The 'New' Private Security Industry', the Private Policing of Cyberspace and the Regulatory Questions

Mark Button[1]

Published in *Journal of Contemporary Criminal Justice*

Abstract

This paper explores the growth of the 'new' private security industry and private policing arrangements, policing cyberspace. It argues there has been a significant change in policing which is equivalent to the 'quiet revolution' associated with private policing that Shearing and Stenning observed in the 1970s and 1980s, marking a 'second quiet revolution'. The paper then explores some of the regulatory questions that arise from these changes, which have been largely ignored, to date, by scholars of policing and policy-makers making some clear recommendations for the future focus of them.

Keywords

private security, private policing, regulation, cybercrime and cyberspace

Introduction

Writing in the late 1970s and early 1980s Shearing and Stenning observed the substantial changes to policing taking place at the time in North America, describing the transformation

[1] Institute of Criminal Justice Studies,

University of Portsmouth,

Portsmouth PO1 2HY, UK.

Email: mark.button@port.ac.uk

as a 'quiet revolution.' They noted the substantial growth of private security, linked to the advance of mass private property and the under-funding of the police, with a sector focused upon preventative, rather than curative policing (Stenning and Shearing, 1979a). They also observed how these significant changes had been occurring with little debate or scrutiny from scholars and policy-makers. A significant number of researchers have built upon their body of research noting the continued augmentation of private security and other forms of private policing and the need for special regulatory and governance structures (Stenning and Shearing, 1979b; Jones and Newburn, 1998; Prenzler and Sarre, 1999; Loader and White, Crawford, 2003; Johnston and Shearing, 2003; 2017; Nalla and Gurinskaya, 2017). This paper will argue that partly parallel to these changes a 'second quiet revolution' has been occurring.

Over the last 20 years there have been other significant changes in society fuelling a further transformation in policing. This transformation is linked to the technological revolution which has changed many aspects of the way things are done. These include the new cyber-spaces of play and work, the crimes and transformation of old crimes that technology has enabled and the new structures of policing that have emerged to deal with them. The combination of these changes this paper will argue has fuelled a 'new' private security industry, new corporate security structures and a variety of other forms of new private policing, largely rooted in voluntarism and vigilantism. These changes, like those of the first quiet revolution have occurred with little scholarly debate and consideration of the potential policy implications that might be needed as a result of them.

This paper will begin by outlining the 'second quiet revolution' in policing that this paper argues is taking place. This will include a consideration of some of the background changes to the way people do things and how organisations provide services. It will also illustrate the private sector dominance in policing these new domains and an exploration of some of the

new corporate security roles and functions that have emerged to fill this gap. The paper will argue that a 'new' private security industry has emerged alongside the 'old'. The substantial new opportunities for voluntary policing will also be demonstrated. The paper will then move on to consider the implications for some of these changes and what issues they might raise in terms of potential regulation, using largely the UK. The paper will end with a discussion and conclusion bringing together the arguments made in this paper.

The 'Second Quiet Revolution' in Policing

The background changes

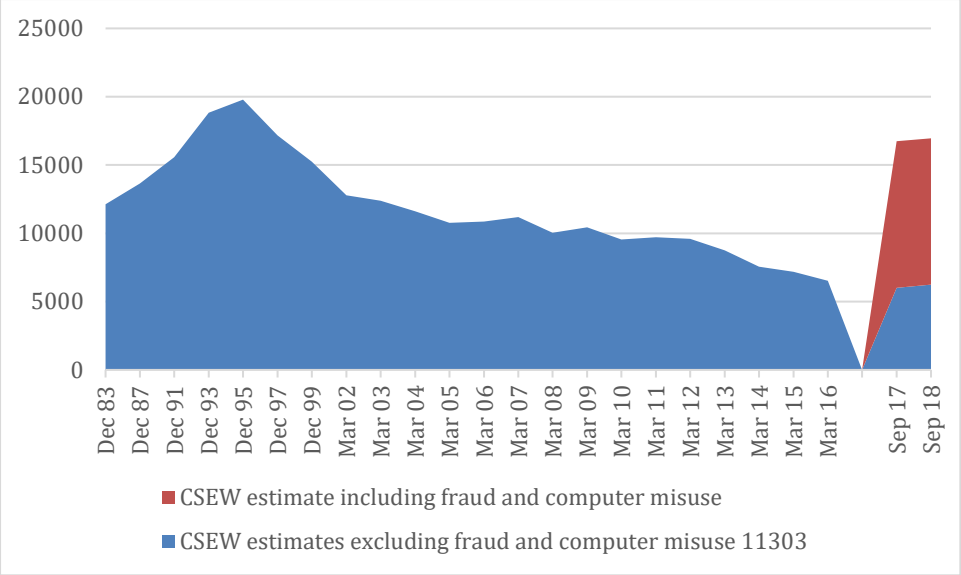
The way that most people shop, play, bank, date to name some is very different to 20 years ago, as is the way many organisations offer services. Central to this transformation has been the growth of the internet and the growing ubiquity of devices offering easy access to it. In Great Britain in 2006 the number of adults who used the internet daily was 36 percent. This had risen to 86 percent in 2018 and in that same year 78 percent of adults used mobile smartphones to access the internet (ONS, 2018a). Such changes have been occurring across the globe. Central to the growing use of the internet has been its use for social networking, shopping, banking and gaming.

