yield Community Policing (CITYCoP)." *CORDIS*. Accessed November 12. http://cordis.europa.eu/project/rcn/197273_en.html.

———. 2016b. "Inspiring CitizeNS Participation for Enhanced Community PoliCing Actions (INSPEC2T)." *CORDIS*. Accessed May 18. http://cordis.europa.eu/project/rcn/194895_en.html.

———. 2016c. "TRusted, CItizen - LEA coILaboratIon over sOcial Networks (TRILLION)." *CORDIS*. Accessed May 18. http://cordis.europa.eu/project/rcn/194841_en.html.

———. 2016d. "Unity." *CORDIS*. Accessed May 18. http://cordis.europa.eu/project/rcn/194893_en.html.

Deleuze, Gilles. 1992. "Postscript on the Societies of Control." *October* 59 (Winter): 3–7.

Doyle, Aaron. 2011. “Revisiting the Synopticon: Reconsidering Mathiesen’s “The Viewer Society” in the Age of Web 2.0.” *Theoretical Criminology* 15 (3): 283–99.

Dubbeld, Lynsey. 2006. “Telemonitoring of Cardiac Patients: User-Centred Research as Input for Surveillance Theories.” In *Theorizing Surveillance: The Panopticon and beyond*, edited by David Lyon, 182–205. Abingdon: Routledge.

ETSI. 2015. “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.

Federal Bureau of Investigation. 2016. “Next Generation Identification.” *FBI*. Accessed July 15. https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi.

Fishwick, Elaine, and Heusen Mak. 2015. “Fighting Crime, Battling Injustice: The World of Real-Life Superheroes.” *Crime, Media, Culture* 11 (3): 335–56. doi:10.1177/1741659015596110.

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

Fox, Jesse, and Jennifer J. Moreland. 2015. “The Dark Side of Social Networking Sites: An Exploration of the Relational and Psychological Stressors Associated with Facebook Use and Affordances.” *Computers in Human Behavior* 45 (April): 168–76. doi:10.1016/j.chb.2014.11.083.

Galič, Maša, Tjerk Timan, and Bert-Jaap Koops. 2016. “Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation.” *Philosophy & Technology*, May. doi:10.1007/s13347-016-0219-1.

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

———. 2006. “Quixotics Unite! Engaging the Pragmatists on Rational Discrimination.” In *Theorizing Surveillance: The Panopticon and Beyond*, edited by David Lyon, 318–36. Abingdon: Routledge.

Gelles, David. 2016. “Taser International Dominates the Police Body Camera Market.” *The New York Times*. July 12. http://www.nytimes.com/2016/07/13/business/taser-international-dominates-the-police-body-camera-market.html.

Goff, Tanguy le, Virginie Malochet, and Tiphaine Jagu. 2011. “Surveiller À Distance. Une Ethnographie Des Opérateurs Municipaux de Vidéosurveillance.” Île-de-France: Institut d’aménagement et d’urbanisme.

Goold, Benjamin J. 2006. “Open to All? Regulating Open Street CCTV and the Case for Symmetrical Surveillance.” *Criminal Justice Ethics* 25: 3–17.

Groombridge, Nic. 2002. “Crime Control or Crime Culture TV?” *Surveillance & Society* 1 (1): 30–46.

Haggerty, Kevin D. 2015. “What’s Wrong with Privacy Protections? Provocations from a Fifth Columnist.” In *A World without Privacy: What Law Can and Should Do*, edited by Austin Sarat. New York: Cambridge University Press.

Haggerty, Kevin D., and Richard V. Ericson. 2000. “The Surveillant Assemblage.” *British Journal of Sociology* 51 (4): 605–22.

Harshaw, Pendarvis. 2015. “Nextdoor, the Social Network for Neighbors, is Becoming a Home for Racial Profiling.” *Fusion*. March 24. http://www.fusion.net/story/106341/nextdoor-the-social-network-for-neighbors-is-becoming-a-home-for-racial-profiling/.

Hier, Sean P., Kevin Walby, and Josh Greenberg. 2006. “Supplementing the Panoptic Paradigm: Surveillance, Moral Governance and CCTV.” In *Theorizing Surveillance: The Panopticon and Beyond*, edited by David Lyon, 230–44. Abingdon: Routledge.

Joh, Elizabeth E. 2007. “Discretionless Policing: Technology and the Fourth Amendment.” *California Law Review* 95 (1): 199–234.

———. 2014. “Policing by Numbers: Big Data and the Fourth Amendment.” *Washington Law Review* 89 (1): 35–68.

———. 2016. “The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing.” *Harvard Law & Policy Review* 10 (1): 15–42.

Kammerer, Dietmar. 2012. “Surveillance in Literature, Film and Television.” In *Routledge Handbook of Surveillance Studies*, edited by Kirstie Ball, Kevin D. Haggerty, and David Lyon, 99–106. Abingdon: Routledge.

Kinsley, Samuel. 2016. “Vulgar Geographies? Popular Cultural Geographies and Technology.” *Social & Cultural Geography* 17 (6): 793–96. doi:10.1080/14649365.2016.1152394.

Koskela, Hille. 2003. “ “Cam Era” — the Contemporary Urban Panopticon.” *Surveillance & Society* 1 (3): 292–313.

