DEFENCE FORCE DISCIPLINE APPEAL TRIBUNAL

Randall v Chief of Army [2018] ADFDAT 3

|  |  |
| --- | --- |
| Appeal from: | Restricted Court Martial |
|  |  |
| File number: | DFDAT 4 of 2017 |
|  |  |
| Members: | **TRACEY (PRESIDENT), LOGAN (DEPUTY PRESIDENT) AND HILEY (MEMBER) JJ** |
|  |  |
| Date of decision: | 10 July 2018 |
|  |  |
| Catchwords: | **DEFENCE AND WAR** –application for extension of time to appeal – application for leave to appeal against convictions by Restricted Court Martial – unauthorised access to restricted data – *Defence Force Discipline Act 1982* (Cth) s 61(3), *Criminal Code* (Cth) s 478.1 – related alternative prejudicial conduct charges – *Defence Force Discipline Act 1982* (Cth) s 60 – obligation of prosecution to prove absence of access authority beyond reasonable doubt – conclusion of panel as to proof of absence of authority on the evidence unsafe and unable to be supported – convictions quashed  **EVIDENCE** – proceeding for service offence before service tribunal – proof of absence of authority for conduct charge – general service knowledge – *Defence Force Discipline Act 1982* (Cth) s 147 – cannot be used to contradict authority conferred by service instructions and explained in duty statements |
|  |  |
| Legislation: | *Criminal Code* (Cth) ss 6.1, 6.1(1)(a), 6.1(b), 6.1(2), 6.1(3), 13.1-13.5, 13.2(1), 13.2(2), 476.1, 476.2, 476.2(2), 478.1, 478.1(1), Ch 2  *Defence Force Discipline Act 1982* (Cth) ss 3, 10, 60, 60(1), 61, 61(3), 61(6), 147, 154  *Defence Force Discipline Appeals Act 1955* (Cth) ss 21, 23, 23(1)(a), 23(1)(d)  Army Act 1881 (UK), 44 & 45 Vict, c 58  Army Discipline and Regulation Act 1879 (UK), 42 & 43 Vict, c 33  Naval Discipline Act 1957 (UK), 5 & 6 Eliz 2, c 53, s 58(2)  Rules of Procedure 1947 (UK)  Rules of Procedure 1907 (UK) r 74 |
|  |  |
| Cases cited: | *Attorney General’s Reference No 4 of 2002; Sheldrake v Director of Public Prosecutions* [2005] 1 AC 264  *Environmental Protection Authority v Caltex Refining Co Pty Ltd* (1993) 178 CLR 477  *Fulton v Chief of Army* [2005] ADFDAT 1  *Komljenovic v Chief of Navy* (2017) 319 FLR 215; [2017] ADFDAT 4  *Lee v The Queen* (2014) 253 CLR 455; [2014] HCA 20  *Li v Chief of Army* (2013) 250 CLR 328; [2013] HCA 49  *M v The Queen* (1994) 181 CLR 487  *MFA v The Queen* (2002) 213 CLR 606; [2002] HCA 53  *Momcilovic v The Queen* (2011) 245 CLR 1; [2011] HCA 34  *Nigerian Air Force v Obiosa* (2003) 4 NWLR (pt 810) 233; (2003) 1 NILR 311  *R v Baden-Clay* (2016) 258 CLR 308; [2016] HCA 35  *Re Manion’s Appeal* (1962) 9 FLR 91  *Sorby v Commonwealth* (1983) 152 CLR 281  *Woolmington v Director of Public Prosecutions* [1935] AC 462 |
|  |  |
| Date of hearing: | 26 and 27 April 2018 |
|  |  |
| Date of last submissions: | 9 May 2018 |
|  |  |
| Place: | Brisbane |
|  |  |
| Category: | Catchwords |
|  |  |
| Number of paragraphs: | 121 |
|  |  |
| Counsel for the Appellant: | R Pearce |
|  |  |
| Solicitor for the Appellant: | Salerno Law |
|  |  |
| Counsel for the Respondent: | R Cawte with H Dempsey |
|  |  |
| Solicitor for the Respondent: | Office of the Director of Military Prosecutions |

ORDERS

|  |  |  |
| --- | --- | --- |
|  | | DFDAT 4 of 2017 |
|  | | |
| BETWEEN: | PETER ALLEN RANDALL  Appellant | |
| AND: | CHIEF OF ARMY  Respondent | |

|  |  |
| --- | --- |
| MEMBERS: | TRACEY (PRESIDENT), LOGAN (DEPUTY PRESIDENT) AND HILEY (MEMBER) JJ |
| DATE OF ORDER: | 10 JULY 2018 |
| WHERE MADE: | MELBOURNE |

THE TRIBUNAL ORDERS THAT:

1. The period within which the appeal and application for leave to appeal herein must be lodged be extended to the date on which it was lodged.
2. Leave to appeal, to the extent necessary, be granted.
3. The appeal be allowed.
4. The convictions of the appellant be quashed.

REASONS FOR DECISION

# THE TRIBUNAL:

## “The golden thread”

1. In *Woolmington v Director of Public Prosecutions* [1935] AC 462 at 481-482,the then Lord Chancellor, Viscount Sankey, with whom the other members of the House of Lords who sat on that appeal agreed, famously stated:

Throughout the web of the English Criminal Law one golden thread is always to be seen that it is the duty of the prosecution to prove the prisoner’s guilt subject to ... the defence of insanity and subject also to any statutory exception. If, at the end of and on the whole of the case, there is a reasonable doubt, created by the evidence given by either the prosecution or the prisoner ... the prosecution has not made out the case and the prisoner is entitled to an acquittal. No matter what the charge or where the trial, the principle that the prosecution must prove the guilt of the prisoner is part of the common law of England and no attempt to whittle it down can be entertained.

1. Unsurprisingly, given the British heritage of our legal system, this “golden thread” is also woven into the web of Australian common law: *Environmental Protection Authority v Caltex Refining Co Pty Ltd* (1993) 178 CLR 477 at 501 (Mason CJ and Toohey J). In Australia, the proposition that it is for the prosecution to prove the guilt of the accused has been described as “a cardinal principle of our system of justice”: *Sorby v Commonwealth* (1983) 152 CLR 281 at 294 (Gibbs CJ); see also *Momcilovic v The Queen* (2011) 245 CLR 1 at 47; [2011] HCA 34 at [44] (French CJ). This feature of our criminal justice system has been said to reflect “a balance struck between the power of the State to prosecute and the position of an individual who stands accused”: *Lee v The Queen* (2014) 253 CLR 455 at 466-467; [2014] HCA 20 at [32] (French CJ, Crennan, Kiefel, Bell and Keane JJ). In *Momcilovic*, at 51-52 [54], French CJ also stated that “[t]he presumption of innocence has not generally been regarded in Australia as logically distinct from the requirement that the prosecution must prove the guilt of an accused person beyond reasonable doubt.” In 2005, in *Attorney General’s Reference No 4 of 2002; Sheldrake v Director of Public Prosecutions* [2005] 1 AC 264 at 292 [9] Lord Bingham stated that the underlying rationale for the presumption of innocence was that to place the burden of proof on a defendant was “repugnant to ordinary notions of fairness”.
2. Shortly after its establishment, the Defence Force Discipline Appeal Tribunal (“the Tribunal”), then known as the Courts-Martial Appeal Tribunal, held that this “golden thread” was a governing principle in respect of Australia’s then service discipline law system: *Re Manion’s Appeal* (1962) 9 FLR 91 at 103-104 (Deputy President McInerney QC, Members Wright and O’Sullivan). That remained the position upon the enactment and commencement of the *Defence Force Discipline Act 1982* (Cth) (“the DFDA”) because, as enacted, s 10 made the principles of the common law with respect to criminal liability applicable to service offences. Since then, Parliament has found attraction in a codification of those principles and in the application of that codification to service offences. But this has not led to the unravelling of the “golden thread”. It remains woven, both directly and indirectly, into the web of Australia’s current service discipline law.
3. The direct thread is created by the present s 10 of the DFDA, which provides that Chapter 2 of the Commonwealth *Criminal Code* (“the Criminal Code”), being the Schedule to the *Criminal Code Act 1995* (Cth), applies to all service offences. Division 13 (set out below) is amongst the general principles of criminal responsibility found in Chapter 2 of the Criminal Code. In relation to offences against the Criminal Code, Division 13 gives statutory expression both to the common law principle that the burden of proving beyond reasonable doubt “every element of an offence relevant to the guilt of the person charged” falls on the prosecution and to the recognition in *Woolmington* that Parliament may provide for exceptions to this principle. Save in respect of the class of service offences created by s 61(3) of the DFDA, as to which see the next paragraph in these reasons, s 10 of the DFDA thus makes the principle that the prosecution must, subject to any express exception, prove guilt beyond reasonable doubt directly applicable to the trial of every person charged with a service offence.
4. The indirect thread is created by s 61(6) of the DFDA with respect to conduct which, if it took place in the Jervis Bay Territory, would be a “Territory offence”, as defined (s 3, DFDA), and which is made a service offence by s 61(3) of the DFDA. The otherwise direct effect of s 10 of the DFDA is modified by s 61(6) of that Act, which provides:

(6) To avoid doubt, section 10 of this Act does not have the effect that Chapter 2 of the *Criminal Code* applies to the law in force in Jervis Bay, for the purpose of determining whether an offence against this section has been committed.

The note to s 61(6) of the DFDA accurately describes the effect of that subsection:

Note: Section 10 of this Act applies Chapter 2 of the Criminal Code to the content of this section, but not to the content of the law in force in Jervis Bay. To determine, for the purposes of this section, whether Chapter 2 of the Code applies to Jervis Bay law, it is necessary to consult Jervis Bay law.

1. The offences set out in the Criminal Code are, in terms of the definition of “Territory offence” in s 3 of the DFDA, offences against a law of the Commonwealth in force in the Jervis Bay Territory. They form part of the law in force in that Territory. So, too, accordingly, do the provisions of Chapter 2 of the Criminal Code, applicable to such offences, form part of that law. In this indirect fashion, Division 13 of the Criminal Code applies to contraventions of the Criminal Code which, by s 61(3) of the DFDA, are made service offences.
2. The present application for an extension of time and related leave to appeal raises, in an acute way, whether, on the whole of the evidence and in light of the application of Division 13 of the Criminal Code to the proof or, as the case may be, defence of the service offences charged, it was reasonably open to the members of the panel of a restricted court martial convened under the DFDA to conclude that the guilt of the appellant was proved beyond reasonable doubt. For the reasons which follow, our conclusion is that such a conclusion was unreasonable and cannot be supported and that the convictions are unsafe or unsatisfactory. Principally, that is because, on the whole of the evidence, the prosecution did not make out its case of unauthorised access (or modification) to the required standard such that the appellant is entitled to acquittal.