Facebook, for instance, has 1.47 billion daily users and 2.23 billion monthly users (Facebook, 2018). The users of Facebook communicate with one another, share insights, photos and videos to name some. It is also used by corporations, NGOs and political groups to campaign and share ideas. On average a user spends 50 minutes of their day on Facebook (New York Times, 2016). In the course of using Facebook and its platforms a wide range of crimes and deviant acts can take place from: sexual abuse, uploading illegal images, bullying, fraud, the use of offensive language to name some. There are also extensive rules of conduct set by Facebook in their terms and conditions that need to be policed.

Consider Xbox Live which has over 57 million active players across the world playing video games (Statista, 2018a). It has been estimated the average child in the UK aged 12-15 plays 12.2 hours of video games per week and an 8-11 year old 10 hours (Statista, 2018b). Players in the course of gaming have multiple opportunities to commit crimes and engage in deviant acts. These range from abusing children, using pirated games, using racially or other offensive language, bullying players to simply cheating at games (Gray, 2012). Amazon, founded in the mid 1990s, has grown to one of the largest companies in the world with global revenues of $177 billion; over 2.4 billion visitors per month to the Amazon website (Statista, 2018c). It typifies how the nature of shopping for most has changed from a visit to a mall or high street, to an online retailer such as Amazon.

Crime has also changed as consequence of where people do things (Wall, 2007a). There has been a long debate over whether the real rates of crime against individuals are falling (Farrell et al 2011). In England and Wales successive data from the Crime Survey for England and Wales (CSEW) showed a decline in crime, particularly volume property crimes such as burglary and theft. The CSEW had shown a peak in crime of around 20 million crimes in 1995 with a gradual decline to around 6 million in 2016. However, with the addition of the new questions in June 2017 the 5.8 million was doubled to 10.7 million when fraud and computer misuse related offences were added, illustrated in figure 1 (ONS, 2018b).

Figure 1. Estimated crime in England and Wales according the Crime Survey England and Wales, year ending December 1981 to year ending September 2018 (thousands)



ONS (2018b)

The end of public police dominance

Debates about the public police and private security have often focused upon the growing size of the latter and the growing networks or nodes of which private security form an important part (Cunningham et al, 1990; Johnston and Shearing, 2003; Dupont, 2006). There can be no denying the substantial growth of the 'old' private security industry in many countries and the eclipsing of the public police in terms of size (see Van Steden and Sarre, 2007; Small Arms Survey, 2011). However, the public police are still at the centre of this policing web (Brodeur, 2010). They are essential to most criminal investigations that go to court, are the most important in the vast majority of policing partnerships, are who most turn to when serious criminal incidents occur and they often have the best knowledge: in terms of intelligence and knowhow. When the highly important act of prevention through patrolling is also considered they are also still seen as the key leaders (Wakefield, 2006).

In the cyberworld they are much more clearly minor (but important) players (Wall, 2007b). Other state bodies outside the police structures have also been created such as the Computer Emergency Response Teams (CERT) of many countries (FIRST, n.d.). There are very few resources dedicated to preventative policing in this sphere by the state police. The mirror of the physical world of preventative patrol is virtually non-existent and their contribution to policing in terms of investigation hardly scratches the service. Take the example of computer misuse offences (hacking, computer viruses, denial of service attacks, ransomware etc) in England and Wales. The CSEW estimated in year ending June 2018 there were 1.1 million offences, of which around 22,000 were recorded by Action Fraud (the state reporting agency for fraud and cybercrime offences) (ONS, 2018b). It must also be noted the CSEW data excludes organisations who are victims of this crime of which there are many thousands too (see, Finnerty et al, 2018). In most years since 2007, however, there have been less than 50 prosecutions each year for these offences by the state (ONS, 2018c). Although some of this attrition can be accounted for by other more serious offences, such as frauds, becoming the offence that is counted (because of the Home Office counting rules), the marginal place of the public police in dealing with this offence is starkly illustrated. Also when an organisation suffers a major cyber incident they are more likely to turn to specialist consultants to deal with it and any subsequent investigations, such as companies such as RSA (see RSA, n.d.).

New corporate security roles and cyber police

Organisations have sought to protect themselves from the growing problem of cybercrime by developing their own cybersecurity structures and purchasing the services from the 'new' private security industry to better protect themselves. In most large organisations there are cybersecurity structures led by what are generally called chief information security officers (CISO) (Karanja, 2016). These run departments of various functions whose role is to

prevent and deal with most cybercrimes against the organisation. Rashid et al. (2017, p. 11) have identified 19 knowledge areas, from 5 broad categories of cybersecurity. The Tech Partnership (2017) estimated there were 58,000 cyber security specialists working in the UK and globally Silensec (2017) cite a report that globally there will be 6 million jobs in cybersecurity (with a gap of 1.5 million).

