UDK: 343.85:004.738.5
doi: 10.5937/crimen2003255M
Originalni naučni rad
primljen / prihvaćen: 26.10.2020. / 23.11.2020.

*Sanja Milivojevic**
La Trobe University, Melbourne, Australia

*Elizabeth Marie Radulski***
La Trobe University, Melbourne, Australia

THE "FUTURE INTERNET" AND CRIME: TOWARDS A CRIMINOLOGY OF THE INTERNET OF THINGS***

Abstract: The Internet of Things (IoT) is poised to revolutionise the way we live and communicate, and the manner in which we engage with our social and natural world. In the IoT, objects such as household items, vending machines and cars have the ability to sense and share data with other things, via wireless, Bluetooth, or Radio Frequency IDentification (RFID) technology. "Smart things" have the capability to control their performance, as well as our experiences and decisions. In this exploratory paper, we overview recent developments in the IoT technology, and their relevance for criminology. Our aim is to partially fill the gap in the literature, by flagging emerging issues criminologists and social scientists ought to engage with in the future. The focus is exclusively on the IoT while other advances, such as facial recognition technology, are only lightly touched upon. This paper, thus, serves as a starting point in the conversation, as we invite scholars to join us in forecasting—if not preventing—the unwanted consequences of the "future Internet".

Keywords: Internet of Things, Smart Things, Surveillance, Technology, Crime.

INTRODUCTION

> The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it. (Weiser 1991, 94)
>
> [W]hen everything is connected, everyone is vulnerable. The technology we routinely accept into our lives with little or no self-reflection or examination may very well come back to bite us. (Goodman 2016, 13)

[*] Research Fellow, S.Milivojevic@latrobe.edu.au

[**] Researcher, E.Radulski@latrobe.edu.au

[***] Rad predstavlja neznatno izmenjeni članak koji je pod istim naslovom objavljen u časopisu *Current Issues in Criminal Justice* 32(3): str. 1–15.

Imagine the following scenario: Police officers arrive to a crime scene. There is a body on a pavement, and a 3D printed gun next to it. An officer approaches the gun and points an object to it. The connection is established. The object reads information about the gun: the date and place of printing, who printed it and from what materials, who bought it, and maybe even who handled/fired it. Or the following: A prospective terrorist goes to a hardware store to get things they need to make a bomb. All the components have sensors that communicate with other objects, leaving a unique data trail. The things communicate this information to law enforcement who come to a conclusion about the likely outcome of this purchase. And in the final scenario, think about this: prisons may soon become obsolete, thanks to the IoT technology. A would-be terrorist' house from the previous scenario could serve as a prison cell: the front door would deny entry or exit, if so-ordered by the court of law. In the future, many objects in our house, workplace, and public spaces – from front doors, chairs and beds, to vehicles and planes – are likely to be connected through the IoT network. They will communicate to other "smart things" in the grid, record and monitor our behaviour, location, health, and mental state. Objects will also be able generate an action on our behalf, potentially bypassing us in the process. They are likely to become smarter, learning from and adapting to the embedded algorithms and the environment.

While some of the above scenarios might materialise in the future, certain elements of the IoT revolution are already a reality. The IoT technology is growing, while our engagement with these ground-breaking developments remains limited at best. From humble beginnings in late 1980s, when only about 100,000 hosts were connected to the Internet (Baras and Brito 2018), today's world is a fundamentally changed by this technology. One of the very first examples of the technology that connects ordinary objects to the Internet was a Coca-Cola vending machine located at Carnegie Mellon University; the programmers working at the University IT department decided it would be good to contact the machine to check the stocktake before making the trip for refreshment, and wrote a software that did just that (Foote 2016). Kevin Ashton from the Massachusetts Institute of Technology coined the expression "the Internet of Things" in the late 1990s, to describe a network of objects connected to the Internet, and one another (Claveria 2019). In 2008, the number of devices connected to the Internet surpassed the world's population (Baras and Brito 2018). This development continues at pace: some projections state that that by the year 2032, an individual will be connected to 3,000 to 5,000 things (Barrett 2012). While such projections should be taken with caution, in a not so distant future we are likely to witness 'the dawn of a new era; one in which today's internet (of data and people) gives way to tomorrow's Internet of Things' (International Telecommunications Union 2005, 1).

Manifold potential ramifications and practical implications can stem from the introduction of these technologies to debates pertinent to crime and criminal justice. It is important to acknowledge that, given the scarcity of criminological literature on the topic, we do not purport to offer an in-depth theoretical account of the IoT in criminology, nor do we strive to answer the many legal, ethical, and political questions raised when pondering these technologies in a criminological context.

What this paper seeks to do is to start a conversation about how criminologists should approach the IoT in the future. While flagging this critical point of juncture, this article focuses on four key areas of inquiry. We start with the definition of the IoT, followed by debates around privacy and data security in the IoT, the “internet of evidence” and the future of offending. A particular emphasis is placed upon the concept of “smart homes” and “smart cities”, and a theoretical exploration of how these technologies may eventually evolve into “smart states” and “smart borders”. We also cast a brief look on how the IoT can further marginalise “the Other” – people with limited mobility potential and populations already subject to extensive surveillance and control. The final segment of the paper provides some theoretical insights on the matter, in which we suggest that we should aim to develop innovative frameworks in order to engage with challenges we face in the future. Finally, the conclusion brings together key points in the debate, as well as a call for multidisciplinary research on this important topic that ought to include social scientists, researchers from STEM disciplines, and IT experts.

