Scan and Rob! Convenience Shopping, Crime Opportunity and Corporate Social Responsibility in a Mobile World

Professor Adrian Beck and Dr Matt Hopkins[1]

Abstract

One of the unintended consequences of technological innovation is that it can promote opportunities for crime. These opportunities not only have the potential to generate significant financial costs but can also have wider social consequences. This paper considers the development of technologies designed to enable customer convenience in the retail sector and focuses specifically on the potential of mobile scan and payment systems (MSP) to generate opportunities for crime. Through interviews with retailers, store observations and analysis of shrinkage data both the potential opportunities for crime and impact on loss are identified. The wider potential criminogenic impact of such innovation is also considered and whether large businesses have a social and moral responsibility to mitigate for any negative effects of such developments.

Introduction

This paper explores the potential criminogenic impact of mobile scan and payment (MSP) systems within retail environments. Within most developed countries the retail sector accounts for 'between 16 and 22% of GDP' (Bamfield, 2012: 4) and in the UK alone, retail comprises around 10% of the total business population employing 20% of the workforce (BIS, 2014). The sector is also known to generate high rates of theft, for example, in the UK in 2012, there were an estimated 4.1 million shoplifting incidents (by way of comparison there were an estimated 8.9 million incidents of crime recorded against *all households* over the same period) (Home Office, 2013) and in the USA, 75% of inventory loss is estimated to be due to shoplifting (Cardone and Hayes, 2012). However, the sector is also extremely competitive and businesses constantly aim to develop new ways to promote customer convenience and loyalty to their brand. The competitive nature of the market can be no better illustrated than in current developments in relation to mobile scan and pay systems[2]. These are part of on-going developments that have seen increased customer autonomy and self-service at the expense of formalised staff/customer interactions. For example, the move from counter-service to self-selection at the beginning of the 20th century allowed customers to find, select and pay for items of choice. In the 1990s self-scan technologies emerged that allowed customers to not only self-select items but also expected them to take responsibility for the scanning and payment components of their shopping trip as well. More recent developments have seen a move towards mobile commerce and online shopping, allowing customers to search and pay for products online via their own computer, tablet or mobile device and either have products delivered to an agreed address or collect them from a physical store at an agreed time. The move to mobile commerce is very much connected with the emerging development of offering the customer the opportunity to use their own mobile device 'in-store' to not only scan items they wish to purchase, but also pay for them using the same technology, through the use of downloadable Smartphone Apps, anywhere in the store.

It has been argued that the evolution of the retail landscape has had two main consequences (Curtis (1971; Beck, 2009). First, it has provided economic benefits to retailers – changes in store design have generally meant fewer staff need to be employed and the maximisation in the display of goods has increased sales and profits. However, the more open and less controlled retail style has, by reducing perceptions of risk for all customers, made it easier to steal products and encouraged would-be offenders to take advantage of the new opportunities for deviancy presented to them (Beck, 2009). While the move to allow customers to self-scan at fixed checkout points (SCO) was considered to be a considerable leap of faith in the integrity and honesty of the shopper (Beck, 2011), allowing customers to scan and pay using their own mobile phone, potentially anywhere in the store, arguably takes this leap of faith to a new level. Indeed, higher rates of theft have been recorded in supermarkets with SCO systems (Home Office, 2015), though work on the criminogenic risks generated by MSP is limited. Two pioneering studies of MSP in Australia (Taylor, 2013) and the USA (Aloysius and Venkatesh, 2013) hypothesised that (as with SCO) incidents of: purposeful non scanning of items; customers walking through exit barriers with goods scanned but not paid for (walking); employee-aided loss; and customers collecting receipts to steal or return goods later, were all likely to increase. In addition, these studies identified that non-malicious losses might be generated through 'honest' mistakes where items did not scan because of a technical glitch or simple human error.

These previous studies are useful as they begin to highlight some of the potential malicious and non-malicious risks associated with MSP. This paper aims to build upon their findings in three principal ways. First, through fieldwork with retailers based in four countries (UK, USA, Holland and Belgium) expand the geographical coverage of the previous work. Second, develop an appropriate theoretical framework to explore how and where in the MSP shopping journey criminogenic opportunities are generated. Third, through analysis of data from 12 million mobile scanning shopping journeys, for the first time, quantify the potential loss generated by MSP. Finally, the paper discusses some of the wider potential social implications of the findings. In particular, considering if the implementation of such technology needs to be better balanced with crime prevention concerns and whether the findings raise questions about the social and moral responsibilities of retailers to the communities they purport to serve.

Theoretical Framework

It has been theorized that much offending is a result of offenders taking advantage of opportunities for crime that arise in their everyday routine activities (Clarke, 1980, 1992, 1997; Clarke and Homel, 1997). Opportunity theory is based on the notion that offenders make rational choice decisions to offend and when exposed to a potential crime opportunity, choice structuring decisions around the effort required to commit to crime, the risks of getting caught and potential rewards on offer are made (Cornish and Clarke, 1986). It has also been noted that, within particular contexts there can be particular provocations for crime and some contexts provide offenders with ready-made excuses for their behaviour (see Smith and Clarke, 2010). Indeed, much criminological research has already shown that the propensity to steal is a function of effort, anticipated rewards, perceived likelihood of being caught and the perceived severity of any likely subsequent punishment (Cornish and Clarke, 1986). Crucially, in relation to shoplifting, Cardone and Hayes (2011) illustrate how offenders' decision-making is closely related to the ease of access to goods, ease of escape and

perception of the risk amplified by the presence of CCTV and the number of 'place managers' such as employees in store or security personnel.

