**Insider unauthorised use of authorised access: What are the alternatives to the Computer Misuse Act 1990?**

Abstract

Case-law developments in the United States have supported narrower interpretations of the Computer Fraud and Abuse Act 1986 (CFAA) in cases of unauthorised use of authorised access. This issue has been one that UK courts have also debated in the past and thus this renewed interest in the concept of insider unauthorised access offers an opportunity to bring this debate to the fore again. Starting from discussing the recent US case law, this paper further analyses relevant UK precedent and identifies legal provisions that are applicable when dealing with such incidents in addition to the Computer Misuse Act 1990. More particularly, it identifies provisions, mainly in the Data Protection Act 1998 and the Fraud Act 2006, which could substitute for the Computer Misuse Act 1990 in prosecuting insiders and thus clarifies the extent of the prosecutors’ legal arsenal and manoeuvring space when dealing with exceeding unauthorised access.

Keywords: unauthorised access, computer misuse, data protection, fraud, cybercrime

1. Introduction

In recent years, there has been a new trend in case-law and potentially even influencing amendment discussions for US cybercrime law (Lofgren and Wyden, 2013) which has set a new standard for perceiving access as unauthorised in the US, predominantly with the cases of *United States v. Nosal*, 642 F.3d 781, (9th Cir. 2011) (*Nosal 1*) and mainly *United States v. Nosal* 676 F.3d 854, (9th Cir. 2012) (*Nosal 2*) This new trend in US case-law has narrowed the interpretation of ‘exceeding authorised access’, a concept that in the past has been broadly understood in cases involving charges under the extensive Computer Fraud and Abuse Act 1986, the main cybercrime legislation in the US (Larkin, 2011-2, p.261). As will be seen in this paper, exceeding authorised access is the unauthorised access which is based, not only on the bypassing of technological restrictions, but mainly on the exceeding of the limits and purposes of the given authorisation to access information by those already

---

1 Paper published in the International Journal of Law, Crime and Justice, March 2016. DOI: 10.1016/j.ijlcj.2016.08.003
possessing some degree of authorisation. Before Nosal 2, authorisation would be considered lacking, if the access was violating the predetermined terms of use of a particular website or explicit employer/employee agreements or even an abstract duty of loyalty to whoever was entitled to authorise the access of the perpetrator in question (Kerr, 2003; Karagiannopoulos 2014).

However, the court in Nosal 2, as will be seen, opposed such interpretations and called for more clarity and the criminalisation only of those bypassing technical restrictions. This interesting shift in the perception of unauthorised use of authorised access, which has much broader implications for cybercrime law, has also been included as an option for EU member states' legislatures by the European Commission and is reflected in its new cybercrime Directive 2013/40/EC on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Although the new UK Serious Crime Act 2015 does not seem to take into account the suggested direction of the Directive with no changes made to the concept of authorisation, these developments highlight the contested nature of the concept of exceeding authorised access. This fragile interpretive balance in turn generates concern as to whether prosecutors would have other alternatives for prosecuting such cases, in addition to the UK Computer Misuse Act 1990, if unauthorised use of authorised access were to be construed more narrowly in the future.

This paper will thus assess the new case law developments in the US and highlight the underlying rationale in Nosal 2 and then will discuss how this rationale relates to major UK cases dealing with CMA prosecutions based on unauthorised use of authorised access, mainly the cases of DPP v Bignell [1998] 1 Cr App R8 (Bignell) and Regina v Bow Street Magistrates Court and Allison (A.P.) Ex Parte Government of the United States of America, [1999] All ER (D) 972 (Allison). After showing how similar to Nosal 2 rationales have been discussed within the UK litigation, the essay will move to discuss whether the UK legal system provides additional legal tools to support prosecutors in pursuing cases of insider unauthorised use of authorised access. The choice to discuss the US rationale in relation to the UK and not more internationally is that there seem to be case-law similarities between the cases discussed and of course both are common law countries. Although this area of research could benefit from a wider international comparative perspective, this is beyond the scope and the structural/length limitations of this paper.

The first part will thus look at the US case-law in order to understand the alternative approach it introduces to the concept of insider unauthorised access. Although the predominant case introducing this different approach was Nosal 2, it will be useful to briefly discuss LVRC Holdings LCC v. Brekka, 581 F.3d 1127, (9th Cir. 2009) (Brekka), which was one of the main cases that opened the road for the Nosal 2, diverging from the usual path that case law had set until then.
2. The US-originating wind of change:

2.1 Brekka

Mr. Brekka was an employee of LVRC Holdings and had extensive authorisation to access LVRC’s computer network in order to find and use information necessary for his work. At some point there were discussions between Mr. Brekka and LVRC in relation to a potential investment of Mr. Brekka in LVRC. However, negotiations broke down and he stopped working for LVRC shortly after. During these negotiations, Mr. Brekka had used his access to the LVRC computer network and database and had emailed to his and his wife’s email accounts information regarding LVRC’s business and financial affairs. At a later date, network administrators found that someone was accessing the LVRC database using Brekka’s account and after deactivating the account, LVRC informed the FBI that someone had accessed LVRC’s network without authorisation and eventually sued Mr. Brekka for a violation of the CFAA for emailing the aforementioned information to himself and his wife using his work password to access that information. This led to the court discussing whether Mr. Brekka had exceeded his authorisation given by LVRC, when he sent emails to himself, while he was still an employee of LVRC.

According to the facts, it was common practice for Mr. Brekka to email work-related information to his personal email during the course of his work. LVRC did not have written employment agreement/guidelines with Mr. Brekka dictating the computer use terms explicitly. Based on the above, the district court initially decided that, during the time Mr. Brekka was employed he had authorization to access the emails and documents found on his home computer and his laptop and that LVRC did not prove he lacked authorization prior to leaving the company and consequently granted the defendant a summary judgment motion. Apart from the existence of authorization for Mr. Brekka to email the documents, since the company employed him, the court argued that there was no evidence that there was a confidentiality agreement regarding the documents emailed or an explicit obligation on Mr. Brekka’s behalf to return or destroy the documents upon conclusion of his LVRC employment. Moreover, the district court had found that LVRC had not produced evidence from which a reasonable jury could find that Mr. Brekka logged onto the LVRC websites after leaving employment with them, thus dismissing all charges and claim for restitution under 1030(g). After that, LVRC appealed the decision.