1. UNPACKING THE WONDERWORLD OF THE IOT

While there is no universal definition of the IoT, many share the following common elements: it is a *network* of objects made by humans, with *unique identity* (unique identification number and Internet Protocol address), small *power supplies, sensors* (with sensing/actuation capability that can capture context and provide information about the thing itself or its environment), and *connection* – ability to communicate to one another and transmit and receive data (Howard 2015, xi; see also Bunz and Meikle 2018). These objects are often characterised by *a higher degree of computing, analytical, and action abilities* (Burgess 2018). We adopt the following definition: the IoT as ‘a variety of things or objects – such as Radio-Frequency IDentification (RFID) tags, sensors, actuators, mobile phones, etc. – which, through unique addressing schemes, are able to interact with each other, and *cooperate with their neighbors to reach common goals*’ (Atzori, Iera, and Morabito 2010, 2787; emphasis added). Objects on the IoT have several layers of connection. According to Li (2017), the lower/sensing layer is comprised of sensing technology such as RFID tags, intelligent sensors, and RFID readers. The middle (network) and upper (service) layers are constituted of networked systems that enable communication and connection between things, such as cloud internetwork (social and mobile networks, WLAN). The application-interface layer is where the interaction and activity occur – in smart cities, smart manufacturing, smart power grids, smart transportation, and so on. Importantly, things in the IoT can be changed or altered from anywhere, ideally with little to no human intervention (Baras and Brito 2018; Tuptuk and Hailes 2019). In the “future Internet” (Gubbi et al. 2013) some of us will be unaware that objects around us are sensing and exchanging data, as microcontrollers in some of them make a decision based on the readings. Many of us who will be aware of what is going on, as we argue later, are unlikely to opt out of things-run surveillance. Critically, some objects in the IoT will have the ability to configure themselves autonomously, adapt to change, and take action.

It is essential at this point to outline the typology of "things". They are indeed diverse; some are physical-first, meaning that they generate or exchange data only when augmented or manipulated – such as desks or fridges. Others are digital-first, specifically designed to generate and exchange data, such as smartphones (Greengard 2015, 16) Physical-first object exchange data, but not to the extent as digital-first ones. Connected things can be physical (ie. physical objects) or virtual (ie. software, code). Finally, there is a distinction between the "conventional" IoT that require human involvement and analysis (such as connected contact lenses that send information to your doctor for diagnosis), and the autonomous IoT that have the capacity to bypass humans (for example, the autonomous self-healing systems used in manufacturing that can predict and repair machines without human involvement). Autonomous IoT are examples of the intersection of the IoT and Artificial Intelligence (AI), in which objects make sense of data, learn from it and one another, and change its "behaviour". We talk about all the aforementioned types of the IoT technology in this paper.

1.1. The surge and impact of smart things: from homes and cities, to crime and mobility

The future Internet is often described as a smart environment (Gubbi et al. 2013), in which our bodies, homes, transport systems, workplaces, communities, and states will be transformed by technology. The IoT has already been applied in many areas of social life, predominantly in what are now known as "smart cities". Baig et al. (2017, 3) describes the smart city as a 'connected environment for all its citizens... [whose] services can extend into many diverse domains including the environment, transportation, health, tourism, home energy management and safety and security'. In smart cities, regulation of water, electricity, waste, traffic, parking and alike is gradually transferred from humans to the networked objects. Smart homes and buildings with automated lighting, heating, energy consumption and greenhouse production are at the forefront for the IoT systems of today (Baras and Brito 2018). Healthcare, energy sectors and transportation are also areas where the IoT is breaking new ground. The future Internet enables doctors to monitor elderly patients in their homes, thus reducing hospitalisation costs through early intervention (Gubbi et al. 2013). Self-driving cars with sensors that prevent crashes are rapidly becoming mainstream. While the impact of the IoT has been the topic of science and technology literature for quite some time now, the questions pertinent to links between crime and the IoT, as well as its social applications remain largely unanswered. Current literature mostly focuses on cybercrime and risk of potential attacks on the IoT network (Gubbi et al. 2013; Tuptuk and Hailes 2019; Baig et al. 2017). This indicates the need for research in social sciences that focuses both on risks and vulnerabilities the future Internet brings, but also how technology can assist us in addressing various crime and human rights concerns, such as the right to privacy.

2. WHO IS WATCHING WHO?: UBIQUITOUS SURVEILLANCE, SECURITY, PRIVACY, AND AGENCY

The digital era's undisputable fact is that 'we are living in a time when more information is gathered, collected, sorted and stored about the everyday activities of more people in the world than at any other time in human history' (Andrejevic 2012, 91). This type of surveillance is called ubiquitous to depict the world in which it is difficult, if not impossible to "opt out". Surveillance is also ongoing: computers, smartphones, and other smart devices continuously collect and share information about our activities. The IoT as a future Internet where both physical-first and digital-first objects sense and share information about and around us 'could be the most effective mass surveillance infrastructure we've ever built' (Howard 2015, xvii). Surveillance in the IoT does not happen via a tall tower with an omnipresent guard Jeremy Bentham envisioned when he developed his utopian prison design – the Panopticon, nor as a self-discipline surveillance and control mechanism described by Foucault. We come back to this important point in the final section of the paper. For now, it is important to note that the IoT innovations have been marketed to us as desirable, a must-have technology that will improve our lives. The IoT systems are seen to provide 'a convenient way [for people] ... to keep an eye on the inside and outside of their homes from any location with internet access' (Dixon 2017, 37; see also Weber 2017). Yet, as we keep an eye on our possessions and properties, these little helpers relentlessly monitor and exchange information about us, often inconspicuously. They send data to manufacturers, developers, and other agencies that can be used for a variety of commercial and non-commercial purposes. As Andrew Guthrie Ferguson would have it, '[w]e are now all living with little smart spies in our houses' (CBC Radio 2018). Your Amazon Alexa or Google Home Smart Speaker monitor your movements, listen to your commands, and record events around you even when you think they are switched off. Surveillance in the IoT is pervasive, conducted by many different things, a super-sized version of "surveillance assemblage" (Haggerty and Ericson 2000). It is performed through the continuous gathering of data through many sensors connected in the IoT.

