Blue Sky Buzz, Privacy and Data Protection

By: Devin Klassen[1]

Introduction

This article discusses four issues regarding a fact pattern focused on drone services and sales. Part I deals with two of the four issues. The first issue dealt with in Part I canvasses (as per the facts) the type of considerations Blue Sky Buzz (Blue Sky) must pay attention to when operating and selling their drone services and new drone tech within Queensland, New South Wales (NSW), and Victoria (their primary places of operation). The second issue dealt with by Part I discusses what obligations Blue Sky must fulfil to be confident they will be able to export their new drone to the European Union. Part II deals with Blue Sky's rights and obligations regarding their optical and telecommunications monitoring of staff. Lastly, Part III discusses the potential offences that 'Nell Mangel' may face for his/her (presumed his) actions connected with privacy breach and fraud. Given the discrete nature of each of the parts of this article, no overarching conclusion is appropriate.

PART I

Using and Selling Drones in Queensland, Victoria, New South Wales, and the EU

1.1 Statutory Regulation within Australia

Regarding both the commercial operation and selling of drones within Australia, there are two levels of statutory regulation, namely Commonwealth and State/Territory statutes. For this article, it is presumed that Blue Sky operates its drone services and/or seeks to market its upcoming drone technology (within Australia) solely within the states of Queensland, NSW, and Victoria. Additionally, as Blue Sky operates in several states and is developing and marketing new drone technology, it is likely that Blue Sky has annual revenues in excess of three million dollars and therefore falls under the Commonwealth's *Privacy Act 1988* (Cth) (Privacy Act).[2] Not only does the Privacy Act apply to Blue Sky, but also the Australian Privacy Principles apply as found in Schedule 1 of the Privacy Act.[3] Notwithstanding the Commonwealth Privacy Act, there are a number of state statutes that also apply. The state statutes are similar for most intents and purposes and create offences/prohibitions on the audio and visual recording and publishing of 'private' conversations, activities, and similar interactions. In Queensland, the primary statute is the *Invasion of Privacy Act 1971* (Qld) (QLDact).[4] For NSW, it is the *Surveillance Devices Act 2007* (NSW) (NSWact).[5] And lastly, for Victoria, the relevant act is similarly named the *Surveillance Devices Act 1999* (Vic) (VICact).[6] While the Commonwealth has a surveillance act, this act does not apply to non-government agencies and therefore is not applicable.[7] The privacy issues that Blue Sky faces are best described in relation to the laws that govern them. It should be noted that not only do persons in public not have a reasonable expectation of privacy, but

[1] BA Philosophy and Political Science, University of British Columbia.
[2] *Privacy Act 1988* (Cth) ss 6(1), 6D(1), 6DA(1).
[3] Ibid sch 1.
[4] *Invasion of Privacy Act 1971* (Qld). ('*QLDact*')
[5] *Surveillance Devices Act 2007* (NSW). ('*NSWact*')
[6] *Surveillance Devices Act 1999* (Vic). ('*Vic*')
[7] *Surveillance Devices Act 2004* (Cth) s 3.

even the overlooking onto private premises has not traditionally been protected at common law,[8] therefore, import is focussed on the statutory regimes.

1.2 *Privacy Act 1988* (Cth) and Blue Sky's Drone Services

The Privacy Act applies to Blue Sky's activity presuming Blue Sky takes in more than three million dollars per annum.[9] Blue Sky operates its drone services for the commercial purpose of surveying. This implies that Blue Sky flies its drones over large swathes of land which could include farms, mines, forests, large construction projects both residential and non, dams, roads, beaches, and more. Drone surveying is generally the collection, at the least, of optical and/or radar data by air, although some drones record audio.[10] Given the broad nature of commercial surveying, it is inevitable that Blue Sky will be flying drones over and adjacent to properties and locations which would often have persons within view. This is important as the Privacy Act is concerned with the collection of personal information that may become reasonably identifiable with an individual.[11] However, it is only to the extent that information may become reasonably identifiable with an individual that the Privacy Act (notwithstanding the APPs) may cause issues for Blue Sky. Parliamentary committees,[12] the Commonwealth AG and other commentators,[13] have noted that the Privacy Act is silent to the operation of drones. The Privacy Act would affect Blue Sky were they to disclose reasonably identifiable (personal) information, whether intentionally or by negligence as captured from the drones, presuming a lack of consent.[14] Disclosure brings penalties in the range of 60 penalty units and/or imprisonment for up to one year.[15] To avoid liability under the Privacy Act, Blue Sky should ensure that persons are not caught in the audio-visual recordings, or, if that is impossible, that such data should be redacted or deleted. Blue Sky faces other Privacy Act obligations under the APPs.

