Security experts say: hybrid voting machines are not secure.

Examples:
ES&S ExpressVote, XL & Dominion ICE

☑ Can be HACKED – no internet connection needed.
☑ Can produce WRONG election results.
☑ Can give an election to the wrong candidate.

…and NO ONE WOULD EVER KNOW.

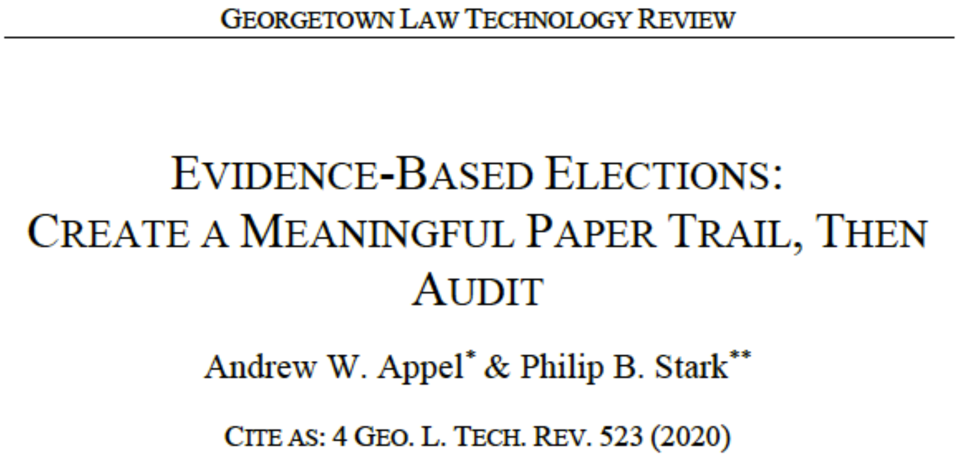
SMARTelections.us
December 2020

Security experts say: hybrid voting machines…

☑ Cannot produce a trustworthy paper ballot.
☑ Cannot be confirmed by an audit.
☑ Cannot produce results that we can have confidence in.

This is a presentation and summary of highlights from the paper:

“EVIDENCE-BASED ELECTIONS: CREATE A MEANINGFUL PAPER TRAIL, THEN AUDIT”



GEORGETOWN LAW TECHNOLOGY REVIEW

EVIDENCE-BASED ELECTIONS:
CREATE A MEANINGFUL PAPER TRAIL, THEN AUDIT

Andrew W. Appel* & Philip B. Stark**

CITE AS: 4 GEO. L. TECH. REV. 523 (2020)

The paper appeared in the *Georgetown Law Technology Review* in 2020.

It is by nationally recognized security and auditing experts:

- Andrew Appel, PhD
  - Princeton, Eugene Higgins Professor of Computer Science
  - Computer Security, Software Verification
- Philip Stark, PhD
  - UC Berkeley, Assoc Dean of Mathematical and Physical Sciences
  - Applied & Theoretical Statistics

https://georgetownlawtechreview.org/wp-content/uploads/2020/07/4.2-p523-541-Appel-Stark.pdf

Stark & Appel evaluate hybrid *(All-In-One)* ballot-marking devices:

Examples: ES&S ExpressVote, XL & Dominion ICE

*"These machines are **even less secure**—and less acceptable for use in public elections—than pure BMDs [ballot-marking devices]. The same paper path contains both the printer (for marking ballots) and the optical scanner (for scanning ballots). **The legitimate software … presumably will not print additional votes onto the ballot … but hacked software could**. **The software** … **has complete control** over all the physical functions of the paper path: printing, scanning, and paper transport. Therefore**, the hacked computer can print votes on the ballot after the voter's last opportunity to inspect the paper**."*

