PUBLIC NOTICE IS HEREBY GIVEN THAT THE

BOARD OF COMMISSIONERS OF UTAH COUNTY, UTAH

WILL HOLD A PUBLIC MEETING
IN THE COMMISSION CHAMBERS - ROOM 1400
OF THE UTAH COUNTY ADMINISTRATION BUILDING
100 East Center Street, Provo, Utah
February 26, 2020 - 03:00 P.M.

Board members may participate electronically at will, with the anchor location as stated above.

~MEETING MINUTES~

Commissioner Ainge (Chair), Commissioner Ivie and Commissioner Lee in Attendance
Others in Attendance: See Attached Attendance Sheet
(Start time: 3:00 pm)

PRAYER/READING/THOUGHT: **Commissioner Ainge**
PLEDGE OF ALLEGIANCE: **Member of Audience w/family**

CONSENT AGENDA

1. APPROVE AND AUTHORIZE THE COMMISSION TO SIGN THE UTAH COUNTY GRANT AWARD AGREEMENT MODIFIED JANUARY 2020 WITH THE UTAH INDIGENT DEFENSE COMMISSION
-Commissioner Ivie

APPROVED ON CONSENT

2. APPROVE AND AUTHORIZE A SIGNING OF AN AGREEMENT WITH SPRINGVILLE MUSEUM OF ART ASSOCIATION

APPROVED ON CONSENT

3. APPROVE AND AUTHORIZE THE SIGNING OF A RESOLUTION CONSENTING TO THE APPOINTMENT OF ALEX ANTHONY, ALICE BLACK, HALENE INOKE, AND SCOTT CARTER AS DEPUTY CLERK/AUDITOR'S.
-Paul Jones

APPROVED ON CONSENT

4. APPROVE AND AUTHORIZE THE COMMISSION TO SIGN AN AMENDMENT TO AN AGREEMENT BETWEEN UTAH COUNTY AND THE UTAH COUNTY PUBLIC DEFENDER ASSOCIATION FOR ADDITIONAL PAYMENTS FROM THE UTAH STATE INDIGENT DEFENSE COMMISSION.
-Commissioner Ivie

APPROVED ON CONSENT

5. ADOPT A RESOLUTION APPOINTING ERIC NIELSON AS A UTAH COUNTY BAIL COMMISSIONER

-David Shawcroft

APPROVED ON CONSENT

6. APPROVE AND AUTHORIZE A SIGNING OF AN AGREEMENT FOR EXPERT WITNESS SERVICES

-Anthony Loubet

APPROVED ON CONSENT

7. TO ADOPT A RESOLUTION APPROVING AND AUTHORIZING THE RENEWAL OF UTAH COUNTY'S COMMITMENT TO THE MASTER LEASE AGREEMENT BETWEEN THE MUNICIPAL BUILDING AUTHORITY OF UTAH COUNTY UTAH, AS LESSOR, AND UTAH COUNTY, AS LESSEE OF THE MOUNTAINLAND APPLIED TECHNOLOGY COLLEGE SPANISH FORK FACILITY FOR THE PERIOD FROM JANUARY 1, 2020 TO DECEMBER 31, 2020

-David Shawcroft

APPROVED ON CONSENT

8. ADOPT A RESOLUTION ESTABLISHING THE UTAH COUNTY FINANCE COMMITTEE AND APPOINTING MEMBERS THERETO

-David Shawcroft

APPROVED ON CONSENT

9. ADOPT A RESOLUTION APPOINTING BRYCE MOORE AS A UTAH COUNTY BAIL COMMISSIONER

-David Shawcroft

APPROVED ON CONSENT

10. APPROVE AND AUTHORIZE COMMISSION SIGNATURE ON MODIFICATION OF GRANT OR AGREEMENT FOR FY2020 ANNUAL OPERATING AND FINANCIAL PLAN

-Wayne Keith/Sheriff

APPROVED ON CONSENT

11. ADOPT A RESOLUTION APPOINTING A NEW UTAH COUNTY PROPERTY TAX OFFICER AND AN ALTERNATE UTAH COUNTY PROPERTY TAX OFFICER

-Anthony Loubet

APPROVED ON CONSENT

12. APPROVE PROPERTY TAX ACTIONS CONTAINED IN RECOMMENDATION LETTER 2020-2

-Paul Jones

COMMISSIONER AINGE – APPLICANT STATED THEY PROCESSED SOMETHING ONLINE.

ANTHONY LOUBET, COUNTY ATTORNEY- THEY PROCESSED IT THROUGH THE WEBSITE. THERE'S A SPOT IN THE PROCESS FOR THEM TO PUT IN THEIR EMAIL ADDRESS SO IF THERE

IS AN ISSUE, IT WILL COME BACK TO THEIR EMAIL LETTING THEM KNOW THAT THERE WAS A PROBLEM WITH THEIR ACCOUNT. THEY DID NOT PUT IN THEIR EMAIL ADDRESS. THEY HAD PUT THEIR ROUTING AND BANK ACCOUNT NUMBER IN INCORRECTLY. PROCESSING DIDN'T WORK BUT THERE WAS NO WAY TO RESPOND IMMEDIATELY BACK TO THEM. THE ASSESSOR'S OFFICE MAILED THEM A PAPER NOTICE. BY THE TIME THEY RECEIVED IT, IT WAS ALREADY TOO LATE. THE AMOUNT OF PENALTY IS $27.12. THERE IS PROOF OF THE ATTEMPTED PROCESSING.

COMMISSIONER AINGE – GIVEN THAT WE KNOW THEY TRIED TO PROCESS, WILL CERTAINLY ENTERTAIN FORGIVING THE PENALTY.

ANTHONY LOUBET - TALKED WITH THE COUNTY TREASURER'S OFFICE TO SEE IF THERE IS A WAY TO MAKE THE EMAIL FIELD A REQUIRED FIELD, SO THIS WILL NOT HAPPEN IN THE FUTURE.

COMMISSIONER LEE – SECOND ONE IS AMERICAN FOR INDUSTRIAL PARK – NO ONE IN AUDIENCE REPRESENTING.