Lauer, Josh. 2012. “Surveillance History and the History of New Media: An Evidential Paradigm.” *New Media & Society* 14 (4): 566–82. doi:10.1177/1461444811420986.

Lee, Stan. 1962. “Spider-Man!” In vol. 15 of *Amazing Fantasy*. New York: Marvel Comics.

Leistert, Oliver. 2013. From Protest to Surveillance: The Political Rationality of Mobile Media: Modalities of Neoliberalism. Frankfurt am Main; New York: PL Academic Research.

Levin, Sam. 2016. “What Happens When Tech Firms End up at the Center of Racism Scandals?” *The Guardian*. September 30. http://www.theguardian.com/technology/2016/aug/30/tech-companies-racial-discrimination-nextdoor-airbnb.

Los, Maria. 2006. “Looking into the Future: Surveillance, Globalization and the Totalitarian Potential.” In *Theorizing Surveillance: The Panopticon and Beyond*, edited by David Lyon, 69–94. Abingdon: Routledge.

Mantelero, Alessandro. 2016. “Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection.” *Computer Law & Security Review* 32: 238–55.

Marx, Gary T. 2013. “The Public as Partner? Technology Can Make Us Auxiliaries as Well as Vigilantes.” *IEEE Security & Privacy* 11 (5): 56–61. doi:10.1109/MSP.2013.126.

Milaj, Jonida, and Jeanne Pia Mifsud Bonnici. 2014. “Unwitting Subjects of Surveillance and the Presumption of Innocence.’ *Computer Law & Security Review* 30 (4): 419–28. doi:10.1016/j.clsr.2014.05.009.

Nationale Politie. 2015. “Politie App.” Accessed December 3. https://www.politie.nl/app.

Nederlandse Omroep Stichting. 2016. “Contact Met de Politie? Stuur Een Appje!” *NOS*. December 8. http://nos.nl/artikel/2147234-contact-met-de-politie-stuur-een-appje.html.

Nolan, Christopher. 2008. *The Dark Knight*. Burbank, California: Warner Bros.

Norris, Clive, and Gary Armstrong. 1999. “CCTV and the Social Structuring of Surveillance.” *Crime Prevention Studies* 10: 157–78.

PredPol. 2015. ‘How PredPol Works: We Provide Guidance on Where and When to Patrol.’ *PredPol*. http://www.predpol.com/how-predpol-works/.

RapidSOS. 2016. “Haven.” http://www.rapidsos.com.

Reilly, Paul. 2015. “Every Little Helps? YouTube, Sousveillance and the “Anti-Tesco” Riot in Stokes Croft.” *New Media & Society* 17 (5): 755–71. doi:10.1177/1461444813512195.

Schneider, Christopher J., and Daniel Trottier. 2012. “The 2011 Vancouver Riot and the Role of Facebook in Crowd-sourced Policing.” *BC Studies* (175): 57–72.

Simon, Bart. 2005. “The Return of Panopticism: Supervision, Subjection and the New Surveillance.” *Surveillance & Society* 3 (1): 1–20.

Smith, Gavin J. D. 2016. “Surveillance, Data and Embodiment: On the Work of Being Watched.” *Body & Society* 22 (2): 108–39. doi:10.1177/1357034X15623622.

The National 911 Program. 2016. “The Future of 911.” *911.gov*. Accessed December 19. http://www.911.gov/futureof911.html.

Timan, Tjerk, and Anders Albrechtslund. 2015. “Surveillance, Self and Smartphones: Tracking Practices in the Nightlife.” *Science and Engineering Ethics*, August. doi:10.1007/s11948-015-9691-8.

Timan, Tjerk, and Nelly Oudshoorn. 2012. “Mobile Cameras as New Technologies of Surveillance? How Citizens Experience the Use of Mobile Cameras in Public Nightscape.” *Surveillance & Society* 10 (2): 167–81.

Trottier, Daniel. 2014. “Crowdsourcing CCTV Surveillance on the Internet.” *Information, Communication & Society* 17 (5): 609–26. doi:10.1080/1369118X.2013.808359.

Véliz, Carissa. 2017. “In the Privacy of Our Streets.” In *Surveillance, Privacy, and Public Space*, edited by Bruce Clayton Newell, Tjerk Timan, and Bert-Jaap Koops. Abingdon: Routledge.

Vigilant Solutions. 2014. “LPR Data.” www.vigilantsolutions.com/wp-content/uploads/2014/08/LPR_Data_AUG2014_LFS.pdf.

Welsh, Brandon C., and David P. Farrington. 2002. “Crime Prevention Effects of Closed Circuit Television: A Systematic Review.” Home Office Research Study 252. London: Home

Office Research, Development and Statistics Directorate. http://webarchive.nationalarchives.gov.uk/20090410070401/http://www.homeoffice.gov.uk/rds/pdfs2/hors252.pdf.

Westin, Alan F. 1967. *Privacy and Freedom*. London: The Bodly Head.

Winston, Ali. 2015. "Los Angeles Sheriff Invests in New Tech to Expand Biometric Database." *Reveal*. July 3. https://www.revealnews.org/article/los-angeles-sheriff-invests-in-new-tech-to-expand-biometric-database/.