However, the move from counter shopping to customer self-service (and latterly MSP) has complicated matters in relation to proving the intent, motivation and rationale of the non-paying customer. While the move to MSP *might* offer greater opportunities for theft, it also offers greater opportunities for customers to make not only genuine errors in an increasingly complicated and technologically driven process, but also generate 'excuses' for non-payment through the use of neutralising techniques (Sykes and Matza, 1957; Cromwell and Turman 2003). Indeed, Beck (2011: 211) notes that in relation to SCOs, proving guilt on the part of the offender is difficult as they have a series of ready-made excuses – 'I thought I had scanned that item' or 'I thought my credit card had been accepted'. Such techniques of neutralisation might not only be developed by those not intending to pay for goods, but might also be used in circumstances where customers can feel justified in taking items if SCO systems do not operate smoothly – thus enabling customers to construct what they perceive as legitimate excuses for theft (Beck, 2011). Aloysius and Venkatesh, (2013: 36) note this might not only lead to discrepancies over what losses are malicious and non-malicious, but also 'erroneous customer accusations' – can stores realistically seek criminal prosecution when a non-scanned item is found in a customer's bag when the retailer expects them to use SCO technologies?

This simplistic framework clearly offers a useful structure to aid our understanding of the proximal factors that might generate crime. By considering the following questions, it also can also be utilised to help us understand how MSP could generate crime and loss in the retail environment:

1. How does MSP impact on the effort required for theft?
2. How can it increase rewards for offenders?
3. How is risk reduced in the MSP environment?
4. How does it provide excuses for offending?
5. How does it increase provocations for crime?

Methodology

The data were collected as part of an Economic and Social Research Council[3] funded project that involved working with four major UK retailers, two USA retailers, one from Belgium and one from The Netherlands[4]. In depth semi-structured interviews were conducted with staff involved in the development and implementation of MSP systems, visits were made to stores where systems were in use and analysis conducted of shrinkage data from a large retailer.

Table 1 presents a list of the participants interviewed in the study and their respective roles. Two interviews were also completed with two developers/security experts. The key personnel interviewed were involved in developing or piloting MSP systems or were loss prevention personnel responsible for identifying risk and monitoring shrinkage across the company.

Table 1: Interview Groups in Study

Retailers	Respondents Within Retailers
UK Retailer 1: pilot rolled out across several stores.	Head of Profit Protection; Profit Protection Manager; National Operations Manager; Loss Prevention Project Manager; Digital Technology Programme Team; Omni-Channel Coordinator
UK Retailer 2: trial phase in one store.	Director of Process and Asset Protection; Retail Innovations Team; Project Manager for MSP trial; Investigations Team; Operations Manager; Head of Security Resource; App Developer (in-house).
UK Retailer 3: one aborted trial.	Project Manager Loss Prevention; Operations Manager; Head of Marketing Team
UK Retailer 4: plans for MSP in development stage but no trial underway.	Head of Loss Prevention
USA 1: MSP rolled out across hundreds of stores and continuing to be used.	Director of Shrink; Asset Protection Team; Security Investigations
USA 2: MSP trialled across several stores but then withdrawn.	Director of Asset Protection; Innovations Team; Self-service Team
The Netherlands: MSP rolled out across numerous stores and currently in use.	Head of Corporate Security; Store Development and Design Team
Belgium: MSP rolled out across numerous stores and currently in use.	Director of Health, Safety and Head of Risk Management
App developers/security provider	Product Manager, product protection company; Technology Consultant

The interviews with retailers, App developers and security providers covered a number of themes including; current roll out of MSP in the company; views on the development of mobile scan and pay across retailing; the risk of loss in the retail environment; and crime prevention approaches to manage MSP.

All interviews were recorded and analysed using a themed analytical approach (Turley et al, 2011). In addition to these interviews, visits were made to stores where versions of MSP systems were in operation. In all companies (accept one) visits were overt in that they were in made with staff from the organisation. However, several covert visits were also made to a UK store where an MSP system was in operation. The aim of these store visits was to use the MSP systems in order to identify problems that might be experienced by users, potential opportunities for theft and opportunities for crime prevention. Extensive fieldwork notes were taken after these store visits and then analysed.

Shrinkage[5] data were also collected from a ❖multibillion[6] turnover retailer that offered customers the opportunity to mobile shop via a scan gun provided by the retailer as well as through a bespoke App to undertake shopping using a consumers' smart phone. A measurement of shrinkage was calculated from over one million audits of 12 million shopping trips across hundreds of trial stores over a one year period[7]. These audits were conducted by a member of store staff at the final payment point of the shopping trip by

physically checking which items had been scanned and which had not. This allowed a dataset to be constructed that included:

- The number of items purchased
- The value of the items purchased
- The average number of items audited
- The value of items found not to have been scanned

Although these data allowed for comparison to be made between losses that were generated through self-scan systems against those generated through more conventional forms of shopping, there were two major limitations. First, the member of staff undertaking the audit was tasked to only check a relatively small number of items – on average 6 – out of a typical basket size of 30 items. If one or more unscanned items were found amongst the 6 items selected for audit, the remaining items would not be checked for accuracy. So, in effect, the 6 items were used as a 'sample' of the total contents of the shopping basket. Of course, while retail staff undertaking an audit were told to try and select the 6 items randomly from a bag, basket or trolley, inevitably items from the top are much more likely to be selected, which could allow malicious thieves to 'bury' non-scanned items at the bottom to avoid selection and hence reduce the number of non-scanned items recorded. Also, if one or more non-scanned items were found amongst the 6 items chosen for audit then this is highly likely to suggest that other non-scanned items are present in the bag, basket or trolley, but these would not be found. This will inevitably reduce the overall number and value of items found to have not been scanned via these audits.

Second, the data provided by the retailer did not separate audit data relating to shopping trips using scan guns provided by the retailer and those shopping trips which used a customers' mobile phone – the data was only available in aggregate form. While this limits our ability to talk specifically about the risks associated with MSP devices, the processes employed by the retailer were almost identical in terms of the way in which payment and audit were carried out.