The appellate court considered two issues. First, it focused on the existence of authorization, following the plain language of the statute, since the word authorization is not defined explicitly and, therefore, words should be taken to have their ordinary, contemporary meaning. The court thus resorted to dictionary definitions of authorization, defining it as endorsing, empowering, justifying, permitting by or as if by some recognised or proper authority, as per Webster’s Third International Dictionary (2002, p.146). The court, based on this definition, argued that the employer gives the employee authorization to access a company computer, when he gives the employee permission to use it.
LVRC’s side employed the decision in *International Airport Centers, L.L.C. v Citrin* 440 F. 3d 418, (7th Cir. 2006) (*Citrin*) where the employee was considered to have lost authorization, when he acted against the employer’s interests, breaking a duty of loyalty that authorization was deemed to be based on. The court here responded that the wording of the CFAA does not support the *Citrin* approach that authorization ceases, when an employee uses the computer contrary to the employer’s interest. Instead, the court agreed that Mr. Brekka had authorization to access the computer, as his job required such access, while Mr. Brekka was indeed still employed when he emailed these documents to himself and his wife. Conversely, the appellate court found that the application of *Citrin* to Mr. Brekka’s case would result in him being considered to be lacking authorization from the moment the information transfer to his computers from the LVRC was done with the purpose to start his own competing business, a mental state transforming him from a loyal, to a disloyal employee. Instead the court argued that:

‘The definition of the term "exceeds authorized access" from § 1030(e)(6) implies that an employee can violate employer-placed limits on accessing information stored on the computer and still have authorization to access that computer. The plain language of the statute therefore indicates that "exceeding authorization" depends on actions taken by the employer to pose explicit limitations on the use of the authorization given to his/her employees. Nothing in the CFAA suggests that a defendant’s liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer.’ “ Brekka at 1135”

The court reached this conclusion to avoid a more abstract interpretation of the criminal statute, as it felt that such interpretations could impose unanticipated penalties on the defendants. Consequently, the court submitted that, unless the employer had actually taken steps to revoke the employee’s authorization, Mr. Brekka would have no way of knowing he lacked authorization, since there was no explicit use policy that prevented Mr. Brekka from acting as he did. Consequently, the court argued he could not be found guilty of the said CFAA offences just because his behaviour was in breach of a fiduciary duty to an employer.

2.2. *US v Nosal (1 and 2): Completing the turn*

Mr. Nosal worked as an executive for a company called Korn/Ferry International, an executive search firm. When Mr. Nosal left the company, he signed a Separation and General Release agreement and an independent Contractor Agreement. Mr. Nosal agreed to serve as an independent contractor and to avoid competing with his former employees for a year in exchange for some pecuniary compensation. Shortly after leaving, Mr. Nosal approached three other employees of Korn/Ferry in order to convince them to help him set
up a competing business. It was alleged that these three employees obtained trade secrets and other proprietary information through their accounts, which allowed them access to the Korn/Ferry network. They, then, transferred to Mr. Nosal information coming from the Searcher database of Korn/Ferry, which was considered a highly confidential, proprietary, global database of executives and companies.

Korn/Ferry actually took extensive measures to secure its database, as was documented during the hearings, by controlling electronic and physical access to it. Each Korn/Ferry employee, for example, was awarded a specific username and password to use in order to access the database, making sure only employees could access it. Furthermore, the company required its employees to sign an agreement that both explained the confidential, proprietary nature of the Searcher database and restricted the use of all information in it, except for legitimate company business. Korn/Ferry further declared the confidentiality of the information by stamping reports using information from that database with the phrase: ‘Korn/Ferry Proprietary and Confidential’. Finally, upon accessing the company computer system, there was a notification highlighting the proprietary nature of the information in the database and the need for specific authorization from the company for accessing the database, under threat of disciplinary action or criminal prosecution.

The case relates to charges of a computer fraud 1030(a)(4) amongst other non-CFAA offences that are irrelevant here for the issue of authorization we examine- alleging that Mr. Nosal's co-conspirators had exceeded their authorization to access the Korn/Ferry computers. This was done by obtaining information from their employer’s computers for the purpose of defrauding Korn/Ferry and assisting Nosal in setting up his competing business.

Although there were multiple hearings of this case, this essay will focus on the last en banc hearing, which established the different rationale and was the final decision of the court. During this en banc hearing in 2012 (Nosal 2), the 9th Circuit eventually moved even further than Brekka in its ultimately final decision. In short, the court decided that employer-employee and company-consumer relationships, both based on private agreements, are usually regulated by tort and contract law and not criminal law. The court opposed the prior precedent of the ‘intended function’ test, introduced in United States v. Morris, 928 F.2d 504 (1991) (Morris) as Kerr (2003, p.1629) identifies, which bases the existence of authorisation on an implicit or explicit use agreement/declaration between authoriser and authorisee.

The Nosal 2 court argued that such a rationale would result in the illegality of computer access being manipulated by private parties in order to police users through criminal law. More particularly, the court expressed its concern that attaching CFAA-based felonious liability on the violation of vague and unknown or arbitrarily changeable Terms of Service of websites and online services could criminalise plain users just for violating terms of use of websites. As the court further argued, despite government assurances that prosecutors
would not resort to superficial cases of exceeding authorisation, the current interpretation of exceeding authorisation could not be allowed, as it would force citizens to greatly rely on the discretion of the prosecutors for avoiding excessive prosecutions. The 9th Circuit further reinforced its concerns by citing the court in the case of *United States v. Kozminski*, 487 U.S. 931, (1988), where it was argued that the previously broad interpretation of exceeding authorization that the government supported would “delegate to prosecutors and juries the inherently legislative task of determining what type of . . . activities are so morally reprehensible that they should be punished as crimes” and would “subject individuals to the risk of arbitrary or discriminatory prosecution and conviction.” “Nosal 2 at p.932”

Unsurprisingly, thus, the court in *Nosal 2* decided to follow *Brekka* regarding the criminalization of unauthorized access to information and not its misuse. Consequently, the court found Mr. Nosal and his accomplices, who had access to the company’s databases, could not be charged with computer fraud as they did not lack, nor had they exceeded authorization, accepting that the government could prosecute for the rest of the counts of the indictment apart from the CFAA-related ones, which were reliant on establishing lack of authorisation. This rationale established that for such cases, computer misuse offences in their current wording would not be considered as appropriate as other offences, such as trade secret theft, mail fraud and conspiracy.

The findings of *Brekka* and *Nosal 2* regarding the broadness of perceptions in relation to lacking or exceeding authorisation were further magnified after the broad interpretations of exceeding authorized access led to the highly aggressive prosecution and eventually contributed to the suicide of an Internet prodigy and activist, Aaron Swartz, thus fuelling the already existing discussion regarding necessary amendments to the CFAA (EFF, 2013). In the bill suggested by Rep. Zoe Lofgren and Sen. Ron Wyden (2013), shortly after, it was proposed that the term of exceeding authorized access is eliminated and only the term access without authorization is retained which will mean: ‘(A) to obtain information on a protected computer; (B) that the accesser lacks authorization to obtain; and (C) by knowingly circumventing one or more technological or physical measures that are designed to exclude or prevent unauthorized individuals from obtaining that information;’.