**COMMISSIONER LEE: MOTION TO APPROVE NOTING THAT THAT THE PENALTIES AND FEES FOR SANDRA AND KIRSTEN BRAUMLEY THAT TOTAL $27.12 ARE TO BE WAIVED.
COMMISSIONER IVIE: SECOND
AYE: ALL IN FAVOR
PASSED: 3/0**

13. APPROVE AND AUTHORIZE COMMISSION SIGNATURE ON AGREEMENT BETWEEN UTAH COUNTY AND IHC HEALTH SERVICES, INC FOR LABORATORY SERVICES FOR UTAH COUNTY JAIL INMATES
-Dale Bench

APPROVED ON CONSENT

14. TO APPROVE AND AUTHORIZE THE COUNTY COMMISSION TO REVIEW AND TAKE ACTION TO CONTINUE FOR AN ADDITIONAL 20 YEARS AND AUTHORIZE THE COMMISSION CHAIR TO SIGN THE NOTICE OF CONTINUATION OR TO REFER TO THE PLANNING COMMISSION AND AGRICULTURE PROTECTION AREA ADVISORY BOARD TO REVIEW AND SUBMIT RECOMMENDATIONS TO CONTINUE, MODIFY OR TERMINATE THE STEWART FARMS AGRICULTURE PROTECTION AREA CONSISTING OF APPROXIMATELY 40.1 ACRES.
-Peggy Kelsey

APPROVED ON CONSENT

15. TO APPROVE AND AUTHORIZE THE COUNTY COMMISSION TO REVIEW AND TAKE ACTION TO CONTINUE FOR AN ADDITIONAL 20 YEARS AND AUTHORIZE THE COMMISSION CHAIR TO SIGN THE NOTICE OF CONTINUATION OR TO REFER TO THE PLANNING COMMISSION AND AGRICULTURE PROTECTION AREA ADVISORY BOARD TO REVIEW AND SUBMIT RECOMMENDATIONS TO CONTINUE, MODIFY OR TERMINATE THE CORPORATION OF THE PRESIDEING BISHOP OF THE CHURCH OF JESUS CHRIST OF LATTER-DAY SAINTS PHASE 3 AGRICULTURE PROTECTION AREA CONSISTING OF APPROXIMATELY 8074.328 ACRES.
-Peggy Kelsey

APPROVED ON CONSENT

16. TO APPROVE AND AUTHORIZE THE COUNTY COMMISSION TO REVIEW AND TAKE ACTION TO CONTINUE FOR AN ADDITIONAL 20 YEARS AND AUTHORIZE THE COMMISSION CHAIR TO SIGN THE NOTICE OF CONTINUATION OR TO REFER TO THE PLANNING COMMISSION AND AGRICULTURE PROTECTION AREA ADVISORY BOARD TO REVIEW AND SUBMIT RECOMMENDATIONS TO CONTINUE, MODIFY OR TERMINATE THE MCMULLIN/PALMER AGRICULTURE PROTECTION AREA CONSISTING OF APPROXIMATELY 134.3 ACRES.

-Peggy Kelsey

APPROVED ON CONSENT

17. TO APPROVE AND AUTHORIZE THE COUNTY COMMISSION TO REVIEW AND TAKE ACTION TO CONTINUE FOR AN ADDITIONAL 20 YEARS AND AUTHORIZE THE COMMISSION CHAIR TO SIGN THE NOTICE OF CONTINUATION OR TO REFER TO THE PLANNING COMMISSION AND AGRICULTURE PROTECTION AREA ADVISORY BOARD TO REVIEW AND SUBMIT RECOMMENDATIONS TO CONTINUE, MODIFY OR TERMINATE THE CORPORATION OF THE PRESIDEING BISHOP OF THE CHURCH OF JESUS CHRIST OF LATTER-DAY SAINTS PHASE 1 AGRICULTURE PROTECTION AREA CONSISTING OF APPROXIMATELY 11,213.397 ACRES.

-Peggy Kelsey

APPROVED ON CONSENT

18. TO APPROVE AND AUTHORIZE THE COUNTY COMMISSION TO REVIEW AND TAKE ACTION TO CONTINUE FOR AN ADDITIONAL 20 YEARS AND AUTHORIZE THE COMMISSION CHAIR TO SIGN THE NOTICE OF CONTINUATION OR TO REFER TO THE PLANNING COMMISSION AND AGRICULTURE PROTECTION AREA ADVISORY BOARD TO REVIEW AND SUBMIT RECOMMENDATIONS TO CONTINUE, MODIFY OR TERMINATE THE CORPORATION OF THE PRESIDEING BISHOP OF THE CHURCH OF JESUS CHRIST OF LATTER-DAY SAINTS PHASE 2 AGRICULTURE PROTECTION AREA CONSISTING OF APPROXIMATELY 4286.93 ACRES.

-Peggy Kelsey

APPROVED ON CONSENT

19. APPROVE AND AUTHORIZE THE SIGNING OF AN AGREEMENT BETWEEN UTAH COUNTY AND SHERWOOD LANDSCAPE INC FOR REMOVAL OF A DEAD SYCAMORE TREE AND GRIND DOWN THE STUMP FOR $2750.

-Richard Nielson

RICHARD NIELSON, DIRECTOR OF PUBLIC WORKS – THIS IS CONCERNING A TREE THAT HAS ALREADY BEEN REMOVED. THOUGHT WITH THE COST LIMIT, THAT WAS GOOD TO GO AHEAD AND REMOVE. AFTER THE WORK WAS COMPLETE IS WHEN WE FOUND A CONTRACT WAS NEEDED. TREE WAS NORTH OF COURTHOUSE.

COMMISSIONER LEE: MOTION TO APPROVE
COMMISSIONER IVIE: SECOND
AYE: ALL IN FAVOR
PASSED: 3/0

20. APPROVE AND AUTHORIZE THE SIGNING OF A MEMO TO SURPLUS COUNTY PROPERTY AS EITHER SOLD THROUGH PUBLIC AUCTION OR TRADED INTO A DEALERSHIP TOWARD THE PURCHASE OF A NEW VEHICLE.

-Richard Nielson

APPROVED ON CONSENT

21. ADOPT A RESOLUTION AUTHORIZING THE COMMISSION CHAIR TO SIGN AN INTERLOCAL AGREEMENT WITH SPRINGVILLE CITY FOR A PROJECT FOR THE CONSTRUCTION OF 1200 WEST - PHASE 2, 400 SOUTH TO 550 NORTH

-Richard Nielson

RICHARD NIELSON, DIRECTOR OF PUBLIC WORKS – RESOLUTION IS LATEST VERSION THAT WAS UPLOADED LAST NIGHT. WAS DONE THROUGH COG. DOES NOT INCLUDE THE COURT OF PRESERVATION.

ROBERT MOORE, COUNTY ATTORNEY – THE EMAIL THAT WAS SENT BY ROB MOORE'S ASSISTANT AND THE ONE THAT WAS UPLOADED BY ROB MOORE, ARE THE SAME DOCUMENT.