Findings: The Opportunity for Crime and Impact upon Shrinkage

Respondents suggested that moving towards the 'ultimate in self-service' (Interview 10) might not only send out the wrong 'physical cues' to potential offenders (Cardone and Hayes, 2012), but those shoppers who might not necessarily plan to steal could take the opportunity to exploit weaknesses in systems if possible. Similar to research conducted on SCO (Beck, 2011), it was thought retailers might actually encourage shoppers who fully intend to scan and pay for products to engage in criminal activity. As one respondent said: 'what you might see is people who traditionally don't intend to steal but realise… when I buy 20, I can get five for free… maybe I'll continue to do that' (Interview 4). Primarily, it was identified that MSP might generate crime or loss in four ways: theft through malicious non-scanning of goods; non-malicious loss through non-scan/scanning errors; physical and verbal abuse against staff generated via audit checks; and transaction frauds or fraudulent use of payment wallets. Using the language of opportunity theory the respondents identified several crime generating properties of MSP**.**

Ease of Effort/Access to Products*:* Whereas traditional counter shopping limited access to goods, the rationale for customer self-service, SCO and MSP is that customers have open

access to products and within the SCO and MSP model, the customer takes responsibility for payment with limited or no staff involvement at all. As one respondent commented 'it's the ultimate in trust' (Interview 6) or as another said 'they call it 'Scan and Rob'' (Interview 8). Thus, MSP potentially promotes ease of effort for theft by removing any human contact throughout the shopping process and removing (possibly most importantly) human contact at the final payment stage of the shopping journey. As succinctly put by one interviewee; 'you scan it and you walk it… you've got no controls in place' (Interview 5). Of course the self-service culture has meant retailers have implemented a range of product protection devices – hard tags, soft tags, spider tags, safer boxes/cases – to promote risk throughout the shopping journey as well as employing visible security cues such as guards, CCTV and attentive store staff. However, the unintended effect of MSP might be a sort of 'displacement effect… where due to the ease… we [might] see a greater number of non-protected items going missing' (Interview 4). Another respondent revealed that in mystery shopping trials of one MSP system, even where production protection alarms were activated there was little response from retail staff: 'he didn't pay for half… set the alarms off, they ignored him, walked back in, set the alarms off, they ignored him' (Interview 5). Indeed, in one store trial conducted for this research, it was identified that when a validation check was not conducted at the point of payment it would have been easy to steal non-protected items. In another store visit the main reason for the ease at which goods could have been stolen was because validation staff were more concerned with processing customers quickly through the payment process (as staff were getting frustrated over the continual technical glitches with the payment wallet option) rather than conducting re-scan/audit checks.

Previous research has also suggested that MSP might promote ease of effort for those wanting to engage in transaction frauds (Bamfield, 2012) – using false barcodes, bogus receipts, card fraud and colluding with staff ['sweethearting']. Our respondents seemed less concerned about fraudulent activity than non-scanning. However, three did highlight concerns around fraudulent activities. One noted that a concern in the business was around the production of self-scan labels that might be stuck on products. While any shopper can label switch, it might be easier for MSP customers to do so without being detected as it might not look so unusual for them to be carefully looking at product barcodes in the aisle – which might offer an opportunity to change labels. Other concerns were expressed over fraudulent payments with one respondent giving an example:

> …in the early days of the [electronic payment] wallet, we had some attempted fraud and we recognised that because an account was created, a number of small shops [trips] were done through a card and then a big shop was attempted, on the same day. So what someone was trying to do was validate that the process worked (Interview 8).

While it was thought that the payment wallet 'could open up a new world for fraud if customers payment details could be stolen and used via the App' (Interview 8) it was also suggested that not only might electronic payment wallets facilitate the ease at which stolen credit card details can be used, there was also the potential for the use of fraudulent electronic vouchers or coupons. Indeed, Taylor (2013) notes ease of repudiation fraud – where customers may claim that they had not purchased certain items or goods that they appear to have paid for. Overall, it was apparent greater consideration needed to be given around possible fraudulent uses of MSP systems. As one respondent stated:

What we would need to understand, is the vulnerability around card fraud and how fraudsters use it either through getting other people's details from a mobile wallet perspective, or payment method. If I steal your phone, how do we protect the App so… I can't just steal your phone, do all the shopping I want, pay for it and I'm out the door with a one touch payment (Interview 4).

Increased Rewards for Offenders/Non-scanners*:* The MSP environment might generate long-term rewards for offenders/non-scanners. Indeed, several respondents suggested that non-scanning behaviour could become part of the routine behaviours of some shoppers. At present, there is some evidence that non-scan is a part of the behaviours of some SCO customers; 'people will always take advantage of opportunities. You see the self-service figures, one in five admit to stealing on self-service' (Interview 1). Therefore, there is a possibility that some shoppers might begin to perceive certain stores as easy targets and thus increase the frequency at which they use/target them. Indeed, studies of repeat victimisation illustrate that offenders select targets based upon *risk heterogeneity* factors – where a target is so attractive they will select it to commit crime (regardless of whether it has been a successful target for them previously) and as a result of successfully committing a crime then return on another occasion to the same target – known as 'event dependent repeat victimisation' (Farrell, 2005; Farrell and Pease, 1993). Several interviewees suggested that – as with SCO – MSP could act as a risk heterogeneity factor – where people are attracted to stores in the knowledge that they can choose to not scan certain products with relatively little risk of being caught. As one respondent said, 'you get away with it once and then you can just repeat it again and again…' (Interview 7).

Reduction in Risk Perception*:* Several studies have shown that surveillance or various forms of capable guardianship are important in the prevention of shop theft (Beck, 2011; Butler, 1994; Cardone and Hayes, 2012; Tilley, 2010). For example, the number of 'place managers' (store employees) throughout the store, using customer meet and great practices (Tilley, 2010), increasing staff vigilance (Butler, 1994) and formal surveillance (such as security guards) can all impact upon risk perception (Butler, 1994; Cardone and Hayes, 2012). Thus, increased anonymity reduces the perception of risk (Aloysius and Venkatesh, 2013). Within the MSP environment, the sense of risk perception or control is reduced as all elements of the customer journey can be completed without human interaction. Indeed, a further likely long-term consequence of MSP is that the number of place managers will be reduced, as one respondent said 'there are benefits [from MSP] in labour savings, but there could be other problems with that' (Interview 4).