1.3 *APPs* and Blue Sky's Drone Services

The APPs are found in schedule 1 of the Privacy Act.[16] If Blue Sky has not already done so, it is expected that Blue Sky will need to formulate its own privacy policies coherent with the APPs.[17] Outside of developing an up-to-date policy that promotes understanding and transparency, Blue Sky must comply with the APPs themselves. Particular APPs important for Blue Sky are those of principles two, four, five, and six. Principles one, and seven through thirteen, are unlikely to be important should Blue Sky take the suggestions and delete or thoroughly make any collected and stored information unidentifiable with individuals; while principle three (collection of solicited information) is likely a low concern given the solicited nature of clients for drone surveying.[18] Principle two (anonymity and pseudonymity) can be satisfied should Blue Sky be certain to redact and/or destroy any possibly identifying personal info as soon as practicable. Regarding Principle four, unsolicited personal information should be satisfied in the same manner noting that many people caught on the properties are certainly not consenting parties. As for principle five it is impracticable for Blue Sky Buzz to accomplish post-facto notification of collection with any persons caught in the audio-

[8] *Lord Bernstein of Leigh v Skyviews & General Ltd* [1977] 2 All ER 902, 907; *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 1a IPR 308, 311.
[9] *Privacy Act 1988* (Cth) ss 6(1), 6D(1).
[10] Courtney Robertson, 'CASA's new drone regulations highlight the need for more robust privacy laws in Australia' (2017) 14(3) PRIVLB 48, 50. ('*Roberts*')
[11] *Privacy Act 1988* (Cth), s 6(1).
[12] Standing Committee on Social Policy and Legal Affairs, Parliament of Australia, *Eyes in the Sky Inquiry into Drones and the Regulation of Air Safety and Privacy* (Report: 14 July 2014) Chapter 4 [4.10].
[13] Statement from Attorney-General Mark Dreyfus to Timothy Pilgrim, 5 March 2013 <https://www.oaic.gov.au/media-and-speeches/statements/regulation-of-drone-technology>; *Privacy Law*, Office of the Australian Information Commissioner (OAIC), <https://www.oaic.gov.au/ privacy-law> (last visited Apr. 7, 2016), archived at <https://perma.cc/92LB-2QH3>; 'Drones and Privacy: What are my Rights?', Robert Hills, *Gotocourt.com.au*, (Web Page, 2018) <https://www.gotocourt.com.au/legal-news/drones-privacy-rights/>; *Roberts*, 48.
[14] *Privacy Act 1988*, s 80Q.
[15] Ibid.
[16] Ibid, sch 1.
[17] *Privacy Act 1988*, sch 1, app 1.3.
[18] Ibid apps 1–13.

visual data. However, a practice of posting signs in and around the area to be surveyed may be a prudent step where appropriate. Principle six, like those issues dealt with at 1.2, is best managed by prompt redaction or destruction where needed. Otherwise, Blue Sky's liability for their drone services under the Commonwealth regimes is limited.

1.4 New South Wales and Victoria Statutes

Blue Sky provides its services to NSW and Victoria; it is important that the corporation abides by the respective states' laws. Comparing the two, both NSW and Victoria have close but not matching statutes for our purposes. Notable though, the *Surveillance Devices Regulation 2014* (NSW) expresses that the VICact is a corresponding law for the purposes of the NSWact.[19] Taken collectively, the main concern for Blue Sky when operating within NSW and Victoria is the prohibitions on the recording and/or publishing of private conversations or activities, and the prohibition of the possession of such non-consensual records.

Section 7 of the NSWact and section 6 of the VICact prohibit the use of listening devices for the purposes of eavesdropping or recording private activities whether the offender is a party or not.[20] However, there is a slight difference between the two jurisdictions. In NSW an offender who unintentionally records a private conversation may be exempt from liability,[21] this intentionality excuse is not present in the VICact. This is important for Blue Sky operating in these jurisdictions to ensure they do not record or are careful to gain consent, where the drone may capture the audio recording of a private conversation or activity. In NSW, Blue Sky will most often have the unintentionality excuse but cannot avail itself of that excuse in Victoria.

