CERIAS

Protecting Consumer Privacy in Reusable Digital Devices

Brad Moseng & Marc Rogers, PhD.

Abstract

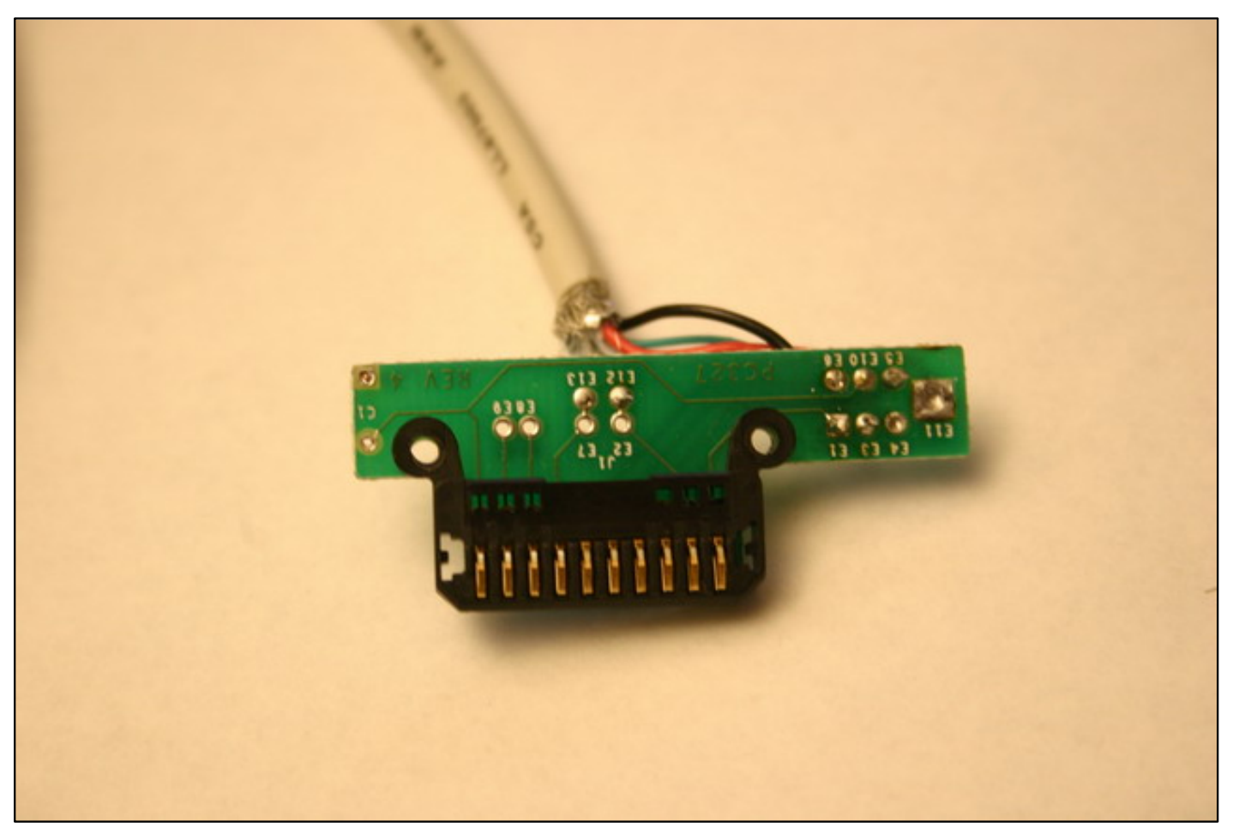
The increasing use of disposable digital devices is leading to expanding vulnerabilities in personal privacy. In an effort to bring digital devices to the mass populace, manufacturers have started to market single-use, recyclable digital devices. One such device, the Dakota single-use digital camera, is designed to compete in the disposable photography market. However, with reusable digital devices, there is often sensitive residual data left behind from previous users. The purpose of this research is to determine if Pure Digital, the makers of the Dakota camera, are providing enough data security in their device recycling process.