Nevertheless, this change has not come and courts in the US are still confused as to whether violating an employer’s terms of use restrictions would render an employee liable under CFAA charges for exceeding authorised access. The EFF (2015) has discussed the case of Gilberto Valle, relating to a police officer using a police database for personal reasons thus violating NYPD terms of use. On appeal, *United States v. Valle*, No. 14-2710-CR, 2015 WL 7774548, (2d Cir. Dec. 3, 2015) the court applied the rule of lenity interpreting the statute so as to benefit the defendant and considered the concept of exceeding authorised access to be ambiguous, consequently finding Valle’s searches using his work-related computer access legal (Rosenbloom, 2015). This way the court avoided criminalising the use of work computers and networks for personal purposes. Kerr (2013) has highlighted another case of exceeding authorised access conviction based on terms of use, *US v Auernheimer*, Criminal
No.: 2:11-cr-470 (SDW) (Dist. Court, New Jersey 2013), where the defendants had accessed a publicly accessible website of AT&T in order to obtain email addresses that AT&T had linked with the ipads of their owners. On appeal, Auernheimer was acquitted, but this was based on a jurisdictional issue and the court did not explicitly focus on the issue of unauthorised access (EFF, 2014).

Having seen the different perspective of the 9\textsuperscript{th} Circuit, let us now turn to see whether UK courts have expressed any similar views and what is the precedent followed at the moment.

3. The relevant UK case-law

In the UK, the offence of unauthorised access and the computer misuse offences in general are included in the CMA 1990, which has been amended by the Police and Justice Act of 2006 and the Serious Crime Act 2015. The dominant rationale regarding our issue in question, that of unauthorised use of an existing authorisation has been shaped by \textit{R v Bow Street Magistrates Court and Allison (A.P.) Ex Parte Government of the United States of America}. This case essentially overturned a previously influential case that had adopted a more consistent view with \textit{Nosal 2}, the aforementioned \textit{Bignell} case, establishing that, when the use of authorisation to access certain information is not carried out for the purpose for which the authorisation was given, that access exceeds the limits of the authorisation provided and therefore, we have an unauthorised access offence, as per s.1 of the CMA 1990	extsuperscript{x}, as well as the following offences of unauthorised access with intent to commit or facilitate commission of further offences (S.2) and unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc (s.3)

The concept of lack of authorisation is interpreted in s.17.5 of the CMA as:

\begin{quote}
(5) Access of any kind by any person to any program or data held in a computer is unauthorised if—
(a) he is not himself entitled to control access of the kind in question to the program or data; and
(b) he does not have consent to access by him of the kind in question to the program or (part of a program) or data from any person who is so entitled.
\end{quote}

The important phrase is ‘control access of the kind in question’ which essentially could relate to total lack of access, but also some type of access that is beyond a certain degree of access already allowed to the authorisee or even, as will be seen in \textit{Allison}, be interpreted to relate not just to the actual practical access, but also to the use of the information that one could be authorised to access. The court in \textit{Allison} extensively discussed this concept and still remains the authority on the issue, so it is useful to discuss it more extensively, but before that, it is necessary to discuss \textit{Bignell}, which was the case \textit{Allison} overturned.
4.1 DPP v Bignell

In this case, two police officers had been convicted by the stipendiary magistrate under s.1 of the CMA. The officers had caused a police computer operator to obtain for them from the National Police Computer system (NPC) information relating to the ownership and registration of two cars, without having the authority to make the request or obtain that information for reasons unrelated to their police duties, by misrepresenting their purpose to the computer operator. The Bignells were aware that they should only use the PNC records for police purposes. (McEwan, 2008) The two convicted officers appealed to the Crown Court, which allowed the appeal, but the prosecution requested the Crown court to state a case for the Divisional Court in relation to the allowance of the appeal. The Divisional court also agreed with the Crown Court in allowing the appeal.

The Divisional Court then decided that the defendants had not violated s.1 as they had merely asked for the computer operator to perform an authorised act, i.e. to respond to information requests by police officers. It also stated that the police officers could have perhaps been prosecuted under s.5.3 of the 1984 Data Protection Act yet the prosecution did not pursue this after the officers’ acquittal (Lloyd, 2011, p.228). Whether the Data Protection Act could assist in prosecuting cases of misuse of information will be discussed later on.

We see here that the courts decided that there might be an alternative to the CMA in cases of insider information misuse. However, the decision was criticised for creating a loophole and leaving prosecutors without a functional legal tool for prosecuting insider unauthorised access, thus limiting the act to external hackers only (Lloyd, 2014, p.208; Walden, 2007, p.165). As MacEwan (2008, p.958) argues, “Authorisation involves the giving of permission. That permission relates not only to the area of conduct but to the conduct itself within it.” This would mean that both the existence of authorisation to access a specific database or network, but also the nature of the use the authorisee makes of that access are important. Voicing the above concerns, the HoL in Allison, further highlighted the misconceptions entailed in the acquitting decision in Bignell and set up the existing precedent for unauthorised use of authorised access.

4.2 Allison

4.2.1 The rationale

The final decision in Allison overturned Bignell, which had declined that, users with some measure of access to information, could be found guilty under the CMA 1990 for using their given authorisation in order to access information for purposes that were not within the limits of their given authorisation.

The facts of the case though here are quite different and this one had much more complex issues to deal with which were all relying on whether unauthorised use of authorised access could be established. More particularly, in 1997 Mr Allison was arrested upon a provisional
warrant based on the Extradition Act 1989 at the request of the US government. Allegedly, Allison had conspired, while in the UK, with Joan Ojomo, located in the US, and others, to violate sections 2 and 3 of the CMA 1990; essentially, to (1) to secure unauthorised access to the American Express computer system with intent to commit theft,

(2) to secure unauthorised access to the American Express computer system with intent to commit forgery, and

(3) to cause unauthorised modification to the contents of the American Express computer system.

According to the facts, Ojomo was working for American Express as a credit analyst and she had the technical capability to access all customers’ accounts, but she was only authorised to access accounts assigned to her. Nonetheless, she did access files of customers not assigned to her and gave the information to Mr Allison and others allowing them to encode credit cards and supply pin numbers to withdraw money illegally from ATMs.

Obviously, Ojomo did not have authorisation to access the data she used for the above purposes (passing the information onwards for the coding of counterfeit cards) as she lacked any blanket authorisation to access accounts that were not directly related to her work duties. Any such access to accounts was thus in breach of AE’s private computer policies and would be considered unauthorised access in the US based on the ‘intended use’ test’ that Morris established. The result was that Ojomo and her associates defrauded AE of approx. US$1 million.

When Mr Allison was apprehended in London using one of the debit cards illegally made with data provided by Ojomo, he was charged with alleged conspiracy with Ojomo for her to secure unauthorised access to data of the AE computer with intent to commit the further offences of forging cards and stealing money from AE. A core element in establishing these conspiracy charges for Allison was Ojomo’s alleged lack of authorisation to access the data in question from the AE accounts and this is also the element that is of core interest to this essay, thus we now turn to examine the rationale followed on this particular issue by the courts.