A range of actors (governments, IT companies, military-industrial complex, and private enterprises) aspire to surveill and manipulate people's behaviour via the IoT (see Howard 2015). Indeed, surveillance *per definitionem* is 'the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction' (Lyon 2007, 14). In the IoT, surveillance is so omnipresent that privacy emerges as the key issue: more specifically, the right to be let alone (Warren and Brandeis, cited in Bunz and Meikle 2018, 123). An abundance of literature explores privacy concerns in relation to the IoT (Williams 2016; Baig et al. 2017; Dixon 2017; Claypoole 2016). The European Commission on the IoT Governance recently recommended that developers adopt "privacy by design" approach when fostering new IoT systems (Vos 2018). While some of us might be alarmed by the prospect of ever-expanding data sharing, our desire for smart things is likely to prevail. We will, therefore, get Alexa or Google Home, a self-driving car, or that spying smart chair because they offer 'status, approval, enjoyment' (Lyon 2018, 82). Privacy as a concept is likely to experience substantial changes in the future Internet. What should be of interest to social scientists, however, is not just the extent of surveillance per se, but who has access to data, and what legal frameworks we need to address issues that might emerge in the future.

One of the most discussed concerns in IoT literature and public discourse is that large networks of connected things could be open to potential hacks (Roman, Najera, and Lopez 2011; Gubbi et al. 2013; Claypoole 2016; DeNisco Rayome 2017), as 'each connected device could be a potential doorway into the IoT infrastructure or personal data' (Li 2017, 2; 4). While some of these privacy intrusions are indeed disturbing[1], other issues with more duplicitous attributes could become more pressing. Let's use a common (and often mocked) case study in the IoT: a smart fridge. Your local bottle shop is likely to deliver your favourite beer as requested by a smart fridge when your supplies run out. The benefit of convenience, however, could be offset in the event that the fridge overrules your recent decision to quit drinking. Or, consider the more serious ethical dilemma smart car developers face when embedding algorithms that will have the power to decide which person to "sacrifice" in a case of an emergency (Bonnefon, Shariff, and Rahwan 2016). Automated objects around us have an ability to share and evaluate data, but also make decisions on our behalf, while our preference on the matter – for example, whether or not we would like particular information to be shared with our doctors, employers, government, or family members – becomes irrelevant. As such, the impact of IoT technology on human agency and autonomy is just one of many conundrums social scientists, lawyers and criminologists will have to unpack in years to come.

3. LAW AND ORDER: OFFENDING AND "THE INTERNET OF EVIDENCE" IN SMART CITIES/HOMES

While the literature offers an insightful overview of ethical debates pertinent to the IoT, somewhat absent from these discussions is the potential for IoT to be used in committing and/or solving crime. Samuel Greengard (2015, xv) suggests that the technology and in particular the IoT 'will affect everything from the way people vote to the way we eat at restaurants and take vacations', and that 'the future could introduce new types of crime, weapons, and warfare'. Some end-users have called the IoT technology 'a security disaster waiting to happen' (CompTia 2016, 3). If, as described above, our lifelines such as energy grids, healthcare, transportation, and even our bodies are all on one mega-grid, the issue of disrupting the grid becomes a major concern indeed. A malfunction or interruption of the future Internet could affect a large proportion of the population – from financial institutions, hospitals, to public transport and distribution of goods. Denial of Service (DoS) and more sinister, large-scale Distributed Denial of Service (DDoS) or Ransom Denial of Service (RDoS) attacks that aim to restrict or deny access to services to legitimate

[1] For example, incidents where hackers broke into baby monitoring systems and even talked to at least one sleeping baby – (Greengard 2015); (Bunz and Meikle 2018, 26).

users, are already a major headache for developers, early adopters, businesses, and governments (DeNisco Rayome 2017; for a range of potential scenarios see Tzezana 2016; Tuptuk and Hailes 2019). Most concerningly, the human body itself could be hacked through the IoT (Ashton 2017; Goodman 2016), via pacemakers or medical implants. In 2013, former US Vice President Dick Cheney disclosed that doctors deactivated wireless function on his heart implant to prevent a potential terrorist attack (Tuptuk and Hailes 2019). As Marc Goodman, founder of the Future Crimes Institute explains (cited in Chabinsky 2015), '[w]hen your heart is online for your doctor to access, it is also available to the kid next door. ... For the first time in human history, the human body itself has become susceptible to cyber attack'.

Warnings that the legal system and crime control agencies need to "catch up" with technology have also been revived (Ashton 2017). Law enforcement agencies across the Global North have been increasingly using the IoT in their daily activities. Some well-known examples are the Los Angeles Police Department's Real-Time Analysis Critical Response Division (detailed in Ferguson 2017), or the 'first-ever smart patrol car system that fully integrates video captured from in-car and body-worn cameras' (Ives 2015, 2; Zimmer 2017). The IoT in smart cities assists with building maintenance and repair, waste and traffic management, pollution monitoring and regulation, smart lighting (Zanella et al. 2014), but also crime prevention and investigation. Sensing devices in smart cities, for example, track the movement of pedestrians in dark streets, turn on the street lighting and cameras when needed, and send data to police for processing (Lee 2015). Machine learning enabled video camera could also help a potential victim detect in milliseconds whether a purported robber holds a real gun or not, and alert law enforcement if the former is confirmed (TEDx Talks 2018).