Beneath the CISO a wide range of new specialist cybersecurity roles have emerged. Some of the most prominent include: security architects, who design cybersecurity systems; security software developers, who develop the software for online security systems; cyber-incident responders, who deal with security incidents; security auditors, who check compliance with systems; and penetration testers (or ethical hackers), who test systems to see if they can hack them. There are many other specialist roles (see Tech Partnership, 2017).

The growing online space that people use has also led to new forms of private policing to deal with the deviance that takes place online. Facebook has created the 'Community Operations Team' who investigate complaints and moderate the content placed on it (The Independent, 2015). Their work is supported by technology via automated tools which facilitate both automatic actions and highlight riskier areas for their attention. Microsoft has built a system of private policing and justice to police this online community called 'Xbox Live Enforcement'. There is an extensive system of private justice where gamers can have their accounts suspended through to outright bans for breaching their terms and conditions. Indeed it was revealed in 2009 over one million users had been banned from Xbox Live for using pirated games (CNET, 2009).

One role, however, which deserves slightly more consideration as it is often neglected in the cybersecurity literature are the moderators. Like security guards police access and behaviours on private space in the physical world, moderators are assuming similar roles

online (Wall, 2007b). They also share some common traits such as low pay, high labour turnover and having to deal with incidents that lead a psychological toll on them (Vanheule et al, 2008; The Business Insider, 2017). The Sunday Times in 2019 reported Facebook had increased the number of moderators contracted to it from 4,500 to 15,000 in the previous 18 months with thousands more used by other tech companies such as YouTube, Google, Twitter etc (Bleach, 2019).

Moderators are employed (or volunteer) to regulate the content which is posted on them. This can include removing posts, images and videos containing illegal, disturbing or inappropriate content through to less policing roles of facilitation (Wright, 2009). Websites use a variety of models including employing their own staff, using specialist companies and sourcing volunteers. The nature of the web means than some moderators will be removing content from a website based in the USA, with users from the UK and moderators from another country, such as the Philippines (New York Times, 2015). There has been very little insight or research into their role. An article in the Guardian highlighted the work of one moderator policing the discussion forum of the television show, 'This Morning', working from the comfort of her own home contracted by a company called Emoderation (now renamed The Social Element). It illustrated she had tools that highlighted certain keywords and could use these to delete inappropriate posts. Content removed could include racist comments, through to unacceptable remarks on a presenters' appearance or those appearing on the programme. Some comments may highlight the need for help such as suicidal feelings, requiring the moderator to report such posts (The Guardian, 2012).

There have been other reports on moderators that have illustrated the very difficult job they face. Many have suffered having to watch videos from warzones of beheadings, gutting of soldiers and child soldiers engaged in killing. Gross acts of cruelty against animals, bestiality and very offensive comments are some of the other content they have to observe.

There has been critique that many are not adequately supported for the content they have to view (Newton, 2019). The consequences of this is that many do not last in the job and there is high labour turnover (The Business Insider, 2017).

The 'new' private security industry

The needs of organisations and individuals to deal with the growing cybersecurity problems has spawned a wide range of new companies to offer such services as well as some traditional security companies and others moving into this area too. Some of the companies that have emerged from the 'old' security industry, offering the full range of services include G4S, which has a Risk Consulting arm that offers these services. There have been companies from other sectors that have moved into this area, such as the traditional consultants. For example PWC offers cyber security services amongst all the other extensive services offered. BAE Systems has also developed such services coming from a largely defence manufacturing background and mainstream IT services providers like IBM. Others are new and like the tech giants have grown rapidly, for example Checkpoint Security Technologies, Symantec, RSA, Kaspersky to name a few. Like the 'old' industry there are large players, catering predominantly for big organisations; down to petite companies focussing upon smaller firms. There are also many companies operating in niche areas like penetration testing, such as companies like Bulletproof (see https://www.bulletproof.co.uk). The supply of moderators has also spawned companies such as The Social Element and (https://thesocialelement.agency/).

This is a new and expanding sector which is very dynamic as technology evolves and threats change. There has been very little research on this sector from a policing perspective, so below in Figure 2 is a list of some of the key segments of the 'new' private security industry.

Figure 2. Activities of the 'new' private security industry

Outsourced cybersecurity solutions (some organisations completely outsource this function to specialist providers)

Design, build and maintenance of security systems (organisations offering services to others to do all or some of these functions).

Threat intelligence, analytics, monitoring and moderating (monitoring for emerging threats and putting in place measures to deal with such risks as they emerge)

Penetration/vulnerability testing (ethically penetrating systems to check for vulnerabilities)

Phishing awareness (raising awareness of phishing scams)

Incident response (responding to attacks and incidents)

Digital investigation services (conducting investigations relating to digital services)

Disaster recovery (dealing with recovery following major attack)

Data compliance and protection (ensuring systems comply with data regulations and are suitably protected)

Data (mining and matching) systems for the prevention of crimes (largely fraud)

Cyber security software products (anti-virus, malware detection etc)

Moderating websites

The size of this sector globally is huge and growing. Market reports (which must be considered carefully as many do not reveal their methodology and are often predictions) show a sector that is beginning to catch up if not eclipse the 'old' private security industry. Marketsandmarkets (2017) estimated the global cyber security market was worth $137.85 billion in 2017, predicted to grow to $231.94 billion in 2022 and Allied Market Research (2016) estimated the same sector would be worth $198 billion by 2022. These can be juxtaposed to reports on the 'old' private security industry which have estimated a global security market worth US$70.02 billion in 2016 (Grand View Research, 2017) to $244 billion estimated by Freedonia (2013).

