

## DATE

Board of Directors  
c/o Bill Reid  
Chief Legal Counsel  
Woolworths Group Limited (the "Group")  
PO Box 8000  
Baulkam Hills, NSW, 2153

Daniel Leong  
Culture and People  
Primary Connect Pty Ltd ("Primary Connect")  
70 Distribution Street  
Larapinta Qld 4110

### **Legal Questions around compulsory masking and Smart Band**

We are a group of Woolworths customers and employees.

It has come to our attention that you are imposing missives on the Primary Connect workforce requiring them to be fully masked and to also wear a Smart Band, ostensibly for "social distancing" and "contact tracing". The purpose of this letter is to ask the Group or the relevant authorities of Primary Connect to respond to the concerns raised in this letter. This letter is not legal advice.

### **Smart Band and the Law**

We would like to draw your attention to the following United States Executive Order.

<https://web.archive.org/web/20210120155311/https://www.whitehouse.gov/presidential-actions/executive-order-taking-additional-steps-addressnational-emergency-respect-significant-malicious-cyber-enabled-activities/>

We are concerned that the Group, in particular Primary Connect, may be in breach of this Executive Order through the coercive tactics being employed by Primary Connect to force its employees to wear Smart Bands.

This raises the concern that the Group and/or Primary Connect is potentially misusing US Internet Infrastructure. As I am sure you are aware US Internet Infrastructure as a Service Provider is inter alia Google, Amazon and Microsoft and all aspects of the Smart Band from Beacon, to AuthO/Okta will use at least one of these Infrastructure as a Service Provider/Product.

This Executive Order applies to the Group as it is extraterritorial in scope. Further, the

Group has ADR's registered with the US SEC and is therefore a US Person under US laws. Several of your board members are also US persons for the purposes of this Executive Order and related laws.

In particular, we would like to point you to Clause 3 C (i) which states:

“The report and recommendations provided under subsection (b) of this section shall consider existing mechanisms for such sharing and collaboration, including the Cybersecurity Information Sharing Act (6 U.S.C 1503 et seq) and shall identify any gaps in current law, policy, or procedures. The report shall also include;

(l) Information related to the operations of foreign malicious cyber actors, the means by which such actors use IaaS products within the United States, malicious capabilities and tradecraft, and the extent to which persons in the United States are compromised or unwittingly engaged in such activity.

The definition of Tradecraft refers to the techniques, methods and technologies used in modern espionage and generally as part of the activity of intelligence assessment. In other words, SPYING on people. It may even extend to using technology to inflict harm on people.

The servers of the abovementioned Infrastructure as Service Provider will be located in the US or will have a connection to the US. Therefore, all use MUST comply with United States law.

### **Questions around Smart Band**

We understand that the Employees have been provided with a print off of these FAQs in relation to Smart Band. We have also been informed that Primary Connect is instructing employees to take the Smart Bands home with them. What is the reason for this? Employers do NOT have the right to instruct what people do outside their work hours. We know you think you do through the use of repackaged military technology such as Clearforce, but the reality is it's not lawful.

<https://www.smartbadge.com.au/faqs>

Please answer the following questions. We will address the legal questions around data and consent first.

### **DATA**

1. Have you obtained fully informed consent from the employees as to the use of their data?
2. Can you represent and warrant that the employee's data is not being sold or transferred to a third party for any reason whatsoever?
3. How is the data being transferred to the relevant Government Health Authority for

“contact tracing”? In Queensland it is going through the Dept of Communities and Housing, so once again we fail to see how any of this is connected to our health.

4. How are you protecting employee’s personal data from being accessed through Bluetooth and the Nodes? Where are these Nodes located and what are these Nodes? Where are the online software portals located?

5. How can you guarantee that the data remains in Australia? Technically it should remain in the STATE where the HEALTH data is being collected. Have you ensured that this is the case?

6. The terms state that the Company can perform the contact tracing. How does this fit in with the relevant Health Departments contact tracing? Where do you derive legal authority from to perform contact tracing under (unlawful) health directives?

## **BLUETOOTH AND EMF**

Please comment on the attached Google Patent relating to EMF through “devices” <https://patents.google.com/patent/US6506148B2/en>

Please represent and warrant that the Smart Band does not utilise this technology. Further represent and warrant that the use of the Smart Band will not cause any harm either intentional or non-intentional to your employees.

There is evidence that Fitbits use the Beacon technology that the Smart Band uses. Fitbits may cause the following in humans. See the link below. Please represent and warrant that you have conducted proper health and safety testing on the Smart Bands and that you can guarantee to your employee’s their health and wellbeing will not be adversely affected in any way. Please pay careful attention to the following article.

<https://educateemf.com/fitbit-emf-radiation/>

## **MODERN SLAVERY AND HUMAN RIGHTS ASSESSMENTS**

1. Have you done a Modern Slavery Risk Assessment and can you represent and warrant that forcing people to wear tracking devices is not in breach of either the Modern Slavery Act 2019 (Cth) or the relevant Human Rights legislation as well as any relevant provisions under the Commonwealth Criminal Code relating to Modern Slavery. We urge you to carefully consider all international obligations in relation to Human Rights.