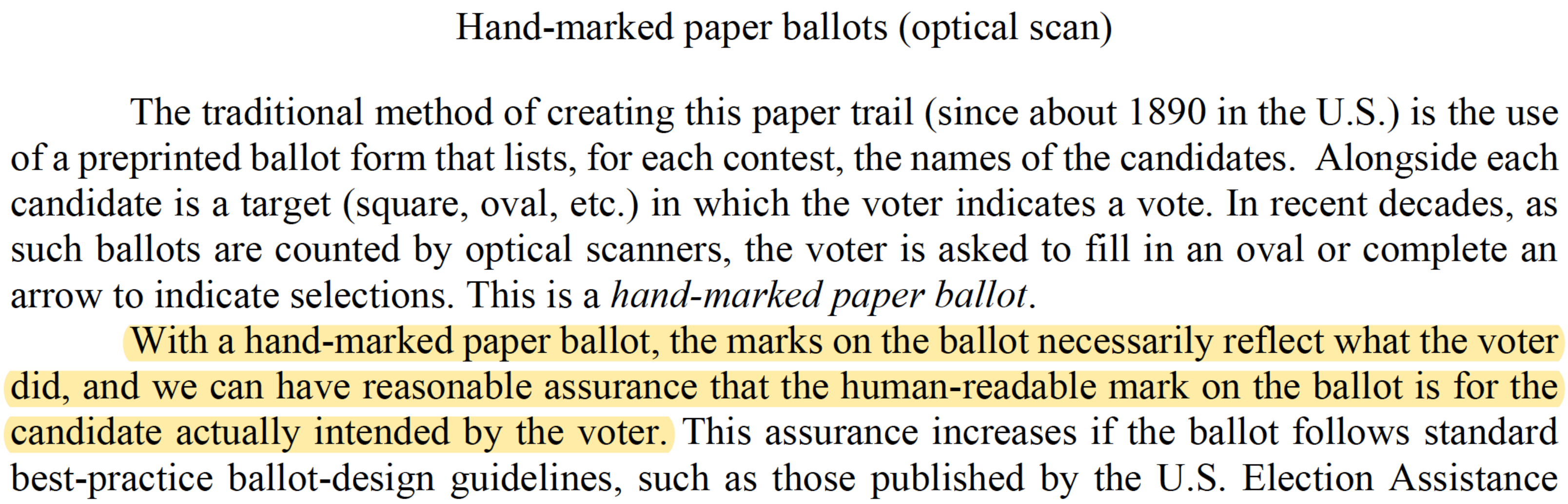
What is more reliable than a hybrid voting machine?

Hand-marked paper ballots.

☑ CAN be reliably audited.
☑ CAN give voters & candidates confidence in result.
☑ CANNOT be hacked.

- *with proper chain of custody*

“With a hand-marked paper ballot, the marks on the ballot necessarily reflect what the voter did, and we can have reasonable assurance that the human-readable mark on the ballot is for the candidate actually intended by the voter.”

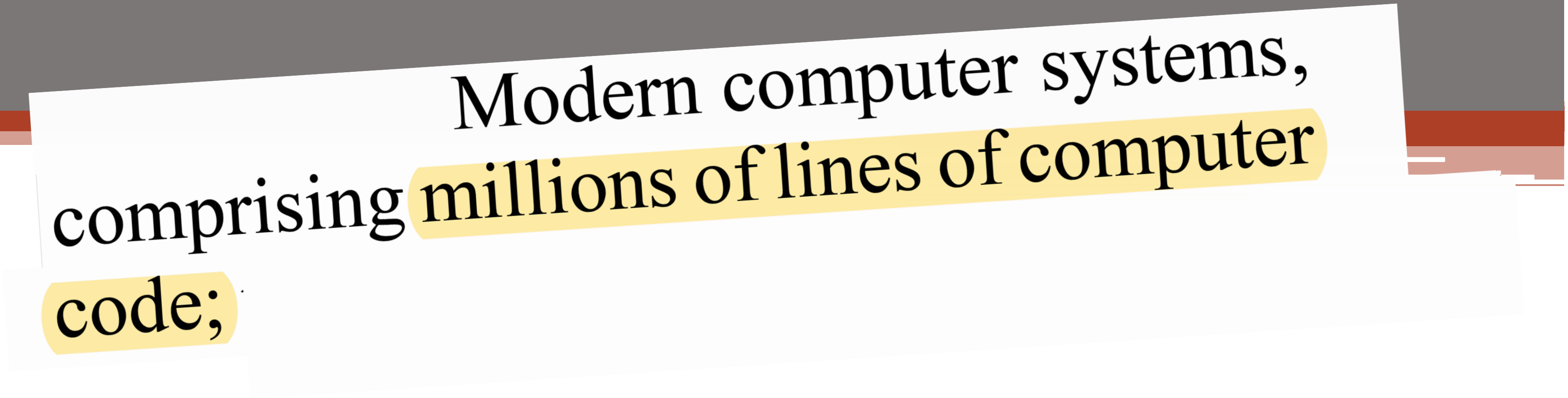


Hand-marked paper ballots (optical scan)

The traditional method of creating this paper trail (since about 1890 in the U.S.) is the use of a preprinted ballot form that lists, for each contest, the names of the candidates. Alongside each candidate is a target (square, oval, etc.) in which the voter indicates a vote. In recent decades, as such ballots are counted by optical scanners, the voter is asked to fill in an oval or complete an arrow to indicate selections. This is a *hand-marked paper ballot*.