New openings for voluntary participation in policing

The technological changes have also fuelled new opportunities for people to voluntarily participate in policing (Huey et al, 2012; Chang et al, 2018; Grabosky and Urbas, forthcoming). These opportunities span a wide range of potential activities. The internet

creates opportunities for open source research such that anyone with the time and skills can to engage in desk based investigations. For example in one famous case in the UK a woman using Google images was able to show a man who had been presumed dead in a canoeing accident, whose wife had claimed the life insurance policy, was clearly a fraudster. She did this by finding an estate agent's brochure online from Panama, with a picture of them both after his presumed 'death', and then alerting a national newspaper who informed the police, who had not yet discovered this (The Telegraph, 2007). There are even websites offering those with the time the ability to watch CCTV cameras and report potential problems (see https://www.insecam.org/).

Most controversially, however, it has facilitated a new form of vigilantism. The world of scams and particularly cyber-frauds has also spawned a variety of more organised online vigilante action, 'digilantism' or 'netilantism', which is based upon websites and/or official groups. Some of these are linked to countries, others are more globally based. One prominent website *http://www.419eater.com/* seeks to engage in 'scambaiting', which is simply engaging with scammers to waste their time.

The 419eater website is focused upon 419 scams but encourages action against other types too. The site provides news on scams and tips on how to waste the scammers' time. There are a variety of other websites which can be found that fit this genre such as http://baita.mugu.co.uk/ , http://www.ebolamonkeyman.com/ and http://www.romancescambaiter.com/. Another such as http://www.scamorama.com/ with a focus more on showcasing the variety and comedy value of some attempted scams, rather than baiting them. Youtube also provides a powerful resource for scambaiters too, where many examples of scammers placed on this website by some of the websites already noted as well as individuals. Some 'scambaiters' have not only wasted the time of the scammers

and exposed them, but effectively implemented amusing and shaming punishments on them sometimes involving racism (Byrne, 2013).

These types of vigilante action tend to be facilitated online and are open to the global (English speaking) community, although there maybe a bias to particular countries. Little research has been conducted upon them and the extent and deeper analysis of their contribution and effectiveness is in need of further research. Such vigilante action, however, is rarely officially supported by the state police and is often viewed negatively.

The most contentious form of internet vigilantism that has emerged are the so-called 'paedophile hunters'. Most of these groups pose as children online in chatrooms with the aim of exposing the paedophiles in varying ways. The most prominent groups in the UK have included: 'Letzgo Hunting', 'Paedophile Hunter', 'Daemon Hunter', 'Dark Justice' and 'Hunters 24/7' and it has been estimated there are 75 groups operating in the UK alone, described as a 'cottage industry' (The Telegraph, 2018b). The groups justify their acts on the basis of exposing paedophiles and passing the information they gather to the police (Hill and Wall, 2015). The actions of these groups have clearly helped the police and led to the exposure of real paedophiles who have subsequently been charged and convicted. For instance in 2018 a man was jailed in the UK after engaging in explicit messages with what he believed was a 12 year old girl, amongst others. He had actually been targeted by at least three groups of paedophile hunters (The Telegraph, 2018a). In 2018 it was also revealed that many police forces in England and Wales have used the evidence gathered by such groups with 150 persons charged as a result of their evidence in the previous year (BBC News, 2018b).

However, some groups have live streamed exposures and confrontations have occurred. There has been a concern innocent people could be exposed and the humiliation for some has led to suicide. In 2014 it was claimed the suicide of one man exposed by the paedophile hunter 'Stinson Hunter' was attributed to his public exposure (BBC News, 2014). There has also been concern on the suitability of some for conducting such 'justice', as 'Stinson Hunter' had been jailed in the past for 10 years for arson (Coventry Telegraph, 2014).

Private policing, private security and regulation

Policy responses to the growth of private policing have largely been focused upon statutory regulation of parts of the 'old' private security industry (Loader and White, 2017) with few considering wider regulation and governance (Gurinskaya and Nalla, 2018). The body of research exploring regulation includes: the case for regulation of the 'old' private security industry; assessments of existing regulatory structures in countries; comparisons of different systems and proposals for model systems (Gimenez-Salinas, 2004; Minnaar, 2005; Nalla and Crichlow, 2017; Nalla and Gurinskaya, 2017; De Waard, 1993; Prenzler and Sarre, 1999; Button, 2007; Button and Stiernstedt, 2018; Prenzler and Sarre, 2008; White, 2010; Loader and White, 2017). Most regulatory systems gravitate around some form of licensing/registration of either the companies offering security officers as well as private investigators and/or the individual operatives, predominantly based upon a character standard and minimum standards of training (to a lesser extent). Common themes in the literature are the gaps between the parts of the private security regulated and the broader sector, with some of the most common gaps being:

- The in-house (proprietary) sector (Cunningham et al, 1990; Button, 2007);
- Security managers and corporate teams (Button, 2011);

- Some technical parts of the sector such as intruder alarms (Button, 2008).

