International Journal of Law in Context (2019), **15**, 177–182
doi:10.1017/S1744552319000107

§

ARTICLE

Policing the smart city

Elizabeth E. Joh*

Professor of Law, University of California, Davis, School of Law
*Corresponding author. E-mail: eejoh@ucdavis.edu

Abstract
What will be the consequences for policing as cities become increasingly 'smarter'? The emerging questions about policing and the smart city have thus far focused primarily on the increased surveillance capacity that a highly networked urban setting provides for law enforcement. More cameras and sensors will mean more watching and less freedom from being watched. The perception of ubiquitous government surveillance might quell dissent and inhibit free expression. As a result, concerns about policing and the smart city echo other responses to surveillance technologies. This essay proposes a different analysis: as cities become 'smarter', they increasingly embed policing itself into the urban infrastructure. Policing is inherent to the smart city.

Keywords: policing; surveillance; smart city

1 Introduction

Urban life can be unpredictable and inefficient, with traffic jams, coin-operated public machines, and wasted water and electricity. The smart city promises a future in which city living will mean being managed through the networked communications of sensors, artificial intelligence and robots that are part of a city's infrastructure. The real-time collection and assessment of data promise to improve the management of pedestrian and vehicle traffic, weather preparedness and energy use. And, while purpose-built smart cities like Songdo, South Korea (Borowiec, 2016) and Dongtan, China (Brenhouse, 2010) have failed, many existing cities are eager to retrofit themselves to gain the benefits of connectivity and data collection.

There are many examples. In Copenhagen, an array of sensors brighten streetlights only as vehicles approach (Cardwell, 2014). The city of Jun, Spain, relies on Twitter to do everything from receiving crime reports to booking appointments (Kiss, 2015). Public housing units in Singapore provide data about household energy use, waste production and water use (Souppouris, 2016). In 2017, Sidewalk Labs – owned by Google's parent company, Alphabet – announced that it will develop 800 acres in Toronto of federally owned waterfront into a smart, sensor-laden neighbourhood (Austen, 2017).

And, if the smart city improves the delivery of services of uncontroversial value, like traffic management, parking-space allotment and package delivery, it may also enhance the power of a more contested service: policing. Every data point useful for the efficient distribution of resources in the city can also be of potential value in a criminal investigation or to prevent crime from occurring in the first place.

What will be the consequences for policing as cities become increasingly 'smarter'? The emerging questions about policing and the smart city thus far have focused primarily on the increased *surveillance* capacity that a highly networked urban setting provides for law enforcement. More cameras and sensors will mean more watching and less freedom from being watched. The perception of ubiquitous government surveillance might quell dissent and inhibit free expression (Brundage *et al.*, 2018, p. 28). As a result, concerns about policing and the smart city echo other responses to surveillance

technologies. Regulatory proposals include minimising unnecessary data collection, anonymising data when possible and deleting data as soon as practicable (e.g. ACLU, 2017; Hardy, 2016).

To be sure, the smart city will enhance further the 'surveillance capacity' of the police (Ericson and Haggerty, 1997, p. 95). Gaining access to sensors collecting real-time information throughout a smart city increases the ability of the police to watch and to act. While few urban police departments have the human capacity to watch every source of data collection, 'smart' cameras and similar technologies can automate the process of flagging suspicious persons and activities (Joh, 2016). But enhanced surveillance is not the only effect of increased connectivity that will alter policing.

This essay proposes a different analysis: as cities become 'smarter', they increasingly embed policing itself into the urban infrastructure. Policing is inherent to the smart city. In exchange for receiving the benefits of more efficiently delivered services like public transportation and garbage collection, city dwellers agree to the monitoring of and response to their own behaviours.

From that premise, we can make a few broad observations. First, policing the smart city will be a hybrid model: relying upon both private and public forms of data collection and response. Second, policing in this environment will increasingly resemble the methods of private security rather than traditional public policing. Third, any attempts to regulate policing in the smart city will highlight the growing clash between intellectual-property rights and public accountability. New methods of policing will increasingly rely on privately created technologies whose details are guarded by the companies that created them.

These consequences arise not from wholly new technological developments, but rather developing trends that we can observe already in policing. The essay first reviews these developments before turning to what they mean in the context of smart cities.

2 Artificial intelligence and policing

Relying on the collection and analysis of data is not new in policing. The use of rogues' galleries and DNA databases reflects the importance of information gathering in policing (e.g. Cole, 2002). But what is new and different today is the sheer quantity of data and the technological capability to analyse it. So, while it is true that policing has long relied on data, today there are many technologies that permit the police to draw inferences from information in ways ordinary human beings cannot.

