Certificate of Volatility

Manufacturer: Xerox

Equipment Name: WorkCentre

Model: 5030 – 5050 Copier

Configuration: This item is standalone_____X_____.

General description: Standalone Digital Copier

Purpose: Monochrome Copier

Type of memory:

Volatile memory: What is the amount? What period of time does the unit need to be powered off to completely erase this memory?

User Interface Volatile memory:
DRAM: 8 MB
Flash ROM: 8 MB

Marking Engine Volatile memory:
EPC DRAM: 64-96 MB
SRAM: 16 MB
Flash ROM 8 MB

Scanner Volatile Memory:
SRAM: 128 KB
DADF firmware: 8 KB (DADF=Digital Automatic Document Feeder)

Other Memory Devices
There are other memory devices in the multi-functional device, but these are used solely for low level I/O control. Some examples of this distributed control are:
· Power distribution, Photoreceptor and main drive motors control
· Raster Output Scanner (ROS)
· Paper Registration
· Finisher
No user image data is stored in any of these memory devices.

Video Volatile Memory:
There are also a number of RAM buffers in the video path that are used for image manipulation (Reduce/Enlarge, etc.), and all have no data retention capability. When power is removed all data is lost. These buffers are typically built into the ASICs.

Typical bleed down time for all volatile memory is 10 seconds.

Non-Volatile Memory:

1. **Type:** What type(s) of non-volatile memory are included, EPROM, EEPROM, Flash memory, NVRAM, and battery backed, etc. (fill in)

Marking Engine Non-Volatile Memory:
NVRAM 32 KB / 128 KB, battery back-up

2. **Accessibility:** Is it accessible by accidental/intentional keystroke, or software malfunction?
No. However, the login system administrator or service technician (via diagnostic operation) may adjust certain machine operational parameters. User data is never accessible.

3. If "YES, it **is** accessible, describe location and purpose.
Purpose: typical uses for non-volatile memory location are system identification number and system configuration, boot, and initialization parameters, for example (battery-backed NVRAM on SUNs); put in for future design needs, internal depot repair, clock circuit, "nice" to have, or to flag unauthorized software, etc.

If "NO", it is not accessible, ____**X**___ (Check here).

4 *Required memory:* Is device needed for normal operation, i.e. required for this processing period?
All memory listed is required for normal operation.

5. *Removal consequences:* If device memory chip is erased, what impact will this have on operation and normal function of device?

Example: If the SUN is turned on without this means of checking for the authorized configuration, the system will not boot and therefore the data cannot be processed per the standard Practice Procedure (SPP).
ROM/PROM memory device content is required and essential for operation and normal function of the device. Loss would render the device inoperable.
ROM/PROM memory, as stated above, never contains user data. This memory is never overwritten or erased during normal operation.
DRAM/SRAM memory processes user data. DRAM/SRAM is overwritten with test data at each power off and power on cycle.

6. *Method of access:* How is it accessed? Is non-volatile memory location theoretically accessible with any system code, not just via the operating system or low level booting firmware?
Marking Engine non-volatile memory is used for storing Multifunction Device application settings and is accessible by application level code.

Remember: Modifying internal programming to access is not the same thing as unknowingly accessing from an accidental keyboard stroke.

7. *Warranty:* Does chip removal or EEPROM erasure void the warranty?

Yes, chip removal or EEPROM erasure will void the warranty.

8. *Size:* How much memory is contained? Number of bytes, etc.
See pg 1, Type of Memory

9. *Spacing:* Is the memory fully utilized or does it have available memory space for additional information to be placed?
The non-volatile memory devices are sized to contain the necessary amount of data required for system operation. Usually there are some unused memory addresses where additional information could be theoretically stored. Without access to the software developers' memory maps, determining the location of this unused memory would require reverse-engineering the software.

Certificate of Volatility, continued

10. Can this non-volatile memory be addressed to ensure that only authorized information is resident? If yes, how?
At boot-up, the system computes a checksum for each non-volatile memory device. (Note: The computed checksum is compared against a value stored in the device itself. This is sufficient to detect hardware failures, but not necessarily intentional corruption.)

Evaluation and summary of this equipment was completed by the following:

R. Cusick (Signature)

Randall R. Cusick (Printed name)

Technical Marketing Manager (Title)

Product Security Program Manager (Job function)