Essentially, for Mr Allison to be extradited to the US, it should be proven in the UK that he had conspired to violate s.2 of the CMA 1990, since S.2 falls within the scope of sections (1)(a) and (2) of Order in Council 1976 No. 2144 which in turn gives effect to the extradition treaty between the UK and the US. After deciding positively on the matter of extraditability and the need to establish that s.2 of the CMA had been breached for the offence to be extraditable, the court went on to discuss the CMA offences more particularly, especially focusing on the reliance of s.2 of CMA to s.1, since a prerequisite of s.2 is the establishing of unauthorised access of s.1."

The magistrate and Divisional courts did not find Allison guilty of ss.1 and 2, as they were both influenced by the interpretation of s.17vi by the Divisional Court in the case of Bignell and did not find that Ojomo had perpetrated unauthorised use of authorised access. However, contrary to the lower courts, the HoL in Allison moved away from the
interpretation of Astill J. in Bignell. Lord Hobhouse argued instead that s.17 establishes two levels of access, ‘access of any kind’ and ‘access of the kind in question’. This distinction identifies two types of unauthorised access, one for external intruders, where there is no authorisation and a second type, where some level of authorisation to access exists, but not for the use (kind) that the perpetrator of the offence uses this authorised access. Essentially, this means that the HoL acknowledges that there could be limits to authorisation that depend on the nature of use of the granted access. The court argued that the authority to view certain data did not extend to copying or modifying the data. This would mean that, focusing their authorisation for purposes that were not related to the reasons their employer gave them the authorisation for.

The HoL essentially found that the Bignell court’s interpretation changed the basic concept of ‘entitled to control access’ in s.17.5 of the CMA from being interpreted as ‘being entitled to authorise’ to mean ‘authorised to cause a computer to function’, identifying the phrase ‘entitled to control access’ with ‘entitled to cause a computer to function somehow’. Moreover, as per the Allison decision, the judge in Bignell read the concept of ‘access to a program or data’ to mean ‘access to a computer at a particular level’. This meant that lack of authorisation could not be constituted for instances where some level of authorisation existed already for particular information, irrespective of whether those were used for purposes unrelated to those for which authorisation had been given. This of course renders unauthorised use of authorised access impossible to establish.

4.2.2 Conclusions from Allison

The HoL decision in Allison moves away from the reading of the court in Bignell - and that of the Divisional Court of Allison, which followed Bignell. It establishes the concept of unauthorised use of authorised access by interpreting the term ‘authority to access data of the kind in question’ to mean not access to certain categories of data in abstract, but authority to access specific information in relation to the particular context for which authorisation had been given. Obviously, when no technological controls are established to restrict the access of employees solely to the data and uses for which they are authorised, (something which can often be technically complicated) the assessment of whether someone has exceeded their employer’s authorisation is based on explicit or even implicit private agreements or computer use policies and/or expected practice.

However, the most basic element that Lord Hobhouse in Allison highlights as a misconception was the assessment of the purpose of the Act, where maintaining the ‘integrity of computer systems’ was interpreted as criminalising the intrusion/breaking into computer systems. This of course excludes the element of protecting the integrity of information included in those computer systems from the scope of the Act, consequently eliminating the need and capacity to have an offence of unauthorised use of authorised access altogether, if there is no bypassing of technical restrictions or any other actual computer misuse.
Lord Hobhouse goes through an extensive assessment of the preparatory documents of the CMA in Allison, i.e the Working Party Paper and Report of the Law Commission, where he essentially disproves the claims made by Astill J. in Bignell and by the counsel of Mr Allison, that s.1 refers only to outsider hackers or insiders for which authorisation has been explicitly prohibited, rather than those insiders simply misusing their authorisation. As he argues: ‘The consideration of the mischief which the Act was designed to meet confirms and does not contradict the clear meaning of s.1 of the Act and the equally clear purpose of s.17(2) and (5).’

One has to admit, however, that especially the part of the Working Party Paper that has been put forward by Lord Hobhouse suggesting that: “It should be made clear that ‘unauthorised’ refers to the obtaining of access to a computer system. Our preliminary view is that it would be undesirable for a hacking offence to extend to an authorised user who is using the computer system for an unauthorised purpose.” (para. 6.24) as well as the Law Commission’s request for explicit limits of authorisation to be set by employers to employees (An employee should only be guilty of an offence if his employer has clearly defined the limits of the employee’s authority to access a program or data (para. 3.37)) seem to support the Bignell court decision, something that Lord Hobhouse admits. MacEwan (2008, p.957) further highlights this, citing the Law Commission’s discussions (1989, para.2.13), where it was argued that “the case for a criminal offence of basic hacking [did] not turn on the need to protect information”.

As can be seen then, the whole idea behind Nosal 2 (and even the suggestions of the new Directive) is not alien to the UK legal system, despite it not being considered for the amendments that have been included in the Serious Crime Act 2015. In fact, if anything, it seems to be more consistent than the approach eventually adopted by the HoL in Allison. Is Allison then a reflection of the gradual need to make information integrity protection more robust, which has come about by the gradual increase in relying on information systems and the need to deal with insiders? (Lloyd, 2014, p.228) Although one cannot be certain, the legislature has decided to keep the CMA as it is during the last amendment stage, thus not rewording unauthorised access in a Nosal-consistent way that could challenge the rationale Lord Hobhouse offered in Allison.

Bearing in mind though the complexities and interpretive challenges that such complex terms could entail for courts, it would be useful to assess the existence and usefulness of potential alternative tools the prosecutors can use in order to prosecute unauthorised uses of authorised access without relying on the CMA. The paper will now discuss these legislative tools and whether they could be considered effective and adequately inclusive of most possible scenarios of unauthorised use of authorised access.

5. Alternative solutions?

5.1 s.55 of the DPA
In *Bignell*, the court argued that, although the integrity of the system was not compromised in terms of having misuse of a computer, this did not mean that the act of the police officers did not entail any wrongfulness. It highlighted another relevant piece of legislation that could be more plausibly applicable, the Data Protection Act 1984. Today that Act has been superseded by the Data Protection Act 1998. Could there be a provision in the 1998 DP Act that can deal with misuses of information? A case that has followed *Allison*, but can also highlight the connection of unauthorised use of information with Data Protection-related offences is *R v Mandiya Khan* [2012] EWCA Crim 2032.