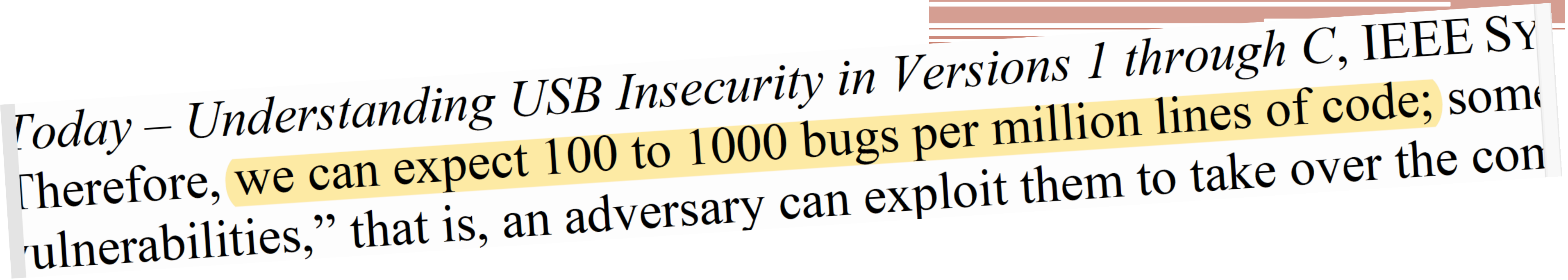
With a hand-marked paper ballot, the marks on the ballot necessarily reflect what the voter did, and we can have reasonable assurance that the human-readable mark on the ballot is for the candidate actually intended by the voter. This assurance increases if the ballot follows standard best-practice ballot-design guidelines, such as those published by the U.S. Election Assistance

Computers (voting machines) and removable drives have “***millions* of lines**” of code…

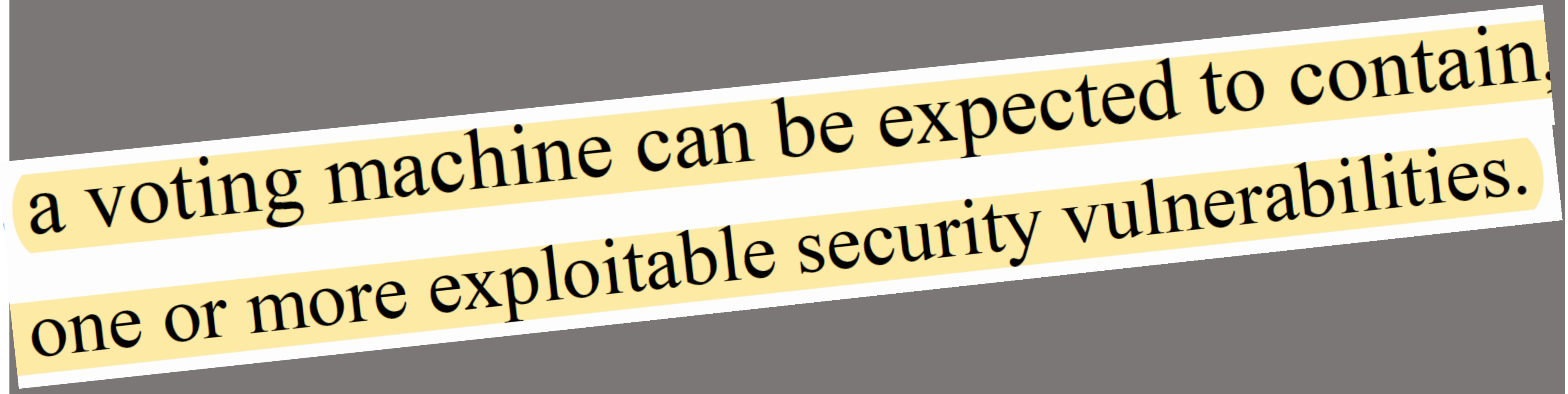


Modern computer systems, comprising millions of lines of computer code;

“…we can expect ***100 to 1000 BUGS*** per million lines of code;”



Today – Understanding USB Insecurity in Versions 1 through C, IEEE Sy
Therefore, we can expect 100 to 1000 bugs per million lines of code; some
vulnerabilities,” that is, an adversary can exploit them to take over the con



a voting machine can be expected to contain, one or more exploitable security vulnerabilities.

"…those bugs are ***security vulnerabilities that permit attackers to modify or replace the software*** in the upper layers; ***so we can never be sure that the legitimate vote-counting software … is actually the software running on election day."***

Evidence-based elections should …

☑ "Find the true winner(s) of an election"

☑ "Provide … convincing evidence that they did"

That is not possible with a hybrid (All-In-One) ballot-marking device

Examples:
ES&S ExpressVote, XL & Dominion ICE

☑ A hybrid's design is not "trustworthy."

☑ If hacked, it "can print votes on the ballot after the voter's last opportunity to inspect the paper."