## Court martial proceedings and outcome

1. The appellant is Warrant Officer Class Two (“WO2”) Peter Allen Randall, a member of the Royal Australian Corps of Signals (“RA Sigs”) within the Australian Army. He was brought to trial before a restricted court martial and charged with 28 offences against s 61(3) of the DFDA, constituted by unauthorised access to (or modification of) restricted data, contrary to s 478.1(1) of the Criminal Code. In respect of each of these primary charges, an alternative charge of prejudicial conduct, contrary to s 60(1) of the DFDA, was additionally preferred against him. Originally, 46 charges were preferred but 18 of these were abandoned by the prosecution before the final hearing commenced.
2. The offences upon which the prosecutor proceeded were alleged to have occurred variously in 2013 and 2014, during the course of WO2 Randall’s deployment in the United Arab Emirates as a member of the Force Communications Unit (“FCU”), serving under the Australian National Headquarters – Middle East Area of Operations (“MEAO”), known as Headquarters Joint Task Force 633 (“JTF 633”). At the time, WO2 Randall was acting in the next most senior Army rank, Warrant Officer Class One (“WO1”), in an information systems appointment within the FCU. He held a number of roles at this time. He was the Information System Engineer and the Information System Manager. He had the status of a System Administrator and a System Manager. He was also the Information Security Systems Officer.
3. There were disparate outcomes at trial in respect of the charges. On 21 June 2016, the court martial convicted him of some of the charges and acquitted him of others, either by express direction of the Judge Advocate or on the panel’s own assessment of the evidence. The panel did not need to consider prejudicial conduct charges brought as alternatives to primary charges under s 478.1 of the Criminal Code where it found the primary charges proven.
4. The charges of which WO2 Randall was convicted and the related sentences consequentially imposed by the panel were as follows.
5. Charge 4 provided:

**Unauthorised access to restricted data**

Being a defence member in Al Minhad Air Base, United Arab Emirates, on 28 May 2014, did intentionally cause unauthorised access to restricted data held in a Commonwealth computer, knowing that the access was unauthorised, by accessing the email account of LEUT Arthur Jagiello on the ADF Deployed Defence Secret Network.

**Particulars**

1. On 28 May 2014 at about 0539h, WO1 Randall accessed the Lotus Notes email account of LEUT Arthur Jagiello on the ADF Deployed Defence Secret Network (DDSN), titled *arthur.jagiello* (“the email account”).

2. The email account was held on a Commonwealth computer system, and had been restricted in its accessibility by way of an access control system associated with a function of the computer, namely a username and password for access to the computer network, as well as system-based restrictions that limited who could open email accounts to the relevant user, system administrators and specifically authorised personnel.

3. WO1 Randall used his administrator privileges to access the email account without authorisation.

The sentence imposed for Charge 4 was: “To be reprimanded.”

1. Charge 5 provided:

**Unauthorised access to restricted data**

Being a defence member in Al Minhad Air Base, United Arab Emirates, on 30 May 2014, did intentionally cause unauthorised access to restricted data held in a Commonwealth computer, knowing that the access was unauthorised, by accessing the email account of LEUT Arthur Jagiello on the ADF Deployed Defence Secret Network.

**Particulars**

1. On 30 May 2014 at about 0719h, WO1 Randall accessed the Lotus Notes email account of LEUT Arthur Jagiello on the ADF Deployed Defence Secret Network (“DDSN”), titled *arthur.jagiello* (“the email account”).

2. The email account was held on a Commonwealth computer system, and had been restricted in its accessibility by way of an access control system associated with a function of the computer, namely a username and password for access to the computer network, as well as system-based restrictions that limited who could open email accounts to the relevant user, system administrators and specifically authorised personnel.

3. WO1 Randall used his administrator privileges to access the email account without authorisation.

The sentence imposed for Charge 5 was: “To be severely reprimanded.”

1. Charge 6 provided:

**Unauthorised access to restricted data**

Being a defence member in Al Minhad Air Base, United Arab Emirates, on 28 May 2014, did intentionally cause unauthorised access to restricted data held in a Commonwealth computer, knowing that the access was unauthorised, by accessing the email account of LEUT Arthur Jagiello on the ADF Deployed Defence Restricted Network.

**Particulars**

1. On 28 May 2014 at about 1010h, WO1 Randall accessed the Lotus Notes email account of LEUT Arthur Jagiello on the ADF Deployed Defence Restricted Network (“DORN”), titled *arthur.jagiello* (“the email account”).

2. The email account was held on a Commonwealth computer system, and had been restricted in its accessibility by way of an access control system associated with a function of the computer, namely a username and password for access to the computer network, as well as system-based restrictions that limited who could open email accounts to the relevant user, system administrators and specifically authorised personnel.

3. WO1 Randall used his administrator privileges to access the email account without authorisation.

The sentence imposed for Charge 6 was: “To be reprimanded.”

1. The alternative to Charge 8 alleged prejudicial conduct contrary to s 60(1) of the DFDA:

**Prejudicial conduct**

Being a defence member in Al Minhad Air Base, United Arab Emirates, on 05 May 2014, did an act likely to prejudice the discipline of the Defence Force by accessing without authorisation the email account of CAPT Ami Hansen on the ADF Deployed Defence Secret Network.

The sentence for the alternative to Charge 8 was as follows: “Conviction without punishment recorded on condition that Warrant Officer Randall undertake to be of good behaviour for 12 months.”

1. Charge 12 provided:

**Unauthorised access to restricted data**

Being a defence member in Al Minhad Air Base, United Arab Emirates, on 08 June 2014, did intentionally cause unauthorised access to restricted data held in a Commonwealth computer, knowing that the access was unauthorised, by accessing the email account of CAPT Melissa Healy on the ADF Deployed Defence Secret Network.

**Particulars**

1. On 08 June 2014 at about 1253h, WO1 Randall accessed the Lotus Notes email account of CAPT Melissa Healy, on the ADF Deployed Defence Secret Network (DDSN), titled *melissa.healy* (“the email account”).

2. The email account was held on a Commonwealth computer system, and had been restricted in its accessibility by way of an access control system associated with a function of the computer, namely a username and password for access to the computer network, as well as system-based restrictions that limited who could open email accounts to the relevant user, system administrators and specifically authorised personnel.

3. WO1 Randall used his administrator privileges to access the email account without authorisation.

The sentence imposed for Charge 12 was: “To be reprimanded.”

1. Charge 13 provided:

**Unauthorised access to restricted data**

Being a defence member in Al Minhad Air Base, United Arab Emirates, on 08 June 2014, did intentionally cause unauthorised access to restricted data held in a Commonwealth computer, knowing that the access was unauthorised, by accessing the email account of CAPT Melissa Healy on the ADF Deployed Defence Restricted Network.

**Particulars**

1. On 08 June 2014 at about 1257h, WO1 Randall accessed the Lotus Notes email account of Army CAPT Melissa Healy on the ADF Deployed Defence Restricted Network (DORN), titled *melissa.healy* (“the email account”).

2. The email account was held on a Commonwealth computer system, and had been restricted in its accessibility by way of an access control system associated with a function of the computer, namely a username and password for access to the computer network, as well as system-based restrictions that limited who could open email accounts to the relevant user, system administrators and specifically authorised personnel.

3. WO1 Randall used his administrator privileges to access the email account without authorisation.

The sentence imposed for Charge 13 was: “To be reprimanded.”

1. Charge 14 provided:

**Unauthorised access to restricted data**

Being a defence member in Al Minhad Air Base, United Arab Emirates, on 19 February 2014 at about 0420h, did intentionally cause unauthorised access to restricted data held in a Commonwealth computer, knowing that the access was unauthorised, by accessing the email account of CAPT Peter Kimberley on the ADF Deployed Defence Restricted Network.

**Particulars**

1. On 19 February 2014 at about 0420h, WO1 Randall accessed the ADF Deployed Defence Restricted Network (DORN) Lotus Notes email account of CAPT Peter Kimberley, titled *peter.kimberley* (“the email account”).

2. The email account was held on a Commonwealth computer system, and had been restricted in its accessibility by way of an access control system associated with a function of the computer, namely a username and password for access to the computer network, as well as system-based restrictions that limited who could open email accounts to the relevant user, system administrators and specifically authorised personnel.

3. WO1 Randall used his administrator privileges to access the email account without authorisation.

The sentence imposed for Charge 14 was: “To be reprimanded.”

1. Charge 15 provided:

**Unauthorised access to restricted data**

Being a defence member in Al Minhad Air Base, United Arab Emirates, on 19 February 2014 at about 0420h, did intentionally cause unauthorised modification of restricted data held in a Commonwealth computer, knowing that the modification was unauthorised, by modifying data in the email account of CAPT Peter Kimberley, held on the ADF Deployed Defence Restricted Network.

**Particulars**

1. On 19 February 2014 at about 0420h, WO1 Randall accessed the ADF Deployed Defence Restricted Network (DORN) Lotus Notes email account of CAPT Peter Kimberley, titled *peter.kimberley* (“the email account”).

2. At about 0420 hours on 19 February 2014, WO1 Randall removed one email, titled “Employment opportunities at BAE Systems”, from the email account and placed it in his own email account, and in doing so., erasing the email from CAPT Kimberley’s email account.

3. The removal of the email by WO1 Randall modified the email data is such a way that it prevented CAPT Kimberley from accessing the email or the data contained within.

4. The email account was held on a Commonwealth computer system, and had been restricted in its accessibility by way of an access control system associated with a function of the computer, namely a username and password for access to the computer network, as well as system-based restrictions that limited who could open email accounts to the relevant user, system administrators and specifically authorised personnel.

5. WO1 Randall used his administrator privileges to access the email account without authorisation.

The sentence imposed for Charge 15 was: “To be severely reprimanded.”

1. Charge 16 provided:

**Unauthorised access to restricted data**

Being a defence member in Al Minhad Air Base, United Arab Emirates, on 19 February 2014 at about 1724h, did intentionally cause unauthorised access to restricted data held in a Commonwealth computer, knowing that the access was unauthorised, by accessing the email account of CAPT Peter Kimberley on the ADF Deployed Defence Restricted Network.

**Particulars**

1. On 19 February 2014 at about 1724h, WO1 Randall accessed the ADF Deployed Defence Restricted Network (“DORN”) Lotus Notes email account of CAPT Peter Kimberley, titled *peter.kimberley* (“the email account”).

2. The email account was held on a Commonwealth computer system, and had been restricted in its accessibility by way of an access control system associated with a function of the computer, namely a username and password for access to the computer network, as well as system-based restrictions that limited who could open email accounts to the relevant user, system administrators and specifically authorised personnel.

3. WO1 Randall used his administrator privileges to access the email account without authorisation.

The sentence imposed for Charge 16 was: “To be severely reprimanded.”

1. The alternative to Charge 19 provided:

**Prejudicial conduct**

Being a defence member in Al Minhad Air Base, United Arab Emirates, on 29 December 2013, did an act likely to prejudice the discipline of the Defence Force by accessing without authorisation the email account of WO1 Phillip Saunders on the ADF Deployed Defence Secret Network.