COMMISSIONER LEE: MOTION TO ADOPT NOTING THAT IT IS THE LATEST VERSION AND DOES NOT INCLUDE COURT OF PRESERVATION.
COMMISSIONER IVIE: SECOND
AYE: ALL IN FAVOR
PASSED 3/0

22. APPROVE AND AUTHORIZE THE SIGNING OF A SUBDIVISION IMPROVEMENT AND WARRANTY AGREEMENT BETWEEN UTAH COUNTY AND CLAIR JAUSSI FOR THE JAUSSI ESTATES PLAT A FOR CONSTRUCTION BOND OF $24,283.35 AND CASH WARRANTY BOND OF $1,942.66

-Richard Nielson

APPROVED ON CONSENT

23. APPROVE AND AUTHORIZE A FEE WAIVER FOR THE EVENT PERMIT APPLICATION FOR RUN FOR HOPE 5K ON MAY 16, 2020 ON THE JORDAN RIVER PARKWAY TRAIL AND FINDING THAT THE FEE WAIVER CONTRIBUTES TO THE HEALTH AND MORAL WELL-BEING OF THE COUNTY'S INHABITANTS; OR DENY THE FEE WAIVER.

-Richard Nielson

COMMISSIONER LEE – PROCESS TO GET APPLICATION AMENDED SUGGESTED CONCERNING LAVATORY FACILITIES AND NEEDS OF DISPOSABLE WASTE. THE WAY THEY FILLED OUT THE APPLICATION STATES THAT THEY WOULD USE THE TOILETS FOR BAGGED WASTE. THEN THE APPLICATION STATES THAT THE APPLICANT SHALL PROVIDE TOILET FACILITIES FOR THE EVENT. APPLICANT AND EVENT PARTICIPANTS ARE NOT PERMITTED ACCESS. THEY SIGNED, BUT NOT CLEAR.

RICHARD NIELSON, DIRECTOR OF PUBLIC WORKS – MISCOMMUNICATION ON THE APPLICATION. THE LOCATION THEY ARE USING, THE OLYMPIC PARK, IS A LEHI CITY FACILITY. THEY WILL BE USING THE FACILITIES AT THAT PARK. WHAT THEY ARE ASKING FOR ON THE EVENT PERMIT IS JUST FOR THE USE OF THE JORDAN RIVER TRAIL FOR THE RACE ITSELF, THE LEHI CITY RUN. THERE ARE NO TOILET FACILITIES ALONG THE PORTION OF THE TRAIL THEY WILL BE USING. SO THOSE SECTIONS ARE NOT APPLICABLE. HE WILL MAKE A NOTE ON THE APPLICATION CONCERNING THIS.

COMMISSIONER LEE – HAS INSURANCE BEEN VERIFIED?

DAVE SHAWCROFT, COUNTY ATTORNEY – THE AGENDA ITEM TODAY IS ONLY CONCERNING THE FEE WAIVER. EITHER WAY IT WILL STILL HAVE TO GO THROUGH THE FINAL PROCESS OF THE EVENT PERMIT WHERE THERE WILL BE VERIFICATION OF INSURANCE.

COMMISSIONER IVIE: MOTION TO APPROVE WITH NOTE THAT WAIVER CONTRIBUTES TO THE HEALTH AND MORAL WELL-BEING OF THE COUNTY'S INHABITANTS.
COMMISSIONER LEE: SECOND
AYE: ALL IN FAVOR
PASSED: 3/0

24. APPROVE AND AUTHORIZE THE COMMISSION CHAIR TO SIGN AN AGREEMENT BETWEEN UTAH COUNTY AND WOODHOUSE AVIATION FOR AIRCRAFT MAINTENANCE.

-Lt. Wally Perschon

APPROVED ON CONSENT

25. APPROVE AND AUTHORIZE COMMISSION CHAIR TO SIGN PRICING AGREEMENT WITH PRIORITY DISPATCH

-Dalene Higgins

APPROVED ON CONSENT

26. APPROVE AND AUTHORIZE THE COMMISSION CHAIR TO SIGN AN AGREEMENT WITH THE UTAH COUNTY DEPUTIES ASSOCIATION, A NON-PROFIT CORPORATION, TO PROVIDE SUPPORT SERVICES FOR THE BASIC SWAT SCHOOL TO BE HELD ON APRIL 24, 2020 THROUGH APRIL 28, 2020; K9 SCHOOL WITH DATES TO BE DETERMINED; AND A SNIPER SCHOOL WITH DATES TO BE DETERMINED

-Shawn Radmall

APPROVED ON CONSENT

27. APPROVE AND AUTHORIZE COMMISSION CHAIR TO EXECUTE USE AGREEMENT FOR COUNTY FACILITIES BETWEEN UTAH COUNTY AND THE UTAH COUNTY DEPUTIES ASSOCIATION.

-Shawn Radmall

APPROVED ON CONSENT

28. APPROVE AND AUTHORIZE THE COMMISSION CHAIR TO SIGN AN AGREEMENT WITH THE UTAH DIVISION OF PARKS AND RECREATION FOR THE EMERGENCY VEHICLE RADIO SYSTEM GRANT.

-Lt. Wally Perschon

APPROVED ON CONSENT

29. APPROVE AND AUTHORIZE THE COMMISSION CHAIR TO SIGN A MEMORANDUM OF UNDERSTANDING BETWEEN TUSK/MONTGOMERY PHILANTHROPIES, THE NATIONAL CYBERSECURITY CENTER, AND VOATZ REGARDING A PILOT PROJECT FOR UOCAVA VOTERS

-Josh Daniels

COMMISSIONER LEE – SECURITY VULNERABILITY CONCERNS FROM A REPORT THAT WAS PUBLISHED.

JOSH DANIELS, COUNTY CLERK AUDITOR'S OFFICE – BEEN IN TOUCH WITH SOFTWARE PROVIDER, THE DEPARTMENT OF HOMELAND SECURITY AS WELL AS THE RESEARCHERS

AND DISCUSSED IN DETAIL AS TO WHO THIS REPORT IS REALLY DONE BY AND HOW IT WAS DONE. HAVE REVIEWED THE REPORT IN ITS ENTIRETY. THE VERSION THAT THEY ARE TALKING ABOUT IS 27 VERSIONS OLD, NOT THE VERSION OF THE APP THAT THE COUNTY WOULD BE USING. THEY ATTEMPTED TO FIND WEAKNESSES. THEY WERE NOT ABLE TO CONNECT TO THE ACTUAL SERVER THAT SERVES THE ENTIRE PROCESS OF VOTING SO THEY MADE UP A GUESSTIMATE OF WHAT THE SERVER MIGHT DO AND USED IT AND THEN TRIED TO FIND WEAKNESSES. AS COUNTY HAS GONE THROUGH THESE WEAKNESSES, WE HAVE FOUND THAT NONE OF THE WEAKNESSES THEY OUTLINED ARE ONES THAT COULD OCCUR THROUGH THE CURRENT VERSION.

