International Journal of Law, Crime and Justice 47 (2016) 85–96

Contents lists available at ScienceDirect

International Journal of Law, Crime and Justice

journal homepage: www.elsevier.com/locate/ijlcj

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

Vasileios Karagiannopoulos

University of Portsmouth, Institute of Criminal Justice Studies, St Georges Building, 141 High Street, Room 524, Old Portsmouth PO1 2HY, UK

ARTICLE INFO

Article history:
Received 10 March 2016
Received in revised form 23 June 2016
Accepted 12 August 2016
Available online 8 September 2016

Keywords:
Unauthorised access
Computer misuse
Data protection
Fraud
Cybercrime

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.

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 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[1] (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

E-mail address: vasileios.karagiannopoulos@port.ac.uk.

[1] 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).

http://dx.doi.org/10.1016/j.ijlcj.2016.08.003
1756-0616/

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.[2] 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

[2] 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).*