The sentence imposed for the alternative to Charge 19 was: “To be reprimanded.”

1. Charge 22 provided:

**Unauthorised access to restricted data**

Being a defence member in Al Minhad Air Base, United Arab Emirates, on 15 May 2014, did intentionally cause unauthorised access to restricted data held in a Commonwealth computer, knowing that the access was unauthorised, by accessing the email account of WO1 Phillip Saunders on the ADF Deployed Defence Secret Network.

**Particulars**

1. On 15 May 2014 at about 0425h, WO1 Randall accessed the Lotus Notes email account of WO1 Phillip Saunders, titled *phillip.saunders* on the ADF Deployed Defence Secret Network (DDSN) (“the email account”).

2. The email account was held on a Commonwealth computer system, and had been restricted in its accessibility by way of an access control system associated with a function of the computer, namely a username and password for access to the computer network, as well as system-based restrictions that limited who could open email accounts to the relevant user, system administrators and specifically authorised personnel.

3. WO1 Randall used his administrator privileges to access the email account without authorisation.

The sentence imposed for Charge 22 was: “To be severely reprimanded.”

## Extension of time and leave to appeal

1. WO2 Randall’s notice of appeal was filed outside the period fixed by s 21 of the *Defence Force Discipline Appeals Act 1955* (Cth) (“the DFDAA”). He has sought an extension of time pursuant to s 21 of the DFDAA. The reasons for the delay are fully explained in an uncontroversial affidavit made by his solicitor, Captain Emma Salerno, an Army Reserve Legal Officer. They relate both to the understandable and not unreasonable disposition of WO2 Randall first to exhaust DFDA review procedures, his deployment for extended periods following the communication to him of the outcome of the last of these reviews, the need by counsel (Colonel R A Pearce, who appeared as defending officer at the court martial) and solicitor to analyse many thousands of pages of transcript and numerous exhibits from the court martial proceeding and provide related advice, and the availability of counsel and solicitor to seek instructions, having regard to their travel and Service commitments.
2. Somewhat surprisingly, in light of this explanation, the respondent Chief of Army chose to resist the granting of an extension. Be this as it may, taking into account both the explanation given as well as WO2 Randall’s prospects in respect of the grounds of appeal which he chose to press, we regard the granting to him of an extension of time as necessary in the interests of justice. Further, and if only out of an abundance of caution, we shall grant him leave to appeal in so far as the same may be necessary.

## Grounds of appeal

1. The grounds of appeal pressed by WO2 Randall are the third and fourth of those pleaded in his notice of appeal namely:

(c) The findings of guilt are unreasonable and/or cannot be supported having regard to the evidence; and

(d) In all the circumstances of the case, the findings of guilt are unsafe and/or unsatisfactory and should be quashed.

1. These grounds reflect two bases upon which, by s 23(1)(a) and s 23(1)(d) of the DFDAA respectively, the Tribunal may allow an appeal and quash a conviction. As to these two provisions, we take their meaning and effect to be as stated by the Tribunal in *Fulton v Chief of Army* [2005] ADFDAT 1,with reference to *M v The Queen* (1994) 181 CLR 487 and *MFA v The Queen* (2002) 213 CLR 606; [2002] HCA 53. The Tribunal (at [55]) there observed:

Little, if any distinction, can be drawn between par (a) and (d). Both reflect the law as expounded by the High Court in *M v R* (1994) 181 CLR 487 and *MFA v R* (2002) 213 CLR 606. The two joint judgments in the latter case affirmed the principle expounded in the former, at 493:

Where, notwithstanding that as a matter of law there is evidence to sustain a verdict, a court of criminal appeal is asked to conclude that the verdict is unsafe or unsatisfactory, the question which the court must ask itself is whether it thinks that upon the whole of the evidence it was open to the jury to be satisfied beyond reasonable doubt that the accused was guilty (See *Whitehorn v The Queen* (1983) 152 CLR at 686; *Chamberlain v The Queen (No 2)* (1984) 153 CLR at 532; *Knight v The Queen* (1992) 175 CLR 495 at 504‑505, 511).

In the application of this principle, we must consider both the sufficiency and the quality of the evidence.

1. In *Fulton* (at [56]) referring to *MFA v The Queen*, the Tribunal added:

McHugh, Gummow and Kirby JJ said at 623-624 that in this context the expressions “unsafe or unsatisfactory”, “unreasonable” and “cannot be supported having regard to the evidence” have the same meaning. With respect to the jury’s advantage of seeing and hearing the evidence, their Honours said that in a case where the appellate court experiences a doubt about the conclusion of a guilty verdict and there appears a significant possibility that an innocent person is being convicted, the verdict must be quashed unless the fact that the jury has seen and heard the evidence can explain the different conclusions.

1. The qualification in the passage quoted from *Fulton* in relation to the fact that the jury has seen and heard the evidence is salutary. It is applicable, by analogy, in appeals against conviction under the DFDAA, in relation to the verdicts of courts martial and Defence Force Magistrates.
2. This qualification was a key feature of the Chief of Army’s submissions. However, as will be seen, in this case much turned not on an advantage of this kind enjoyed by the panel but on documentary evidence, found in service manuals, instructions and duty statements, with respect to the duties of the holder of the position to which WO2 Randall was then posted. Further, as to oral testimony, the panel had before it the uncontradicted evidence of another, well qualified and experienced, RA Sigs Warrant Officer, WO1 Mark Neville Wright, called by the prosecution, who gave evidence as to the tasks and responsibilities of an Information System Manager and an Information System Engineer, the practical application on deployment of those duties, and WO2 Randall’s expertise. As it happened, WO2 Randall gave oral evidence consistent with this body of documentary and oral prosecution evidence.
3. In *R v Baden-Clay* (2016) 258 CLR 308 at 324; [2016] HCA 35 at [48], the High Court observed of a trial in respect of an alleged offence against civilian criminal law that it was “accusatorial but also adversarial”. The same is true in respect of the trial of an alleged service offence before a court martial or a Defence Force Magistrate. It necessarily follows that, as in the civilian criminal jurisdiction, so, too, in the service discipline jurisdiction, a party is bound by the conduct of his or her case. In the present proceeding, even in respect of instances where there was evidence of an “apology” by him, the conduct of WO2 Randall’s case never involved a concession that he lacked authority.

## The offence provisions

1. So far as is presently material, s 478.1 of the Criminal Code, as in force at the time of the commission of the alleged offences in 2013 and 2014, provided:

**478.1 Unauthorised access to, or modification of, restricted data**

(1) A person is guilty of an offence if:

(a) the person causes any unauthorised access to, or modification of, restricted data; and

(b) the person intends to cause the access or modification; and

(c) the person knows that the access or modification is unauthorised.

Penalty: 2 years imprisonment.

(3) In this section:

***restricted data*** means data:

(a) held in a computer; and

(b) to which access is restricted by an access control system associated with a function of the computer.

1. By s 476.1 of the Criminal Code, the term “unauthorised access, modification or impairment” is given the meaning set out in s 476.2. It is there provided, materially:

**476.2 Meaning of *unauthorised access, modification or impairment***

(1) In this Part:

(a) access to data held in a computer; or

(b) modification of data held in a computer; …

…

by a person is unauthorised if the person is not entitled to cause that access, modification … .

(2) Any such access, modification … caused by the person is not unauthorised merely because he or she has an ulterior purpose for causing it.

(3) For the purposes of an offence under this Part, a person causes any such unauthorised access, modification … if the person’s conduct substantially contributes to it.

…

1. As to the service offence of prejudicial conduct, s 60 of the DFDA materially provided at the time of the commission of the alleged offences in 2013 and 2014:

**60 Prejudicial conduct**

(1) A defence member is guilty of an offence if the member does an act that is likely to prejudice the discipline of … the Defence Force.

Maximum punishment: Imprisonment for 3 months.

…

(2) An offence against subsection (1) … is an offence of strict liability.

Note: For ***strict liability***, see section 6.1 of the *Criminal Code*.

(3) It is a defence to a charge under subsection (1) if the member proves that he or she had a reasonable excuse for the relevant act.

Note: The defendant bears a legal burden in relation to the matter in subsection (3). See section 13.4 of the *Criminal Code*.

…

1. WO2 Randall relied upon the defence in s 60(3) of the DFDA which required him to prove that he had a reasonable excuse for engaging in the impugned conduct. The “reasonable excuse” invoked was that WO2 Randall believed that he had authority at each of the relevant times.

## Criminal Code — Burden and standard of proof

1. It is now necessary to set out the material parts of Division 13 of the Criminal Code:

**13.1 Legal burden of proof—prosecution**

(1) The prosecution bears a legal burden of proving every element of an offence relevant to the guilt of the person charged.

Note: See section 3.2 on what elements are relevant to a person’s guilt.

(2) The prosecution also bears a legal burden of disproving any matter in relation to which the defendant has discharged an evidential burden of proof imposed on the defendant.

(3) In this Code:

***legal burden***, in relation to a matter, means the burden of proving the existence of the matter.

**13.2 Standard of proof—prosecution**

(1) A legal burden of proof on the prosecution must be discharged beyond reasonable doubt.

(2) Subsection (1) does not apply if the law creating the offence specifies a different standard of proof.

**13.3 Evidential burden of proof—defence**

(1) Subject to section 13.4, a burden of proof that a law imposes on a defendant is an evidential burden only.

(2) A defendant who wishes to deny criminal responsibility by relying on a provision of Part 2.3 (other than section 7.3) bears an evidential burden in relation to that matter.

(3) A defendant who wishes to rely on any exception, exemption, excuse, qualification or justification provided by the law creating an offence bears an evidential burden in relation to that matter. The exception, exemption, excuse, qualification or justification need not accompany the description of the offence.

(4) The defendant no longer bears the evidential burden in relation to a matter if evidence sufficient to discharge the burden is adduced by the prosecution or by the court.

(5) The question whether an evidential burden has been discharged is one of law.

(6) In this Code:

***evidential burden***, in relation to a matter, means the burden of adducing or pointing to evidence that suggests a reasonable possibility that the matter exists or does not exist.

**13.4 Legal burden of proof—defence**

A burden of proof that a law imposes on the defendant is a legal burden if and only if the law expressly:

(a) specifies that the burden of proof in relation to the matter in question is a legal burden; or

(b) requires the defendant to prove the matter; or

(c) creates a presumption that the matter exists unless the contrary is proved.

**13.5 Standard of proof—defence**

A legal burden of proof on the defendant must be discharged on the balance of probabilities.