Some of these more longstanding gaps are under-debated. Take the example of security managers running the corporate security of large organisations. These functions wield considerable power and direct what many of the regulated roles, such as security officers and private investigators have to do. Weiss's (2017) study of corporate security at Ford in the early twentieth century is a stark illustration of the immense capability of such departments to wield power in and beyond the workplace. Dupont (2006) has also noted the extensive networks delivering security of which security managers form important parts. Some writers have noted the importance of some of these functions (Nalla and Morash, 2002). As Lippert et al, (2013, p 206) note:

> Corporate security is less visible, often wields more authority or power and depends on higher quality technology and training than contract guard security. Yet… corporate security has failed to capture much attention from security and policing scholars (Lippert, et al, 2013, p 206).

Responding to the 'new' private security industry and policing

The rationale for regulating the 'old' private security industry has generally been built upon removing criminals, raising standards and making the sector more accountable (Palmer and Button, 2011, United Nations Office for Drugs and Crime, 2014). There have been very few scandals in the UK of criminals securing roles in the 'new' private security industry and some roles, such as penetration testers/ethical hackers, some organisations actually want to hire 'reformed' past criminal hackers because of their proven skills. Not all 'new' private security roles require such past experience, however, and the lack of scandals does not indicate there isn't a problem or an issue. There is, however, clearly some evidence of past criminals becoming involved in paedophile hunting (see for example Stinson Hunter) and

although such voluntary activities are not part of the private security industry, as a broader form of private policing that is growing and having a real impact of many people's lives, perhaps there is a debate to be had over the regulation of who can engage in such activities? Just because a pilot is flying for herself and not being paid by an airline would not negate the need for regulation of such activities.

To which the next issue of standards is also an important issue. Much of the regulatory control aimed at private security is directed at the standards of operatives and to a lesser extent companies. The major exceptions are the aviation and maritime sectors where there are extensive standards on how security should be undertaken (Button, 2008). The low pay, long hours, limited training and not surprising poor quality of many security officers has culminated in the case for minimum standards in these areas to address them been introduced in many jurisdictions (United Nations Office for Drugs and Crime, 2014).

There is, however, a limited base of evidence of poor standards of the growing number of providers and staff operating in the 'new' private security sector. There would seem to be some evidence of low standards in terms of training, support and pay among moderators (Bleach, 2019; Newton, 2019). The regular cyber and data breaches of corporates losing the data of their staff and customers may also indicate not all is well, as poor standards might be contributing to such breaches (See Finnerty et al, 2018). Much of the 'new' private security industry is dominated by higher barriers to entry and there is less of a 'grudge cost' mentality dominating decisions in comparison to some of the 'old' private security industry (Goold et al, 2010). Indeed such are the barriers to entry in terms of skills there is much evidence of a substantial skills gap (Silensec, 2017). The economics of much of the 'new' private security industry are different, although some sub-segments such as moderators and their global supply, may indicate something different. This does not mean there are no

problems in the 'new' sector. It just means we need to investigate this more to determine if there are issues which may require policy solutions.

The roles and accountability aspect to the regulation debate has not been one of the most prominent arguments in the regulation discourse, but it is one of the most important, if not the most important. Perhaps the exception to this are private investigators and door supervisors, which have attracted more interest in this aspect of the debate (Button, 1998; Lister et al, 2001). Primarily this is because of the breaches of privacy and excessive force associated with these occupations. Excessive force is not an issue to be concerned with in the 'new' sector, but privacy and a wide range of others are. The 'new' private security industry activities and the voluntary contributions to the broader range of private policing activities raise a variety of issues that illustrate the need to consider greater controls to ensure accountability for some of the decisions that are taken by such operatives and the data they have access to.

Moderators in their role policing what goes online may have access to illegal pornography, sensitive information and images that should not be in the public domain to name some. Alongside these, even more powerful roles such as CISOs, security architects and penetration testers to name some may also warrant the need for licensing as many other 'old' security roles already are.

There has been huge concern raised by companies operating big data related services in the political sphere, such as the activities of some such companies in the election of Donald Trump and the UK Brexit referendum (Christl, 2017; House of Commons Digital, Culture, Media and Sports Committee, 2018). There is a large industry offering data related services to reduce the risk of cyber related financial crime to organisations, among many other areas (Button et al, 2016; Christl, 2017). The designation of a person as higher risk in a financial

decision can have implications for whether a person secures a loan, mortgage or even keeps a bank account and many of these companies operating in this area are making judgements about persons on an industrial scale with little public scrutiny of their processes or effectiveness.

For example in one quarter, the company Threatmetrix assessed over 8.3 billion transactions for their legitimacy based upon hundreds of attributes. They found over 151 million attacks and 1.6 billion Bot attacks (Threatmetrix, 2019). Many of the prevented attacks will involve the effective designation of the customer as a fraudster, without reference to formal criminal justice structures. There are many other data companies offering such services around the world designating individuals and data associated with them as potential fraudsters (see, Christl, 2017). Some private entities also have access to cyber-tools as potent as the state's which are used to engage in corporate espionage and other acts of damage against competitors (see Maurer, 2018; and Zilber, 2018).