Whether referred to as a change in software, big data or algorithms, police today increasingly rely upon automated technologies in the same way as providers of dating services, retail shopping, health care and financial services do. Automated license-plate readers can collect and identify thousands of plates per second (Angwin and Valentino-DeVries, 2012). Place-based predictive policing software forecasts where crime might occur in the future (Sengupta, 2013). Social-network analysis predicts which persons might be future victims or perpetrators of gun violence (Eligon and Williams, 2015). Facial-recognition technology can identify individuals out of a crowd of thousands (BBC, 2018). None of these feats was possible, or not easily so, with human beings alone (but see Keefe, 2016).

Thus far in the US, these new technologies have taken the form of products adopted by local police departments. Sometimes, as in the case of police body cameras, the federal government has provided initial funding to local departments to purchase new technologies (Phippen, 2016). For the most part, though, these are local decisions by police departments to procure new technologies on a case-by-case basis (Joh, 2017). While there are increasing calls by civil-liberties organisations and others to impose new rules on departments to purchase new technologies (e.g. Crump, 2016), for the most part, American police departments enjoy considerable freedom in deciding which investigative technologies to purchase and deploy.

And, once purchased, these technologies can be used by police agencies with few legal restraints. Data collected about persons and activities in public spaces are not protected by the Fourth Amendment of the US Constitution. And, if the police retrieve data from third parties – usually private companies collecting data for their own purposes – there are few restrictions under current American law.

3 Consequences for policing in smart cities

Smart cities will integrate technologies that collect and analyse information into the urban architecture. Streets, sidewalks, buildings and vehicles will all contain sensors. No source of data will be too insignificant to analyse or to yield some insight. While the increased collection of data certainly means that there will be greater surveillance within a smart city, the ability of the smart city to respond to the data that are collected also includes automated responses to unwanted behaviours as well.

Consider how urban police officers respond to service calls today. A call to respond to a problem – a public argument, a suspicious person, a burglarised car – might yield a quick police response, a slower one or none at all. And, even if a police officer arrives, that officer's response will likely depend on several discretionary, and ultimately human, considerations. These might be as varied as the race of the perpetrator and complainant or how close the call is to the end of the officer's shift (e.g. Black, 1971).

In a smart city, controls might arise from the urban infrastructure itself. Those identified as probable shoplifters or credit-card thieves might be banned from entering certain places. An all-purpose public autonomous robot might identify you as a threat and automatically deploy an electric stun gun (cf. Lin and Singer, 2016). Your own autonomous car – in conjunction with road sensors –might make it impossible to speed, change lanes illegally or run red lights. Some forms of law breaking might be rendered impossible and others discouraged through denials of entry and provision of incentives.

3.1 Public and private data sources

The American smart city will embed policing into the city's own infrastructure: one that is both public and private. Public roads will collect and analyse data. But so too will private companies assemble facial-recognition databases for their own use and for sharing with the police. Automated license-plate-reader data will be collected both by public smart cameras looking for criminal activity and financial services firms looking for delinquent account holders. None of these activities is wholly novel; some exist right now. But the smart city accelerates these trends and assumes that policing is central to what the city's technologies accomplish.

And even traditionally public agencies will not escape private entanglements. Smart-city technologies – whether in the form of hardware, software or both – are privately developed products sold to public and private customers. Surveillance technologies already used by American police agencies today – such as social-media threat-analysis software and location-based predictive policing programs – are developed by private corporations that consider the police customers like any other. These companies might rely upon strategies that are familiar in the business world but novel in policing. For instance, a technology company might provide free or nearly free services to a police agency with the hope of ensuring customer loyalty and dependence on its products (Joh, 2017). The dominant provider of police body cameras, for instance, has offered American police agencies a year of free cameras that require use of its subscription-based technology platform (Weise, 2017).

3.2 The model of private policing

Moreover, the type of policing made possible through the smart city more closely resembles approaches we typically associate with private security. First, private security organisations focus on a much wider scope of activity: not just crime, but accidents and errors of all kinds (Shearing and Stenning, 1983). Second, private police organisations stress prevention and compliance over apprehension and coercion (Shearing and Stenning, 1983). Private policing organisations are far more interested in avoiding the disruption of routine activity than they are on the punishment of individual wrongdoers.

More than thirty years ago, Shearing and Stenning discussed how Disney World represented an unlikely paradigm of private policing (Shearing and Stenning, 1985). Accompanying its promise to provide a fun and safe experience to visitors is a set of nearly invisible but powerful policing tools.

The company anticipates and prevents possibilities for disorder through constant instructions to visitors, physical barriers that both guide and limit visitors' movements and through 'omnipresent' employees who detect and correct the smallest errors (Shearing and Stenning, 1985, p. 301). Neither the costumed characters nor the many signs, barriers, lanes and gardens feel coercive to visitors. Yet, through constant monitoring, prevention and correction, embedded policing is part of the experience.