Privacy and agency issues discussed above, stemming from automation of the IoT technology are also of concern in smart cities. As devices for sensing, detecting, and data transmission are becoming mainstream, human agency might soon be bypassed:

> An illicit driver enters a smart city attempting to subvert all policing controls in place for traffic regulation. The driven vehicle enters the city and increases speed past the stipulated limit ... an incident response team will be alerted immediately by sensory data which is transmitted over to the centralized Cloud and measured as being anomalous by the relevant data analysis engine. Subsequently, the traffic control authority (the police) will be alerted with the data emerging from the Cloud, and necessary tactical action will be taken to control the incident. (Baig et al. 2017, 10)

As illustrated in the above example, in the IoT-run smart cities people will not necessarily have control over whether data is sent/received, and the discretion of government agencies (i.e. police or courts) might also be diminished.

Some elements of this technology are seeing widespread, and largely uncontested implementation in major cities around the world. In 2010 Victoria Police in Australia quietly awarded permission from Melbourne's Transport Ticketing Authority to access and utilise myki (smart travel card) records for law enforcement and criminal justice purposes. Victoria Police have since been tracking the movements of potential offenders, to determine their whereabouts at the time a given crime may have been committed (Hunter 2010). At present, Victoria Police need to individually identify a person as a "threat," and manually seek a record of that person's myki touch-on and touch-offs. In smart cities, however, "smart tickets" could monitor and automatically alert/action law enforcement and border police to citizen/non-citizens' location at any given time.

There is 'no doubt that, in the future, IoT will be handy in solving crimes' (Alohali 2017, 177; see also Kearns 2018). The IoT technology has many applications in criminal proceedings, as government agencies use the IoT for prosecutorial benefit. In the United States, judge Dixon (2017) has identified various legal contexts in which "smart home" evidence – evidence collected via networked home items– has been presented in the court of law. Orr and Sanchez (2018) also highlight a case in which police in the US state of Arkansas presented IT giant Amazon with a warrant for recorded voice data stored in an Amazon server, after collecting the device from a murder suspect. They conclude that smart IoT devices, in particular Amazon Echo and Alexa, have the capacity to provide valuable legal evidence in criminal justice proceedings. There were since other cases where technology has been used in criminal trials, so much so that we can now talk about '"the internet of evidence", where lots of pieces of smart devices are going to show up in criminal prosecutions' (Andrew Guthrie Ferguson, cited in CBC Radio 2018), often to testify against their owners. Importantly, as we investigate in the following section, law enforcement and government agencies should be closely monitored for signs that they may be constructing a "smart state", in the name of criminal justice and/or border security.

4. "SMART STATES" AND "SMART BORDERS": THE IOT AND MOBILITY

Contemporary states seem to embrace two outwardly juxtaposed developments in bordering practices: erection of border walls and fences, and development of border security technologies. Technology has been at the forefront of governing mobility for several decades. Its range is not limited to the national borders; technological innovations ebb and flow to and from countries of origin, transit, and destination. A range of security technologies (Neal 2009; Milivojevic 2013, 2019a) – technology-human interconnections developed to regulate and govern mobility have been developed and applied in the Global North and the Global South. They comprise of strategies, policies, hardware, and software that aim to strengthen borders and regulate the flow of citizens, non-citizens, goods and trade (see Koslowski 2004; Brouwer 2008; Cote-Boucher 2008; Ceyhan 2008; Popescu 2015). Surveillance of mobile populations is emerging as a preferred method for strengthening risky borderlands. As Adey (2012, 193) accurately points out, 'borders are married to the practice and evolution of surveillance'. Countries of origin and transit have emerged as principal sites for the detection, surveillance, and classification of border crossers. The goal is to 'check individuals as far from [the nation state] as possible and through each part of their journey' (UK Cabinet

Office, cited in Vaughan-Williams 2010, 1073). The contemporary "biometric state" has an 'almost obsessive preoccupation with where you are going and who you are' (Muller 2010, 8).

In times of increased mobility, however, conventional security measures that require human decision-making struggle to process and respond to big data. High-tech border checkpoints—with scanners, security cameras, and screening processes—are still staffed with security personnel, who must check passport photos, and monitor the border via thermal imaging cameras. Border guards, thus, make a judgement on incoming travellers' rights to enter the country, and act to intercept "illegal" migrants. The IoT could fundamentally change this process and in doing so, further extend the border by screening mobile bodies before they board planes, ships, and cars. "Risky" individuals will be identified at arm's length, while desired travellers will be acknowledged as such well before they reach the physical border. The IoT technology carried or worn by border crossers sensor and transmit data about people's migratory projects: where they are, who are they with, what trajectory they intend to take, and what is their body temperature and heartbeat. As people embark on a journey across state borders, information about their plans and activities might be sent to recipients' databases, making it harder if not impossible to engage in a covert cross-border activity. The IoT could thereby advance 'futuristic and high-tech security fantasies' (Adey 2012, 193) of pervasive, seamless contemporary borders that segregate wanted from unwanted mobility. While the "digital divide" – an uneven access and distribution of these technologies is the factor to have in mind when discussing technology and mobility (Milivojevic 2019b; Dekker and Engbersen 2014), the seamless IoT borders are undoubtedly in the making.

The narrative that is likely to underpin the development of smart states is the one of countering risk. Justification for new technological borders will be the notion that people smugglers, human traffickers, and illegalised non-citizens are likely be detected before they approach physical borders. Non-citizens or visa over-stayers could also be detected automatically, in hospitals, classrooms or workplaces, and border officials tipped off as to their location. Smart states with secure and entirely digitised smart borders will enable the passage and the right to stay for *the right number* of *the right people* (Milivojevic 2019a): the "risky", "dangerous" or unproductive "Other" will be held at arm's length, or as we demonstrate below – targeted from within.