Section 8 of the NSWact and section 7 of the VICact make prohibitions regarding optical surveillance.[22] The NSWact limits itself to the prohibition of operation or installation of optical devices which result in the non-consensual use or interference of the premises or vehicles facilitating the recording or being recorded.[23] The VICact on the other hand resembles the listening prohibition above and prohibits the non-consensual optical recording of any private activities.[24] The penalties for breaches of the respective statutes also differ with the VICact giving a higher penalty of up to 1200 penalty units for corporate offenders, and the NSWact maxes out at 500 penalty units for corporate offenders.[25] Blue Sky would be wise to try to keep its drone recordings tightly limited to the areas it's contracted to survey in order to avoid liability.

Lastly, both Victoria and NSW prohibit certain storage and publication of such recorded audio-visual information. NSW prohibits the publishing of non-consensual recordings, as well as the possession of such.[26] Victoria merely prohibits the non-consensual publishing of such collected information.[27] The respective penalties for corporations mirror that of the previous offences. Blue Sky should ensure that any recordings depicting private activities are promptly destroyed, and where impossible/impracticable, that such information is securely stored so as not to be published.

NSW and Victoria have legislation that exempts civil liability of any aircraft operating at a reasonable height, while Queensland does not.[28] While this statutorily protects a reasonably operating Blue Sky from nuisance/trespass claims in NSW and Victoria, it is presumed the precedent in *Berstein v Skyviews* would protect Blue Sky in a similar manner in Queensland.[29]

---

[19] *Surveillance Devices Regulation 2014* (NSW) cl 3(d).
[20] *NSWact*, s 7(1)–(2); *VICact*, s 6(1).
[21] *NSWact*, s 7(2)(c).
[22] *NSWact*, s 8(1); *VICact* s 7(1).
[23] *NSWact*, s 8(1)(a)–(b).
[24] *VICact*, s 7(1).
[25] *NSWact*, s 8(1); *VICact*, s 7(1).
[26] *NSWact*, ss 11, 12.
[27] *VICact*, s 11(1).
[28] Pam Stewart, 'Drone Danger: Remedies for damage by civilian remotely piloted aircraft to person or property on the ground in Australia' (2016) 23 *Torts Law Journal* 290, [5].
[29] *Lord Bernstein of Leigh v Skyviews & General Ltd* [1977] 2 All ER 902, 907.

1.5 Queensland Statute

When operating within Queensland, Blue Sky must be aware of the prohibitions found in the QLDact. Unlike its counterparts, the QLDact limits its prohibitions to listening devices.[30] Sections 43 and 44 prohibit the non-consensual use, recording, and publication of private conversation of parties to which the recorder is not a party to the activity.[31] Unlike in Victoria and NSW, there is nothing in the QLDact limiting Blue Sky's use of optical recording. However, Blue Sky should note that under the definition of instrument under section 4, and the purposes of 'entering' defined at section 48A(13) of the QLDact, Blue Sky could be liable for an offence of unlawful entry into a dwelling of a house where a drone equipped with a listening device trespasses into the yard or another part of a dwelling.[32] This effectively enshrines a sort of tort of trespass where audio drones are involved.

1.6 Complying with EU Obligations

In May of 2018, the EU commenced an updated privacy protection scheme known as the *General Data Protection Regulation (EU)* (GDPR).[33] These regulations govern the protection of personal information of natural persons within the EU. Blue Sky will be required to comply with the GDPR because it seeks to offer goods or services to EU data subjects.[34] Fortunately, the GDPR's definition of personal data, including its personally identifiable nature, shares a 'high degree of similarity' with that of the Privacy Act.[35] As with the Privacy Act, recital 26 of the GDPR also excludes information that is not reasonably identifiable with a natural person. But, because Blue Sky seeks to sell its drones in Europe it may have to implement certain safeguards if it processes the sales itself as EU citizens could, for instance, be using its website to place orders and enter their private information. It would be better for Blue Sky to partner with an Australian retailer to sell the drones to the EU for if it decides to directly do so itself the size and scope could require it to comply with significant GDPR obligations. Due to the burden of the legal issues tied up with this article, there is little room to go into these obligations. However, should Blue Sky 'go it alone' and be defined as a data controller or data processor pursuant to art 4 of the GDPR, then they are likely to need to appoint a data protection officer,[36] hire a representative located within the EU,[37] and create a processing registry.[38] Given the significant burden of the GDPR, it might be in Blue Sky's interest to partner with a firm specialising in reselling from Australia to the EU to shift this burden.