1. As can be seen, the combined effect of s 13.1 and s 13.2(1) of the Criminal Code is to codify what in *Woolmington* was described as “the golden thread”, namely that it is for the prosecution to prove the guilt of the person charged beyond reasonable doubt. Subsection 13.2(2) of the Criminal Code recognises that this general position may be subject to express exception. The offence of prejudicial conduct contrary to s 60 of the DFDA offers, in s 60(3), an example of an express exception. The note to that subsection correctly recites that its effect is to place the legal burden, as described in s 13.4 of the Criminal Code, on the person charged. So it does in respect of the defence found in s 60(3) of the DFDA.
2. For reasons set out below, even in relation to the prejudicial conduct charges, absence of access authority was an element the proof of which fell on the prosecution. It was only in respect of the defence of a reasonable excuse under s 60(3), for example, a belief that the access was authorised, that any legal burden fell on WO2 Randall in relation to the prejudicial conduct charges under s 60(1).

## Criminal Code — Effect of other provisions of Chapter 2

1. The taxonomy apparent in Chapter 2 of the Criminal Code which characterises the elements of offences created by that code into physical and fault elements has a superficial, attractive simplicity which, in practice, has admitted of difficulties of characterisation. In the service discipline context, this is illustrated by the disparate views as to the offence elements concerned, evident at various stages in the proceedings which culminated in the High Court in *Li v Chief of Army* (2013) 250 CLR 328; [2013] HCA 49*.* We gratefully adopt the summary of the general effect of the other provisions of Chapter 2 of the Criminal Code offered by the High Court in *Li* at 337-338 [19]-[22] (French CJ, Crennan, Kiefel, Bell and Gageler JJ):

19 The DFDA applies Ch 2 of the *Criminal Code* (Cth) to all of the service offences it creates [s 10 of the DFDA]. The relevant effect of Ch 2 of the *Criminal Code* so applying can be summarised as follows.

20 To establish guilt of a service offence, the prosecution must prove each physical element of the offence as well as a fault element for each physical element [s 3.2 of the Criminal Code]. A particular physical element may be: conduct (which may itself be an act, an omission to perform an act or a state of affairs); or a result of conduct; or a circumstance in which conduct, or a result of conduct, occurs [s 4.1 of the Criminal Code]. A fault element for a particular physical element may be: intention; or knowledge; or recklessness; or negligence [5.1 of the Criminal Code].

21 The fault element for a physical element that consists only of conduct is intention [s 5.6(1) of the Criminal Code]. A person has intention with respect to conduct if the person means to engage in that conduct [s 5.2(1) of the Criminal Code].

22 The fault element for a physical element that consists of a circumstance or a result is recklessness [s 5.6(2) of the Criminal Code], although proof of intention will also satisfy that fault element [s 5.4(4) of the Criminal Code]. A person has intention with respect to a circumstance if the person believes that the circumstance exists or will exist [s 5.2(2) of the Criminal Code], and has intention with respect to a result if the person means to bring that result about or is aware that it will occur in the ordinary course of events [s 5.2(3) of the Criminal Code]. A person is reckless with respect to a circumstance or a result if the person is aware of a substantial risk that the circumstance exists or will exist, or that the result will occur, and, having regard to the circumstances known to the person, it is unjustifiable to take that risk [ss 5.4(1), (2) of the Criminal Code].

(Footnote references incorporated.)

1. As to the charges of unauthorised access to restricted data contrary to s 478.1(1) of the Criminal Code and in terms of the physical element/fault element taxonomy summarised in the passage quoted from *Li*, each offence charged consisted of a physical element (causing unauthorised access to restricted data) and two fault elements (an intention to cause that access and knowledge that the access was unauthorised). The legal burden of proving each of these elements beyond reasonable doubt fell on the prosecution. It was not incumbent on WO2 Randall to prove that his access was authorised. Rather, in the proof of the physical element of this offence, it was incumbent on the prosecution to prove not only that he caused access to (or modified) restricted data but that that access (or modification) was unauthorised.
2. Because s 60(1) of the DFDA creates an offence of strict liability, the effect of s 6.1(1)(a) of the Criminal Code is that there are no fault elements for any of the physical elements of that offence. However, the existence of strict liability does not make defences unavailable: ss 6.1(2), 6.1(3) of the Criminal Code.
3. The physical element of the prejudicial conduct charge was, necessarily, identical to the physical element of the charge alleging an offence against s 478.1 of the Criminal Code namely, causing unauthorised access to (or modification of) restricted data. Causing *authorised* access (or modification) could hardly be said to be prejudicial conduct. On this analysis, it was, in respect of the prejudicial conduct charge, likewise incumbent on the prosecution to prove an absence of authority beyond reasonable doubt. Because the prejudicial conduct charge was one of strict liability, the prosecution did not additionally have the legal burden of proving any fault element for the physical element of the offence, for example, that WO2 Randall knew that the access was unauthorised.
4. In context, a defence to the prejudicial conduct charge would necessarily be that WO2 Randall reasonably thoughtthat the conduct concerned was authorised; that he had at least tacit approval. That would amount to a reasonable excuse in terms of s 60(3) of the DFDA. In respect of the prejudicial conduct charges, the judge advocate summed up (see, for example, transcript, p 2370) on the basis that this would amount to a “statutory defence”. WO2 Randall’s evidence certainly raised a reasonable excuse for access defence in relation to the prejudicial conduct charges.

## The central issue

1. It was submitted on WO2 Randall’s behalf that the central issue on the appeal was whether, on the whole of the evidence, the prosecution had proved beyond reasonable doubt that he lacked authority to access the email accounts as particularised. As a general proposition and in relation to the unauthorised access (or modification) charges, this is borne out by an analysis of the evidence led at trial and the verdicts returned by the panel. For the reasons given above, it is also, in our view, the central issue in respect of the prejudicial conduct charge convictions.
2. Putting aside the conviction in respect of the prejudicial conduct alternative to Charge 8, which looks to be a special case, the charges upon which the panel has convicted WO2 Randall are those where access was either conceded by WO2 Randall or readily to be inferred from his concessions. The panel’s acquittals are readily explicable on the basis of an absence of concession as to access and the existence of a doubt, based on a concern held by the panel about the reliability of the expert evidence that CAPT Peter Martin Kimberly gave on the subject of access. Concessions by CAPT Kimberley in the course of evidence which he gave on a *voire dire*, his possible partiality and the unreliability of some of the raw data in relation to network access had, in combination, earlier been responsible for the prosecution’s decision not to proceed with certain charges. If the panel were persuaded beyond reasonable doubt that the access was unauthorised, it was no great step, in light of the evidence as to WO2 Randall’s knowledge and experience, to be likewise persuaded, for the purposes of s 478.1, that the access was intentional and known not to have been authorised.
3. Thus, in relation to the charges of unauthorised access (or modification) contrary to s 478.1 of the Criminal Code, whether want of authority was proved beyond reasonable doubt by the prosecution was indeed critical. As to the alternative prejudicial conduct charges, and assuming the legal burden fell on the prosecution, it was the same body of evidence as to authority which was critical.
4. As to formal orders and instructions, the judge advocate put this to the panel (transcript, p 2352):

It is common ground that the relevant provisions of the Defence Security Manual do apply, together with DI(G) CIS 6-1-001, Appropriate and Inappropriate Use of Information and Communications Technology Resources, exhibit 68. The [DSM] and the DI(G) have the force of general orders. It is also common ground that JTF 633 Standing Instruction OPS 06-11, DLAN User Policy, exhibit 65, and JTF 633 Standing Instruction OPS 06-09, Network Access Policy, exhibit 66, also applied. The lawfulness of such orders and instructions, their proper construction and the way in which such directions might stand with one another, are matters of law where you are bound by my direction.

To assist the understanding of the reader, we set out below an explanation, derived from the evidence, of the service acronyms used in this passage and which have not earlier been identified:

* “DI(G)” means “Defence Instructions (General)”, as made jointly by the Chief of the Defence Force and the Secretary to the Defence Department under the *Defence Act 1903* (Cth);
* “DSM” means “Defence Security Manual”; and
* “DLAN” means “Deployable Local Area Network”.

1. On the subject of authorisation, the judge advocate further directed the panel (transcript, p 2355):

On the basis of the orders and instructions applying here, the prosecution must prove:

(a) that WO2 Randall had no legitimate need to know in connection with the access in question; and

(b) that the access or modification was not sanctioned by a policy, duty statement or directive.

This, in turn, requires proof that any access or modification was not for security compliance and maintenance purposes and did not otherwise fall within the scope of WO2 Randall’s duty statement. You will recall that the latter specifically provided responsibility for provision of advice for classified information systems and deployable local area networks.

1. The judge advocate added, accurately on the evidence, that “WO2 Randall has consistently maintained that he considered that any access made by him was authorised by his position and duties”.
2. Part 2, Chapter 2.60, of the Defence Security Manual (“the DSM”), appeared at Exhibit 85. Paragraph 60.41 provided, under the heading “Access to Information and Security-Protected Assets”, the following:

Access to information and security protected assets is based on a need to know and a need to restrict to authorised people only. Access is unauthorised if it is not based on a legitimate need to know or sanctioned by a policy duty statement or directive.

This was the source of the “need to know” principle referred to in the court martial proceedings. There was no issue at the trial that each of the networks mentioned in the charges, the Deployed Defence Secret Network (“DDSN”) and the Deployed Defence Restricted Network (“DDRN”), the computers which served those networks, and the information on those computers, were “Information and Security Protected Assets” within the terms of the DSM and a “Commonwealth computer system” as pleaded in the charges. Nor was it in issue and the evidence was that the computers on these networks housed “restricted data” for the purposes of s 478.1 of the Criminal Code. What was in issue and for the prosecution to prove was that WO2 Randall had no legitimate “need to know” *and* that access (or modification) was not sanctioned by a “policy, duty statement or directive”; in others words, that the access (or modification) charged was unauthorised.

1. Neither party sought to make anything of the Defence Instructions (General) (“the DI(G)”) (Exhibit 68) mentioned in the judge advocate’s summing up. It appears to be directed to the subject of the terms on which personnel are permitted personal (as opposed to duty) access to Defence Department computer networks and what is appropriate and inappropriate personal access. It does not specify the limits of access to such networks associated with the position within the FCU to which WO2 Randall was posted. It is not necessary further to consider the DI(G).
2. Sitting under the DSM and DI(G), as apparent from the explicit reference to them in each document, are the JTF 633 Standing Instruction OPS06-11, DLAN User Policy (Exhibit 65), and the JTF 633 Standing Instruction OPS 06-09, Network Access Policy (Exhibit 66). These do give particularity to the role of the appointment held by WO2 Randall and related access rights and limits.
3. Exhibit 65 received particular prominence in the course of submissions on the appeal. It was also a restricted exhibit in the court martial proceeding. For these reasons, it is necessary to set out and consider this instruction’s contents and application, as well as the authority it conferred, in some detail but to do so in a way which respects the existing restriction.
4. This instruction expressly (at paragraph 4) applied to both networks, the DDSN and the DDRN. It identified (at paragraph 6) a hierarchy or level of user within the MEAO. There were three levels:

a. **System User.** A general user of JTF633 ICT systems who has basic access granted after an approved Network Access Request (“NAR”) has been submitted.

b. **System Administrator (SA)**. A System User who has been granted administrator privileges by virtue of their employment within TG 633.14. The roles and responsibilities of the SA are detailed in annex A.

c. **System Manager (SM)**. The SM is the senior SA within TG 633.14 and would normally be the Information System Engineer (ISE) or the Information Systems Manager (ISM). The SM is responsible for obtaining and maintaining security accreditation of the Commander Joint Operations Command (CJOPS) force assigned networks. The roles and responsibilities for the SM are detailed in annex B.