As reported in the above appeals case, Ms Khan was convicted on multiple charges of ss.1 and 3 of the CMA 1990, for having accessed personal records of individuals for purposes outwith the purposes of her employment. The violations occurred while she was employed by Lancashire County Council social care team. Despite having signed an explicit agreement of confidentiality regarding her computer systems’ access, allowing her access only to records for purposes for which she was explicitly authorised, Ms Khan accessed multiple files of individuals for personal reasons, mainly relating to alleged child abduction charges that her partner Mr Amjad was facing. Social services had detailed information regarding both the teenager involved in the case, as well as her husband, his family and other individuals related to the case. Ms Khan repeatedly accessed those files, until she was discovered by a co-worker, which eventually led to her prosecution and conviction. Ms Khan’s appeal was rejected by the court on the basis of the potential seriousness of her behaviour, which had an impact not only on the public’s trust of social services record-keeping integrity, but potentially also to the development of the case against her partner.

It is extremely interesting that throughout the appeal’s report, the main concerns for maintaining the conviction are the breach of public trust and the undermining the public confidence in the security of their personal information, which could equally be an issue of data protection. Prima facie, Ms Khan, as an employee of the controller would be considered to be a controller as an employee of the controller herself (Lloyd, 2011, pp.55-6). Therefore, there is a violation of the data protection principles and especially of principle two, which declares that: ‘Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.’ Breaching principle two would affect the organisation directly, i.e. the local Council and not the particular individual, so it would not be useful in an effort to substitute a CMA prosecution for a data protection based prosecution.

However, one has to wonder: is what Ms Khan did actually an act of the data controller, just because she is employed by the controller? She is definitely not accessing information as part of her employment and she might not even have accessed the data during working hours. Should we, therefore, consider Ms Khan’s actions as a data protection breach of the Lancashire County Council? In such cases, one could safely argue that the obtaining of information was perpetrated not as part of Ms Khan’s employment, but by abusing her role.
Based on the above premise, it would be interesting to examine the applicability of s.55 of the DPA 1998 to Ms Khan’s actions as an alternative to the CMA. S.55 relates to the unlawful obtaining of personal data and subsection 1 reads:

(1) A person must not knowingly or recklessly, without the consent of the data controller—
(a) obtain or disclose personal data or the information contained in personal data, or
(b) procure the disclosure to another person of the information contained in personal data.’

As subsection 3 adds, that contravention of subsection 1 is an offence.

But is s.55 applicable? One would argue not, if we consider Ms Khan to be a representative of the controller. If however, we were to consider Ms Khan to be acting, as she was, out with the limits of the controller’s consent, which obviously she knowingly exceeds based on her violating of her employee agreement regarding access to information, then Ms Khan could be considered just a third party unlawfully obtaining personal data from the controller.

The DPA was created to protect data subjects from misuses of their personal information by controllers, with the data protection principles reflecting that core concern. However, s.55 seems to have been created in order to punish those that take advantage of the collected data by controllers without their consent and thus also to absolve the controllers from cases where the violation of privacy rights of individuals is not a decision of the controller per se or at least with the controller’s consent. In support of the view that Ms Khan should not be considered a controller, the Information Commissioner’s Office (ICO) in its 2011-2 report (p.13) has declared that it has successfully prosecuted under s.55 ‘a health sector employee who unlawfully obtained her sister-in-law’s medical records in order to find out about the medication she was taking.’ Two more cases one in the health sector and one in the banking sector explicitly demonstrate how employees can be prosecuted under s.55 for misuses of information held by their employer/controller, thus making it clear that employees could be considered third parties, when acting outside their duties, such as when accessing records for personal purposes (ICO, 2013). Even earlier, in 2002, the ICO investigated misuse of the NPC by police officers based on s.55, a case not too different from the facts in Bignell. (ICO, 2006, p.15) We can see then that there have already been prosecutions of insiders under s.55 in cases where one could definitely also apply the current CMA unauthorised use of authorised access approach instead of s.55, based on violations of employer computer use policies. Therefore, applying s.55 offers the prosecutor an added tool in their effort to achieve a conviction in cases, where the applicability of the CMA would be challenged on bases similar to the challenges the Nosal 2/Bignell courts suggested.

The parallel applicability of s.55 is also particularly important, if one were to consider that such information could have been kept in manual files rather than computerised. How could one prosecute Ms Khan then, where the CMA would have been inapplicable, since there
would be no computer involved in the process? Or what would happen, if some of the
misuses of information related to information on paper and some to computerised files? We
could have the ludicrous result of prosecuting the same unlawful action with two different
Acts, the CMA and the DPA, based on the digitisation or not of the relevant information.
Wasik (1989, p.260) highlighted criticisms against the CMA, which criminalised unauthorised
access to confidential information in electronic form. As he argues (Wasik, 1989, p.260),
unauthorised access to the same information held on card index would not be equally
criminal, thus rendering the storage medium the essential criminalising factor instead of the
actual harm caused by the breach of confidentiality – an element existing in both cases. That
would definitely be inefficacious, if not irrational. Using s.55 as an alternative could protect
prosecutors and courts from the above irrationality, as it applies to both electronically-
stored information, but also to ‘relevant filing systems’ (ICO, n.d.). These systems are
compilations of personal data found in systematically organised manual files, which fall
within the scope of the DPA, but would definitely be outwith the scope of the CMA (Lloyd,
2014, pp.53-6).

However, there are also concerns in relation to the applicability of s.55 to insider
information misuse cases. As Wasik (2008) clarifies, although s.55 is applicable for
disclosures of confidential information, personal browsing without any further disclosure
might not fall within the scope of s.55 as the HoL has decided in the case of R. v Brown
[1996] 2 Cr App R 72 (Brown). Mr. Brown was a police officer, who abused his authorisation
to access the PNC in order to browse at information regarding vehicles owned by debtors on
behalf of a debt collection agency. The HoL argued that browsing could not be considered
use of personal data, if there was no proof that further use of that information had been
made. Obviously this case was prior to s.55 of the 1998 DPA and related to the previous
1984 Act, although the wording, was not very dissimilar to s.55, criminalising both obtaining
(s.5(c)) and disclosing information (s.5(d)). As Sumroy (1997, p.120) argues though, before
the rationale adopted in Brown would have allowed every curious data processor to browse
our personal information without any data protection implications, something which would
have been opposed to the requirements of the Data Protection Directive, 95/46/EC, where
Member States should protect the rights to privacy of individuals from having their personal
data being retrieved or consulted by others without the approval of the data controller.

Consistent with Sumroy’s view, it would appear that the rationale of Brown has been
superseded by a similar case, R v Rooney (Jaqueline Mary) [2006] EWCA Crim 1841 (Rooney).
In Rooney, the appellate court upheld the conviction of Rooney JM under s.55 for two
counts of unlawfully obtaining information, which related to accessing the personal data of
both the ex-husband of her sister Angela and his new partner and one charge of disclosing
information included in personal data to her sister regarding the new town, where her ex-
husband had moved to (Wasik, 2008, pp.137-8). Considering that Rooney was convicted
both for obtaining (the accessing of personal information for reasons irrelevant to her
duties) and for disclosing the town to which the couple had moved, one could argue that
obtaining would be the same as browsing, since the court assessed different charges for the accessing of both individuals’ personal information (two counts of obtaining) and additionally, a separate count of disclosing (relating to the disclosure to the appellant’s sister) and convicted for both acts.