THE ONLY ALTERNATIVE FOR THESE VOTERS, UNDER STATE AND FEDERAL LAW, IS TO SUBMIT THEIR VOTES TO US THROUGH THE TRADITIONAL PAPER MEANS. THE PROBLEM WITH OVERSEAS, WE MAY NOT BE ABLE TO GET THEIR ABSENTEE BALLOT TO THEM IN ENOUGH TIME FOR THEM TO VOTE AND GET IT BACK TO US. SO FEDERAL LAW CREATES AN OPPORTUNITY FOR THEM TO EMAIL OR FAX IT BACK OR USE OTHER ELECTRONIC MEANS AS PROVIDED BY THE JURISDICTION, WHICH THIS APP FALLS UNDER. PEOPLE HAVE THE OPTION. THE APP OPTION IS MUCH MORE SECURE. WE HAVE AN AUDIT TRAIL FOR THESE VOTES. THIS IS ONLY FOR OVERSEAS OR DISABLED VOTERS. THE FEDERAL LAW IS CALLED UOCAVA (UNIFORMED OVERSEAS CITIZENS AND VOTING RIGHTS ACT).

COMMISSIONER LEE – WHAT IS THE PROCESS WHEN USED THROUGH THE APP?

JOSH DANIELS – OUR BALLOT SYSTEM IS NOT CONNECTED TO THE INTERNET OR NETWORK OF THE COUNTY. EVERY VOTE THAT COMES INTO THE OFFICE. THEY ARE SCANNED AND TABULATED ON AN INTERNAL SYSTEM. WITH APP VOTES – WE PRINT THEM ON PAPER BALLOTS, VERIFY AND THEY ARE SCANNED AND THEN TABULATED WITH THE OTHER VOTES. WE HAVE AN AUDIT AND VERIFY SYSTEM FOR THESE TYPES OF VOTES. AFTER THE ELECTION, WE CAN MATCH THE PAPER BALLOTS WE RECEIVED TO THE RECEIPTS THAT WERE ISSUED TO VOTERS.

**COMMISSIONER LEE: MOTION TO APPROVE
COMMISSIONER IVIE: SECOND
AYE: ALL IN FAVOR
PASSED: 3/0**

30. COMMISSION APPROVAL TO FOREGO THE REQUIREMENT FOR A BILATERAL CONTRACT FOR SIGN LANGUAGE SERVICES ALREADY PERFORMED IN NOVEMBER AND DECEMBER 2019.
-Robert Baxter

APPROVED ON CONSENT

31. ADOPT A RESOLUTION APPROVING AND AUTHORIZING THE INTERLOCAL AGREEMENT BETWEEN UTAH COUNTY AND OREM CITY REGARDING THE PURCHASE OF TWO BALLOT DROP BOXES.
-Rozan Mitchell

APPROVED ON CONSENT

32. APPROVE AND AUTHORIZE THE COMMISSION TO SIGN AN AGREEMENT WITH MESA MOVING AND STORAGE TO LOCATE ELECTION EQUIPMENT THROUGHOUT THE COUNTY FOR THE 2020 ELECTIONS.
-Rozan Mitchell

APPROVED ON CONSENT

33. APPROVE AND SIGN 60-DAY NOTICE OF TERMINATION LETTER TO UTAH DEPARTMENT OF HEALTH STIPULATING THE DEPARTMENT OF DRUG & ALCOHOL PREVENTION & TREATMENT WILL NO LONGER BE A PREPAID MENTAL HEALTH PLAN (PMHP) CONTRACTOR EFFECTIVE JUNE 30, 2020

-Richard Nance

APPROVED ON CONSENT

34. APPROVE AND AUTHORIZE THE SIGNING OF AN AGREEMENT WITH LEHI CITY SENIOR CENTER.

-Ralph Clegg

APPROVED ON CONSENT

35. APPROVE AND AUTHORIZE THE SIGNING OF AN EVENT AGREEMENT WITH PROVO TOWNE CENTRE (BRIXTON PROVO MALL, LLC) FOR HOUSEHOLD HAZARDOUS WASTE COLLECTION DAY ON APRIL 11, 2020.

-Ralph Clegg

APPROVED ON CONSENT

36. APPROVE AND AUTHORIZE THE SIGNING OF AMENDMENT 7 TO AGREEMENT # 2016-451 WITH UTAH DEPARTMENT OF HEALTH FOR THE BREAST AND CERVICAL CANCER SCREENING PROGRAM.

-Ralph Clegg

APPROVED ON CONSENT

37. AUTHORIZE A STAFFING PLAN CHANGE IN THE NURSING DIVISION OF THE HEALTH DEPARTMENT TO ADD A FULL-TIME, CAREER SERVICE SENIOR CLINICAL ASSISTANT POSITION AND DELETE A FULL-TIME, CAREER SERVICE CLINICAL ASSISTANT II POSITION. [ACCOUNT NUMBER: 230-43120 / HEALTH DEPT.-NURSING, SONIA DALE'S SUPERVISORY ORGANIZATION. ADD ONE (FTE 1.0) POSITION OF JOB CODE 6605, GRADE 503. DELETE ONE (FTE 1.0) POSITION OF JOB CODE 6604, GRADE 502; POSITION TO DELETE DETERMINED AFTER RECRUITMENT PROCESS.]

-Merritt Fullmer

APPROVED ON CONSENT

38. AUTHORIZE A CHANGE TO THE SURVEYOR DEPARTMENT PORTION OF THE STAFFING PLAN, ADDING ONE (1) FULL-TIME, CAREER SERVICE FIELD DIRECTOR POSITION AND TWO (2) FULL-TIME, CAREER SERVICE SURVEY TECHNICIAN II POSITIONS. [SUPERVISORY ORGANIZATION: ANTHONY CANTO; COST CENTER:100-44550 SURVEYING; ADD 1 POSITION OF FIELD DIRECTOR (CODE TBD), GRADE TBD; ADD 2 POSITIONS OF JOB CODE 3049, GRADE 508].

-Julene Elgueta

CONTINUED FOR 2 WEEKS

39. APPROVE AND AUTHORIZE SIGNING THE UPDATED LEASE FOR NORTH COUNTY CJC SATELLITE IN AMERICAN FORK.

-Rebecca Martell

APPROVED ON CONSENT

40. APPROVE TAX CREDITS AND REFUNDS RECOMMENDED BY THE COUNTY ASSESSOR'S OFFICE IN CANCELLATION AND CORRECTION LETTER #60411 DATED 02/20/2020

-Jim Stevens

APPROVED ON CONSENT

41. RATIFICATION OF WARRANT REGISTER FOR FEBRUARY 25, 2020, INCLUDING NOTES AND COMMENTS FROM THE COMMISSIONERS AS RECORDED ON THE INTERNAL SYSTEM.