Likely Excuses*:* Previous research has highlighted that SCO allows consumers to use 'ready-made excuses' (Beck, 2011: 210) for offending (the self-scan defence). Therefore, giving customers the freedom to self-scan gives them the opportunity to blame faulty technology, problems with the product barcodes or claim that they are not technically proficient as reasons for non-scan (Aloysius and Venkatesh, 2013). Issues around the 'self-scan error' and 'self-scan defence' regularly came up in the interviews. However, one of the key problems where customer mis-scan is observed is in proving intent to steal items and whether prosecutions can be made or not. As one respondent said 'I scan 20 items and I don't scan five, am I a thief or am I someone who's not very competent?' (Interview 4). Another noted, 'I don't think we could ever prosecute anybody as things exist today, because they could always fall back on the argument 'well, I pressed the button, I thought I'd scanned it'

(Interview 2). Indeed, observations conducted in MSP stores for this research were that validation staff were always more than willing to accept this as a form of defence (even when we had knowingly not scanned items).

Deciding when multiple non-scanning events constitute a pattern was something that all of the retailers were keen to understand and efforts have been made within MSP systems at the point of payment to ensure that customers are sure they have scanned all of their items. Most systems have an on-screen prompt, either in the App or on the payment screen, that asks the customer 'are you sure you have scanned all of your items'. If a customer then proceeds to press 'yes' knowing they have not scanned some items this can be proof of intent. One respondent said:

> …but where I'd feel comfortable convicting [on SCO]… this guy scans three items, pays for those three items, punches in his card details… but there's five items that haven't been scanned, and soon as he's got his receipt, he bags those up. That to me would be strong enough to put in front of the police and say this is absolutely premeditated… (Interview 4).

However, across some jurisdictions retailers have been concerned about potential reputational damage that might be caused by prosecuting customers for not scanning a small number of items. One suggested that its self-checkout option was abandoned as 'too many of our desired customers made little mistakes' and as 'theft is strictly regulated here in [name of country], you need to prosecute' (Interview, 6). Indeed, issues in relation to intent are further confused by where the last point of payment will be in future MSP systems. At present it is clear where the last point of sale (POS) is in most retailers, though as MSP payment systems develop, potentially payments could be made in the shopping aisle or (Wi-Fi permitting) in the car park of the store. This creates problems in understanding where in the shopper journey the final payment point is. As one respondent said in relation to MSP, 'there is no longer a last point of payment and by law we would normally stop people after that' (Interview 2).

Likely Provocations: At present, there are a number of points in the MSP shopper journey that could trigger disputes with staff. Our store visits identified frustration points when products would not scan, when staff had to intervene to remove EAS devices/do age verifications and when payment wallets would not work. For example, on one shopping trip the researcher was given a cash discount because of unacceptably long delays in processing an MSP payment. Aloysius and Venkatesh (2013) noted that continual intervention from staff at the POS in relation to age-restricted items (such as alcohol) and exit validation audits (or re-scans) can generate customer frustration. As one respondent suggested in relation to validation audits, 'customers hate it and we know it's a crap experience and we accept that' (Interview 8). Indeed, the process could create difficult situations for staff and one retailer from the USA described a situation where the audit system was accused of being 'racist' and 'programmed to only stop black people' (Interview 9). However, most respondents suggested customers were generally fairly relaxed about having their shopping subject to exit/validation audits as long as checks were conducted in a non-confrontational and educational way. It was noted that validation audits normally 'only lead to aggressive behaviour when customers have not-scanned items correctly' (Interview 6).

The Impact on Shrinkage: The retail community is notoriously shy in sharing data on losses they experience from malicious crime and non-malicious error – it is normally regarded as

highly sensitive commercial data. The researchers were therefore very fortunate that one of the participating retailers agreed to share an unprecedented amount of data relating to MSP. Analysis was conducted of data collected from 1.096 million audits from nearly 12 million completed shopping trips, equating to 6.044 million items checked for scan accuracy. The total value of the audited items was ❖21.268 million with ❖845,000 being found not to have been scanned. This equates to a shrinkage rate (calculated as a percentage of retail turnover) of 3.97%.

When compared with other measures of shrinkage the MSP shrinkage rate appears high. Table 2 presents four comparison measures of shrinkage: the overall shrinkage rate for the retail case study taking part in this study; the Global Retail Theft Barometer which is the survey with the broadest global reach (the 2011 edition has been selected because it is considered as the most recent reliable version of the survey) (Bamfield, 2011); the National Retail Security Survey (2012), which is the longest running shrinkage survey, but only covering the US, (Hollinger and Adams, 2014); and a survey carried out by the UK's British Retail Consortium which covers business generating around 50% of all UK retail turnover (2012).

Table 2 Comparisons of Mobile Scan Shrinkage Data

Comparable Shrinkage Rates	Shrinkage Rate	Difference
Mobile Scan Shrinkage Rate	3.97%	
Case Study Company 2014[8]	1.47%	+170%
Global Retail Theft Barometer 2011[9]	1.29%	+208%
National Retail Security Survey 2012[10]	2.60%	+53%
The British Retail Crime Survey, 2012[11]	1.21%	+228%
Overall Average[12]	1.79%	+122%

What can be seen is not only is the rate of shrinkage generated by Mobile Scanning considerably higher than the overall rate recorded by the case study company (170% higher), but it is higher than all the other studies – the highest difference being found with the British Retail Consortium where it was 228 per cent higher. Overall, when the average rate for the grocery sector data is compared, then the rate of shrinkage in Mobile Scanning is found to be 122% higher. This is a profound difference in the rate of loss and given that one estimate suggests the overall margin of profit in the European Grocery Sector is just 4%, then taken at face value, this rate of loss generated by Mobile Scanning could be seen as at best a not-for-profit retail venture if deployed extensively in this market.