“ICT” is yet another service acronym. On the evidence, it means Australian “Information Communication and Technology”. In service parlance, a Defence Department computer connected to either or each of the two networks mentioned would be an “ICT asset”.

1. According to his “Army Other Ranks Performance Appraisal Report” of 25 April 2014 (Exhibit 73), WO2 Randall’s employment category within the FCU was “Information Systems”. The evidence was that, within this employment category and while posted to the FCU, WO2 Randall, acting as a WO1, simultaneously undertook the roles of Information System Engineer (“ISE”) and Information System Manager (“ISM”). He was also the Information System Security Officer. In terms of the hierarchy of users described in Exhibit 65, he was both a “System Administrator” and a “System Manager”. In undertaking these roles, he was what CAPT Kimberly described in evidence as a “Domino administrator”. CAPT Kimberley described (ibid) the access rights of a “Domino administrator” in this way:

[A] Domino administrator has the ability to open any mailbox they choose on the server they are connected to. And, in some cases in theatre, as was explained yesterday, they could also access mailbox between locations as well.

1. The JTF 633 Standing Instruction, which was Exhibit 65, specified (at paragraph 8) the following over-arching objective for the computers, networks and other information systems operated by JTF 633:

JTF 633 provides computer devices, networks and other electronic information systems to assist in meeting its mission objectives. To meet these objectives JTF 633 must manage these resources responsibly to maintain the confidentiality, integrity and availability of its information. This policy requires the users of information assets to comply with departmental policies and protect Defence and Government against potentially damaging reputational and legal issues.

Read in context, where, in this instruction, the words, “manage” or “management” are used, they necessarily refer to the management of the JTF 633 resources mentioned in this paragraph to the end of maintaining “the confidentiality, integrity and availability of its information”.

1. In his capacity as a “System Administrator”, WO2 Randall was bound by and had the roles and responsibilities specified in Annex A to the instruction which is Exhibit 65. Materially, this annex emphasised in its introduction the need for strict adherence to specified administration processes in order to ensure the deployable ICT systems in the MEAO performed at an optimal level to support the operational scheme of manoeuvre. It also offered the guidance that a System Administrator should have completed “Deployable Standard Operating Environment (DSEO) training”.
2. Though there was no evidence as to the formal content of “Deployable Standard Operating Environment (DSEO) training”, there was evidence, as will be seen, of what, in practice, were the necessary administrative processes for someone in WO2 Randall’s position in order to “support the operational scheme of manoeuvre”. It was common ground between the parties that, although WO2 Randall had not undertaken that course, in so far as the course was intended to ensure that System Administrators had the necessary background knowledge to undertake that role, there was no deficit in WO2 Randall’s knowledge.
3. Annex A recognised that System Administrators required a privileged level of network access but did not detail the nature and extent of this permitted access. Rather, it specified the types of accounts which System Administrators were to maintain. Consistent with the sentiments in its introduction, Annex A reiterated in its closing summary that deployable ICT systems in the MEAO were a key operational capability that required careful management and administration.
4. Given that WO2 Randall was also a “System Manager” for the purposes of standing instruction which constituted Exhibit 65, Annex B to that instruction was also applicable to his role. Materially, this annex:
   1. emphasised the critical nature of the provision of secure and reliable ICT services to the command and control of deployed ADF elements;
   2. highlighted the importance of management and maintenance of equipment to ensure that it was up-to-date; and
   3. made reference to privacy rights when personnel accessed Defence ICT systems but emphasised that users did not have a right to total anonymity.
5. The position which emerges from this instruction is that the administration and management of deployed ICT systems and related assets to the end of supporting operations was the core responsibility of a System Manager such as WO2 Randall. It was this end which governed the nature and extent of permitted access. For that purpose, a person so posted was given sweeping access privileges to network accounts. That was corroborated by CAPT Kimberley’s evidence as to the rights enjoyed by a “Domino administrator”. These included an ability to access personal email accounts on the networks for the purpose of discharging that responsibility. The existence of those rights explains why Annex B to Exhibit 65 stated (at paragraph 21) that, while users’ rights to privacy are “maintained”, “users do not have a right to total anonymity”.
6. The Chief of Army submitted that a limitation in those access privileges was to be found in paragraph 27 of Exhibit 65. That is true only in respect of personal, as opposed to duty-related, access when that paragraph is read in context. Paragraph 27 provides:

An effective test of “inappropriate” use is not a personal test. Rather, ask yourself would you be comfortable discussing the type of use with your supervisor, Commanding Officer, CJTF633, or the Chief of the Defence Force. If you have any concerns, then the usage is very probably inappropriate and must not be conducted. Detailed guidance on appropriate use can be found in ref C.

1. Paragraphs 24 to 27 of this instruction are directed to the terms on which members are granted access to the JTF 633 provided internet services for personal use. Read in context, paragraph 27 makes it plain that the list of prohibited, personal use purposes specified in paragraph 26 is not exhaustive. It imposes an overarching touchstone in respect of personal use by a member. It may be accepted that paragraph 27 of this instruction identifies types of usage which would be inappropriate unless otherwise authorised (because that usage fell within the duties of a particular appointment) but it has nothing at all to say about the network access (or modification) privileges of a member when undertaking the duties of a System Manager.
2. Given the rights of access (and modification) which WO2 Randall enjoyed, by virtue of the position which he held, the evidence led by the prosecution from the holders of the various personal accounts as to their not having given him permission to access those accounts was never, even if accepted in full by the panel, sufficient to prove absence of authority beyond reasonable doubt.
3. Exhibit 66, the JTF 633 Standing Instruction OPS 06-09, Network Access Policy, applied to all personnel deployed to the MEAO. It provided direction on access to the DDSN and DDRN by such personnel (at paragraph 4). The “MEAO Network Access Request Form”, which appeared at Annex A of the standing instruction, required an applicant, under the heading “Part C – Applicant Declaration”, to acknowledge, in relation to both networks, that he or she was “aware that the Chief Information Officer Group (CIOG) and local CIS [Communications and Information Systems] staff may access any information stored on the system for administrative purposes and the investigat[ion] of any security issues.”
4. A question arose as to the scope of the word “administrative” in Exhibit 66. Counsel for the respondent drew on evidence from the appellant at trial to submit that the term should be confined to tasks related to the appellant’s roles as an ISE and ISSO as they pertain to system management; it should not be read as encompassing other aspects of his job or personal administration. Paragraph 11 of Exhibit 65 was also said by the respondent to give some content to the term “administrative”. That paragraph provided: “For security, compliance and maintenance purposes authorised personnel monitor equipment, systems and network traffic. Breaches will be referred to the chain of command, Defence investigative authorities or the Australian Federal Police as appropriate.” It was agreed between the parties that, at the relevant times, WO2 Randall fitted within the description of “authorised personnel”. It may be observed, however, that Exhibit 66 is directed more to what a user of the networks may expect rather than to the duties and authorisation of a person in WO2 Randall’s position.
5. In terms of documentary evidence, greater particularity as to the duties undertaken by WO2 Randall when posted to the FCU was provided by the duty statement which formed part of Exhibit 73. In that document, his duties were specified as the following:

1. Assisting in the production of all CIS Operational Orders, Directives and Instructions.

2. Provision of advice for Classified Information Systems and Deployable Local Area Networks.

3. Management of UNCLAS Amenities Internet Access across the MEAO.

4. Liaison with external agencies on Information Systems Issues.

5. Attend meetings and teleconferences with BAE wrt FCU Sharepoint issues.

6. Provide direction and advice on Information systems to Squadron Communications Control Groups.

7. Supervise Information Systems projects and implementations.

8. Any other tasks assigned by the OPSO.

Within this duty statement, we understand that the meaning of the service abbreviations used is as follows:

* “wrt” means “with respect to”;
* “CIS” means “Classified Information Systems”;
* “OPSO” means “Operations Officer”; and
* “UNCLAS” means “Unclassified”.

The express reference in this duty statement to “BAE” and to “SharePoint” will be noted. It is also a feature of these specified duties that they are broadly stated (especially paragraph 7) and ultimately open-ended (having regard to paragraph 8).Nominally, this duty statement has a limited duration but in context it appears to be descriptive of WO2 Randall’s duties while posted to the FCU.

1. WO2 Randall was also the Information System Security Officer (“the ISSO”). The duties of a person in this role were detailed in Exhibit 84, the Defence Security Manual, Part 2.6 Security Officer, at Annex B:

**Information System Security Officer duties**

1. In support of a system owner, Information System Security Officers (ISSO) may be required to carry out the following duties:

a. Implement and maintain network security in accordance with the Defence Security Manual (DSM);

b. Maintain system-specific standard operating procedures;

c Maintain a system-specific security register;

d. Provide advice and briefings to that system owner and to commanders and managers on ways in which network security could be enhanced;

e. Perform administrative tasks in support of network security and the application of Defence security policies and standards as required;

f. Perform network security incident response if instructed by Defence Investigative Authorities (for further information see DSM Part 2:12 Security Incidents and Investigations);

g. Liaise with the accreditation authority and other information system security organisations within Defence, other ISSOs, Information System Security Liaison Officers (ISSLO), and security officers on matters related to network security; and

h. Undertake post-accreditation activities as required by the DSM, system-specific instructions and the Australian Government Information and Communications Technology Manual (ISM), including ongoing testing for vulnerabilities.

1. A pithy way of describing the position occupied by WO2 Randall within the FCU was offered in evidence (transcript, p 1745) by a peer of commensurate experience, WO1 Wright, in expressing his agreement with the proposition that WO2 Randall was “the top of the pile, so to speak, in terms of the technical chain of command”. WO1 Wright was familiar both with the duties undertaken in practice on deployment by a member posted to this position as well as with the particular skills and repute of WO2 Randall. As to WO2 Randall’s skills and repute, WO1 Wright was asked to assess his level of knowledge of policy during the period in 2009 in which he was deployed in the United Arab Emirates and the appellant was deployed in Afghanistan. WO1 Wright offered this view (transcript, p 1739) in his evidence in chief:

*WO2 Randall is held in high regard and there’s probably two things that I can say that he is probably very good at, from my opinion, is policy and the other one is Lotus Notes as well*. So I would defer on occasions to his knowledge because I believe he’s got a very good understanding of that.

(Emphasis added.)