-Justin

APPROVED ON CONSENT

42. AUTHORIZE THE ADDITION OF 3 POSITIONS TO THE STAFFING PLAN OF THE SURVEYOR'S OFFICE. 2 FULL-TIME CAREER SERVICE SURVEY TECHNICIAN POSITIONS AND 1 FULL-TIME CAREER SERVICE FIELD DIRECTOR POSITION

-Gary Ratcliffe

STRIKEN ON CONSENT

43. APPROVAL OF THE PAYROLL WARRANT SUMMARY FOR PAY PERIOD 4-2020

-Justin

APPROVED ON CONSENT

44. RECEIVE THE RECOMMENDATION OF THE UTAH COUNTY INVESTMENT/BENEFITS COMMITTEE AND ADOPT THE RESOLUTION AUTHORIZING FUND CHANGE OFFERINGS IN THE UTAH COUNTY EMPLOYEES RETIREMENT PLAN

-Mark Brady

APPROVED ON CONSENT

45. APPROVE AND RATIFY THE SIGNATURE OF A NOTICE OF NON-RENEWAL OF QUALTRICS MASTER SERVICES AGREEMENT BETWEEN UTAH COUNTY AND QUALTRICS, LLC.

-Adam Beck

APPROVED ON CONSENT

REGULAR AGENDA

1. ADOPT A RESOLUTION DECLARING UTAH COUNTY A SECOND AMENDMENT SANCTUARY, AND FOR THE SUPPORT OF THE CONSTITUTIONAL RIGHT TO BEAR ARMS

-Nathan Ivie

COMMISSIONER IVIE - MET WITH SHERIFF SMITH AS WELL AS MANY LEADERS OF THE GUN COMMUNITY CONCERNING THESE RIGHTS. FEEL WE NEED TO MAINTAIN THE HERITAGE OF PROTECTING INDIVIDUAL LIBERTIES AND THAT WE NEED TO TAKE A STAND IN THIS COUNTY. OUTSIDE FORCES CANNOT ROB US OF WHAT GOD HAS GIVEN US.

COMMISSIONER LEE – #3 OF THE 'NOW THEREFORE'S' – IS AN IMPORTANT ONE. THE BOARD OF COUNTY COMMISSIONERS HEREBY DECLARES IT'S OPPOSITION TO UNCONSTITUTIONAL RESTRICTIONS ON THE RIGHT TO BEAR ARMS AND INTENDS TO OPPOSE, WITHIN THE LIMITS OF THE CONSTITUTION OF THE UNITED STATES AND THE STATE OF UTAH, ANY EFFORT TO UNCONSTITUTIONALLY RESTRICT SUCH RIGHTS AND USE SUCH LEGAL MEANS AT IT'S DISPOSAL TO PRESERVE THE CONSTITUTIONALLY PROTECTIVE RIGHT OF THE CITIZENS TO KEEP AND BEAR ARMS. SECOND AMENDMENT IS THERE TO KEEP US FREE.

COMMISSIONER AINGE – STATED THAT HE IS ALWAYS GOING TO BE ON THE SIDE OF THE CONSTITUTION AND THE BILL OF RIGHTS AND WITH THIS RESOLUTION AS WELL. CANNOT COMMAND THE STATE OR GOVERNMENT. FEELS THIS IS IMPORTANT. NOTED IN THE RESOLUTION THAT IT OPPOSES UNCONSTITUTIONAL RESTRICTIONS. IT DOESN'T NECESSARILY OPPOSE ALL FORMS OF REGULATION. IT SPECIFICALLY REFERENCES THE UTAH CONSTITUTION WHICH RESERVES TO THE STATE LEGISLATURE THE ABILITY TO DEFINE WHAT THE LAWFUL USE OF ARMS IS AND TO SET REASONABLE, CONSTITUTIONAL REGULATIONS. HAPPY TO SUPPORT THIS.

OPEN FOR PUBLIC COMMENT

SHAWN LOREE, RESIDENT –IS A 10-YEAR UTAH COUNTY RESIDENT. TALKED ABOUT CERTAIN WORDS IN THE 2ND AMENDMENT THAT CAUSE DIFFERENT MEANINGS TO DIFFERENT PEOPLE. TALKED ABOUT THE 2007 MALL SHOOTING STOPPED BY OFF-DUTY OFFICER WITH RIGHT TO CARRY. FEELS GUNS SAVE LIVES.

COMMISSIONER IVIE: MOVED TO APPROVE
COMMISSIONER LEE: SECOND
AYE: ALL IN FAVOR
PASSED: 3/0

2. AUTHORIZE THE ADDITION OF ONE FULL-TIME, CAREER SERVICE LIEUTENANT - ENFORCEMENT TO THE SHERIFF, ENFORCEMENT DIVISION OF THE STAFFING PLAN. [SUPERVISORY ORGANIZATION: SHAUN BUFTON, COST CENTER: 100-42100 SHERIFF - ADMINISTRATION, ADD ONE (1) POSITION OF JOB CODE 2531, GRADE 517].
-Julene Elgueta

RALPH BARNES, DIRECTOR OF HUMAN RESOURCES – FIELD COMMANDER/MAJOR CRIMES POSITION BECAME OPEN – FOUND DURING THE PROCESS THAT THERE'S A RESOLUTION IN 2012 THAT THE POSITION IS NOT TO BE REPLACED WHEN IT WAS VACATED. WERE NOT AWARE AT THAT TIME. PUT THE REPLACEMENT ON HOLD. SHERIFF SMITH IS ASKING FOR THIS REPLACEMENT.

COMMISSIONER AINGE – NUMBER OF REQUESTS FOR POSITIONS – STILL STAFFED AT THE SAME WITHIN BUDGET.

MATT HIGLEY, SHERIFF'S OFFICE – READ MEMO FROM SHERIFF SMITH REQUESTING FOR FIELD COMMANDER POSITION SHOWING CONCERN FOR THE NEED OF THIS POSITION TO CONTINUE. THIS POSITION WILL BEGIN BRINGING THE PUBLIC TO THE SHERIFF'S OFFICE AND THE SHERIFF'S OFFICE TO THE PUBLIC THROUGH MEDIA. NOT ONLY WILL THIS HELP THE STAFF WITH MENTAL WELLNESS BUT WILL OVERSEE THE COLONELS PROGRAM AND PEER SUPPORT.

SHAWN CHIPMAN, SHERIFF'S OFFICE – THIS IS NEEDED TO IMPROVE RELATIONS BETWEEN THE PUBLIC, SHERIFF'S OFFICE AND THE POLICE. GREAT WAY TO START THIS PROCEDURE.

COMMISSIONER LEE – IT HAS TO DO WITH PROCESS OF THE RESOLUTION FROM 2012. WAS PUT IN DELIBERATELY FOR IT TO END. FUNDING IS NO LONGER. THE INTENT WAS FOR THIS POSITION TO ROTATE AND IT WILL COME BACK AROUND AGAIN.

SHAWN CHIPMAN, CHIEF DEPUTY SHERIFF – NOTED THAT IN 2009, THEY DID LOSE 2 LIEUTENANT POSITIONS THAT HAVE NEVER BEEN FILLED.