PART II

Surveillance in the Workplace

2.1 Cameras

The facts imply that the office of Blue Sky is in Queensland. For cameras in the workplace, the retention of certain data may be covered by the Privacy Act but otherwise the use of cameras is regulated by

[30] *QLDact*, ss 4(1), 43, 44.
[31] *QLDact*, ss 43(1)–(3), 44(1).
[32] *QLDact*, s 48A(1)–(13).
[33] *Council Directive 2016/679 on General Data Protection Regulation* [2016] OJ L 119/1, art 4(1). ('*GDPR*')
[34] Ibid recital 23.
[35] Eli Fisher, Geoff Bloom, Nupar Sachdev, '*The EU's General Data Protection Regulation: Overview, comparison to the Australian Privacy Act, and what it means for Australian organisations with EU Dealings*' (Date: Unknown) (Vol: Unknown) *Australian Privacy Reporter* (Page: Unknown). ('*Fisher*'). *Note* – This article was accessed in a non-traditional format with lack-lustre citations but in its entirety as found at 2-200 of Hein Online's 'Australian Privacy Commentary' and was otherwise inaccessible in its original form as I did not have access to the *Australian Privacy Reporter*.
[36] *GDPR*, recital 97, art 29, art 37.
[37] Ibid art 27, recital 80.
[38] Ibid art 30.

state legislation.[39] However, the QLDact does not regulate the use of optical devices.[40] Were their offices in NSW and Victoria then their respective acts would apply,[41] Presuming the Privacy Act applies as it did in Part I, Blue Sky should be careful regarding the retention of surveillance information that might capture the employees in private or personal acts for much the same reason as was discussed regarding the drone services for both collection and destruction.[42] At this point, unless the cameras are in areas of expected privacy (like a bathroom) Blue Sky is likely entitled to monitor their staff in the workplace with cameras.[43] Notably, July 2019 should see the release of a QLRC report into workplace surveillance.[44]

2.3 Internet Use and Correspondence Monitoring

Whether Blue Sky's monitoring of staff internet/e-mail use is lawful depends upon whether the staff were entitled to and/or did use such resources for personal use. Blue Sky will be in a better position where a clear policy outlining the use of the company's hardware, software, and internet services is made evident to employees and announces either/or the monitoring of the resources or the restriction of staff for using those resources for personal use.[45] Still, the Privacy Act will apply for any collection of personal information (which must be promptly destroyed) and it is not to be used for any purpose not connected to employment.[46] However, a concern is that Blue Sky may be acting unlawfully where third parties in the emails have not been notified of the potential for interception, monitoring, or storage and such emails contain personal information.[47] Blue Sky should implement a clear policy on workplace communications as well as attach a footer to their emails saying that information contained therein may be monitored/stored at or after a date unless the third party requests otherwise. This recommendation is because, unlike telephone calls which can prompt the user at the beginning, it's impossible to pre-prompt an email conversation, while automatic tracking email notification is expensive, and irritating to customers.

2.4 Interception and Recording of Telephone Calls

Blue Sky's interception and recording of calls may be unlawful. The appropriate governing statutes are the *Telecommunications (Interception and Access) Act 1979* (Cth) (INTERCEPTact) the QLDact and the *Criminal Code 1899* (Qld) (the Code). Under the INTERCEPTact, it is an offence to intercept a communication like a telephone call without notification and/or consent.[48] It is also an offence to deal with information obtained in contravention of section 7.[49] Queensland offences under the QLDact and the Code prohibit recordings in breach of expected privacy.[50] All the concerns that an audio-equipped drone raised (as found above at 1.5) also apply toward Blue Sky's recording of calls without consent. Queensland does not