There are two further points worth making. First, the case study company has not provided data on potential savings generated by the introduction of self-scan technologies that could mitigate against the significantly higher rates of loss found – reductions in staffing and traditional check out technologies for instance. It may be that in the future this higher rate of loss may be sustainable if other store costs can be reduced to compensate for the elevated shrinkage risks associated with this type of retailing. Secondly, the data does not shed any light on the motivation of the shoppers found to have non-scanned items in their bag, basket or trolley – were they deliberately not scanning items because they were trying to steal them or had they genuinely forgotten to scan the items due to difficulties with the technology, distraction or absentmindedness? Thus, a critical unanswered question to date is whether the elevated levels of loss are mainly due to malicious or non-malicious behaviour, although

research conducted in relation to self-checkout (see Carter, 2014; Beck, 2011) indicates that users may regularly take advantage of the system to take items. Indeed, in a self-report survey of 2,634 SCO users in 2014 around 1 in 5 (19%) admitted to stealing from self-service checkouts (Carter, 2014). While the validity of such a self-report study may be questioned, there is little reason to think the rate of malicious theft for MSP would be any less.

MSP and Crime Prevention

The findings suggest MSP creates opportunities for crime and consequentially, increases shrinkage. While one might expect retailers to have grave concerns about implementing technology that can potentially have such negative outcomes, relatively little forethought had been given at all as to how crime opportunities could be *designed out* of the MSP shopper journey. Indeed, a key priority appeared to be around 'proof of concept' – to understand if a working MSP system could be implemented in store free from technological glitches that would reduce its attractiveness to users. As one respondent said:

> Retail is a funny game, get the technology out there, understand that it works in a number of stores and then we will, if the business case is good enough figure the rest out (Interview, 4).

Where forethought had been given to crime prevention, often technological, process and economic factors were cited as obstacles to proactive design. Indeed, Aloysius and Venkatesh (2013: 6) state that, 'surveillance and control becomes more difficult in the mobile scan world' and this is evident here. As MSP places trust in consumers to scan and pay for products using their own mobile devices, difficulties arise in (1) establishing that customers are actually scanning and paying and (2) identifying when miscreant behaviour has occurred. Efforts to prevent shoplifting have traditionally been based around 'risk amplification' by giving would-be offenders the sense that they are being subjected to surveillance (through CCTV, the presence of staff in stores etc.) or through physically 'increasing effort' to steal (i.e. by placing tags on items, using exit barriers etc.) (See Cardone and Hayes, 2012). It was acknowledged that not only are these amplifiers less likely to be effective in the MSP environment, but efforts that slow down the shopping journey (such as tags on items) run contradictory to the MSP ethos of quick and convenient shopping. Therefore the challenge is integrating the physical world of the store with the virtual world of the mobile phone so that systems can identify when the shopper has not performed a physical action – i.e. scanning and paying for products – but that can also amplify risk through the user's personal mobile phone (i.e. through messaging and other 'nudge' or behavioural change opportunities (Ariely, 2012; Winter 2014); shutting them out of the system etc.).

While few respondents had considered how these technological issues would be overcome it was also clear that the balance between the cost of crime prevention, likely increase in sales from MSP and reductions in labour costs (as a result of installing MSP) would be important in shaping proactive crime prevention: 'if we do see an increase in shrinkage in five years' time, there's a pay off between that and the wage numbers' (Interview 2). As one respondent stated, a strong business case was required in order to implement new crime prevention solutions:

> It's always harder to justify having mitigation if the problem hasn't already happened… so until that problem actually is in your face, then you're kind of almost chasing shadows in a way, because we have to then pay money for that solution, and if we haven't seen a loss as

yet, then the business could turn around and say "we've not lost anything, why would I want to pay x amount of money for this type of solution?" (Interview 1).

This view echoes claims by some scholars that security can actually be a low priority for some businesses as it is seen as 'expenditure… that detrimentally affects profit margins' (Lippert and Walby, 2014: 884). Although security staff and crime prevention mechanisms might not 'directly enhance profits' (Lippert and Walby, 2014:884) it has also been recognised that where the expense of crime prevention efforts are seen to outweigh any potential savings to the business, then crime will be tolerated (Tilley, 2010). In the context of MSP in the retail sector, both technological 'headaches' and economic concerns have a clear bearing on the way that risk amplification is built in to the shopper journey. Current crime prevention measures being used by the retailers taking part in this study primarily focussed on increasing a sense of risk or reducing anonymity of users at the start and end of the shopper journey. While the process of registration varied considerably between the case-study companies, all required the MSP shopper to 'register' their presence in the store. Indeed, some registration systems were more likely to promote a sense of risk than others. For example, in some stores you could pick up a loyalty card at customer service and immediately 'register' on the system and begin shopping, while others were more robust – requiring a valid email address/mobile telephone number. For the most part the registration processes currently being used were open to easy manipulation through inputting false information, including the potential to use stolen credit card details. However, respondents expressed little appetite for excessive rigour when registering customers at this stage as they were concerned that 'this would put potential users off' (Interview 2). Thus, encouragement of usage was considered a higher priority than designing a potent risk amplifier through anonymity denial.

Once the MSP user has successfully registered their presence in the store at the start of their shopping journey, they are then very much left alone until they reach the end of the shopping journey – no other means of risk amplification are currently used. Once the customer has selected and (hopefully) scanned all the items they wish to purchase, they then encounter the only other risk amplifier currently available – the 'random' audit check. In risk generation terms, the process is relatively straightforward – the user is made aware that on a randomised basis they will be subject to a check by a member of staff on what they claim to have scanned and what is actually in their basket/trolley/bags. In order for this to work, however, (1) the risk has to be credible – the audits do need to happen; and (2) the customer needs to know there will be sufficiently robust consequences for any miscreant behaviour. All of the retailers conducted audits based upon customer profiling (length of time since last audit, accuracy of preview audit etc) though dealing with the outcome of a mismatch between claimed and actual basket content proved to be difficult. Some ignored it completely by not matching up the manual scan of all items with what was supposedly listed on the App (the difference was recorded but not made apparent to the member of staff undertaking the audit); others used it as a trigger to undertake a full scan of all items (where a partial scan had been requested by the audit algorithm); while some used the event to recalibrate the audit algorithm so that the user would be liable for much more frequent audit checks in the future (a form of punishment through audit-driven irritation). However, none of the retailers had much appetite for prosecuting those who were found to have a mismatch in claimed and actual 'scanned' items.