Visitors also willingly co-operate in the structures of control designed into Disney World. The kind of order sought by the company is presented as an interest shared with the visitors. So, for example, having been convinced that these measures exist for their safety, visitors are willing to wait in long lines grouped by families (Shearing and Stenning, 1985, p. 302). There are no police uniforms, guns, batons or handcuffs. Instead, Disney policing is 'embedded, preventative, subtle, cooperative, and apparently non-coercive and consensual' (Shearing and Stenning, 1985, p. 304).

As cities become 'smarter', urban policing might look more like Disney's private policing: embedded in the environment itself. Traffic stops are the most common form of police–citizen interactions in the US (Eith and Durose, 2011). An artificially intelligent car could eliminate most of the traffic-law-related reasons for these sometimes hostile encounters (Joh, 2007). Autonomous vehicles programmed to follow rules (and that can be halted by police if necessary) might render certain kinds of regulatory offences impossible (Rich, 2013).

In other cases, policing could become instantaneous when artificial intelligence shrinks the gap between identification and adjudication. In the Chinese city of Shenzhen, facial-recognition technology will identify jaywalkers and immediately send fines to their cellphone by text message (Tao, 2018). Too many instances of traffic-rule violations will affect a person's social credit score: the Chinese national ranking system to be rolled out nationwide by 2020. This government-sanctioned measurement of 'trustworthiness' considers good behaviours (financial solvency) and bad ones (traffic fines). Those with high credit scores enjoy perks like bank loans with favourable terms while those with low scores may be denied access to airline travel or high-speed trains (Mistreanu, 2018).

Countries like the US are unlikely to develop centralised public ranking systems, but even local governments can embed systems of policing as they retrofit their urban environments. For as little as six dollars a month, the American technology company Amazon has offered a subscription facial-recognition service to police agencies and marketers alike (Dwoskin, 2018). Customers add known images of persons into a database and artificial intelligence scans new images – fed by public-facing cameras, for instance – to look for matches. While marketers might use the Amazon Rekognition program to identify celebrities in crowds, police might rely on the service to identify suspected criminals (Wingfield, 2018). Persons deemed suspicious or dangerous could be deliberately stopped by their own cars, by robotics or by other features of the existing smart city.

3.3 The regulatory gap

Smart-city capabilities are dual-use technologies. Any technology designed to create and manipulate data to increase the efficiency of city management will also serve as a convenient tool for law enforcement. A self-monitoring garbage can might also flag suspicious contraband. Automated sewer-system monitoring might also identify opioids and other substances flushed from individual residences. In order to function at all, autonomous public buses and shuttles must continuously monitor and collect data on the environment around them, including potential criminal activity.

A key challenge for cities in the US will be how to maintain oversight over these new forms of policing. With traditional policing, practical considerations like 'limited police resources and community hostility' can check the police from intruding too much on civil liberties.[1] When a city embeds powerful but inexpensive systems of prevention, deterrence, surveillance and enforcement into its structure, however, meaningful oversight becomes much more difficult.

[1] *United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor J., concurring).

Regulating the policing aspects of the smart city will post an even greater challenge because of the source of these new technologies. One consequence of greater automation in policing is the increasing influence of privatisation (Wexler, 2018, p. 1349). Police agencies do not create licence-plate readers, facial-recognition programs and other uses of artificial intelligence. New technologies are developed and sold instead by private companies. These companies use private law mechanisms to protect their own interests in ways that disadvantage public agencies and communities.

In practice, this claim of private power has meant that companies have succeeded in hiding information about their products by citing intellectual-property concerns. There are a small but growing number of legal cases that provide examples. The dominant manufacturer of cell site simulators, used by police to trick suspects' phones into providing location information, has relied upon non-disclosure agreements to prevent police agencies from disclosing information about their products in open records requests (Joh, 2017). Similarly, criminal defendants have been unable to learn about the source codes in forensic DNA software and in audio surveillance software used to help prosecute them because of developers' trade secrets claims (Wexler, 2018). As police agencies and smart cities increase their reliance on privately developed technologies, we can expect to see more confrontations between public claims to transparency and private assertions about intellectual property.

4 Conclusion

As cities become 'smart', connected and watchful, policing will become a less visible and a more embedded aspect of the urban environment. These developments represent but one more step in the rapid changes brought to policing by the increasing use of digitised data and artificial intelligence. In a smart city, however, we might see some qualitative changes to policing, too.

