

AFFIDAVIT OF DANIEL LOPRESTI

I declare under penalty of perjury under the laws of Pennsylvania that the following is true and correct.

1. I am the Chair of the Department of Computer Science and Engineering at Lehigh University. I was a founding research staff member at the Matsushita Information Technology Laboratory in Princeton, and later served on the research staff at Bell Labs working on document analysis, handwriting recognition, and biometric security. At Lehigh, my research examines fundamental algorithmic and systems-related questions in pattern recognition, bioinformatics, and computer security.

2. I submit this affidavit in support of petitions to recount/re canvass the vote in Philadelphia County and Montgomery County.

3. I believe that the direct recording electronic (“DRE”) voting machines used throughout Pennsylvania, including Philadelphia and Montgomery counties, are vulnerable to fraud, tampering, and hacking, and are unreliable.

The Machines Used in Philadelphia and Montgomery Counties Are Vulnerable

4. In early 2007, I acquired a Danaher Shouptronic (“Shouptronic”) 1242 full-face DRE voting machine, the type of electronic voting machine used in Philadelphia County.¹

I examined the machine and supervised its dismantling by a Lehigh student to understand how the machine functions and to identify its vulnerabilities. This included identifying the ROM chip which stores the machine’s firmware (i.e., built-in programming) and the microprocessor that controls the operation of the machine. I also reviewed the

¹ See <https://www.verifiedvoting.org/verifier/#year/2016/state/42/county/101>.

manufacturer's manual entitled "Shouptronic 1242 Election System Information and Technical Specifications." (Shouptronic is now known as Danaher.)

5. At the same time, I also acquired a Sequoia AVC Advantage full-face DRE, the type of voting machine used in Montgomery County. Along with another Lehigh student, I opened the rear panel of the Advantage and examined its construction. This included identifying the ROM chips which store the machine's firmware (i.e., built-in programming) and the microprocessor that controls the operation of the machine. I also reviewed the manufacturer's manual on security entitled "AVC Advantage Security Overview."

6. In my opinion, none of the DREs certified in Pennsylvania, including the AVC Advantage and the Shouptronic 1242, is capable of retaining a permanent physical record of each vote cast as required by the Pennsylvania Election Code. As such, the machines cannot be said to reflect the actual tally of votes with 100% certainty.

7. My opinions are based on by own independent review and knowledge of the types of machines in question, as well as well-documented results of later examinations conducted by independent technical experts in other states that have identified serious security vulnerabilities in DRE systems that had previously been certified for use in Pennsylvania. Voting systems deemed acceptable for use in Pennsylvania were later found to be unacceptable for use in California and Ohio based on evaluations using testing methodologies widely known and practiced in the field of software security.

How DRE Machines Work

8. Each DRE voting system is designed to, and ostensibly does, record the voter's choices on various forms of computer memory. Electronic memory technologies used in DRE systems include:

- a. RAM (random access memory): electronic memory that is freely readable and writable under software control, but whose contents are not maintained when electrical power is turned off to the system. RAM can be further subdivided into "dynamic" RAM, or DRAM, and "static" RAM, or SRAM, a distinction which is important at the hardware level but not with respect to how information is stored. Because RAM is volatile memory, it is most often used for the temporary storage of data and program code in voting systems, and not for information which must be maintained after the machine is turned off. RAM is the most common form of memory in a computer system, so generic references to "computer memory" or "internal memory" usually refer to RAM. DRE systems sometimes provide a small amount of SRAM with a battery backup so that its contents can be maintained over time.
- b. PROM (programmable read-only memory): memory which is permanently programmed at the time of manufacture and hence is unalterable. As a result, PROM is used in "read-only" mode. PROM cannot be used to store vote data, rather, it is used in DRE systems to hold the machine's program code (firmware). PROM is often socketed to make it easier for the manufacturer of the system to install firmware updates by swapping a newer PROM chip for an older one without risking damage to the circuit board.

- c. EPROM (erasable programmable read-only memory): non-volatile memory that can be programmed using a device that supplies higher voltages than a standard electronic circuit used for other memory technologies. Because EPROM is non-volatile, it retains its data even after electric power has been turned off. The contents of an EPROM are erased by exposing the chip to strong ultraviolet light; an EPROM must be erased before data can be written to it. EPROM can be used to hold firmware and/or vote data. Exposure to normal light may make EPROM storage unreliable as most forms of light (including daylight) contain some amount of ultraviolet light. EPROMS are often found socketed for ease of replacement.
- d. EEPROM (electrically erasable programmable read-only memory): non-volatile memory that can be read and written in a standard electronic circuit. In this way EEPROM is similar to RAM, although it retains its data when power is turned off and is more expensive than RAM.
- e. Flash memory: a form of EEPROM that differs from traditional EEPROM in the way the memory is written: byte-wise writable memories are typically referred to as EEPROM, whereas block-wise writable memories are referred to as Flash memory.
- f. PCMCIA ("Personal Computer Memory Card International Association"): frequently referenced in the voting machine literature, PCMCIA is not a memory technology, but rather a form factor and interface specification originally developed for memory expansion in laptop computers. A PCMCIA card may contain RAM or flash memory and is typically the size of a credit

card. Some PCMCIA memory devices may have a “write-protect” option, but this has no effect until the feature is activated, usually through manually moving a physical switch to a pre-specified position.

