Power Protect Pty Ltd
Ph 1300 877 626
www.powerprotect.com.au
service@powerprotect.com.au

27 January 21

Right to Repair
Productivity Commission
4 National Circuit
Barton ACT 2600

Re: Submission to Productivity Commission Right to Repair Inquiry

I am a qualified Electrician and for over 11 years have been the Director of Power Protect Pty Ltd, a privately owned Australian company that specialises in service and repair of primarily Uninterruptible Power Supply (UPS) and Diesel Generator equipment.

Throughout my career I have seen a range of practices that OEMs put in place to restrict the ability for third parties to carry out servicing and repair of the products they sell. The purpose of these restrictions is to limit the availability of service support for these products to the OEM's own service departments and "authorised service partners". In fact Power Protect has been engaged as an authorised service partner for a number of different manufacturers over the years of its operation.

The equipment that we support serves a critical role in ensuring continuity of power to very important equipment and as such typically undergoes frequent service inspections and maintenance, usually on a monthly or quarterly basis. I believe that the consumers who own this equipment, which includes private individuals and businesses, should have the right to choose who carries out maintenance and repair to their equipment and not be limited to use of the OEM service department or authorised service partners through the restrictive mechanisms that OEM companies put in place.

I will detail below some of the typical restrictive mechanisms that I have seen OEM's use to ensure repairs and maintenance are restricted to their authorised channels. OEM's claim that the control of service information and tools is to protect their intellectual property. While in extreme cases this may hold merit, the majority of applications for the service information and tools relates to basic configuration items and resetting of simple alarms. The control by the OEM of the software or information to perform these basic adjustments or alarm acknowledgements frequently sees OEMs charging in the vicinity of $1,200 to $1,600 exclusive of GST for what amounts to a very simple task. This amount can increase for regional locations. Additionally we have witnessed that some OEMs will charge a higher rate to an independent service provider that they see as a competitor, than they offer to the end-user, with the intent of driving the customer away from the independent service provider.

Out of this review I would like to see a mandatory code of conduct adopted that relates to all products, not just those specified in this submission, that prevent manufacturers from restricting access to basic configuration and clearing of service alarms. Additionally, to provide fair access on commercial terms to detailed service and repair information, in a similar manner to that proposed in the automotive industry.

If you require any additional information please do not hesitate to contact me.

Regards,

Jason Marriott

Appendix A - Examples of basic configuration and alarms that require intervention by an OEM or authorised partner

Below are some examples of basic configurations and alarms that occur on UPS and Generator equipment. Third party service providers and even the end-users own staff often have the knowledge and experience to work on the equipment however are unable to perform these basic functions as the access to them is restricted via OEM proprietary software. It is frequently the case, particularly for third party service providers, that companies or individuals who have previously received training and held certification to use the proprietary software are no longer provided access to the software. OEMs will use methods highlighted in Appendix B to restrict the ongoing access to this software.

Examples 1 and 2 are circumstances where a third party might carry out a routine inspection or complete a parts replacement to the same standard or better than the manufacturer however to reset the alarm that has occurred an OEM may charge $1600+GST or more to attend site and plug in a laptop for 15 minutes to perform the reset. This practice substantially increases the cost to the end user and provides a protected revenue stream to the OEM service department.

Examples 3 & 4 are circumstances where configurations and adjustments do not impact the inherent safety and reliability of the product, or impinge on the IP of the OEM, yet the OEM may cite these as reasons why the configurations and adjustments require the proprietary software.

1. An alarm notifying that a service is required. This is a time based alarm typically occurring on an annual basis. This is typically indicated by a fault light (amber or red) on the control panel and an alarm message. The equipment may allow the alarm to be acknowledged (silenced) however this may only pause the alarm for a period of 48 hours to 14 days and usually the fault indicator remains present. The only way the alarm can be reset fully, returning all indicators to green, is via proprietary software controlled by the OEM.