Designation as a fraudster based upon false or inadequate decisions might be bad, but pales in significance to been outed as a paedophile. The activities of the online hunters – despite the condemnation of the police have been used extensively. The instant justice and shaming by some groups have led to serious harm and even suicides by some they have exposed. As already noted there is evidence of unsuitable persons operating in such groups, with some with convictions for violence or criminal motives. For example, the Times newspaper recently exposed gangs of criminals using such groups as means to rob and blackmail paedophiles (Hamilton, 2019). The primary motives of some 'hunters' might seem more directed towards feeding their desire for violence against one of the most despised groups in society, rather than dealing with the problem. The implications for someone wrongly publicly outed as a paedophile could be huge. There clearly is a role for some activities in this area, but the restriction and regulation of this would seem to be one of the more

obvious area of intervention. Some scambaiters have been implicated as engaging in racist practices (Byrne, 2013). These all suggest the need for more controls to be investigated for these activities.

Discussion and Conclusion

This paper has illustrated the significant changes in private policing that have occurred in response to the major technological transformations that have transpired over the last 20 years. The paper argues these constitute a 'second quiet revolution' with the emergence of a wide variety of new forms of private policing, some of which constitute a 'new' private security that has emerged, along with other private policing, largely parallel to the 'old' private security industry and private policing. Like the first quiet revolution these changes have occurred with little scrutiny and public debate.

The regulation of anything related to the internet and involving cross-border activities poses significant challenges (Johnson and Post, 1995; Laidlaw, 2015). This is not a reason to decline to consider the issue. There is already evidence that some of the activities associated with the 'second quiet revolution' in private policing deserve to be considered to be regulated. There is in most countries extensive regulation of data processing, but this does not cover all of the activities of the 'new' private security industry and rarely creates deep licensing systems for personnel. There is clearly a regulatory gap when the 'new' private security industry is considered, but much more research needs to be undertaken to fill that gap with ideas. A priority for policy-makers must be more depth and focused consideration of these new activities to assess if current regulatory and governance mechanisms work and whether new structures should be created to deal with them. As Stenning and Shearing (1979b, p. 263) have argued in relation to the 'old' private security industry:

> If private security personnel are in reality no different from ordinary citizens, a law which treats them alike seems most appropriate. But if in reality they are not, and the law still treats them as they are, it becomes inappropriate…

This paper has shown there are many new roles and services that have emerged that are many steps away from that of what an ordinary citizen or firm engages in. It is time for researchers to start better understanding these new forms of private policing. And where the evidence supports it, develop new policy ideas for the better regulation of these growing and increasingly important activities. The priorities for researchers and policy-makers to fill this gap should be:

- To map the activities and extent of the new private security and private policing;
- To identify areas of concern which require regulatory and other governance responses, with particular reference to new roles that may require licensing;
- To explore the adequacy of existing regulatory and governance structures to undertake such functions where necessary; and
- To identify new models of regulation and governance where existing structures are not deemed appropriate.

References

Allied Market Research (2016). Cyber Security Market by Solutions. Retrieved from https://www.alliedmarketresearch.com/cyber-security-market

BBC News (2014). Man killed himself after Stinson Hunter 'paedophile trap'. Retrieved from http://www.bbc.co.uk/news/uk-england-northamptonshire-26550987

Bleach, S. (2019). It's a dirty, damaging job trying to clean up the internet. *The Sunday Times*, 3 March, 2019, p 25.

Brodeur, J-P. (2010). *The Policing Web*. Oxford: Oxford University Press.

The Business Insider (2017). Content moderators for tech giants like Facebook and YouTube reveal what it's like to sift through some of the most disturbing material on the internet. Retrieved from https://www.businessinsider.com/content-moderators-facebook-youtube-microsoft-whats-it-like-2017-12?r=US&IR=T

Button, M. (2019). *Private Policing*. 2nd Edition. Abingdon: Routledge.

Button, M. (2011). The Private Security Industry Act 2001 and the Security Management Gap in the United Kingdom. *Security Journal*, 24, 118-132.

Button, M. (2008). *Doing Security*. Basingstoke: Palgrave.

Button, M. (2007). Assessing the Regulation of Private Security Across Europe. *European Journal of Criminology*, 4, 109-128.

Button, M. (1998). 'Beyond the Public Gaze' The Exclusion of Private Investigators from the British Debate Over Regulating Private Security. *International Journal of the Sociology of Law*, 26, 1-16.

Button, M., Shepherd, D. and Blackbourn, D. (2016). *The Fraud 'Justice Systems': A Scoping Study on the Civil, Regulatory and Private Paths to 'Justice' for Fraudsters.* Portsmouth: Centre for Counter Fraud Studies.

Button, M. and Stiernstedt, P. (2018). Comparing Private Security Regulation in the European Union. *Policing and Society*, 28, 398-414

Byrne, D. N. (2013). 419 digilantes and the frontier of radical justice online. *Radical History Review*, 117, 70-82.

Coventry Telegraph (2014). Online crime fighter Stinson Hunter comes clean to Telegraph about chequered past https://www.coventrytelegraph.net/news/coventry-news/online-crime-fighter-stinson-hunter-6800023

Chang, L. Y., Zhong, L. Y., and Grabosky, P. N. (2018). Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime. *Regulation and Governance*, *12*(1), 101-114.