5. INTERSECTIONALITIES: THE "OTHER" AND THE IOT

In 2015, Google rolled out a new feature for its Photo app that analysed photos by tagging them as "beaches", "cities", "animals", and "people". After a few months, following a notorious incident in which Google Photos labelled a woman of colour as "gorilla" (see Bunz and Meikle 2018, 90–1), Google admitted it failed to optimise its app for people with black skin. While this is not an example of the IoT technology, we argue that similar to this example objects networked in the IoT can "see" but that their vision is limited. If there is an unfair bias towards accurately mapping and recognising a normative standard for facial structure — as seen in a white "norm" example in above-mentioned "gorilla" incident —then does the software embedded in the IoT also risk homogenising "Others", and unfairly discriminating by potentially labelling them as threats, at a greater frequency? Certainly, as Lyon et al. (2012) argue and as we suggest in this article, contemporary surveillance captures everyone, including groups that historically managed to avoid such scrutiny. However, Lyon et al. continue, this often translates into new asymmetries, in which those in the position of power emerge more powerful, while marginalised end up being over-surveilled. Contemporary ubiquitous surveillance often reinforces and exacerbates existing inequalities. It is, therefore, worth exploring whether marginalised global communities such as refugees, asylum seekers, ethnic and racial minorities, and former colonised subjects are more likely to be unfairly targeted by the IoT. As Simone Browne (2012) powerfully demonstrates, racialised surveillance is alive and kicking, and there is a claim that the IoT is likely to make matters worse, given that surveillance is always accompanied, if not inspired by social sorting (Lyon 2018).

Some of these fault lines are already visible. As Andrejevic (2012, 94) suggests, 'relatively affluent groups and places are subject to more comprehensive forms of commercial monitoring, whereas less affluent groups and places are targeted by policing and security-oriented forms of monitoring'. Similarly, Means Coleman and Brunton (2016) assert that this type of technological institutionalisation of social inequality is evidenced by over-policing and disproportionately high surveillance measures being employed in impoverished African-American neighbourhoods. Through the IoT, the socially stigmatised "Other" could be over-surveilled, with grounds for prevention of exit, visa revocation, or denial of services established before their application for travel, visa or asylum is finalised. The IoT has the potential to monitor those deemed "risky" at all times as they go about their day-to-day lives. As such, technology can be used to unfairly discriminate against populations labelled "deviant" by way of race, ethnicity, religion, and social status, and therefore considered "inherently" inclined towards criminal or anti-social behaviour.

6. THE TECHNOLOGICAL UNCONSCIOUS OF THE IOT: THEORISING SMART DEVICES

Further development of the IoT systems will not bring things to life; however, it will significantly change the dynamic between humans and networked objects. As we demonstrate in this paper, smart things will sense, track, send information, and occasionally exclude us from exercising agency. While this is certainly a principal question for philosophers, ethicists and sociologists, criminology has to join the debate, as the above developments will inevitably impact on crime prevention, offending, policing, and legal and penal policies. Theorising the IoT, however, is a complex exercise. Here, we commence this process by investigating one possible impact of the IoT technology: a diminished agency of humans and its importance for criminology.

Given the centrality of the panopticon and panopticism within the field of criminology, any theorising about the IoT should use these concepts as a starting point. The panopticon, as defined by Jeremy Bentham, is an institution of a control in which those being watched regulate their own behaviour regardless of whether they are actually under the gaze of the watcher. Building on this, Foucault (2002, 70) defines panopticism as,

> a type of power that is applied to individuals in the form of continuous individual supervision, in the form of control, punishment and compensation, and in the form of correction, that is, the modelling and transforming of individuals in terms of certain norms.

However, for many scholars the 'mere mention of the panopticon elicits exasperated groans' (Bauman and Lyon 2013, 49), as the concept of the past is largely perceived as incapable of capturing the nuances of new technologies (Lianos 2003; Haggerty and Ericson 2000). At the turn of the century Haggerty and Ericson (2000) proposed the concept of "surveillance assemblages" to describe a multitude of networked machines that collect, extract, sort, analyse and deliver information. Machines, therefore, play the vital role in this system of surveillance. They not only collect data and surveil the object of surveillance, they also manipulate data within these diffused, dispersed digital networks. Importantly, as we discussed above, machines also challenge human agency via the decision-making powers of the IoT, while at the same blending with the environment.

In new media studies this phenomenon is described as "the technological unconscious" (Beer 2009; Thrift 2004; Wood 2016). Building on the works of new media theorist Scott Lash, the technological unconscious refers to the operation of new technologies that results in producing and modifying everyday life (Thrift 2004). In the 21st century technology and information do not simply mediate; they constitute our existence. Yet, the automated communication between the machines will be a big 'part of how we live, but not a part of our day-to-day conscious existence' (Beer 2009, 988). Technology, thus, sinks 'into its taken-for-granted background' (Thrift 2005, 153), unobserved and unchallenged.

The IoT, as this paper demonstrates, offers a platform for ubiquitous surveillance, in which we will be constantly observed by a multitude of connected things that collect, exchange, and analyse data about us. The objects will sense, learn, adapt, and take action pertinent to our health and wellbeing, transportation, mobility, energy consumption, and workplaces. In smart homes, cities and states, people will be subjected to ongoing lateral and vertical surveillance. Things around us will be deployed as witnesses in criminal proceedings, police officers, and assistant border guards. Just how much is the IoT going to impact on crime and offending, as well as crime fighting, is anyone's guess. Importantly, smart things will become the same as clothes or shoes: we will simply use them, convinced they will improve our quality of life. The subtle coercion of self-governing Panopticon has been replaced by a multitude of automated, networked processes that ultimately produce unconscious obedience of objects of surveillance. While we are likely to be aware of some of its aspects, average citizens might never truly grasp the extent or the depth of this surveillance. Smart things will be so imbedded into our daily lives that we will either consider them 'normal', or will not care enough to sacrifice our preferred use of these technologies—and as such, will *comply* with it.