9. The Shouptronic 1242 records voter choices in six different computer memory locations. Each machine uses a memory cartridge which is inserted in the back of the machine. The memory cartridge contains the ballot definition files which allows the machine to conduct elections. The cartridge also contains three distinct memories for storing vote data: one EPROM and two EEPROMs. Vote data is also stored inside the Shouptronic 1242 itself in three separate RAM locations.

10. The AVC Advantage full-face push button DRE voting system loads ballot definitions and stores vote data using a “Results Cartridge” PCMCIA card. The Advantage system also contains internal memory upon which vote data is stored.

The DRE Machines Are Unreliable and Susceptible to Tampering and Fraud

11. None of the computer memory technologies identified in the preceding paragraphs provide a permanent physical record of each vote cast. Rather, these systems maintain what is best described as an “electronic record” of the activity that occurs on the machine. The accuracy or permanence of data stored electronically cannot be guaranteed due to the inherent characteristics of electronic computer memory. All of the forms of computer memory used in the DRE voting systems cited earlier are freely writable under software control for the period of time that an election is taking place. Computer memory can be written or rewritten with incorrect data unintentionally (as a result of software and/or hardware and/or human error) or intentionally (as a result of a malicious attempt to alter the results of an election).

12. Moreover, the act of writing computer memory is in principle undetectable; it leaves behind no physical evidence. This is true even for flash memory modules that contain a manually activated switch or fuse to disable their rewritability at the end of the election; until writability is disabled, typically at the end of the election, the contents of the flash memory may be altered in arbitrary ways. Since even the initial writing of a record into computer memory is accomplished through the use of software and hardware intermediaries, there is no way for a human observer to confirm that what is written is in fact an accurate record of his/her vote. Software-based techniques that attempt to assure the integrity of the electronic record through, for example, cryptography or digital signatures are only as trustworthy as all of the software components that interact with the computer memory during the recording and tallying of votes.

13. Both the firmware used to direct the operation of DRE voting systems and the voting records stored in computer memory within those systems are vulnerable to tampering in a number of ways. This is true even when voting systems are not connected to the Internet. For example, the PROM chips containing a DRE's firmware can be swapped in a matter of minutes by someone with minimal technical knowledge who has access to the voting machine and a simple screwdriver. Computer security experts have demonstrated how voting machine viruses can be spread in some cases through the use of contaminated memory cards, even for DRE systems that have never been connected to the Internet. Undetected flaws in the programming of a DRE system can result in errors in the electronic voting record as it is stored or retrieved from the memory within the machine. Such undetected flaws can also create opportunities for "hackers" to manipulate the voting data stored in the memory of the DRE under certain circumstances.

A Forensic Analysis Is Necessary to Fully Recanvass/Recount the Vote

14. In my opinion, review of the ballot images retrieved from computer memory is not a reliable way to recanvass and/or recount the vote. A full forensic evaluation of the DRE machines and associated supporting hardware and software (e.g., the computers and software used to program the ballot definition files) is necessary to ascertain whether the original totals reported by the DRE machines represent the votes that were cast on those machines.

15. In the above DRE systems certified for use in Pennsylvania, ballot images are stored in the same forms of computer memory as all other election data, under control of the same hardware / software components. The printed ballots are no more than a convenient, human-intelligible reproduction of the electronic record. Because of the unavoidable and fundamental dependence on software and hardware intermediaries to recover ballot images stored in computer memory, because these same software and hardware intermediaries are also responsible for maintaining and producing the original totals tapes for the election, and because all election data, including the ballot images, are generally stored in equivalent forms of electronic computer memory, simply reviewing the images would not be a reliable way to recanvass or recount the vote.

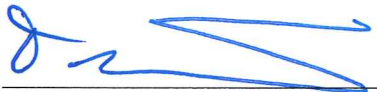
16. A full forensic evaluation of the DRE systems and associated supporting hardware and software would allow examiners to determine whether or not the information stored in the computer memory in those systems represents an accurate record of the votes that were cast on those machines.

17. Based on my knowledge of the DRE systems in place in both Montgomery County and Philadelphia County, I believe that only a full forensic evaluation, by

independent experts, of the relevant materials (detailed below) can ensure that the votes in both counties were fully and accurately counted.

- a. For the AVC Advantage machines, an independent expert must be able to forensically analyze (i) a sampling of the AVC Advantage machines including source code of the software running on those machines, (ii) the audio ballot cartridges, (iii) the results cartridges, and (iv) any computers and associated software used by Montgomery County for preparation of the AVC Advantage machines, including programming ballot definition files before the election and tallying results after the election.
- b. For the Shouptronic machines, an independent expert must be able to forensically analyze: (i) a sampling of the Shouptronic 1242 machines including source code of the software running on those machines, (ii) the results cartridges, and (iii) any computers and associated software used by Philadelphia County for preparation of the Shouptronic 1242 machines, including programming ballot definition files before the election and tallying results after the election

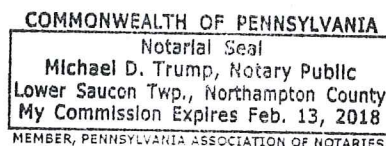
Executed on the 2 day of December, 2016 in Northampton County, Pennsylvania.



DANIEL LOPRESTI

(Commonwealth of Pennsylvania)
County of Northampton)

Sworn and subscribed to before me, A
Notary Public, this 2nd day of December,
2016 by Daniel Lopresti.



Notary Public