Indeed, for some respondents the audit process was incompatible with the spirit of how MSP was likely to transform future developments in retailing: 'Re-scan is labour intensive and potentially negates the business labour saving model' (Interview 4). In addition, the vision for some, where the shopper is given the ultimate freedom to shop when and how they want, was seriously undermined by what could be viewed as a rather draconian, untrusting and intrusive audit process at the end of the shopping experience. Therefore, from a crime prevention perspective, the challenge is developing alternative and perhaps more subtle ways of generating and amplifying risk in the MSP experience. However, this requires better integration of the physical process of the in-store shopper journey with the online mobile Apps the customer uses to 'scan' and 'pay'. Although much of the technological knowhow exists to better integrate the physical and virtual world (biometric payment wallets; radio-frequency identification tags on products etc.); whether there is the desire to invest in systems that will mitigate error or intentional theft is unclear.

Discussion: the Criminogenic Impact of MSP and Corporate Social Responsibility

MSP is promoted as a form of shopping that provides a more convenient and quicker service to customers. However, as this paper illustrates, there are likely to be criminogenic impacts that retailers have done little to mitigate for thus far. Thus, the analysis raises two questions that are worthy of further discussion. First, to what extent does such innovation in retail encourage offending from those who might not otherwise be inclined to offend? Second, if offending is encouraged, do retailers have a moral or social responsibility to make efforts to reduce opportunities for crime?

It has been suggested that often 'shop theft is undertaken by determined offenders who find it a relatively easy offence' Tilley (2010: 65). While research in relation to SCO suggests that offenders think it provides the camouflage for theft (Felson and Boba, 2010), the evidence in relation to MSP is that it will also provide further camouflage for such offenders. However, as with SCO, mobile scan systems could present those customers not normally inclined to shoplift with both the opportunities and excuses to engage in theft. For example, in a survey of 2,634 SCO users it was revealed that 57% of those who admitted to taking goods did so because they could not get an item to scan and as a result simply took it (Carter, 2014). Indeed, concerns were expressed in the interviews for this research about how customers who may mistakenly 'non-scan' items, realise how easy it is and as a consequence may begin to routinely non-scan in the future. Therefore, retailers could find themselves accused of making theft so easy that some customers who would normally (and happily pay) are tempted to commit crime. It has been suggested that in such circumstances customers might deny that they are 'real' offenders and develop techniques of neutralisation to rationalise and excuse their behaviours (Sykes and Matza, 1957; Beck, 2011). Indeed, there appears to be a widespread public perception that mobile/self-scan technologies are primarily implemented by retailers to reduce labour costs (The Weekly Gripe, 2009; Daily Mail, 2009). This not only helps generate negative views about retailers, but also allows neutralisation techniques to excuse 'non-scan' behaviours to be developed. In particular it has been observed that some 'non-scanners' almost feel like they have a sense of entitlement: if we do all the work (scanning items') why don't we get a price reduction? It is also commonly felt that non-scanning has no real victim or consequence as thefts are against large corporations who can afford the loss – 'the retailer saves money on staff, so can afford the costs of a few unscanned items' (see Yahoo Finance UK, 2014; Carter, 2014). Further to this, if MSP does encourage

malicious theft, it is plausible to suggest a more concerning potential impact. Shoplifting is widely considered to be an entry or gateway offence to a criminal career and several scholars claim that successful shoplifters often go on to engage in other 'more serious' forms of crime, which have long-term consequences for policing and the criminal justice system (Bamfield, 2012; Clarke and Petrossian, 2012). Thus, while it would be truculent to suggest retailers are responsible for the onset of criminal careers, it would be true to suggest that if retailers create environments that attract and generate crime this may ultimately help to foster the onset of criminal careers.

Tilley (2010) argues that although retailers operate in ways that facilitate crime, expected rates of shrinkage are built into their business models. Therefore, in the case of MSP, if shrinkage rates are generated that exceed a level that cannot be tolerated, the business can 'self-protect' itself by withdrawing MSP services. However, questions remain over the moral position of retailers. Whyte (2007) claims that in the UK, businesses (and trade bodies such as the BRC) have, in recent years, been quick to publicise the financial burden of crime against them and emphasise the wider consequences (such as increased prices to customers) in order to gain policy support. As a consequence, the concept of 'retailers as victims of crime' has received significant policy support from the Home Office and ACPO. However, if retailers are being innovative in ways that generate crime, then this not only raises important questions around the extent they can be conceptualised as 'victims', but also whether they should take greater moral and social responsibility to mitigate the wider 'criminogenic' impacts of technological innovation through their Corporate Social Responsibility (CSR) strategies. Moon (2014:3) asserts that Corporate Social Responsibility 'concerns the ways which companies manage their relations with society' and it is acknowledged that businesses have obligations 'to pursue policies, make decisions, or follow those actions which are desirable in terms of the objectives and values of our society' (Bowen, as cited in Moon, 2014: 3). Indeed, debates have considered whether businesses should only be accountable to shareholders (the shareholder perspective) or if they do have social and moral responsibilities to society (the stakeholder perspective) that should influence 'the daily decision-making of private companies' (Lund Paterson, 2014: 87). Indeed, analysis of the CSR (and Corporate Ethnical) statements of the retailers involved in this research suggests that they all adhere to the stakeholder perspective and are involved in activities that point to a moral engagement in the interests of wider society (O' Connor, 1994). Thus, CRS is something that is viewed as of mutual benefit to the company/society alike and is evidenced by references made in CRS documents to environmental issues, ethical buying and sustainability. Therefore, by making commitments to such issues retailers seem to willingly extend their moral duties beyond what is required by law and government. Indeed, this extension of CRS, now often referred to as 'corporate citizenship' (Lund Paterson, 2014), implies that such businesses have community interests at heart.