COMMISSIONER AINGE – THIS IS A DECISION THAT SHERIFF SMITH HAS MADE. THE SHERIFF HAS HIS BUDGET AND HE IS DECIDING TO USE PART OF THE BUDGET FOR THIS POSITION. IN FAVOR AS LONG AS HE STAYS WITHIN HIS BUDGET PARAMETERS.

COMMISSIONER IVIE – SALARY BUDGET SET. AS LONG AS THE SALARIES AND STAFF ARE WITHIN THE BUDGET, FEELS HE CAN USE AS HE SEES NEEDED.

MARK ALLEN, PROTECT AND PRESERVE AMERICAN FORK CANYON – MORE CELL TOWERS GOING UP THE CANYON AND WITH THIS SEEING MORE DRUG AND ILLEGAL ISSUES HAPPENING AND ARE IN SUPPORT OF THIS POSITION CONTINUING TO BE PROACTIVE.

COMMISSIONER IVIE: MOTION TO APPROVE
COMMISSIONER LEE: SECOND
AYE: THOSE IN FAVOR (COMMISSIONER AINGE AND COMMISSIONER IVIE)
AYE: THOSE OPPOSED (COMMISSIONER LEE)
PASSED: 2/1

3. APPROVE AND AUTHORIZE THE ADOPTION AND IMPLEMENTATION OF A NEW COUNTY STORMWATER ORDINANCE
- Richard Nielson, Public Works Director -

AUTHORIZED ON CONSENT

4. ADOPT (OR DENY) AN ORDINANCE AMENDING ARTICLE 7.1.1 OF THE UTAH COUNTY CODE TO ADOPT "APPENDIX C GROUP U - AGRICULTURAL BUILDINGS" OF THE MOST CURRENTLY ADOPTED VERSION OF THE INTERNATIONAL BUILDING CODE
-Nathan Ivie

AUTHORIZED ON CONSENT

5. APPROVE AND SET A DATE, TIME AND LOCATION FOR A CLOSED MEETING TO DISCUSS THE CHARACTER, PROFESSIONAL COMPETENCE, OR PHYSICAL OR MENTAL HEALTH OF AN INDIVIDUAL OR INDIVIDUALS (ANNOUNCE THE VOTE OF EACH COMMISSIONER)
- Justin Anderson, Utah County Clerk/Auditor's Office -

COMMISSIONER IVIE – MOVED TO APPROVE AND SET DATE, TIME AND LOCATION FOR TODAY IMMEDIATELY FOLLOW COMPLETION OF REGULAR BUSINESS.
COMMISSIONER LEE – SECOND
AYE: ALL IN FAVOR
PASSED: 3/0

6. APPROVE AND SET A DATE, TIME AND LOCATION FOR A CLOSED MEETING FOR A STRATEGY SESSION TO DISCUSS THE PURCHASE, EXCHANGE, OR LEASE OF REAL PROPERTY, WATER RIGHTS, OR WATER SHARES (ANNOUNCE THE VOTE OF EACH COMMISSIONER)
- Justin Anderson, Utah County Clerk/Auditor's Office -

COMMISSIONER IVIE – MOTION TO STRIKE
COMMISSIONER LEE – SECOND
AYE: ALL IN FAVOR
PASSED: 3/0

7. APPROVE AND SET A DATE, TIME AND LOCATION FOR A CLOSED MEETING FOR A STRATEGY SESSION TO DISCUSS THE SALE OF REAL PROPERTY, WATER RIGHTS, OR WATER SHARES, PREVIOUSLY PUBLICLY NOTICED FOR SALE (ANNOUNCE THE VOTE OF EACH COMMISSIONER)
- Justin Anderson, Utah County Clerk/Auditor's Office -

COMMISSIONER IVIE – MOVED TO APPROVE AND SET DATE, TIME AND LOCATION FOR TODAY IMMEDIATELY FOLLOW COMPLETION OF REGULAR BUSINESS.
COMMISSIONER LEE – SECOND
AYE: ALL IN FAVOR
PASSED: 3/0

8. APPROVE AND SET A DATE, TIME AND LOCATION FOR A CLOSED MEETING FOR A STRATEGY SESSION TO DISCUSS PENDING OR REASONABLY IMMINENT LITIGATION (ANNOUNCE THE VOTE OF EACH COMMISSIONER)
- Justin Anderson, Utah County Clerk/Auditor's Office -

Commissioner Ivie – MOTION TO STRIKE
Commissioner Lee – SECOND
Aye: ALL IN FAVOR
PASSED: 3/0

Commissioner Ivie - MOTION TO ADJOURN
Commissioner Lee – SECOND
Aye: ALL IN FAVOR
MEETING ADJOURNED

WORK SESSION

NO WORK SESSION ITEMS WERE SUBMITTED

PUBLIC COMMENTS

NO PUBLIC COMMENTS

(Moved to closed session at 4:11 pm)
(Closed Session Ended: 4:42 pm)
(Public Meeting Reopened: 4:42)

Commissioner Ivie: Allowing Clerk Auditor's to submit their official response from their applicant vendor to the MIT report (Attached)

Commissioner Ivie: Motion to Adjourn
Commissioner Lee: Second
Aye: All In Favor
Passed: 3/0
Meeting Adjourned

(Meeting Adjourned: 4:44 pm)

PUBLIC COMMENTS

In compliance with the Americans With Disabilities Act, individuals needing special accommodations (including auxiliary communicative aids and services) during this meeting should notify Kelly Adams at (801) 851-8111 at least three days prior to the meeting.

BOARD OF COMMISSIONERS FOR UTAH COUNTY
ATTENDANCE SHEET
FEBRUARY 26, 2020 at 3:00 p.m.

PRINT CLEARLY

Name:	Agency:
Shawn Coree	Resident
Bob Jones	resident
Scott Rigby	Resident
Richard Nielson	UCPW
Jeff Dunn	UCSO
Mike Roberts	MyCourt
Gary Ratcliffe	Surveyor
Jay Brinkerhoff	Utah Firearms Assc.
Chad Keupe	UT Firearms Assoc.
Niklas Stremerz	UT Firearms Assoc.
Shane D Roberts	Resident
Ashley Ulmer	resident
Jeff Robinson	UCSO
Jovana Cicchelli	Resident
Elvia Calderon-Sona	UCHD
Raelle Cunningham	Resident
Rebecca Maxell	CJC
Mark Allen	Protect and Preserve Af Cazu

**BOARD OF COMMISSIONERS FOR UTAH COUNTY
ATTENDANCE SHEET
FEBRUARY 26, 2020 at 3:00 p.m.**

PRINT CLEARLY

Name:	Agency:
Shawn Chipman	UCSO
Wally Perschon	UCSO
Jon Baul	UCHD
Sonia Dale	UCHD
Jim Bean	Assessors
Burt Garfield	Assessors
Robert Baxter	Purchasing
Brian Voeks	Commission
Kris Poulson	Assessor
R(CHARD) NANCE	XDDONT
Eric Edwards	Health
BRANDON CHAMBERS	HR
STACEY BUSH	HR
Bryce C. Larsen	UCHD
Diane Garcia	Assessors
Jeff Smith	Recorder's office

BOARD OF COMMISSIONERS OF UTAH COUNTY, UTAH
Public Meeting Minutes
February 26, 2020
16 | P a g e

UTAH COUNTY CLERK/AUDITOR'S ATTACHMENTS FOR CONSENT AGENDA ITEM #29:

MIT News
ON CAMPUS AND AROUND THE WORLD

MIT researchers identify security vulnerabilities in voting app

Mobile voting application could allow hackers to alter individual votes and may pose privacy issues for users.