1. Significantly, the evidence was that each of the networks (the DDRN and DDSN) in the theatre of operations to which WO2 Randall was deployed had Lotus Notes databases. The evidence also was that, for the purpose of discharging the duties of the position to which he was posted, he was entitled to access all Lotus Notes databases, including the personal user accounts of each of the persons mentioned in the charges.
2. When asked in examination-in-chief (transcript, p 1739) to detail the tasks on deployment of an Information System Manager, WO1 Wright stated:

Look, to list the set of tasks, accreditation is high on one of those tasks, you know, maintenance, monitoring, performance, auditing. I could go through security. I guess you advise policy, advise officers on technology. Some of the tasks that you do is development, so new technology. You provide advice. And improvements to the network would be something that you’d be responsible for as well. That’s a list but essentially *you could say anything to do with computers is the remit of the ISE and the demarcation would be the router, all the way to the user, or the computer. So anything that belongs in that space and has a remit is your responsibility. So it’s pretty wide and pretty broad and there’s a lot of sort of knowledge to be had to sort of be across it all.*

(Emphasis added.)

1. It will be noticed that WO1 Wright used the abbreviation ISE (“Information Systems Engineer”) in this answer. Immediately after giving that answer, the prosecutor specifically asked him (transcript, p 1739) about the tasks of an ISE, to which he replied:

I’m going to say the same but at a higher level. I know it’s probably not the answer but the - I guess you get a broader requirement. You look after more servers and you may step away from some of the - and may go more into policy, would be my characterisation of it.

1. In WO1 Wright’s view (transcript, p 1740), the tasks of Information System Manager and Information System Engineer were not mutually exclusive.
2. In his evidence in chief, WO1 Wright also confirmed (transcript, pp 1741-1742) that the duties of an Information System Manager included a number of tasks, amongst which were:

* planning and managing the implementation of Information Systems (“IS”) networks, domains, to assist the commander in meeting his intent;
* managing an IS node in order to provide integrated information systems support to command;
* managing IS networks and domains within the tactical environment;
* interpreting data-routing requirements and providing solutions to enable routing of data around the battlespace;
* providing advice on and managing all security aspects of IS and data protection;
* managing maintenance of IS for the purpose of assuring system accreditation;
* performing threat risk assessments on local systems for the purpose of assuring system accreditation;
* managing the conduct of trials or tests of equipment configuration at all levels; and
* acting as a communications duty officer.

1. In relation to an ISE, WO1 Wright confirmed (transcript, pp 1741-1742) that the duties of the holder of that position included:

* planning, designing and managing an integrated IS network to support the command and control of subordinate units and headquarters formations;
* acting as an equipment fleet manager for equipment controlled;
* planning future data communications and migration plans;
* interpreting the detailed plans, policies and doctrines for the deployment, employment and management of varied IS devices;
* evaluating employed IS for possible security breaches and implementing security measures to ensure an integrated security approach across the battlespace;
* planning and managing the implementation of IS networks/domains to assist the commander in meeting his or her intent;
* acting as the subject-matter expert in the operations group in his or her role as the manager of command support systems;
* liaising with strategic defence planners for the integration of tactical and operational IS;
* preparing and delivering technical orders for IS equipment configuration and deployment;
* diagnosing faulty complex systems or designing communication systems for implementing formation moves;
* managing classified electronic media;
* liaising with national and foreign service personnel in order to develop interoperable systems, communications and foster cooperation;
* maintaining the confidentiality, integrity and availability of IS applications and data through passive and active computer network defence measures; and
* instructing and counselling trainees, managing instructors and administering training.

1. None of this evidence was challenged in the cross-examination by the defence of WO1 Wright. In the course of that cross-examination, this exchange occurred (transcript, p 1746) between the Defending Officer and him in relation to WO2 Randall:

Is that, to your knowledge, his reputation more widely within the signals community? — So most of my peers would probably agree that - within our trade there are certain people that are good at certain things. Some people specialise in Cisco. Some people specialise in VoIP. WO2 Randall is very professional, a consummate professional, and *I would say his speciality is probably both Lotus Notes and policy. He’s deployed on numerous occasions and has done it more times than anybody I know. So if I have a question about it, I would ask him.*

(Emphasis added.)

Once again, the explicit reference to “Lotus Notes” will be noted.

1. As to whether, either as a System Administrator or System Manager, his understanding was that advance permission from the account holder was needed on deployment to access a personal account on a network, WO1 Wright cited multiple examples as to circumstances when access without such permission might occur. There was some exploration of this in re‑examination with the essence of that being found in this passage (see transcript, p 1760):

The examples you gave, what they are conducting - what is that hypothetical system administrator doing? — So the primary goal of a system administrator in this instance is to make the system run at its peak performance, to ensure that it’s maintained - predominantly maintained and that operational effectiveness of the system is of the highest order. They’re the three sort[s] of mandates that I think I have, or an ISE has, to that system. If you’re not doing it with those three things in mind, then, I suggest, you’re probably doing something wrong, if there’s a nefarious thing.

1. The prosecution led no evidence that any of the access events in respect of which a conviction was recorded by the panel fell outside the “three mandates” to which WO1 Wright referred. Certainly in respect of the unauthorised access (or modification) charges, and also, in our view, in respect of the prejudicial conduct charges, the legal burden of so doing so as to prove beyond reasonable doubt want of authority fell on the prosecution. It was never up to WO2 Randall to prove that any conceded access fell within these “mandates”. At most, the prosecution could point to evidence given in respect of some of the charges of so-called apologies by WO2 Randall. We deal with these below.
2. Given that its own case contained evidence that access to (or modification of) a personal email account could permissibly occur without the approval of the holder of that email account, it was never sufficient for the prosecution to prove that the account holder had not given WO2 Randall permission to access (or modify) his or her personal email account. The respondent’s description in submissions of the evidence of the personal account holders as “competing evidence” to that of WO2 Randall utterly misapprehends this feature of the prosecution evidence and the legal burden which fell on it in relation to lack of access (or modification) authority.
3. Further, it raises the distinct and reasonable possibility that, in respect of the prejudicial conduct charge convictions the panel thought that the negation of the existence of a reasonable excuse was nothing more than a matter of preferring the evidence of the personal account holders over that of WO2 Randall. For reasons already given in relation to what was present in the prosecution’s own evidentiary case, it was never so confined.
4. This same misapprehension by the prosecution and possibility are evident, for example, in the reference in the written submissions on appeal in respect of Charges 4, 5 and 6 (relating to Lieutenant (“LEUT”) Jagiello), to “his computers” and “his email accounts”. The prosecution’s own evidence was that these computers were “ICT assets” owned by the Commonwealth of Australia, not by an individual member, and that no member permitted to have a personal account on the networks had exclusive dominion over that account. That is an apt note upon which to consider the position in relation to particular convictions against the background of the evidence as to authority.

## Charges 4, 5 and 6

1. These charges relate to an alleged accessing without authority of LEUT Jagiello’s DDSN account on 28 May 2014 at 0539 hours (Charge 4) and on 30 May 2014 at 0719 hours (Charge 5) and of his DDRN account on 28 May 2014 at 1010 hours (Charge 6). WO2 Randall gave evidence that he was not sure what the access to the account on 30 May 2014 involved but that it “would have been … work related”; he thought it may have had to do with LEUT Jagiello’s SameTime instant messaging. Each of the emails accessed on 28 May 2014 related to the SharePoint project. The SharePoint project, it will be recalled, fell expressly within WO2 Randall’s duties. LEUT Jagiello was but one of the addressees to these emails. WO2 Randall was not an addressee. LEUT Jagiello gave evidence that, in the past, WO2 Randall had been afforded access by LEUT Jagiello to emails concerning SharePoint which he had received. This had occurred by LEUT Jagiello forwarding the emails to WO2 Randall. Where they differed was whether express permission had been given in respect of the accessing of these emails. WO2 Randall’s evidence was that he had been told by LEUT Jagiello of his receipt of these emails, expressed an interest in reading them and been told that they were in his (LEUT Jagiello’s) email. His evidence was that their further conversation on this subject had been interrupted but that, based on past practice, he thought that he had approval from LEUT Jagiello. His further evidence was that, in any event, he had responsibilities in relation to configuring and managing SharePoint on the JTF 633 systems and related dealings with BAE Systems.
2. The “apology” in respect of access to these emails which LEUT Jagiello related as having been given to him by WO2 Randall was, at best, equivocal and included, on LEUT Jagiello’s own account given at trial (transcript, p 91), this passage:

These are the words that he was using?— … He said, “I know I needed to access them. I should have asked you beforehand,” because - we had a good peer-to-peer relationship, so if he asked me specifically for an email I would forward it to him.

Had you done that in the past?—Yes, I had, in the past.

1. It may be accepted that access to these emails was either expressly or implicitly conceded by WO2 Randall. What was never conceded was want of authority.
2. In respect of WO2 Randall’s duties and access rights, acceptance of LEUT Jagiello’s evidence by the panel was never, in itself, determinative of a want of authority. Contrary to the respondent’s submission, it was not the case in respect of these charges that the panel’s verdict was nothing more than a preference by the panel for LEUT Jagiello’s evidence over that of WO2 Randall. The disposition of these charges cannot be explained by an advantage enjoyed by the panel in seeing and hearing these two witnesses. Even if the panel rejected WO2 Randall’s evidence, there remained LEUT Jagiello’s evidence as to WO2 Randall’s assertion of a “need to know” and, in any event, an apparent “need to know” on his part arising from the prosecution’s other documentary and oral evidence, described above, as to the breadth of WO2 Randall’s duties (which expressly included duties in relation to SharePoint and BAE Systems)and access rights. Further, there was nothing in this additional evidence which expressly proved that LEUT Jagiello’s permission was needed in order for WO2 Randall to access official emails addressed to LEUT Jagiello, as opposed to his personal emails. The emails in question were duty-related, not personal. The prosecution’s other oral evidence (from WO1 Wright) and its documentary evidence contained no such qualification. Further, to the extent that LEUT Jagiello’s evidence went to WO2 Randall’s belief as to the existence of some need to obtain permission, that belief was never evidence that such a requirement truly existed, having regard to the terms of the manuals, instructions and duty statements and practices on deployment, which also formed part of the prosecution case.
3. When this additional evidence is taken into account, the result, in our view, is that, on the whole of the evidence, it was unreasonable to conclude that absence of authority was proved beyond reasonable doubt. There exists the significant possibility that an innocent man has been convicted in circumstances which cannot be explained by an advantage enjoyed by the panel. That being so, these convictions must be quashed.

## Charge 8

1. The primary charge in this instance was an alleged breach of s 478.1 of the Criminal Code. That charge, as particularised, was as follows:

**Unauthorised access to restricted data**

Being a defence member in Al Minhad Air Base, United Arab Emirates, on 05 May 2014, did intentionally cause unauthorised access to restricted data held in a Commonwealth computer, knowing that the access was unauthorised, by accessing the email account of CAPT Ami Hansen on the ADF Deployed Defence Secret Network.