Another conclusion that can be drawn from Rooney and which had also been a serious matter in the appeal, was whether the disclosure of information related to personal data (the exact address) or whether even information extracted from that personal data (the town’s name and not the exact address where they lived) could fall within the scope of s.55, to which the appellate courts responded positively. This could have further implications for cases, where someone does not disclose the exact information accessed, but more general information extracted from the information accessed. Consequently, one could argue that just accessing the information and even abstractly disclosing information that could be produced from the unlawfully accessed personal data could fall within the scope of s.55, thus making it a very inclusive prosecutorial tool.

One additional area of concern regarding the application/applicability of s.55 is that the penalties are much lower than the CMA, as s.60.2 of the DPA provides that penalties are restricted to fines both on summary and indictment conviction. These penalties might be considered low when meant to deter and punish activities that have a seriously adverse impact on important policy concerns, such as information systems integrity and public trust in personal information-processing organisations, as the court in Khan has also shown to be the expectation. However, according to the Criminal Justice and Immigration Act 2008 s. 77, the Secretary of State (SoS) has the power to alter the penalty for a s.55 offence. (CPS, n.d. ‘Data Protection Act 1998 – Criminal offences’) The SoS has not thus far increased the penalty for s.55, (CPS, n.d. ‘Data Protection Act 1998 – Criminal offences’) despite the expectations and recommendations of the Information Commissioner’s Office towards that direction (ICO, 2011-2, p.9). The ICO (2006, p.5) has suggested a maximum of two years custodial sentence on indictment and up to 6 months and/or a fine on summary judgment. Considering that the CMA unauthorised use of authorised access prosecutions could be substituted by s.55 of the DPA, it is important that such a change is considered in order for a more harmonised framework to exist.

It should be noted that the Information Commissioner’s penalty range suggestion is exactly the same as the penalty range for unauthorised access in s.1 of the CMA, with the higher end of the scale being obviously reserved for those violations of s.55 relating to ‘blagging’ and trading in the unlawfully obtained personal information, which was at the time of the report, the main concern of the ICO (2006, p.5). In an effort to analogise or substitute aspects of the CMA (unauthorised use of authorised access) then for s.55, it is positive to see that the legislature and the relevant authorities (ICO) have expressly shown that they could consider an increase of penalties that would match the CMA penalties in seriousness to respond to concerns of personal privacy, customer trust for commercial enterprises and
citizen trust of public sector; all intrinsic elements of building a secure and trusting information society. (ICO, 2006, p.3) Prosecutions have been successful, despite the penalties not being high (ICO, 2006, p.12), which would again imply that s.55 could be an efficient tool.

But what about cases where the information does not relate to personal data, but is of economic value? After all, one main concern for criminalising insiders using information in an unauthorised way is the protection of the financial interests of companies from disgruntled employees and such data will often not be relating to persons, so that they could fall within the scope of the DPA. Is the CMA our only hope here?

5.2 S.4 of the Fraud Act 2006

As Walden (2007, paras 3.47-3.49) argues, there is no criminal law granting protection to commercial information or trade secrets in the UK, as this has been subject to consultation for many years, where an offence for the unauthorised use or disclosure of a trade secret has been proposed, yet without reaching any definite conclusion. However, it could be argued that fraud by abuse of position might be applicable to cases where financial information has been accessed by insiders for unauthorised purposes. It will have to be highlighted here that the CMA criminalises unauthorised access with the intent to commit a series of crimes, fraud included.

However, once the act of fraud is perpetrated s.4 of the Fraud Act 2006 could potentially apply, as it provides that:

‘(1)A person is in breach of this section if he—

(a)occupies a position in which he is expected to safeguard, or not to act against, the financial interests of another person,

(b)dishonestly abuses that position, and

(c)intends, by means of the abuse of that position—

(i)to make a gain for himself or another, or

(ii)to cause loss to another or to expose another to a risk of loss.’

Walden (2007, paras 3.47-3.49) mentions that a typical example of the above would be a departing employee, who uses his access rights to copy valuable information from the employer’s database. This example is, of course, quite similar to Brekka and Nosal, where we also had cyberfraud charges being levelled against the defendants. In such cases, we would argue that a person abuses dishonestly its position as an employee intending to make a profit for himself and cause loss to his employer by getting data that would allow him or her to create a competing business product for example.
The concept of dishonesty has been discussed in a much older case, *R v Ghosh* [1982] QB 1053, where the court requires initially an objective test as to whether dishonesty exists according to the ordinary standards of reasonable and honest people. If that test is positive, a subjective test is to be applied, assessing whether the defendant realised his actions were dishonest by those standards. (Johnson & Rogers, 2007, p.296) As this is a conduct offence that can prevent further crimes, (Johnson & Rogers, 2007, p.296) it suits the same purposes as the CMA ss. 1 and 2 (which includes s.1) in terms of dealing with access to information through abuse of position before any more harm can be caused. As Campbell (2007, p.341) highlights, there is no need for an actual further result beyond the intention to use the dishonest abuse for personal gain or to cause loss. Consequently, this provision would also centre on the abuse of position and thus, the misuse of information, and not the end-result produced by this abuse. Despite the usefulness of this provision, when suggesting the Fraud Act 2006 as a solution, one should also be wary of the concerns that Campbell (2007, p.341) highlights in relation to the fact that criminal liability for fraud and the consequent penalties will be attached to the individual without any harm occurring beyond the dishonest act, something which would be closer to attempted, rather than complete fraud according to his view. Nevertheless, if we were to use this provision for cases relating to unauthorised use of access, there is no need to prove gain or loss have happened, as the main concern would be accessing the information for unauthorised purposes and not whether that unauthorised use resulted in gain or loss.

Naturally, the first question is: which types of position are included within the scope of this offence? As the Law Commission in its Fraud Report (2002, para. 7.38) has clarified, the offence relates to cases of agent and principal as well as employer-employee. As Collins (2011, p.514) argues, the Law Commission has also clarified that the nature of the relationship extends to cases where no fiduciary duty exists, which would allow the inclusion of relationships that are familial or based on voluntary agreements. Consequently, in cases of insiders/employees that take advantage of their position in order to use confidential or other financial information in ways that they are not supposed to, where this has an actual financial impact it would appear that the above s.4 of the Fraud Act 2006 could be applicable. This offence could also cover cases where the information is not in electronic form, or is partly in electronic form - a weakness of the CMA that has been highlighted earlier too as something that s.55 of the DPA could help with. (Wasik, 1989, p.260 cited in McEwan, 2008, p.956) After all, the nature in which the information is written and stored should not necessarily change the nature of the offence.