Abby Abazorius | MIT News Office
February 13, 2020

In recent years, there has been a growing interest in using internet and mobile technology to increase access to the voting process. At the same time, computer security experts caution that paper ballots are the only secure means of voting.

Now, MIT researchers are raising another concern: They say they have uncovered security vulnerabilities in a mobile voting application that was used during the 2018 midterm elections in West Virginia. Their security analysis of the application, called Voatz, pinpoints a number of weaknesses, including the opportunity for hackers to alter, stop, or expose how an individual user has voted. Additionally, the researchers found that Voatz's use of a third-party vendor for voter identification and verification poses potential privacy issues for users.

The findings are described in a new technical paper by Michael Specter, a graduate student in MIT's Department of Electrical Engineering and Computer Science (EECS) and a member of MIT's Internet Policy Research Initiative, and James Koppel, also a graduate student in EECS. The research was conducted under the guidance of Daniel Weitzner, a principal research scientist at MIT's Computer Science and Artificial Intelligence Lab (CSAIL) and founding director of the Internet Policy Research Initiative.

PRESS MENTIONS

MIT researchers have identified security flaws in a mobile voting application that allowed some overseas and military citizens to vote remotely, reports Lydia Emmanouilidou for PRI's *The World.* "When things are opaque – when you can't verify, when you can't see what the code is doing," says graduate student Michael Specter, "there is no way of vetting that it's doing the right thing."

PRI

MIT researchers have found that an internet voting application has security flaws that could make it vulnerable to hackers, reports Anthony Izaguirre for the AP. "In order to maintain trust in our elections system, we must assure that voting systems meet the high technical and operation security standards before they are put in the field," explains principal research scientist Daniel Weitzner.

news.mit.edu/2020/voting-voatz-app-hack-issues-0213   1/4

2/24/2020   MIT researchers identify security vulnerabilities in voting app | MIT News

After uncovering these security vulnerabilities, the researchers disclosed their findings to the Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA). The researchers, along with the Boston University/MIT Technology Law Clinic, worked in close coordination with election security officials within CISA to ensure that impacted elections officials and the vendor were aware of the findings before the research was made public. This included preparing written summaries of the findings with proof-of-concept code, and direct discussions with affected elections officials on calls arranged by CISA.

In addition to its use in the 2018 West Virginia elections, the app was deployed in elections in Denver, Oregon, and Utah, as well as at the 2016 Massachusetts Democratic Convention and the 2016 Utah Republican Convention. Voatz was not used during the 2020 Iowa caucuses.

The findings underscore the need for transparency in the design of voting systems, according to the researchers.

"We all have an interest in increasing access to the ballot, but in order to maintain trust in our elections system, we must assure that voting systems meet the high technical and operation security standards before they are put in the field," says Weitzner. "We cannot experiment on our democracy."

"The consensus of security experts is that running a secure election over the internet is not possible today," adds Koppel. "The reasoning is that weaknesses anywhere in a large chain can give an adversary undue influence over an election, and today's software is shaky enough that the existence of unknown exploitable flaws is too great a risk to take."

Breaking down the results

The researchers were initially inspired to perform a security analysis of Voatz based on Specter's research with Ronald Rivest, Institute Professor at MIT; Neha Narula, director of the MIT Digital Currency Initiative; and Sunoo Park SM '15, PhD '18 , exploring the feasibility of using blockchain systems in elections. According to the researchers, Voatz claims to use a permissioned blockchain to ensure security, but has not released any source code or public documentation for how their system operates.

Specter, who co-teaches an MIT Independent Activities Period course founded by Koppel that is focused on reverse engineering software, broached the idea of reverse engineering Voatz's application, in an effort to better understand how its system worked. To ensure that they did not interfere with any ongoing elections or expose user records, Specter and Koppel reverse-engineered the application and then created a model of Voatz's server.

They found that an adversary with remote access to the device can alter or discover a user's vote, and that the server, if hacked, could easily change those votes. "It does not appear that the app's protocol attempts to verify [genuine votes] with the back-end blockchain," Specter explains.

"Perhaps most alarmingly, we found that a passive network adversary, like your internet service provider, or someone nearby you if you're on unencrypted Wi-Fi, could detect which way you voted in some configurations of the election. Worse, more aggressive attackers could potentially detect which way you're going to vote and then stop the connection based on that alone."

Writing for *Motherboard,* Kim Zetter explores a new study by MIT researchers that uncovers security flaws in a mobile voting app that was used in West Virginia and a number of other states. "It's really impressive that they were able to find such a pervasive set of vulnerabilities," says Prof. Matt Blaze of Georgetown Law School.

MOTHERBOARD

Verge reporter Russell Brandom writes that a team of MIT researchers has found that the Voatz mobile voting application is vulnerable to outside attacks. "After reverse-engineering Voatz's Android app, the researchers concluded that an attacker who compromised a voter's phone would able to observe, suppress, and alter votes nearly at will," writes Brandom.

THE VERGE

Wired reporter Lily Hay Newman writes about a new report by MIT researchers that identifies security vulnerabilities in a mobile voting application. Newman notes that the "MIT research speaks to the pressing need for transparent, auditable voting systems—a point researchers have also strenuously made about existing, in-person voting machines."

WIRED

Fast Company reporter Mark Sullivan spotlights a new study by MIT researchers that provides evidence that a popular voting app could allow hackers to alter, stop or expose how users have voted.

FAST COMPANY

MIT researchers have found that a new mobile voting application has a number of potential security vulnerabilities, reports Hiawatha Bray for *The Boston Globe.* The researchers found that "a hacking attack on the app could intercept votes, and possibly alter them, before they had been encrypted for secure transmission."

The Boston Globe

news.mit.edu/2020/voting-voatz-app-hack-issues-0213   2/4

2/24/2020   MIT researchers identify security vulnerabilities in voting app | MIT News

In addition to detecting vulnerabilities with Voatz's voting process, Specter and Koppel found that the app poses privacy issues for users. As the app uses an external vendor for voter ID verification, a third party could potentially access a voter's photo, driver's license data, or other forms of identification, if that vendor's platform isn't also secure.