The Problem

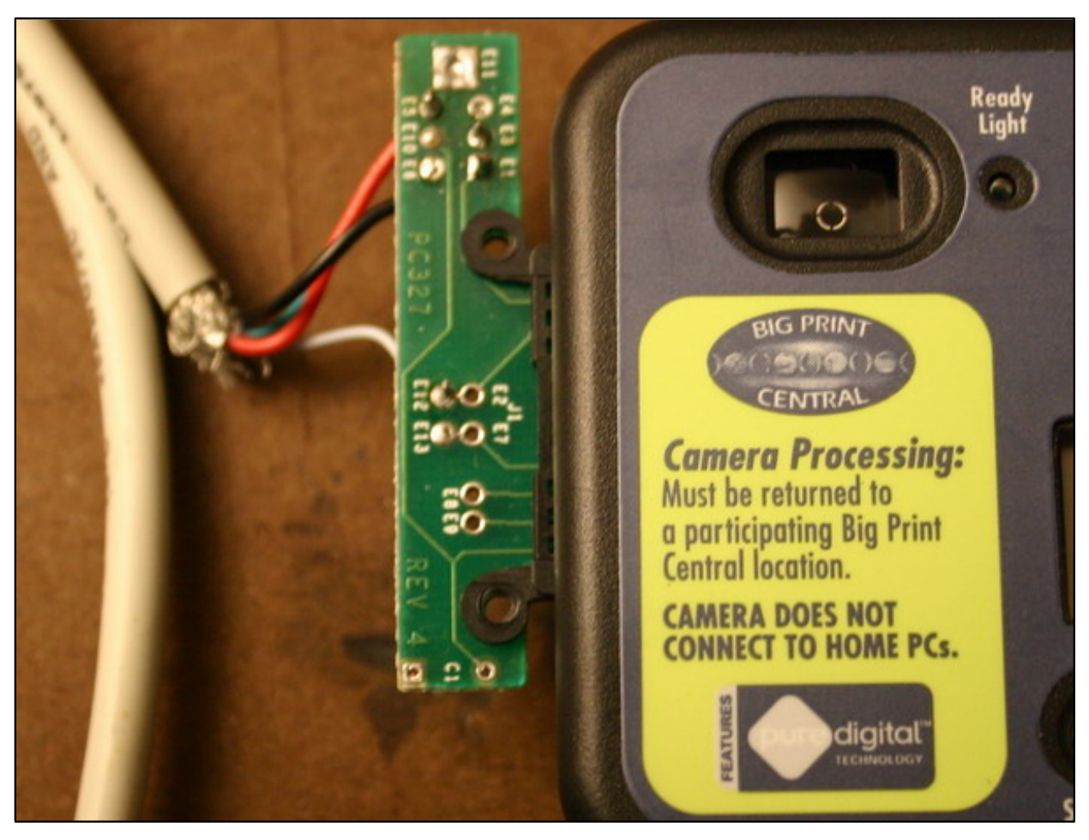
The prohibitive costs to entry in many digital areas have led industry to create a new market of multiple-use devices designed to make the technologies available to everyone. These disposable devices are sold for a price well below the cost of equipment construction, and cost of the device is defrayed in small increments as its services are used. For example, reusable digital cameras are sold far below the cost of traditional digital cameras. In turn, the cameras must be returned, and the consumer receives printed photos for a processing fee. Emerging devices, such as reusable digital cameras, are shrouded by unknown technology and intellectual property protection; consequently, there is little research to ensure this new market is protecting the privacy of its growing set of customers. Are companies developing reusable technology with effective means to protect privacy by properly cleaning devices?

Testing Methodology

To begin, a custom USB data transfer cable was built to provide a standardized link between the analysis PC and camera’s data port. For the purpose of this study, the cable was fabricated using a common USB cable and a data connector salvaged from a Palm III sync cradle. Once the hardware connection is made, specialized USB drivers were installed to allow access to the digital camera via a program dubbed “Single-Use Camera Reader” (SUCR). SUCR was then used to create an bitwise image of the data found in camera’s flash memory. Using a hex editor and several other forensic tools, this bitwise image was investigated for residual image data.



USB Data Sync Cable


Ready Light
BIG PRINT CENTRAL
Camera Processing:
Must be returned to a participating Big Print Central location.
CAMERA DOES NOT CONNECT TO HOME PCs.
digital

Data Connection

Results

This study was punctuated by two distinct setbacks that provided a great deal of information. After initial data analysis proved to be unsuccessful using the connection techniques described above, further investigation revealed that the research camera was in fact a revision of the original Dakota reusable camera. The new revised edition included new security measures, in both hardware and software, to eliminate non-proprietary methods of accessing camera data. The second setback occurred when, after the six-hour memory dumping process, the resulting data images were completely blank. Using the XVI32 hex editor to look at the data from the camera showed that the entire flash memory block consisted of FF**h**, the equivalent of blank space. A blank disk is the likely result of one of two scenarios; either the test cameras had never been used, or the recycling process has effectively protected the privacy of its consumers.

PURDUE
UNIVERSITY

CERIAS®

Discovery Park
e-Enterprise Center