Christl, W. (2017). *Corporate Surveillance in Everyday Life*. Vienna: Cracked Labs

Crawford, A. (2003). The Pattern of Policing in the UK: Policing Beyond the Police. In T. Newburn (Ed) *The Handbook of Policing*. Cullompton (UK): Willan.

Cunningham, W., C., Strauchs, J., J. and Van Meter, C., W. (1990). *Private Security Trends 1970-2000.* Hallcrest Report II. Stoneham (US): Butterworth-Heinemann.

De Waard, J. (1993). The Private Security Sector in Fifteen European Countries: Size, Rules and Legislation. *Security Journal*, 4, 58-62.

Dupont, B. (2006). Delivering security through networks: Surveying the relational landscape of security managers in an urban setting. *Crime, Law and Social Change*, *45*, 165-184.

Farrell, G., Tseloni, A., Mailley, J., and Tilley, N. (2011.) The Crime Drop and the Security Hypothesis. *Journal of Research in Crime and Delinquency,* 48, 147-175.

Finnerty, K., Motha, H., Navin, J., White, J., Button, M. and Wang, V. (2018). Cyber Breaches Survey 2018. London: IPSOS Mori

FIRST (n.d.) About FIRST. Retrieved from https://www.first.org/about/

Freedonia (2013). World Security Services. Retrieved from https://www.freedoniagroup.com/industry-study/world-security-services-2978.htm

Gimenez-Salinas, A. (2004). New Approaches Regarding Private/Public Security. *Policing and Society*, 14, 158–174.

Goold, B., Loader, I., and Thumala, A. (2010). Consuming security? Tools for a sociology of security consumption. *Theoretical Criminology*, *14*, 3-30.

Grabosky, P. and Urbas, G. (Forthcoming) "Online undercover investigations and the role of private third parties" *International Journal of Cyber Criminology*

Grand View Research (2017). Security Market Size Worth $167.12 Billion By 2025 | CAGR: 10.2%. Retrieved from https://www.grandviewresearch.com/press-release/global-security-market

The Guardian (2012). A working life: the website moderator. Retrieved from: https://www.theguardian.com/money/2012/feb/03/a-working-life-website-moderator

Gurinskaya, A., and Nalla, M. K. (2018). The expanding boundaries of crime control: Governing security through regulation. *The Annals of the American Academy of Political and Social Science*, *679*(1), 36-54.

Hamilton, F. (2019). Criminals 'pose as vigilante groups to blackmail and rob paedophiles. *The Times*, 25 January, 2019 p 21.

Hill, G. and Wall, D., S. (2015). How online vigilantes make paedophile policing more difficult. *The Conversation*, June, 3, 2015.

House of Commons Digital, Culture, Media and Sports Committee (2018). Disinformation and "Fake News": Interim Report. Retrieved from https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf

Huey, L., Nhan, J., and Broll, R. (2013). 'Uppity civilians' and 'cyber-vigilantes': The role of the general public in policing cyber-crime. *Criminology and Criminal Justice*, *13*, 81-97.

Johnson, D. R., & Post, D. (1995). Law and Borders--The Rise of Law in Cyberspace. *Stan. L. Rev.*, *48*, 1367.

Johnston, L. and Shearing, C., D. (2003) *Governing Security*. London: Routledge.

Jones, T. and Newburn, T. (1998). *Private Security and Public Policing*. Oxford: Clarendon Press.

Laidlaw, E. B. (2015). *Regulating speech in cyberspace: gatekeepers, human rights and corporate responsibility*. Cambridge University Press.

Lippert, R. K., Walby, K., and Steckle, R. (2013). Multiplicities of Corporate Security: Identifying Emerging Types, Trends and Issues. *Security Journal*, 26, 206-221.

Lister, S., Hadfield, P., Hobbs, D., Winlow, S. (2001). Accounting for Bouncers: Occupational Licensing as a Mechanism for Regulation. *Criminal Justice,* 1, 363-384.

Loader, I., and White, A. (2017). How can we better align private security with the public interest? Towards a civilizing model of regulation. *Regulation & Governance*, *11*, 166-184.

Marketsandmarkets (2017). Cybersecurity Market worth 231.94 Billion USD by 2022. Retrieved from https://www.marketsandmarkets.com/PressReleases/cyber-security.asp

Maurer, T. (2018). Cyber Mercenaries. Cambridge: Cambridge University Press.

Minnaar, A. (2005). Private-public partnerships: Private security, crime prevention and policing in South Africa. *Acta Criminologica: Southern African Journal of Criminology*, 18(1), 85-114.

Nalla, M. K., and Crichlow, V. J. (2017). Have the Standards for Private Security Guards Become More Stringent in The Post 9/11 Era? An Assessment of Security Guard Regulations in the US from 1982 to 2010. *Security Journal*, *30*, 523-537.

Nalla, M. K., and Gurinskaya, A. (2017). Common Past-Different Paths: Exploring State Regulation of Private Security Industry in Eastern Europe and post-Soviet

republics. *International Journal of Comparative and Applied Criminal Justice*, *41*(4), 305-321.