Another issue that has been relatively contested regarding the application of this offence is whose expectation of loyalty/appropriate behaviour should be the one that is of importance in this offence. The most plausible scenarios offered are either that of the victim’s expectation, which is considered the most appropriate to judge the norms and expectations in the particular context or an objective ‘reasonable expectation’ standard (Collins, 2011, p.515) The expectation of the person abusing its power, a third potential alternative, would
in most cases fail to be a safe criterion due to the improbability of the wrongdoer adopting a high expectation of loyalty for its own abuse (Collins, 2011, p.515). Moreover, it would open, as a general criterion, the road to abuse of victims who are usually in a weaker position anyway and would, on top of that, have to rely on the rationale adopted by the alleged fraudster in order to protect their interests.

The extent of abuse as well is quite broad and can be satisfied very easily by any effort to manipulate a situation influenced by the existence of this position of power (Collins, 2011, p.515). Also as the Crown Prosecution Service guidance (the Fraud Act 2006) clarifies: ‘It is immaterial whether or not he (the fraudster) is successful in his enterprise and whether or not any gain or loss is actually made.’ As mentioned above as well, this clarification allows us to use this offence in order to deal with information compromises, even if there is no actual harm or loss. This rationale imbues this offence with the necessary flexibility required to support the CMA unauthorised use of authorised access prosecutions. The existence and extent of those additional elements of gain/loss play their role in sentencing, but not in establishing the offence per se. (CPS, The Fraud Act, 2006)

In terms of penalties, s.1(3) provides that:

(3) A person who is guilty of fraud is liable—

(a) on summary conviction, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum (or to both);

(b) on conviction on indictment, to imprisonment for a term not exceeding 10 years or to a fine (or to both).

These penalties definitely seem adequate to cover the penalties imposed under the CMA offences, even the penalties relating to s.2 of the CMA, which criminalises unauthorised access with the intention of committing fraud, or other offences in the future\(^\text{viii}\). Consequently, it would appear that s.4 of the Fraud Act 2006 could be a second useful tool in dealing with offences relating to financially valuable non-personal information.

### 5.3 More options?

In addition to the above options, there are still some provisions that could be applicable. For example, one might argue that s.2 of the Fraud Act 2006 (fraud by false representation) could be applicable\(^\text{x}\), if we were to consider the fact that someone is using their authorisation credentials in order to make an untrue or misleading representation with the intent of stealing information to be used to cause loss and offer gain to the perpetrator. The representation can be implicit and could be directed at a machine, which was one of the main reasons that the change in law was instigated after deception offences created considerations as to whether they could be applied to machine-related deceptions. (Lloyd,
Consequently, s.2 could apply to cases where existing access credentials are used for access, but the underlying purpose of the access is misrepresented, as being within the official duties of the perpetrator, while it is not. Assuming that the purpose of the access is implicit in the use of access credentials given for specific authorised purposes, as would be the rationale adopted in Allison, the use of the same credentials for purposes outwith the purpose that these were given for, it would be an untrue or misleading representation. In terms of applicability to unauthorised use of authorised access offences one could argue that s.2(5) of the Fraud Act renders the implicit misrepresentation relevant to computer systems (Lloyd, 2011, p.246). However, I believe that going down this route could cause too many complexities in terms of establishing the existence of an implicit false representation in cases where the person actually uses their own log in details but for dishonest purposes and thus s.4 seems to be a safer choice for information abuses by insiders.

Other authors have identified additional possible tools. Wasik (2008, pp.138-9) extensively discusses the prospect of applying the common law offence of misconduct in public office in relation to police officers disclosing confidential information they have accessed on the PNC. Wasik (2008, pp.138-9) defines the offence as “public officers, acting in that capacity, and acting without justification or reasonable excuse, wilfully misconducts himself, or wilfully neglects to perform his duty, to such a degree as to amount to an abuse of the public’s trust in the office holder.” Furthermore, Wasik (2008, pp.140-1) offers examples of various cases and argues that, despite its controversial breadth and vagueness, the offence is a useful tool for prosecutors, as it also allows them to hand down substantial custodial sentences for offences that could be prosecuted under the CMA. Moreover, as Walden (2007, paras 3.15-7) argues, there are other specific types of information that are protected by criminal law, such as governmental information that is protected under the Official Secrets Acts of 1911, 1920 and 1989, relating to insiders in the sense of criminalising disclosure to other parties. Wasik (2008, p.135) also mentions how unauthorised access cases had in the past been prosecuted using the Official Secrets Act of 1911, and even corruption offences. An even more specialised tool could be the common law offence of perversion of the course of justice, in cases like Khan, where the misuse of access to information related to obstructing the truth in relation to another criminal case. Of course, there are also civil law solutions, such as the common law breach of confidence tort as well as multiple preventive technological solutions that could reduce the need to resort to criminal prosecutions, but this paper focuses on criminal law, therefore, such alternatives will not be discussed.

An analysis of all the additional solutions would require a much longer piece of work in order to exhaustively number the tools available to prosecutors in addition to the CMA for unauthorised uses of authorised access to information. It is the author’s view that this purpose is served by the analysis offered, as the aim is not to provide a full account of the possible tools, but to try to establish that UK prosecutors would have alternative avenues to explore, if the courts were to consider a CMA interpretation of unauthorised use of authorised access in accordance with the US examples of Brekka and Nosal. For the extreme
instances, where none of the above alternatives would be applicable, Larkin (2011-2, p.280) offers in his analysis of *Nosal* a rationale that is core for the US and I would say also for the UK legal system:

“there may be cases where it is the CFAA or nothing, and a narrow reading of that law will enable some parties who engage in morally blameworthy conduct to avoid prosecution. But that is a strength of our system, not a weakness. The proposition that it is better for ten guilty defendants to go free rather than to convict one innocent party is one of the axioms that American law always has deemed fundamental to the proper operation of the criminal justice system.”

5. Conclusion:

This paper has focused on the concept of unauthorised use of authorised access in the US and the UK with the aim of discussing whether the UK criminal justice system includes more tools for prosecuting insider misuses of information than the CMA. The 9th Circuit in the US essentially restricts the applicability of computer misuse provisions to insiders and suggests that computer misuse liability should not be incurred when those authorised to access information violate private agreements and terms of use of websites, but only when there are explicit technical restrictions bypassed. Although this is something that the new cybercrime Directive also suggested, such an approach has not been adopted here in the UK. However, the decision in *Nosal* highlights the need to consider what could be possible alternatives to the CMA in relation to similar cases, especially since UK courts in the past have problematized about the concept of insider unauthorised access themselves in *Bignell*. After all, laws and precedent have a tendency to change with time and it is important to be aware of all legal options for dealing with insider misuses. Becoming aware of the alternatives also liberates the debate on the limitations of the CMA, but to also helps us understand the potential dimensions of certain provisions in other laws and how new technologies might be impacting on their interpretations and potential applications. I hope that this paper has contributed to this effort to broaden our understanding and put things in perspective in relation to this important issue.