Sensors, artificial intelligence and robotics will lead not just to increased surveillance within a smart city, but the embedding of policing into the built environment. Private and public sources of data will provide the fuel both for the smart city to become more efficient, but also for the increased capacity for the police to detect and react to crime and disorder. These measures will look less like twentieth-century coercive policing and more like the models of prevention and apparently consensual control found in private policing. And, because many of the tools of smart-city policing will have been developed by private hands, there will be increased difficulties in maintaining oversight over urban policing. Public officials and judges will be asked to weigh competing values of intellectual-property protection, public-agency transparency and the rights of criminal defendants. These challenges will arise because policing will be a part of the smart city itself.

References

ACLU (2017) *Making Smart Decisions about Smart Cities*. Available at https://www.aclunc.org/sites/default/files/20171115-Making_Smart_Decisions_About_Smart_Cities.pdf (accessed 25 March 2019).

Angwin J and Valentino-DeVries (2012) New tracking frontier: your license plates, *Wall Street Journal*, 29 September.

Austen I (2017) City of the future? Humans, not technology, are the challenge in Toronto, *New York Times*, 29 December.

BBC (2018) Chinese man caught by facial recognition at pop concert, *BBC News*, 13 April.

Black D (1971) The social organization of arrest. *Stanford Law Review* **23**, 1087–1111.

Borowiec S (2016) Skyscrapers? Check. Parks? Check. People? Still needed. *Los Angeles Times*, 31 May.

Brenhouse H (2010) Plans shrivel for Chinese eco-city, *New York Times*, 24 June.

Brundage M *et al.* (2018) *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation.* Available at https://maliciousaireport.com/ (accessed June 2018).

Cardwell D (2014) Copenhagen lighting the way to greener, more efficient cities, *New York Times*, 8 December.

Cole S (2002) *Suspect Identities: A History of Fingerprinting and Criminal Identification*. Cambridge: Harvard University Press.

Crump C (2016) Surveillance policy making by procurement. *Washington Law Review* **91**, 1595–1662.

Dwoskin E (2018) Amazon is selling facial recognition to law enforcement – for a fistful of dollars, *Washington Post*, 22 May.

Eith C and Durose M (2011) Contacts between police and the public, 2008. *BJS* **October**.

Eligon J and Williams T (2015) Police program aims to pinpoint those most likely to commit crimes, *New York Times*, 24 September.

Ericson R and Haggerty K (1997) *Policing the Risk Society*. Toronto: University of Toronto Press.
Hardy Q (2016) Technology is monitoring the urban landscape, *New York Times*, 20 July.
Joh E (2007) Discretionless policing: technology and the Fourth Amendment. *California Law Review* **95**, 199–234.
Joh E (2016) The new surveillance discretion: automated suspicion, big data, and policing. *Harvard Law and Policy Review* **10**, 15–42.
Joh E (2017) The undue influence of surveillance companies on policing. *New York University Law Review* **92**, 101–130.
Keefe P (2016) The detectives who never forget a face, *The New Yorker*, 22 August.
Kiss J (2015) Welcome to Jun, the town that ditched bureaucracy to run on Twitter, *The Guardian*, 2 July.
Lin J and Singer P (2016) China debuts Anbot, the police robot, *Popular Science*, 27 April.
Mistreanu M (2018) Life inside China's social credit laboratory, *Foreign Policy*, 3 April.
Phippen J (2016) Funding for body cameras, *The Atlantic*, 26 September.
Rich M (2013) Should we make crime impossible? *Harvard Journal of Law and Public Policy* **36**, 795–848.
Sengupta S (2013) In hot pursuit of numbers to ward off crime, *New York Times*, 19 June.
Shearing C and Stenning P (1983) Private security: implications for social control. *Social Problems* **5**, 493–506.
Shearing C and Stenning P (1985) From the Panopticon to Disney World: the development of discipline. In Doob AN and Greenspan EL (eds), *Perspectives in Criminal Law: Essays in Honour of John Ll. J. Edwards*. Toronto: Canada Law Book, pp. 300–304.
Souppouris A (2016) Singapore is striving to be the world's first 'smart city', *Engadget*, 3 November.
Tao L (2018) Jaywalkers under surveillance in Shenzhen soon to be punished via text messages, *South China Morning Post*, 27 March.
Weise K (2017) Taser is giving body cameras to any cops who want them, *Bloomberg*, 6 April.
Wexler R (2018) Life, liberty, and trade secrets: intellectual property in the criminal justice system. *Stanford Law Review* **70**, 1343–1429
Wingfield N (2018) Amazon pushes facial recognition to police: critics see surveillance risk, *New York Times*, 22 May.

Cite this article: Joh EE (2019). Policing the smart city. *International Journal of Law in Context* **15**, 177–182. https://doi.org/10.1017/S1744552319000107