Despite making commitments in relation to a number of social issues, none of the CRS statements made any commitment to prevent crime or at least make reasonable efforts to block known opportunities for crime to occur. Of course, for an industry where innovation is known to generate opportunity for crime (Curtis, 1971), such a commitment would be unwise. However, this failure to recognise social and moral responsibilities in relation to criminogenic impact could open businesses to two major criticisms. First, while morally engaged in a number of social issues, when it comes to the wider criminogenic impacts of

their actions, retailers could be accused of being 'morally disengaged' (O Connor, 1994). Second, this lack of engagement could open up businesses to critiques of the 'corporate form' that are well rehearsed in the literature on corporate social responsibility. For example, Bakan (2004) suggests corporations are the organizational equivalent of a sociopath in that they have little regard for the environment, workers or wider society. One might infer from this that, despite making claims to have wider moral and societal concerns at heart, the primary concern of the corporation is its own self-interest and ultimately, profit making. This sentiment echoes with Marxist critiques that claim many corporations can be 'implicated in reproducing inequality and the exploitation of entire classes of people' Lippert and Walby, (2014: 887). It might be inaccurate to suggest that through the implementation of MSP (with the known associated criminogenic impacts) that retailers are knowingly absconding from their corporate social responsibilities. However, it is clear that retailers are beginning to deliver new forms of convenience shopping without necessarily balancing this with any adequate form of crime prevention.

Conclusion

Retail is a fiercely competitive world where businesses need to attract and retain customers. Developments in customer self-service have aimed to deliver convenience shopping while enabling businesses to gain a competitive advantage by reducing costs. Retailers will claim they are providing forms of shopping that consumers desire and are aiming to improve the customer experience. Indeed, many benefits exist, though there appears to an uneasy relationship between customer convenience and the wider criminogenic impacts of MSP. Our analysis highlights how MSP reduces effort and risks for offenders, increases potential rewards while at the same time providing ready-made excuses for offending behaviours. In addition, it also increases provocations for conflict with staff. Most critically, where self-scan systems are available, rates of shrinkage increase dramatically. Whether rates of shrinkage are generated by genuine error or malicious intent is unclear, though if such systems encourage otherwise law-abiding citizens to engage in crime then the social implications could be profound. Crucially, further research needs to explore further what proportion of loss generated is a result of intentional theft, though indicators are that around 1 in 5 customers may regularly use SCO systems as camouflage for theft. We have no reason to believe that MSP would reproduce lower rates.

While this paper has not only raised some timely questions about the potential criminogenic impacts of MSP, it has also considered the social and moral responsibilities of retailers to prevent crime. Indeed, the sector has commonly called upon the police and relevant policy officials to provide sufficient action to tackle retail crime, though one might question whether the desire to be innovative has been balanced with the appropriate efforts to prevent crime. While retailers cannot be held responsible for all crime that occurs amongst them, it is clear that the next steps in customer convenience might be better balanced with crime prevention responsibilities. Therefore, when it comes to MSP, whether retailers are corporate citizens or sociopaths remains to be seen.

References

Aloysius, J. and Venkatesh, V. (2013) Mobile Point-Of-Sale and Loss Prevention: An Assessment of Risk. The Sam M. Walton College of Business: University of Arkansas.

Ariely, D. (2012) *The (Honest) Truth About Dishonesty*. New York: Harper Collins.

Baken, J. (2004) *The Corporation: The Pathological Pursuit of Profit and Power*. New York: Free Press.

Bamfield, J. (2011) The Global Retail Theft Barometer 2011. Nottingham: Centre for Retail Research.

Bamfield (2012) *Shopping and Crime*. Basingstoke: Palgrave MacMillan.

Beck, A. (2011) Self-scan checkouts and retail loss: Understanding the risk and minimising the threat. *Security Journal* 24(3): 199-217.

Beck, A. with Peacock, C. (2009) *New Loss Prevention: Redefining Shrinkage Management*. Basingstoke: Palgrave MacMillan.

British Retail Consortium (BRC) (2012) Retail Crime Survey 2012. London: BRC.

Butler, G. (1994) Shoplifters Views on Security: Lessons for Crime Prevention. In: M. Gill (ed.) *Crime at Work: Studies in Security and Crime Prevention*. Leicester: Perpetuity Press, pp. 56-72.

Carter, C. (2014) Shoppers steal billions through self-service tills, *The Telegraph*, 29 January, http://www.telegraph.co.uk/finance/newsbysector/retailandconsumer/10603984/Shoppers-steal-billions-through-self-service-tills.html, accessed 13 April 2015.

Clarke, R.V. (1980) Situational Crime Prevention: Theory and Practice. *British Journal of Criminology*, 20: 136-147.

Clarke, R. V. (ed.) (1992) *Situational Crime Prevention: Successful Case Studies.* Guilderland, NY: Harrow and Heston.

Clarke, R. V. (1997) *Situational Crime Prevention: Successful Case Studies* (Second Edition). Guilderland, NY: Harrow and Heston.

Clarke, R.V. and Homel, R. (1997) A Revised Classification of Situational Crime Prevention Techniques. In: S. Lab (ed.) *Crime Prevention at a Crossroads*. Highland Heights, KY and Cincinnati, pp. 17-27.

Clarke, R.V. and Petrossian, G. (2012) Shoplifting: Guide No 11 (2nd edition), Center for Problem Oriented Policing, http://www.popcenter.org/problems/shoplifting/, accessed 17 March 2015.

Cardone, C. and Hayes, R. (2012) Shoplifter Perceptions of Store Environments: An Analysis of how Physical Cues in the Retail Interior Shape Shoplifter Behaviour. *Journal of Applied Security Research*, 7(1): 22-58.