As it has been shown, there are indeed existing provisions that can apply and cover a multitude of different instances that can also be prosecuted under the CMA relating both to private information through the use of the DPA 1998, but also to financially valuable information through the use of the Fraud Act 2006. Therefore, it would appear that following the understanding of the *Nosal* 2 court could be a plausible option and the gaps it would leave for prosecutors could be covered with the identified alternatives. Even if the change in approach has not been realised through the new amendments introduced by the Serious Crime Act 2015, it is important for everyone, from offenders to prosecutors, lawyers and judges to become more aware in terms of potential overlapping and mutually
complimentary provisions that could be applied to instances of information misuse in order to achieve more relevant and proportionate results with different cases of insider information misuse.

As has been highlighted especially in the US cases of Brekka and Nosal 2, an important element is whether organisational guidelines exist and whether they dictate terms of use for employees. Although, the court in Brekka highlighterd the

As Kerr (2015, pp.3-4) highlights, the problem with resolving the issue of unauthorised access is that the whole rationale of authorisation is based on Internet norms that most lawyers and judges find beyond their scope of understanding. In he (Kerr, 2015, p.4) says: “lawyers and judges are something like the proverbial Martians from outer space trying to figure out the social norms of Earth.” This paper has attempted to highlight both the difficulty in concretising the interpretation of unauthorised access in law and case law and the variety of applicable provisions that exist and make the process of adopting one particular piece of legislation for such prosecutions even more complex. Although it has not resolved the issue, it has attempted to reconcile the different views in showing that even if a narrower interpretation of the CMA is followed, prosecutors will not be helpless as there is an array of existing provisions and common law offences that can even be more case-specific and relevant to the type of information compromised.
Reference list:

Campbell, 2007

Collins, 2011
J. Collins Fraud by abuse of position: theorising section 4 of the Fraud Act 2006

CPS, 2006
http://www.cps.gov.uk/legal/d_to_g/fraud_act/#a10 (accessed 12.06.16.).

CPS, 1998
http://www.cps.gov.uk/legal/d_to_g/data_protection/ (accessed 12.01.16.).

EFF, 2013
Electronic Frontier Foundation (EFF) Computer Fraud and Abuse Act Reform (2013)
https://www.eff.org/issues/cfaa (accessed 12.06.16.)

EFF, 2014

EFF, 2015
ICO, n.d.

Information Commissioner’s Office (ICO) Key Definitions of the Data Protection Act (n.d.)
http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions#type (accessed 20.06.2016)

ICO, 2006

http://ico.org.uk/~/media/documents/library/Corporate/Research_and_reports/WHAT_PRICE_PRIVACY.pdf (accessed 20.06.16.)

ICO, 2012


ICO, 2013


Johnson and Rogers, 2007


Karagiannopoulos, 2014


Kerr, 2003

O. Kerr Cybercrime's scope: interpreting “access” and “authorization” in computer misuse statutes

Kerr, 2013

Kerr, 2015

Larkin, 2011–2

Law Commission, 1989

Law Commission, 2002
Law Commission No. 276, Fraud (2002)

Lloyd, 2011

Lloyd, 2014

Lofgren and Wyden, 2013

MacEwan, 2008

Rosenbloom, 2015

Sumroy, 1997

Walden, 2007

Wasik, 1989

Wasik, 2008

Webster’s Third International Dictionary, 2002
Some of the main cases supporting the view that Nosal opposes are: *United States v Morris*, 928 F.2d 504 (1991), *United States v. Czubinski*, 106 F. 3d 1069 (1st Cir. 1997); *Shurgard Storage Ctrs. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1123 (W.D. Wash. 2000); *International Airport Centers, L.L.C. v Citrin* 440 F. 3d 418, (7th Cir. 2006)

The changes suggested by the new Directive can be found in the guidance (Recital 17) and provisional wording of the illegal access offence (art.3) (unauthorised access in other words) which now explicitly suggest that there should be a requirement of bypassing of technological controls in order for access to be considered unauthorised. More particularly in Recital 17 we can see the explanation that:

“[...]In the context of this Directive, contractual obligations or agreements to restrict access to information systems by way of a user policy or terms of service, as well as labour disputes as regards the access to and use of information systems of an employer for private purposes, should not incur criminal liability where the access under such circumstances would be deemed unauthorised and thus would constitute the sole basis for criminal proceedings. [...]”

Also art.3 provides that: “*Member States shall take the necessary measures to ensure that, when committed intentionally, the access without right, to the whole or to any part of an information system, is punishable as a criminal offence where committed by infringing a security measure, at least for cases which are not minor.*” (emphasis added)

(a) Whoever—(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period; shall be punished as provided in subsection (c) of this section.

S.1.1: (1) A person is guilty of an offence if—

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer [or to enable any such access to be secured];

(b) the access he intends to secure [or to enable to be secured] is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

The reliance is obvious if we examine the initial subsections of the two first sections of the CMA: “1(1) A person is guilty of an offence if—

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

(b) the access he intends to secure is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at—

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer....

2(1) A person is guilty of an offence under this section if he commits an offence under the unauthorised access offence”) with intent

(a) to commit an offence to which this section applies; or

(b) to facilitate the commission of such an offence (whether by himself or by any other person)....

“The relevant subsections of 5.17 reads—

"(1) The following provisions of this section apply for the interpretation of this Act.

(2) A person secures access to any program or data held in a computer if by causing a computer to perform any function he—

(a) alters or erases the program or data;

(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(c) uses it; or

(d) has it output from the computer in which it is held (whether by having it displayed or in any other manner);

and references to access to a program or data (and to an intent to secure such access) shall be read accordingly. .........................
(5) Access of any kind by any person to any program or data held in a computer is unauthorised if -
(a) he is not himself entitled to control access of the kind in question to the program or data; and
(b) he does not have consent to access by him of the kind in question to the program or data from any person
who is so entitled.

vi Relevant filing system is ‘any set of information relating to individuals to the extent that, although the
information is not processed by means of equipment operating automatically in response to instructions given
for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to
individuals, in such a way that specific information relating to a particular individual is readily accessible.’ (ICO,
n.d.) http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions#type

viii Section 2(5) of the CMA provides that A person guilty of an offence under this section shall be liable—
(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a
fine not exceeding the statutory maximum or to both;
(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not
exceeding the statutory maximum or to both;
(c) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

ix A person is in breach of this section if he—
(a) dishonestly makes a false representation, and
(b) intends, by making the representation—
(i) to make a gain for himself or another, or
(ii) to cause loss to another or to expose another to a risk of loss.

x ... a representation may be regarded as made if it (or anything implying it) is submitted in any form to any
system or device designed to receive, convey or respond to communications (with or without human
intervention).