Nalla, M. and Morash, M. (2002). Assessing the Scope of Corporate Security: Common Practices and Relationships with other Business Functions. *Security Journal*, 15, 7-19.

Newton, C. (2019). The Trauma Floor. The Secret Life of Facebook Moderators in America. Retrieved from https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona

New York Times (2015). When the Internet's 'Moderators' Are Anything But. Retrieved from https://www.nytimes.com/2015/07/26/magazine/when-the-internets-moderators-are-anything-but.html

ONS (2018a). Internet access – households and individuals, Great Britain: 2018. Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2018#daily-internet-use-has-more-than-doubled-since-2006

ONS (2018b). Crime in England and Wales: Year Ending September 2018. Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2018

ONS (2018c) Outcome by Offences Tool. Retrieved from https://www.gov.uk/government/statistics/criminal-justice-system-statistics-quarterly-december-2017

Palmer, R. and Button, M. (2011). *Civilian Private Security Services: Their Role, Oversight and Contribution to Crime Prevention And Community Safety*. Expert Group on Civilian Private Security Services, Oct 12-14. Vienna: United Nations Office on Drugs and Crime.

Prenzler, T., and Sarre, R. (2008). Developing a Risk Profile and Model Regulatory System for the Security Industry. *Security Journal*, 21, 264-277.

Prenzler, T. and Sarre, R. (1999). A Survey of Security Legislation and Regulatory Strategies in Australia. *Security Journal*, 12, 7-17.

RSA (n.d.). Incident Response Services. Retrieved from https://www.rsa.com/en-us/services/rsa-risk-and-cybersecurity-practice/rsa-incident-response-practice

Silensec (2017). *Addressing the Cyber Security Skills Gap*. Silensec.

Small Arms Survey (2011). Small Arms Survey 2011. Retrieved from http://www.smallarmssurvey.org/fileadmin/docs/A-Yearbook/2011/en/Small-Arms-Survey-2011-Prelims-Intro-EN.pdf

Statista (2018). Amazon. Retrieved from https://www.statista.com/study/10137/amazoncom-statista-dossier/

Stenning, P. C. and Shearing, C., D. (1979a). The Quiet Revolution: The Nature, Developments and General Legal Implications of Private Security in Canada. *Criminal Law Quarterly*, 22, 220-248.

Stenning, P. C. and Shearing, C., D. (1979) Private Security and Private Justice. British Journal of Law and Society, 6: 261-271.

Tech Partnership (2017). Factsheet: Cyber Security Specialists in the UK. Retrieved from https://www.thetechpartnership.com/globalassets/pdfs/research-2017/factsheet_cybersecurityspecialists_feb17.pdf

The Telegraph (2018b). Paedophile hunters like a 'cottage industry', court hears as three groups target same suspect. Retrieved from http://www.telegraph.co.uk/news/2018/01/09/paedophile-hunters-now-operating-like-cottage-industry-court/

The Telegraph (2007). How Google helped solve canoeist mystery. Retrieved from https://www.telegraph.co.uk/news/uknews/1571690/How-Google-helped-solve-canoeist-mystery.html

Threatmetrix (2019). Q2 2018 Cybercrime Report. Retrieved from https://www.threatmetrix.com/digital-identity-insight/cybercrime-report/q2-2018-cybercrime-report/

United Nations Office for Drugs and Crime (2014). *State Regulation Concerning Civilian Private Security Services and their Contribution to Crime Prevention and Community Safety*. Vienna: UNODC.

Vanheule, S., Declercq, F., Meganck, R., & Desmet, M. (2008). Burnout, critical incidents and social support in security guards. *Stress and Health: Journal of the International Society for the Investigation of Stress*, *24*, 137-141.

Van Steden, R. and Sarre, R. (2007). The Growth of Private Security: Trends in the European Union. *Security Journal*, 20, 222-235.

Wakefield, A. (2006). *The Value of Foot Patrol: A Review of Research*. London: Police Foundation.

Wall, D. (2007a). *Cybercrime: The transformation of crime in the information age*. Polity.

Wall, D. S. (2007b). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research*, *8*(2), 183-205.

Weiss, R., P. (2014). Corporate Security at Ford Motor Company: From the Great War to the Cold War. In, K. Walby and R. Lippert (Eds) *Corporate Security in the Twentyfirst Century*. Basingstoke: Palgrave.

White, A. (2010). *The Politics of Private Security: Regulation, Reform and Re-legitimation*. Basingstoke: Palgrave.

Wright, S. (2009). The role of the moderator: Problems and possibilities for government-run online discussion forums. *Online deliberation: Design, research, and practice*, 233-242.

Zilber, N. (2018) *The Rise of the Cyber Mercenaries*. Retrieved from https://foreignpolicy.com/2018/08/31/the-rise-of-the-cyber-mercenaries-israel-nso/

Author Biography

Mark Button is a Professor of Criminology at the Institute of Criminal Justice Studies, University of Portsmouth and Director of the Centre for Counter Fraud Studies. His interests include white collar crime, cyber-crime, private policing and the regulation of private security. He has helped the UNODC develop standards for the regulation of private security.