Cornish, D. B. and Clarke, R.V. (1986) *The Reasoning Criminal: Rational Choice Perspectives on Offending*. New York: Springer-Verlag:.

Cromwell, P. and Turman, Q. (2003) The devil made me do it: Use of neutralizations by shoplifters. *Deviant Behaviour* 24(6): 535-550.

Curtis, B. (1971) *Security Control: External Theft*. New York: Chain Store Age Books.

Daily Mail. (2010) Are the days of the checkout worker numbered? Tesco pioneers first ever self-service only shop, 14th June, http://www.dailymail.co.uk/news/article-1221940/Death-checkout-worker-Tesco-pioneers-self-service-store.html#ixzz3XHm3AFlO, accessed 7 April 2015.

Department for Business Innovation and Skills (BIS). (2014) Business Population Estimates for the UK and Regions 2014, https://www.gov.uk/government/statistics/business-population-estimates-2014, accessed 24 February 2015.

Farrell, G. (2005) Progress and Prospects in the prevention of Repeat Victimisation. In: N. Tilley (ed.) *Handbook of Crime Prevention and Community Safety*. Cullumpton: Willan, pp. 143-170.

Farrell, G. and Pease, K. (1993). *Once Bitten, Twice Bitten: Repeat Victimization and its Implications for Crime Prevention*. Crime Prevention Unit Paper 46, London: Home Office.

Felson, M. and Boba, R. (2010) *Crime and Everyday Life* (4th edition), London: Sage.

Hollinger, R. and Adams, A. (2014) National Retail Security Survey 2012. Florida: University of Florida.

Home Office (2013) Crime Against Businesses: Findings from the 2012 Commercial Victimisation Survey. London: Home Office.

Home Office (2015) Crime Against Businesses: Findings from the 2014 Commercial Victimisation Survey. London: Home Office.

Lippert, R. and Walby, K. (2014) Critiques of Corporate Security: Cost, Camouflage and Creep. In: M. Gill (ed.) *The Handbook of Security* (2nd ed). Basingstoke: Palgrave, pp. 881-899.

Lund Peterson, K. (2014) The Politics of Corporate Security and the Translation of National Security. In: K. Walby and R, Lippert (eds.) *Corporate Security in the 21st Century: Theory and Practice in International Perspective*. Basingstoke: Palgrave, pp. 78-96.

Moon, J. (2014) *Corporate Social Responsibility: A Very Short Introduction*. Oxford: Oxford University press.

O' Connor, T. (1994) A Neofunctional Model of Crime and Crime Control. In: G. Barak (ed.) *Varieties of Criminology*. Westport, CT: Greenwood press, pp. 143-158.

Sykes, G. and Matza, D. (1957) Techniques of Neutralisation: A theory of delinquency. *American Sociological Review* 22(6): 664-670.

Smith, M. and Clarke, R. V. (2010) Situational Crime Prevention: Classifying Techniques Using 'Good Enough' theory. In: C. Welsh and D. Farrington (eds.) *The Oxford Handbook of Crime Prevention*. Oxford: Oxford University Press, pp. 291-315.

Taylor, E. (2013) Mobile Technologies in Retail: A Review of Benefits and Risk. Kingston, Australia: Efficient Customer Response Australasia.

The Weakly Gripe. (2009) Tesco Self-Service Checkouts, 4 March, http://weeklygripe.co.uk/tesco-self-service-checkout-machines/, accessed 7 April 2015.

Tilley, N. (2010) Shoplifting. In: F. Brookman; M, Maguire; H. Pierpoint and T, Bennett (eds.) *Handbook on Crime.* Willan, Collumpton, pp 48-67.

Turley, C., Ludford, H., Callanan, M. and Barnard, M. (2011) *Delivering the NOMS Offender Management Model: Practitioner Views from the Offender Management Community Cohort Study*. London: Ministry of Justice Report 7/11.

Whyte, D. (2007) Victims of Corporate Crime. In: S. Walklate (ed.) *Handbook of Victims and Victimology*. Cullompton: Willan, pp. 446-464.

Yahoo Finance UK. (2014) 'Are Britons Really a Bunch of Self-Service Shoplifters?' 31 January, https://uk.finance.yahoo.com/news/are-britons-really-a-bunch-of-self-service-shoplifters-131547670.html, accessed 7 April 2015.

Endnotes

---

[1] Professor Beck and Dr Hopkins work at in the Department of Criminology at the University of Leicester, UK. For further information please contact them at: bna@le.ac.uk.

[2] A number of MSP configurations exist. For example customers might scan using their own mobile device or a device provided by the retailer. Payment may be made on their own device, a mobile device provided by the retailer or at a fixed terminal.

[3] The authors would like to thank the UK's Economic and Social Research Council for their generous support of this project.

[4] For reasons of confidentiality, the names of the retailers taking part in this study will not be disclosed.

[5] There is no common definition of the term 'shrinkage' – it is used by the retail industry to describe a basket of losses ranging from shop theft to products going beyond their sell by date.

[6] In order to protect the anonymity of the retailer providing this data, this symbol ❖ is used to represent currency.

[7] Of those trips only 2% or about 250,000 were shopping trips where a mobile phone was used. Of those trips, the vast majority (80%) utilised an iPhone compared with an Android device (20%).

[8] This is calculated based upon the Company's agreed rate of unknown shrinkage, which they regard as the most reliable comparator for this data.

[9] This is the comparable rate for the global grocery sector rather than the overall rate, which was 1.45%.

[10] This is the comparable rate for the US grocery sector rather than the overall rate, which was 1.47%.

[11] This survey does not provide a breakdown by type of retailer.

[12] This is based upon the average of the studies excluding the British Retail Consortium data, which is not a strictly comparable number as it reflects all the retail sector whereas as the others represent only Grocery, which is regarded as more comparable with the mobile scan shrinkage data.