2. An alarm notifying that component replacement is required. Where the alarm is caused by the active monitoring of component performance and a failure has actually occurred the alarm is usually cleared by replacement of the failed component. Far more common particularly with Uninterrupted Power Supplies is the practice of a time-based alarm that will trigger after a pre-set time has elapsed. This is a preventative measure to alert the customer that the relevant component has reached the end of its reliable service life and should be replaced. While this is valid, most of these components can be replaced by suitably experienced technicians, and the parts are frequently commercially available outside the OEM. The resetting of the alarm however can often only be performed with proprietary software or codes controlled by the manufacturer.

3. Configurable inputs and outputs. The control system on a UPS or Generator typically has the ability to take a variety of input signals and provide output signals for a variety of statuses. Frequently there is a limit to the physical connections available and as such the inputs and outputs must be configured through software so the correct status is linked to the correct terminal. The configuration of these inputs and outputs is usually only possible via proprietary software controlled by the OEM. In the event that an end user wants to for example add an additional status to monitor that the generator is running the OEM must be engaged to enable that status with the proprietary software.

4. Basic parameter adjustments. There are many basic parameters within UPS and Generator control systems that can be configured to suit the end user requirements and the application for which it has been installed. It is typical for the OEM to set these up as required at the time of commissioning, however these settings may need to be adjusted through the life of the equipment. A sample of the types of basic settings that might require adjustment are:

    a. Output voltage (ie 230VAC or 240VAC)
    b. Number of batteries
    c. Charge rate (or capacity) of batteries
    d. Adjustable time delays (ie generator start after loss of mains)
    e. Frequency of service alarms
    f. Time, temperature, or other alarm limits

Appendix B - Methods used by OEMs to restrict the access to equipment, applications and information

Below are some examples of how OEMs restrict access to codes or proprietary software used for the service and repair of their equipment. Most OEMs supplying equipment in this industry will engage authorised service partners to ensure that the OEM can provide support in regions where they lack the in-house service capability however they are contracted to deal exclusively with the OEM. This means that they can only perform "authorised service" when acting on behalf of the OEM and are contractually restricted from working on OEM equipment for anyone other than the OEM.

1. Service Codes – OEMs will design equipment with a special code required to access service settings. These codes are often leaked or discovered and end up available to parties outside the authorised service providers

2. Dynamic Service Codes – To enter the service menu the code is different each time, this may be a table of codes that is relevant to the product that changes month to month, or a code that is generated based on the equipment serial number and date of the visit. Codes are typically issued by the OEM to partners on an annual basis or as needed.

3. Proprietary Software – Access to proprietary software can be controlled at time of installation or constantly throughout its use. Modern proprietary software can utilise the availability of internet connectivity to routinely ensure the validity of the installation and allows an OEM to remotely disable the software at any time. Software can also be licence based where the user must purchase a licence to operate the software for a specific period, typically annually. In this case licences are only sold to authorised parties.

There are two specific cases I will detail below where an OEM has exercised control over their proprietary software under circumstances which I feel the Right to Repair inquiry should address as it was anti-competitive in nature

1. Manufacturer X engaged Power Protect as a non-exclusive reseller and authorised service provider for their equipment. Power Protect supplied Manufacturer X's equipment into a customer site and sold Manufacturer X's service contract with the understanding that Power Protect would be engaged by Manufacturer X to carry out the service on their behalf as authorised service agent, using Manufacture X's proprietary software. Twelve months later Power Protect commenced as a non-exclusive reseller and authorised service provider for Manufacturer Y. Upon learning of this, Manufacturer X remotely disabled the proprietary software without notifying Power Protect, preventing Power Protect from meeting its contractual obligations with the customer and damaging its reputation.

2. Manufacturer Z permits equipment end users access to their proprietary software for an annual licence fee. Power Protect acted on behalf of their end user client to secure the hardware and software licence to manage the assets as the government department client does not have a facility to deal directly with Manufacturer Z. Upon the licence expiring Manufacturer Z advised Power Protect that the licence would no longer be made available as Manufacturer Z views Power Protect as a direct competitor.