**Particulars**

1. On 05 May 2014 at about 1049h, WO1 Randall accessed the Lotus Notes email account of CAPT Ami Hansen, titled *ami.hansen* (“the email account”).

2. The email account was held on a Commonwealth computer system, and had been restricted in its accessibility by way of an access control system associated with a function of the computer, namely a username and password for access to the computer network, as well as system-based restrictions that limited who could open email accounts to the relevant user, system administrators and specifically authorised personnel.

3. WO1 Randall used his administrator privileges to access the email account without authorisation.

The panel acquitted WO2 Randall in respect of this primary charge.

1. It is, with all respect to the panel members, distinctly odd to have acquitted WO2 Randall in relation to the primary charge and yet convicted him in respect of the alternative, prejudicial conduct charge. As to the physical element, the conduct alleged to constitute prejudicial conduct, unauthorised access, was the same as that particularised in respect of the alleged breach of s 478.1 of the Criminal Code. The primary charge contained fault elements whereas the alternative prejudicial conduct charge did not. In theory, the panel might have been satisfied in each instance that the physical element of unauthorised access was proved beyond reasonable doubt, not so satisfied in respect of the fault elements in relation to the s 478.1 of the Criminal Code charge, but not satisfied on the balance of probabilities that WO2 Randall had a reasonable excuse for access under s 60(3) of the DFDA. However, given that the first of the Hansen emails, which was accessed on 5 May 2014, concerned an update of SharePoint “look and feel”, such a reconciliation is untenable in light of the prosecution’s documentary and oral evidence (described above) as to the nature and extent on deployment of WO2 Randall’s duties, which expressly included SharePoint responsibilities. The panel could not have been satisfied beyond reasonable doubt that the appellant’s purpose in accessing LEUT Hansen’s email account on 5 May 2014 was not in order to perform duties in relation to SharePoint, a reasonable hypothesis consistent with his innocence.
2. Charge 8 and its alternative were the only charges where the fact of WO2 Randall’s access to the subject email account was not expressly conceded by him or readily inferred from his concessions. He had no recollection of accessing the email account. But there was evidence, independent of CAPT Kimberley’s evidence, that WO2 Randall had accessed LEUT (the reference to her rank as CAPT in the charges is an error of no moment) Hansen’s email account on 5 May 2015 at 1049 hours. So much was accepted by WO2 Randall in his submissions on the appeal. His submissions focussed on the want of proof of absence of authority.
3. Of the emails accessed and copied, as already noted, the first one was in respect of SharePoint. At or about the same time, also accessed was an exchange of emails concerning LEUT Ami Hansen’s participation in 2013 in a visit by a party of Australian service personnel to a United States warship, USS Boxer. WO2 Randall’s evidence was that he had no recollection of effecting this access but assumed from the SharePoint topic that he had needed to access that email and that he must have been requested to access the USS Boxer emails by someone. He readily accepted in his evidence that the USS Boxer exchange was of no interest to him either personally or professionally. There was no other evidence at all which would suggest that he had any personal reason for wanting to access the emails related to the USS Boxer visit.
4. For like reasons to those which we have given in respect of Charges 4, 5 and 6, LEUT Hansen’s evidence as to an absence of permission by her was never a sufficient proof of want of authority. Also for like reasons, when one takes into account the other documentary and oral evidence led by the prosecution as to the nature and extent of WO2 Randall’s duties and access rights on deployment, it was, in our view, on the whole of the evidence, unreasonable to conclude that absence of authority was proved beyond reasonable doubt. The very incongruity of accessing the SharePoint-related email for which, in light of its subject, there was an obvious reason on the prosecution’s own evidence and, at or about the same time, accessing the USS Boxer emails for purportedly non-official purposes, raised an interrogative note which was never negatived by the prosecution in terms of proof of want of authority.

## Charges 12 and 13

1. These two charges are best considered in conjunction with Charges 9, 10 and 11. That is because each related to CAPT Healy’s deployed email accounts. Charges 9, 10, 11 and 12 related, respectively, to her DDSN account on 17 April 2014 at about 1608 hours, 19 May 2014 at about 1316 hours, 3 June 2014 at about 1207 hours and 8 June 2014 at about 1253 hours. Charge 13 related to her DDRN account on 8 June 2014 at about 1257 hours.
2. The panel acquitted WO2 Randall in respect of Charges 9, 10 and 11. One possible explanation for that is that they were not satisfied that his accessing of the account concerned as alleged was proved beyond reasonable doubt. On these charges, in evidence, WO2 Randall expressly conceded access only in respect of the occasions alleged in Charges 12 and 13. So the verdicts of acquittal and conviction are not necessarily inconsistent and WO2 Randall did not seek to overturn these convictions on this basis.
3. WO2 Randall’s explanation for accessing the emails was that he undertook this in order to ascertain the meaning of a particular military acronym otherwise unfamiliar to him in order to complete a situation report (“SITREP”) for Headquarters, Joint Operations Command (“JOC”). That he had such a purpose could not, in light of s 476.2(2) of the Criminal Code, be regarded as inconsistent with the existence of authorisation.
4. Once again, CAPT Melissa Healy’s evidence as to an absence of having given personal access permission to WO2 Randall was never in itself sufficient to prove absence of access authority in respect of these two charges. Nor was her evidence of an “apology” by WO2 Randall, which really amounted to nothing more than a confession of access. The prosecution never expressly proved that the nature and extent of the duties and access rights of an ISE (or System Manager, if that be any different) did not extend to the preparation of a SITREP or to accessing the network for purposes related to that preparation. The documentary evidence (Exhibit 65) and oral evidence (given by WO1 Wright) was at least consistent with the existence of such a duty and related access rights.
5. The respondent submitted that the panel was entitled to use service knowledge in order to conclude that, in conjunction with CAPT Healy’s evidence, want of authority had been proved beyond reasonable doubt as completing a SITREP may well have been part of the appellant’s general staff responsibilities but was not an aspect of his specific roles as the ISE or ISSO. No case authority was cited for this proposition. The point raised is nonetheless an important one in relation to service discipline law generally and warrants detailed consideration. Further, observations which we make on this subject are applicable not just to Charges 12 and 13 but to each of the charges upon which a conviction was recorded.
6. In relation to the use of service knowledge by a court martial panel, s 147 of the DFDA materially provides:

**147 Judicial notice of service matters**

(1) In addition to the matters of which judicial notice may be taken by a court under the rules of evidence referred to in section 146, a court martial … shall take judicial notice of all matters within the general service knowledge of the tribunal or of its members.

…

1. This provision has a very lengthy provenance in service discipline law. It may be traced back at least to the rules of procedure made under the *Army Act 1881* (UK), 44 & 45 Vict, c 58. Those rules were revised or remade from time to time as occasion was thought fit as a result of amendments to that Act. Rule 74 of the *Rules of Procedure 1907* (UK) made under that Act provided:

74. The court may take judicial notice of all matters of notoriety, *including all matters within their general military knowledge.*

(Emphasis added.)

In the British *Manual of Military Law* (1907, War Office) the commentary in respect of rule 74 includes the following at Chapter VI, p 58, paragraph 10:

Thus, evidence need not be given as to the relative rank of officers, *as to the general duties, authorities, and obligations of different members of the service*, or generally as to any matters which an officer, as such, may reasonably be expected to know (a). Nor, again, would it be necessary to prove that an important battle was fought on the 18th of June, 1815.

(Emphasis added.)

As is not uncommon in this work, no authority is cited for this commentary.

1. The 1941 Australian edition of the *Manual of Military Law* (1941, Military Board) repeated, without qualification, the British commentary in respect of rule 74 (see Chapter VI, p 77, paragraph 11).
2. Such is the similarity of language, the British commentary in respect of rule 74 was undoubtedly the source of the following statement (at paragraph 1071) in the Explanatory Memorandum in respect of clause 147 in the Bill which became the DFDA:

1071. The expression “general service knowledge” is taken to mean knowledge of matters relating to an arm of the Defence Force which are matters of general knowledge in that arm (eg, matters such as relative ranks of members or the general duties, obligations and authority of different classes of members).

The explanatory memorandum also notes (at p 268 and paragraph 1072) that cl 147 reflected existing Australian law applicable to courts-martial by virtue of rule 74 of the *Rules of Procedure* *1947* (UK) and by virtue of s 58(2) of the *Naval Discipline Act 1957* (UK), 5 & 6 Eliz 2, c 53.

1. The *Army Act 1881* (UK), 44 & 45 Vict, c 58, re-enacted, with some amendments, the major reforms made to British military law by the *Army Discipline and Regulation Act 1879* (UK), 42 & 43 Vict, c 33. That Act, for the first time, enacted a comprehensive service disciplinary code for the British Army in place of the hitherto disparate provisions found in statutes and the Articles of War. Those statutory reforms and the related rules of procedure were, unsurprisingly, influential in respect of the service discipline law of former colonies within the then British Empire and, later, of members the Commonwealth of Nations.
2. Notwithstanding this breadth of application and influence and the vast number of personnel who served in British or Commonwealth forces in the world and other wars of the twentieth century, and the related volume of service discipline cases, authority concerning the meaning and effect of rule 74 is sparse. In his article, “Courts-Martial Appeals in Australia” (1964) 1 *Federal Law Review* 95, Mr K P Enderby, Barrister-at-Law (afterwards, Commonwealth Attorney-General and then Enderby J of the Supreme Court of New South Wales), with commendable scholarship, refers (at p 120) to two unreported cases, one Canadian, the other British, concerning the proof of prejudicial conduct charges in which, seemingly, the permissible evidentiary application of a provision akin to rule 74 and s 147 of the DFDA was considered:

[I]n *Reg. v. Owen* [(1961) No. 18, unreported], the Canadian Board … said

... the judicial notice of general service knowledge introduced a highly speculative element because of inadequate and meagre prosecution evidence; [but] in the present case there is clearly established a set of facts to which the general military knowledge of the Court can be applied without introducing an element of difficult speculation, for the appellant.

In *Reg. v. Jarman* [(1953) No. 21, unreported] the English court allowed the use of general service knowledge in circumstances consistent with the Canadian test.

(Citations incorporated.)

1. In neither of the excerpts cited by Mr Enderby is there discussion of what may be the permissible limits of the use of general service knowledge to establish guilt once other facts are proved. On this subject, we have located a judgment of Nigeria’s ultimate appellate court, the Supreme Court of Nigeria, *Nigerian Air Force v Obiosa* (2003) 4 NWLR (pt 810) 233; (2003) 1 NILR 311. Such is the dearth of authority in relation to the permissible use of general service knowledge and as this is a considered judgment of an ultimate appellate court, it is desirable to refer to this case in detail.
2. One of the issues in *Nigerian Air Force* *v Obiosa* concerned the permissible evidentiary use of general service knowledge in Nigerian Air Force discipline law, which contained a provision akin to s 147 of the DFDA. As related in the judgment, Nigeria’s *Manual of Air Force Law*, Chapter VI, paragraph 6(a) contained the following commentary:

[C]ourt[s] martial are specially authorized to take notice of all matters within their general service knowledge. Evidence therefore need not be given as to the relative rank of officers, as to the general duties, obligations and authority of different members of the service, or generally as to any matter which an officer as such might reasonably be expected to know.