The utilitarianism-inspired idea of "improved" human wellbeing of all underpins actions taken by the automated IoT: we might not want to look after our health, but the things will do it for us. Things will be irresistible, marketed to us as objects that will improve our lives through an abundance of quantifiable data. Ultimately, however, and similar to Bentham's or Foucault's concepts, our behaviour will be modified, and not by force. We will be *obedient*, but not necessarily because we decide to do so. Our doctor will know about issues we have with body weight and is likely to prescribe diet and medications, but not because we finally booked that long overdue annual check-up; it will be our Fitbit or armchair that will blow the whistle. Our lives will be transformed, modified, just as Foucault argued surveillance will do through technologies of the self, but this time not (only) at our own volition. Finally, there is a potential for the underclass – those already marginalised, over-policed, excluded and silenced– to be disproportionately targeted in the future Internet.

There will be limited self-discipline or agency in the future Internet: automated things will take actions on our behalf. In the panopticon surveillance was limited to contained, physical spaces and conducted by humans; this is not going to be the case with the IoT. Indeed, it will be assemblages of things that function together as an entity (Haggerty and Ericson 2000) that will collect, exchange, and analyse data about us. Crime prevention, offending, and punishment will happen in smart homes, cities, and states. Everyone will be a target of surveillance. An individual moving from their home to workplace, and their community, is going to be monitored without a prior finding of criminality or illegality, regardless of citizenship and belonging. Simply existing in a space located in a particular socio-historical context will be the justification for surveillance. The IoT technology does, in fact, risk degenerating into tyranny because it will be everywhere: in bodies, on bodies, and all around bodies, while never actually being controlled or exercised by bodies.

As smart devices communicate and make autonomous actions without human input, there emerge a dynamic wherein *no* member of society can ever comprehensively see how surveillance functions. Surveillance will occur in the air, as devices communicate in strings of code indecipherable to all but the most highly specialised technology specialists. The sheer quantity of information being transmitted is likely to grow too massive even for these select, highly specialised humans. The technology which surveills humanity will also be, in turn, insurveillable *by* humanity. Importantly for criminologists, these processes will clearly have impact on criminal accountability of future offenders. Finally, privacy, as 'the control we have over information about ourselves' (Fried 1968, 475), will be fundamentally distorted. It is for all these reasons that we can no longer ignore the development of the IoT, and its impact on privacy, security, mobility, law and order, and human agency.

CONCLUSION

Historically, having access to and control over technology translated to having power (McGuire 2012); today, supreme technology and access to data mean political, economic and military supremacy. Political power is likely to become more concentrated in technology through the IoT and become less dependent on territory itself (Howard 2015). Similarly, businesses that sell smart things will be even more empowered, through access to data about us they can chose to share, or not, for profit. They may in turn lead to a new era in which IoT will become inevitable and unavoidable, and social scientists would be wise to consider the potential consequences that existing technology can have if and when it becomes more prevalent in the future. Although we did not address the use of the IoT for commercial or state surveillance purposes, this is something that must be addressed soon. As the report from the American Civil Liberties Union noted,

There's simply no way to forecast how these immense powers – disproportionately accumulating in the hands of corporations seeking financial advantage and governments craving ever more control – will be used. Chances are big data and the Internet of things will make it harder for us to control our own lives, as we grow increasingly transparent to powerful corporations and government institutions that are becoming more opaque to us (Crump and Harwood 2014).

While we do not believe in technological determinism that suggests technology alone drives social development (for more see Bunz and Meikle 2018), we agree with Greengard (2015, xv) who noted that it is impossible to know where the technological revolution is going to take us. Whether we agree with Goodman (2016, 39) who suggested that 'we have entrusted the backbone of civilization to machines', there is no doubt the future Internet will shape the way we engage with crime in the 21st century. The aim of this paper was not to engage in fortune-telling, or fear mongering about the apocalyptical future. Our aim was to start the conversation about a range of important topics this emerging technology brings to social sciences, and to begin to untangle some challenges we will be facing fairly soon. The words of George Monbiot (2017) ring so true right now: we need to act to own new political technologies, before they own us.

Undoubtedly, '[t]he crime scene of tomorrow is going to be the IoT' (Kearns 2018). It is for this reason, and others flagged in this paper that criminology of the future must engage with the IoT as a matter of urgency. As social scientists, however, we are not well equipped or trained to understand where the technology is heading, and what this means for a range of social issues and relationships. We need to multidisciplinary team of experts in areas of technology, security, and social sciences. Most importantly, we need to be proactive. As Howard (Howard 2015, xvii) reminds us, the IoT technology might be 'a final chance to purposefully integrate new devices into institutional arrangements we might all like. Active civic engagement with the roll-out of the internet of things is the last best chance for an open society', the one in which we remain active agents with functional (albeit limited) control and agency.

REFERENCES

Adey P. /2012/: Borders, identification and surveillance: New regimes of border control – in: *Routledge Handbook of Surveillance Studies*, edited by Kristie Ball, Kevin Haggerty and David Lyon, London and New York: Routledge.

Alohali B. /2017/: Detection Protocol of Possible Crime Scenes Using Internet of Things (IoT) – in: *Cybersecurity Breaches and Issues Surrounding Online Threat Protection* (ed. M. Moore), Pennsylvania: IGI Global.

Andrejevic M. /2012/: Ubiquitous Surveillance – in: *The Routledge Handbook of Surveillance Studies* (eds. K. Ball, K. Haggerty and D. Lyon), Abingdon Oxon: Routledge.

Ashton M. /2017/: Debugging the Real World: Robust Criminal Prosecution in the Internet of Things, *Arizona Law Review* 59 (3).

Atzori L., Iera A., Morabito G. /2010/: The Internet of Things: A survey, *Computer Networks* 54 (15).

Baig Zubair A., Szewczyk P., Valli C., Rabadia P., Hannay P., Chernyshev M., Johnstone M. et al. /2017/: Future challenges for smart cities: Cyber-security and digital forensics, *Digital Investigation* 22.