2. Have you sought legal advice under the Work Health and Safety Act particularly in relation to the Bluetooth and EMF issues mentioned above.

3. Have you done a Human Rights audit as to whether forcing employees to wear tracking devices is not a breach of their Human Rights?. Have you considered that this is very similar to the situation in Xinjiang where Uighurs are forced to wear digital tracking devices?

Please see this article for a discussion of how the human rights of Uighurs are abused in China through the use of digital technology.

<https://theintercept.com/2021/01/29/china-uyghur-muslim-surveillance-police/>

We suggest you seek advice from your Reputation Management team immediately as this is not a good parallel to be drawn for the Group and/or Primary Connect. We consider that it will be extremely difficult for the Group/Primary Connect to make an honest representation that these devices are for the purposes advised to your employees. They appear to be surveillance and tracking devices. This is NOT appropriate.

### **Beacon Software and Beacon Technology**

Please confirm or deny if Beacon Technology is part of Project Beacon which is backed by both Google and Apple. Please advise if you have disclosed this to the employees. This technology is a smart IOT (Internet of Things) device. Please explain IN DETAIL how the data stays in the relevant state AND is limited to the purpose of contact tracing ONLY by the relevant Department of Health during the period of the State of Emergency for "COVID".

### **AuthO and Okta**

We understand that AuthO is the authentication and authorization gateway for the "Smart Band". We also understand that AuthO was recently acquired by Okta. Please see attached a Press Release.

<https://www.okta.com/press-room/press-releases/okta-signs-agreement-to-acquire-auth0/>

As per the previous questions can you please advise how this is related to contact tracing for a limited period for a pandemic by the relevant Department of Health.

### **Ownership of Okta**

We note that several of the Shareholders of Okta are also major shareholders of the Group. Have you taken legal advice on Conflicts of Interest?

### **US Privacy Laws**

The US privacy law framework does not allow for people's data to be used for any purpose OTHER than a public safety issue (which must have a sunset clause AND a statement that their data will NOT be used for any other purpose other than the "current soon be over" COVID 1984).

Can you please comment on whether the Group has built these conditions into the

agreements with the Infrastructure Service Provider and/or with the relevant State Government entity? Have you notified the employees whose data you are coercively collecting of these safeguards as required by US law and Australian Commonwealth and State laws?

Can you represent and warrant that the Group is not selling or otherwise using the data that is being collected for purposes OTHER than “contact tracing”. i.e you are not selling data to foreign or domestic governments/entities to be used for surveillance (which will be in contravention of all national laws on surveillance of nationals and the US FISA Acts) or using the data for other purposes such as analytics for commercial activities and therefore profiting from the collection of this data through coercion and without fully informed consent of the owner of that data.

As you are aware, in order to make use of the data of the data owner you MUST obtain fully informed consent. Coerced consent is NOT consent. The employees of the Group are not products nor are they slaves who must give up their privacy for the “greater good”. They also don’t need their employer tracking their health, their habits and their movements. This is a GROSS violation of privacy and if it is being done for a hostile state actor it is also a criminal offence in multiple jurisdictions.

**Please provide the internal privacy policy on the Smart Bands which must include full disclosure of the above questions. As we know employees must consent to the privacy policy. If they do not consent, and you seek to either discipline them or terminate their employment, this letter may be used in a court of law.**

### **Forced Masking**

It is well known that masks are health hazards. Prolonged wearing can also do irreparable damage to a person’s physiology (including bacterial lung infections) as well as their mental health. There is also ZERO evidence they assist in stopping COVID. Please advise what legitimate strongly debated medical evidence (PRE 2020) you used regarding the decisions around masks.

We attach TWO articles for you from reputable sources about the dangerous chemicals contained in face masks that you are requiring people wear throughout their entire shift. They discuss Phthalates and other chemicals such as Graphene in face masks. There are many articles available. Please do some research and seek legal advice.

<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7381927/>

<https://www.ecotextile.com/2021040127603/dyes-chemicals-news/exclusive-chemicalcocktail-found-in-face-masks.html>

It is not difficult to conclude that an agenda is being implemented that has nothing to do with anyone's health. In fact, the intention seems to be to cause harm to people's health, and to their wellbeing and happiness at work as well as "change culture".

We do hope suitable due diligence has been done on the people within Primary Connect who are driving these initiatives and therefore "culture change". We remind you of the provisions of the laws around Foreign Interference and the Commonwealth Crimes Act which protect Australians. We also remind you that Australia is NOT Communist China.

We implore you to seek legal advice on these issues. Your employees are loyal to Woolworths and so are your customers. However, we must draw the line at the people bringing our food to us being coerced to be tracked like animals and masked like slaves. Nobody is your slave and human rights are not negotiable.

Regards

**YOUR NAME AND CONTACT DETAILS (OR):**

**A concerned member of the Commonwealth of Australia**