Voters with disabilities need accessible voting systems that allow them to vote:

☑ Privately
☑ Independently
☑ Securely

Hybrid (All-in-One) voting systems:

☑ Do not meet this criteria

Security experts advise voters with disabilities to:

☑ Use separate devices to print and scan their ballots.

☑ Review their selected choices carefully (with the audio component if necessary) to ensure the machine has printed their selections correctly.

☑ Not send their ballots electronically.

A secure and accurate voting system must be:

☑ “Contestable”

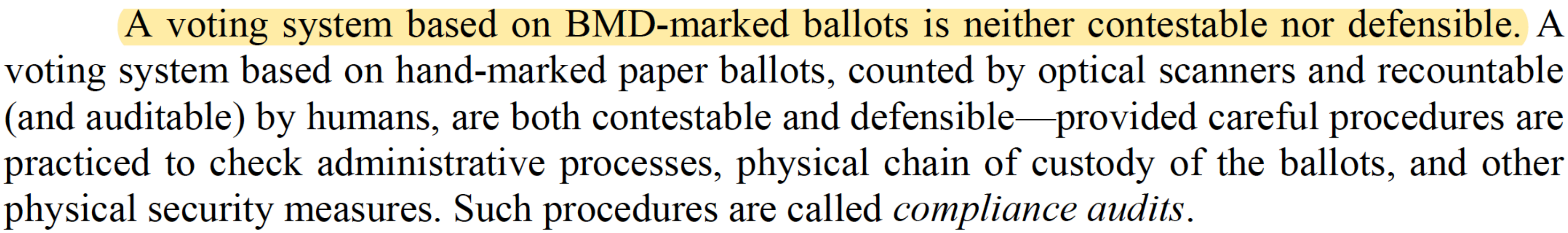
- *(if results are wrong, it can produce evidence that it is wrong)*

☑ “Defensible”

- *(if results are right, it can produce evidence that it is right)*

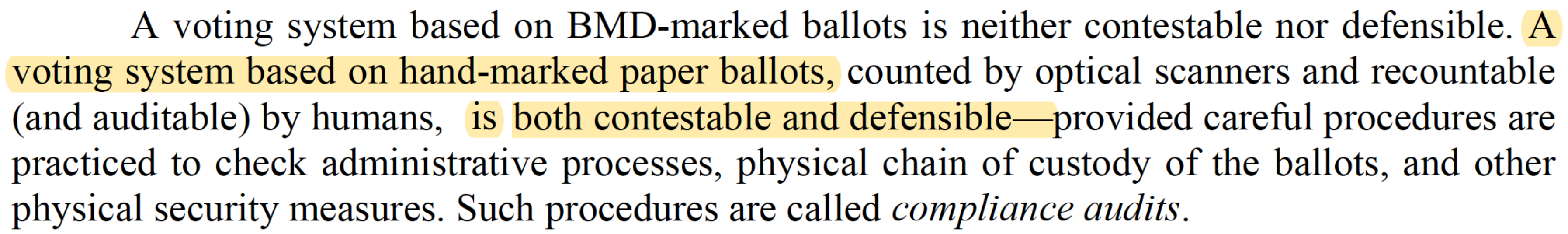
"A voting system based on BMD-marked ballots is neither contestable nor defensible."

Examples: ES&S ExpressVote, XL and Dominion ICE



A voting system based on BMD-marked ballots is neither contestable nor defensible. A voting system based on hand-marked paper ballots, counted by optical scanners and recountable (and auditable) by humans, are both contestable and defensible—provided careful procedures are practiced to check administrative processes, physical chain of custody of the ballots, and other physical security measures. Such procedures are called *compliance audits*.

“A voting system based on hand-marked paper ballots …
is both contestable and defensible …”



A voting system based on BMD-marked ballots is neither contestable nor defensible. A voting system based on hand-marked paper ballots, counted by optical scanners and recountable (and auditable) by humans, is both contestable and defensible—provided careful procedures are practiced to check administrative processes, physical chain of custody of the ballots, and other physical security measures. Such procedures are called *compliance audits*.

Every voting system must be defensible — able to prove to the losers in every election that they really lost.*

**That's what defensible means.*

This will:

☑ Increase public confidence

☑ Reduce corruption

☑ Improve government

- *If the correct officials are elected & the correct ballot measures pass*.

SMART ELECTIONS

This power point has been compiled by SMART Elections to assist voters, legislators and election officials in understanding the risks of “Hybrid” or “All-in-One” voting machines. It is based primarily on the work of Professors Andrew Appel of Princeton, and Philip Stark of the University of California Berkeley.

Elevating Election Reform to an Urgent National Priority

SMARTelections.us