As with the explanatory memorandum in respect of what is now s 147 of the DFDA, the influence of the commentary in the British *Manual of Military Law*, in respect of rule 74, on this commentary, in respect of the Nigerian analogue, is inferentially likely. That there is such a provision and related commentary should not be surprising, given the British heritage of Nigeria’s armed forces and its membership of the Commonwealth of Nations. The respondent, Obiosa, was, at the time of the charge, a Squadron Leader in the Nigerian Air Force. Materially, he was charged (Count 14) with “disobedience to a standing order, contrary to Section 57(l) of the Armed Forces Decree, 1993 (Nigeria) in that he at Lagos in April. 96, contravened Administrative Instruction S/No 3 dated Feb., 96 which Order was known to him or which he might reasonably be expected to know by engaging in private business.” Section 57(1) of the Armed Forces Decree provided:

A person subject to service law under this Decree who contravenes or fails to comply with a provision of an order to which this section applies, *being a provision known to him, or which he might reasonably be expected to know* is guilty [of an] offence under this section and liable to imprisonment for a term not exceeding two years or any less punishment provided by decree.

(Emphasis added.)

The order in question, Administrative Instruction S/No 3 of February 1996, was in these terms:

Except as authorised by HQ, NAF, an officer or airman is not to:

(1) Carry on any profession, engage in trade or accept any profitable employment while still in the NAF service.

(2) Be a member of the governing body of any corporation, company, partnership, undertaking or individual which or who is carrying on any trade, profession or is engaged in trade or is profitably employed.

The respondent was convicted in respect of this and other offences by a general court martial but these convictions were quashed on appeal by Nigeria’s intermediate appellate court, the Court of Appeal. From this order, the Chief of Air Force appealed to the Supreme Court of Nigeria. The Chief of Air Force was successful, save in respect of the issue raised concerning count 14 and relating to the permissible use of general service knowledge.

1. The question raised in relation to count 14 was “[w]hether or not the evidence led by the prosecution in respect of the 14th count had been sufficient to ground a conviction”. One of the issues raised under this ground by the respondent was whether the Court, having regard to its ability to take judicial notice of general service knowledge, could take judicial notice of the fact that an officer was aware of the order; the respondent argued that it was not permissible for an administrative instruction to be “judicially noticed”. Relatedly, the respondent also argued that knowledge by the respondent could not be presumed but must be proved. A second issue was whether there was sufficient proof that the respondent had contravened the administrative instrument: the mere appearance of a person’s name on a particular form was said to be insufficient evidence that that person was participating in the management or running of a business. As to this issue, Akintola Olufemi Ejiwunmi JSC, in delivering the judgment of a unanimous court, stated:

There can be no doubt that the above provision enable[s] courts martial to take judicial notice of all matters within their general service knowledge. Hence, evidence need not be given as to the relative ranks of officers, as to the general duties, obligations and authority of different members of the service, or generally as to any matter which an officer as such might reasonably be expected to know. But the case in hand has raised two questions[. First] can judicial notice be taken that an officer was aware of the order for which the respondent was charged? If for present purpose such knowledge could be presumed, the next question then is, whether the court martial could properly without any evidence to the effect know that an officer was carrying on any profession, etc while still in the NAF [Nigerian Air Force] service? I think not. It is my humble view that in order to successfully establish that the respondent was engaged in any other trade, profession or had accepted any profitable employment while still in the NAF service, there must be credited evidence other than what [Form] C07 revealed that [effect]. As no such evidence had been proved in respect of the 14th count against the respondent, the appeal against the decision of the [court] below must fail. It is therefore dismissed accordingly.

The reference in the passage quoted to “form C07” is a reference to a form containing the particulars of company directors filed with the Corporate Affairs Commission.

1. *Nigerian Air Force* *v Obiosa* thus contains express approval of commentary, in respect of rule 74 in the British *Manual of Military Law*, which is repeated in the explanatory memorandum in respect of s 147 of the DFDA. It also exemplifies, implicitly, if not expressly, a limit as to the permissible evidentiary use of such a provision.
2. We respectfully agree with the view expressed in *Nigerian Air Force* *v Obiosa* as to what a provision such as s 147 of the DFDA permits. It follows that we agree with the view expressed in the explanatory memorandum. But a provision such as s 147 of the DFDA is not a universal palliative for evidentiary deficiencies otherwise present in a prosecution case. The subject must, truly, be one of “general service knowledge”. The relevant subject in *Nigerian Air Force* *v Obiosa*, engaging in other employment or being the member of the governing body of a corporation while a defence member, was, with respect, clearly not a subject of service knowledge, general or otherwise, at all.
3. This is reflected in two paragraphs of the explanatory memorandum of the DFDA which precede the paragraph quoted above at [99]:

1069. Clause 147 requires a service tribunal to take judicial notice of matters within the general service knowledge of the tribunal or its members.

1070. The expressions “judicial notice” and “general service knowledge” are not defined. The expression “judicial notice” means the act by which a court will, of its own motion and without the production of evidence, take cognizance of matters which are so notorious or clearly established that formal evidence of their existence is unnecessary (eg, matters of law and custom and matters of common knowledge and everyday life).

1. On examination, the limits of the duties and rights of access of the position held by WO2 Randall are not a subject for the application of general service knowledge. Those duties and rights of access are the subject of express documentary provision in instructions and duty statements mentioned. General service knowledge could not be used to contradict what is found in these documents.
2. In relation to prejudicial conduct charges, general service knowledge can permissibly be used in the objective assessment of whether particular proved conduct is likely to prejudice the discipline of, or bring discredit on, the Defence Force contrary to s 60 of the DFDA. *Komljenovic v Chief of Navy* (2017) 319 FLR 215; [2017] ADFDAT 4 offers a recent example of the application by a Defence Force Magistrate, upheld on appeal, of general service knowledge so as to convict a naval officer of an offence of prejudicial conduct constituted by an act of physical intimacy whilst in public and in view of fellow crew member view on short term shore leave on deployment abroad. If, however, that relationship had been expressly recognised and authorised under a relevant instruction, which extended to the circumstances of the charged conduct, no amount of general service knowledge as to the likelihood that the conduct would nonetheless prejudice the discipline of, or bring discredit on, the Defence Force could have been used to contradict the authorisation.
3. General service knowledge, as with the worldly experience of a jury, doubtless has a role also to play in the assessment by a panel of witness credibility. This use apart, there may conceivably also be occasions when, if it is to be relied upon by the prosecution for a particular proof, procedural fairness may dictate that advance notice be given of this intention. However, it is neither necessary nor desirable to canvas the limits of permissible application of general service knowledge in relation to the proof of service offences. It is enough for present purposes for us to state that, for the reasons given, general service knowledge does not offer an adequate explanation for any want of proof of authority in respect of Charges 12 and 13 or, for that matter, any other of the charges in respect of which the panel has recorded convictions.
4. The convictions in respect of these charges must therefore be quashed.

## Charges 14, 15 and 16

1. Charge 14 related to WO2 Randall’s accessing on 19 February 2014 an email from CAPT Kimberley to a Mr Campbell in connection with employment opportunities at BAE Systems. Charge 15 related to his moving this email from CAPT Kimberley’s “sent items” into his own email account inbox on the same date. Charge 16 related to a second access by WO2 Randall to CAPT Kimberley’s account also on 19 February 2014.
2. WO2 Randall gave evidence that he had accessed the Charge 14 email as a management function. His further evidence, which was also relevant to Charge 15, was that, as part of his maintenance of the system, he had to remove the email as it was blocking the system and had put it in his own account. In relation to Charge 16 his evidence was that he had accessed CAPT Kimberley’s email account to see if the email to Mr Campbell had actually been sent, which he confirmed later in a telephone conversation with Mr Campbell who told him that he had received the email.
3. For reasons already given, in detailing the responsibilities and authorities which he had as a System Manager, System Administrator, the Information System Engineer and a Domino administrator, as specified in his duty statement and in practice by WO1 Wright, WO2 Randall had express authority to access this email account and to remove from it an email causing blockage. Absence of permission from CAPT Kimberley was never sufficient proof of lack of authority. Further, in light of WO2 Randall’s evidence as to his purposes, it was, and is, not possible, given the evidence as to his authority, to exclude beyond reasonable doubt a hypothesis consistent with his innocence. He also had express authority to deal with BAE Systems as part of his duties.
4. The convictions in respect of these charges are not maintainable.

## Alternative to Charge 19 and Charge 22

1. Charge 19 and its alternative related to WO2 Randall’s accessing two emails in the DDSN email account of WO1 Saunders on 29 December 2013. WO2 Randall admitted to this. His evidence was that he was justified in so doing, because he knew that there were emails related to the upgrade of the phone system that existed, he had asked for them and didn’t get them so he went in and took them for himself (transcript, pp 1948-1949). Charge 22 related to access by WO2 Randall to the email account of WO1 Saunders on 15 May 2014. He also admitted to this. His evidence (at transcript, p 1950) was that he became aware of the email concerned and that the email “contained a whole heap of configuration entries and who was doing them. That was very much in my realm”. He stated that he took it “as it was directly relevant to what I was doing at the network”.
2. Once again, and with all due respect to the panel and as with Charge 8 and its alternative, in relation to the prejudicial conduct alternative to Charge 19, it was distinctly odd to have acquitted WO2 Randall in respect of the primary charge and yet to have convicted him in respect of the alternative.
3. Be this as it may, once again, the evidence, documentary and oral, as to WO2 Randall’s authority in the position that he held and particularly his overarching responsibility in that position to maintain the system so as to support the mission of JF 633 made it unreasonable for the panel to have concluded that it was proved beyond reasonable doubt that he lacked authority to access the account. Absence of express permission from WO1 Saunders was never sufficient proof in this regard.
4. These convictions also are unsafe and unsatisfactory.

## Conclusion

1. For these reasons, the appeal should be allowed, the convictions quashed and the sentences imposed set aside.
2. We wish to add the following. The outcome differs from the conclusions of the respective reviewing officers. Unlike us, they did not have the benefit of the very focussed adversarial exchange which we enjoyed in the course of submissions on the appeal. One of the intentions of Parliament in providing for an appeal of the present kind was that its hearing would entail such a benefit.

|  |
| --- |
| I certify that the preceding one hundred and twenty one (121) numbered paragraphs are a true copy of the Reasons for Decision herein of the Honourable Justices Tracey (President), Logan (Deputy President) and Hiley (Member). |

Associate:

Dated: 10 July 2018