---

[39] Office of the Australian Information Commissioner, *Surveillance and Monitoring*, (Web Page, No Date) < https://www.oaic.gov.au/individuals/faqs-for-individuals/law-enforcement-surveillance-photos/what-can-i-do-about-my-neighbour-s-security-camera>; Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Discussion Paper No 80, 31 March 2014) [3.20]–[3.24]. ('*Serious Invasions*')
[40] *Serious Invasions*, [13.14].
[41] *Workplace Surveillance Act 2005* (NSW); *Surveillance Devices (Workplace Privacy) Act 2006* (Vic).
[42] See, eg, *Privacy Act 1988* (Cth), s 6(1); *R v Company* [2009] PrivCmrA 21.
[43] *Criminal Code 1899* (Qld) s 227A(1); *Toll North Pty Ltd & Anor v Transport Workers' Union of Australia* [2014] FWC 2945, [80]–[86].
[44] Office of the Information Commissioner (QLD), *Camera Surveillance, video, and audio recording – a community guide*, (Web Page, 6 December 2018) < https://www.oic.qld.gov.au/guidelines/for-community-members/Information-sheets-privacy-principles/camera-surveillance,-video,-and-audio-recording-a-community-guide>.
[45] *Privacy Act 1988*, sch 1; Fair work Ombudsman (Cth), *Workplace Privacy*, (Web Page, No Date) < https://www.fairwork.gov.au/how-we-will-help/templates-and-guides/best-practice-guides/workplace-privacy>; *Carolyn Flanagan v Thales Australia Ltd* [2012] FWA 6291, [120]–[126].
[46] *R v Company* [2009] PrivCmrA 21.
[47] *Telecommunications (Interception and Access) Act 1979* (Cth) s 7(1); *Privacy Act* 1988 (Cth) s 21C(1); Peter Leonard, 'Surveillance of Workplace Communications: What are the rules?' [2014] (August) *Privacy Law Bulletin* 115, 118.
[48] *Telecommunications (Interception and Access) Act 1979* (Cth) s 7(1).
[49] Ibid s 63(1).
[50] *Criminal Code 1899* (Qld) s 227A(1).

prohibit parties recording each other without mutual consent, but a third party recording the conversation is not permissible. Nothing indicates that Blue Sky has made the parties aware that 'this call may be recorded for X purpose' likely making Blue Sky liable for prosecution and the remedies found at section 107 of the INTERCEPTact.[51]

PART III

Criminal Liability of Nell Mangel

3.1 Liable Criminal Provisions

The criminal liability for Nell Mangel is significant. Starting with the most serious crime, is the credit card fraud committed by Nell where he purchased an overseas trip with a client's information.[52] Also a criminal offence was Nell's unauthorised access of and dealing with the information found on the director's computer, presuming Nell was forbidden to use the computer and/or there were preventions in place to prevent access.[53] Additionally, Nell has committed an offence under section 80Q(1) of the Privacy Act as the information he accessed, and used, including such things as drivers license numbers, credit card numbers, and customer survey details which are identifiable with the victim qualifying as personal information under the definitions.[54] Between the fraud offence and the Privacy Act offences, Nell may face several years in prison.

3.2 Actions Blue Sky Must Take

With the introduction of a recent amendment,[55] the Privacy Act puts an obligation on Blue Sky[56] to respond to Nell's breaches of this personal information.[57] Blue Sky is not aware of what Nell has done but is on reasonable suspicion that a breach has occurred.[58] Blue Sky must immediately carry out an assessment within 30 days to establish whether a breach has actually occurred.[59] We, having the benefit of knowing a breach has occurred, know that when Blue Sky discovers the breach they must promptly prepare a written statement of the breach to the Information Commissioner describing the breach and including all available contact details for both Blue Sky and those affected.[60] After notifying the commissioner, Blue Sky must notify the affected parties of the breach with a written statement and contact information.[61]

---

[51] *Telecommunications (Interception and Access) Act 1979* (Cth) ss 107, 108.
[52] *Criminal Code Act 1899* (Qld) ss 408C(1)(a)–(b).
[53] Ibid ss 408E, 408D.
[54] *Privacy Act 1988 (Cth)* ss 6, 80Q(1).
[55] *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth).
[56] *Privacy Act 1988* (Cth) s 26WE(1)–(2)(a)(i).
[57] Ibid pt IIIC.
[58] Ibid s 26WH(1)(a).
[59] Ibid s 26WH(2)(a)–(b).
[60] Ibid s 26WK(2)–(3).
[61] Ibid s 26WL.