Baras K., Brito L. /2018/: Introduction to the Internet of Things – in: *Internet of Things: Challenges, Advances, Applications* (eds. Q. Hassan, A. R. Khan and S. Madani), Bocca Raton, London, New York: CRC Press

Barrett J. /2012/: The Internet of Things – in: *TEDxCIT*, Tedx Talks You Tube.

Bauman Z., Lyon D. /2013/: *Liquid Surveillance*, Cambridge: Polity.

Beer D. /2009/: Power through the algorithm? Participatory web cultures and the technological unconscious, *New Media & Society* 11 (6).

Bonnefon J. F., Shariff A., Rahwan I. /2016/: The social dilemma of autonomous vehicles, *Science* 352 (6293).

Brouwer E. /2008/: *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*, Leiden: Martinus Nijhoff Publishers.

Browne S. /2012/: Race and Surveillance – in *Routledge Handbook of Surveillance Studies*, (eds. K. Ball, K. Haggerty and D. Lyon), London and New York: Routledge.

Bunz M., Meikle G. /2018/: *The Internet of Things*, Cambridge and Medford: Polity.

Burgess M. /2018/: What is the Internet of Things? WIRED explains – in: *Wired*.

CBC Radio: "Alexa, who did it?": What happens when a judge in a murder trial wants data from a smart home speaker, 11 September 2019. https://www.cbc.ca/radio/day6/alexa-who-did-it-what-happens-when-a-judge-in-a-murder-trial-wants-the-data-from-a-smart-home-speaker-1.4916556?fbclid=IwAR0fBKsXEanePMcs-7ejyqhX5--_uXcTsM0IetjnFO9WSaZkzcrnqm00Kxg.

Ceyhan A /2008/: Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics – in: *Surveillance and Society* 5 (2).

Chabinsky S. /2019/: "What Does the Future of Cyber Crime Hold for You?" Security: Solutions for Enabling and Assuring Business, 11 September. https://www.securitymagazine.com/articles/86135-what-does-the-future-of-cyber-crime-hold-for-you.

Claveria K.: "Meet Kevin Ashton, the visionary technologist who named the Internet of Things", https://www.visioncritical.com/blog/kevin-ashton-internet-of-things.

Claypoole T. /2016/: Smarter Devices = More Vulnerability to Government and Criminals, *Computer and Internet Lawyer* 33 (11).

CompTia /2016/: Internet of Things and opportunities – in: CompTia.

Cote-Boucher K. /2008/: The Diffuse Border: Intelligence-Sharing, Control and Confinement along Canada's 'Smart Border', *Surveillance and Society* 5 (2).

Crump C., Harwood M. /2019/: Invasion of the Data Snatchers: Big Data and the Internet of Things Means the Surveillance of Everything, ACLU, 11 September 2019., https://www.aclu.org/blog/speakeasy/invasion-data-snatchers-big-data-and-internet-things-means-surveillance-everything.

Dekker R., Engbersen G. /2014/: How social media transform migrant networks and facilitate migration, *Global Networks* 14 (4).

DeNisco R., Alison /2019/: DDoS attacks increased 91% in 2017 thanks to IoT, Tech Repubic, 11 September 2019., https://www.techrepublic.com/article/ddos-attacks-increased-91-in-2017-thanks-to-iot/.

Dixon H. /2017/: The Wonderful and Scary Internet of Things, *The Judges' Journal* 56 (3).

Ferguson A. G. /2017/: *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, New York: New York University Press.

Foote K. /2019/: A Brief History of the Internet of Things, 13 September 2019., https://www.dataversity.net/brief-history-internet-things/.

Foucault M. /2002/: *Power: essential works of Foucault 1954–1984*, London: Penguin Books.

Fried C. /1968/: Privacy, *Yale Law Journal* 77.

Goodman M. /2016/: *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*, New York: Anchor Books.

Greengard S. /2015/: *The Internet of Things*, Cambridge and London: MIT Press.

Gubbi J., Buyya R., Marusic S., Palaniswami M. /2013/: Internet of Things (IoT): A vision, architectural elements, and future directions, *Future Generation Computer Systems* 29 (7).

Haggerty K., Ericson R. /2000/: The surveillant assemblage, *The British Journal of Sociology* 51 (4).

Howard P. /2015/: *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up*, New Heaven and London: Yale University Press.

Hunter T. /2010/: Police track myki users – in: *The Age* Melbourne: Fairfax.

International Telecommunications Union /2005/: ITU Internet reports: The Internet of Things – in: Geneva: ITU.

Ives S. /2015/: IoT and drones to drive wireless video surveillance, *Security System News* 18 (11).

Kearns I. /2018/: Crime and the pros and cons of the internet of things – in: *The Police Foundation* (ed. The Police Foundation).

Koslowski R. /2019/: New Technologies of Border Control in an Enlarged Europe, Wilson Center, 11 September 2019., https://www.wilsoncenter.org/publication/299-new-technologies-border-control-enlarged-europe.

Lee H. J. /2015/: A Study on Social Issue Solutions Using the "Internet of Things" (Focusing on a Crime Prevention Camera System), *International Journal of Distributed Sensor Networks* 11 (9).

Li S. /2017/: Introduction: Securing the Internet of Things – in: *Securing the Internet of Things* (eds. S. Li and L. D. Xu), New York: Elsevier.

Lianos M. /2003/: Social Control after Foucault, *Surveillance and Society* 1 (3).

Lyon D. /2007/: *Surveillance Studies*, Cambridge: Polity.

Lyon D. /2018/: *The Culture of Surveillance*, Cambridge: Polity.

Lyon D., Haggerty K., Ball K. /2012/: Introducing surveillance studies, – in: *Routledge Handbook of Surveillance Studies* (eds. K. Ball, K. Haggerty and D. Lyon), London and New York: Routledge.

McGuire M. /2012/: *Technology, Crime and Justice: The Question Concerning Technomia*, London and New York: Routledge.

Means C., Robin R., Brunton D. W. /2016/: "You might not know her, but you know her brother": Surveillance Technology, Respectability Policing, and the Murder of Janese Talton Jackson, *Souls* 18 (2–4).

Milivojevic S. /2013/: Borders, technology and mobility: Cyber-fortress Europe and its emerging Southeast frontier, *Australian Journal of Human Rights* 19 (3).

Milivojevic S. /2019a/: *Border Policing and Security Technologies*, London and New York: Routledge.

Milivojevic S. /2019b/: 'Stealing the fire', 2.0 style?: Technology, the pursuit for mobility, social memory and de-securitization of migration, *Theoretical Criminology* 23 (2).

Monbiot G. /2017/: Big data's power is terrifying. That could be good news for democracy – in: *The Guardian*, London: The Guardian.

Muller B. /2010/: *Security, Risk and Biometric State*, New York: Routledge.

Neal A. /2009/: Securitization and risk at the EU border: the origins of FRONTEX, *Journal of Common Market Studies* 47 (2).

Orr D., Sanchez L. /2018/: Alexa, did you get that? Determining the evidentiary value of data stored by the Amazon® Echo, *Digital Investigation* 24.

Popescu G. /2015/: Controlling Mobility: Embodying Borders – in: *Borderities and the Politics of Contemporary Mobile Borders* (eds. A. L. Amilhat Szary and F. Giraut), Baskingstoke and New York: Palgrave.

Roman R., Najera P., Lopez J. /2011/: Securing the Internet of Things, *Computer* 44 (9).

TEDx Talks /2018/: IoT and Machine Learning – Changing the Future Dr Dennis Ong – in: https://www.youtube.com/watch?v=mlE03Fj2T9s.

Thrift N. /2004/: Remembering the Technological Unconscious by Foregrounding Knowledges of Position, *Environment and Planning D: Society and Space* 22 (1).

Thrift N. /2005/: *Knowing Capitalism*, London: Sage.

Tuptuk N., Hailes S. /2019/: Crime in the age of the Internet of Things – in: *Routledge Handbook of Crime Science* (eds. R. Wortley, A. Sidebottom, N. Tilley and G. Laycock), London and New York: Routledge.

Tzezana R. /2016/: Scenarios for crime and terrorist attacks using the internet of things, *European Journal of Futures Research* 4 (1).

Vaughan-Williams N. /2010/: The UK Border Security Continuum: Virtual Biopolitics and the Simulation of the Sovereign Ban, *Environment and Planning D: Society and Space* 28 (6).

Vos M. /2018/: Organizational Implementation and Management Challenges in the Internet of Things – in: *Internet of Things: Challenges, Advances, Applications* (eds. Q. Hassan, A. R. Khan and S. Madani), Boca Ratton, London and New York CRC Press.

Weber V. /2017/: The Synergetic Smart City Framework – From Idea to Reality, *Real Estate Issues*.

Weiser M. /1991/: The Computer for the 21 st Century, *Scientific American* 265 (3).

Williams J. /2016/: Privacy in the Age of the Internet of Things, *Human Rights* 41 (4).

Wood Mark A. /2016/: Antisocial media and algorithmic deviancy amplification: Analysing the id of Facebook’s technological unconscious, *Theoretical Criminology* 21 (2).

Zanella A., Bui N., Castellani A., Vangelista L., Zorzi M. /2014/: Internet of Things for Smart Cities, *IEEE Internet of Things Journal* 1 (1).

Zimmer A. /2017/: Boots on The Ground, Eyes in The Sky. (cover story), *Law Enforcement Technology* 44 (9).

Sanja Milivojević[*]
Univerzitet La Trobe, Melburn, Australija

Elizabeth Marie Radulski[**]
Univerzitet La Trobe, Melburn, Australija

„INTERNET BUDUĆNOSTI“ I KRIMINALITET: KA KRIMINOLOGIJI INTERNETA STVARI

REZIME

Internet stvari (The Internet of Things – IoT) revolucionarno menja način na koji živimo i komuniciramo. Osim toga, njime se transformiše do sada uobičajeni način povezivanja sa „društvom i prirodom“. Internet stvari polazi od toga da predmeti poput kućnih uređaja, automata i (samoupravljajućih) vozila mogu da se povežu sa drugim stvarima i razmenjuju podatke uz pomoć bežične (Bluetooth) mreže ili tehnologije identifikovanja putem radio frekvencije (RFID). „Pametne stvari“ mogu da kontrolišu svoje karakteristike i podešavanja, ali i naša iskustva i donošenje odluka. Autorke se u ovom radu bave novim tehnološkim razvojem Interneta stvari (IoT) i značajem koji to ima za kriminologiju. Cilj rada je usmeren na delimično ukazivanje na nedostatke u literaturi i postavljanjem problema kojima bi u budućnosti trebalo da se bave kriminolozi i drugi naučnici u sferi društvenih nauka. Fokus rada je na fenomenu Interneta stvari (IoT), dok se napredak u vidu tehnologije prepoznavanja lica pominje samo neznatno. Imajući u vidu da razvoj tehnologije, pored svih svojih prednosti utiče i na uspostavljanje odnosa političke, ekonomske i vojne moći, autorke ovim radom postavljaju polaznu osnovu za buduću diskusiju u predviđanju i sprečavanju neželjenih posledica koje „internet budućnosti“ nosi sa sobom.

Ključne reči: Internet stvari, pametne stvari, nadzor, tehnologija, kriminalitet.

[*] Naučni saradnik, S.Milivojevic@latrobe.edu.au.

[**] Istraživač, E.Radulski@latrobe.edu.au.