"Though Voatz's privacy policy does talk about sending some information to third parties, as far as we can tell the fact that any third party is getting the voter's driver's license and selfie isn't explicitly mentioned," Specter notes.

Calls for increased openness

Specter and Koppel say that their findings point to the need for openness when it comes to election administration, in order to ensure the integrity of the election process. Currently, they note, the election process in states that use paper ballots is designed to be transparent, and citizens and political party representatives are given opportunities to observe the voting process.

In contrast, Koppel notes, "Voatz's app and infrastructure were completely closed-source; we were only able to get access to the app itself."

"I think this type of analysis is extremely important. Right now, there's a drive to make voting more accessible, by using internet and mobile-based voting systems. The problem here is that sometimes those systems aren't made by people who have expertise in keeping voting systems secure, and they're deployed before they can get proper review," says Matthew Green, an associate professor at the Johns Hopkins Information Security Institute. In the case of Voatz, he adds, "It looks like there were many good intentions here, but the result lacks key features that would protect a voter and protect the integrity of elections."

Going forward, the researchers caution that software developers should prove their systems are as secure as paper ballots.

"The biggest issue is transparency," says Specter. "When you have part of the election that is opaque, that is not viewable, that is not public, that has some sort of proprietary component, that part of the system is inherently suspect and needs to be put under a lot of scrutiny."

Topics: Cyber security   Voting and elections

Computer science and technology   Apps   Technology and society

Internet Policy Research Initiative

Computer Science and Artificial Intelligence Laboratory (CSAIL)

Electrical Engineering & Computer Science (eecs)

School of Engineering

RELATED

Paper: "The Ballot Is Busted Before the Blockchain: A Security Analysis of Voatz"

Michael Specter

James Koppel

Internet Policy Research Initiative

Computer Science and Artificial Intelligence Lab

Department of Electrical Engineering and Computer Science

School of Engineering

ARCHIVES

AI, the law, and our future

Report outlines keys to election security

MIT experts urge Trump administration to take immediate action on cybersecurity

CSAIL report: Giving government special access to data poses major security risks

2/24/2020   MIT researchers identify security vulnerabilities in voting app | MIT News

About This Website

This Website is maintained by the MIT News Office, part of the Office of Communications.

MIT News Office • Building 11-400
Massachusetts Institute of Technology • Cambridge, MA 02139-4307

2/26/2020

Blog @ Voatz
Chronicles of an Audacious Experiment

Search...

13
FEB

Voatz Open Press Call Transcribed from February 13, 2020

Published by Voatz • No comments yet • Permalink

The following Voatz press call took place on February 13, 2020 from 1-1:30pm ET. The contents of the call are transcribed below, lightly edited for punctuation and typos.

Full audio is available here.

Robert Dowling, Moderator:

Use the chat function to send us your questions. Direct all your questions to moderator and that way we will take them on as we have with, on a first come first serve basis. As some of you know, Voatz is regularly called on by members of the media and influencer community to respond to all kinds of conversations, including what's been raised by The New York Times today. Voatz as a small team of technologists and election experts focused on developing technologists that is often, the company is often unable to respond to every query in every way.

So we're doing this in an effort to respond quickly. Everyone is traveling, but they've taken time to jump on this call. We appreciate that, and if we don't get to all the questions or if there's a great amount of demand, we can host another call tomorrow or early next week. So, let's jump right in. Thank you in advance for your participation. We've got three executives from Voatz, Nimit Sawhney, CEO & Co-founder, Larry Moore, Senior Vice President and Hilary Braseth, Vice President. I will continue to prioritize the questions in terms of first come first serve. Hilary, could you kick things off with a quick overview and introduction to Voatz for those who are just getting introduced to the company for the first time?

Hilary Braseth, Vice President:

Definitely. Can everyone hear me okay?

Robert Dowling, Moderator:

You're coming through loud and clear.

Hilary Braseth, Vice President:

Okay. Excellent. Thanks so much, Robert. As Robert mentioned, I'm Hilary and I'm a Vice President at Voatz, and thanks to everyone for joining on such short notice. We very much look forward to responding to your questions about the report from MIT. But before we dive in, I just want to quickly introduce Voatz so that we all have a shared context for having this conversation.

So for the last five years, Voatz has been working on developing accessible, secure, and auditable technology that provides access for people who can't get to the polls or for whom paper ballots just don't work. This includes people with disabilities, the elderly, overseas military service, men and women. In order to do that, we have leveraged the latest security features of smartphones, like Apple and Android, the

---

Recent Posts

Valentine's Day Myth-Busters
Voatz Open Press Call Transcribed from February 13, 2020
Voatz Response to Researchers' wed Report
Voatz Leads Workshop at ck(H)er413 Hackathon in herst, MA
The Road to Online Voting

Categories

→ Activism
→ Africa
→ Awards
→ Democracy
→ Elections
→ Events
→ India
→ Musings
→ Polls
→ Press
→ Technology
→ UK
→ Uncategorized
→ US

phones that many of us use along with facial recognition technology to verify and validate the identity of the voter.

Nimit Sawhney, CEO & Co-founder:

Hilary

Hilary Braseth, Vice President:

Yeah?

Nimit Sawhney, CEO & Co-founder:

One moment. I think just out of courtesy, we should inform everybody that we would like to record this call and make sure everybody's okay with that.

Hilary Braseth, Vice President:

Okay.

Nimit Sawhney, CEO & Co-founder:

Can you, yeah. Hi, everyone, just letting you know that the call is being recorded and will be transcribed as well. Thank you, proceed.

Hilary Braseth, Vice President:

Okay. All right. So as I was mentioning, we leverage a handful of different technologies to provide voting access to those who can't otherwise make it to the polls. So, I was in the midst of mentioning smartphone technology. We pair that with facial recognition technology for verification and validation of the voter's identity. We leverage biometrics to secure and protect that voter's identity, and we use cryptography to automatically produce a paper ballot for tabulation of the jurisdiction, and lastly blockchain for rigorous post-election audits so that we can ensure voter intent is reflected in the overall count without revealing voter identity.

Hilary Braseth, Vice President:

Now, I realize that's a lot of tech buzzwords and I'm sure we can get into the specifics during Q&A. Above all, I want to reiterate that we are always interested in having conversations with people who want to explore the deeper underpinnings of our technology and even experience it. We are more than happy to have that conversation.

Hilary Braseth, Vice President:

I also want to address up front and right away that very often our system is accused of not having a way to ensure that after a voter makes selections on a smart phone, that they don't get changed during transmission. This is false. Every ballot submitted using Voatz produces a paper ballot, and every voter using Voatz receives a ballot receipt once they submit, and both of these documents are anonymized and encrypted, and together they form the building blocks for an end-to-end voter verified feedback loop that allows the jurisdiction to confirm that whatever the voters submitted on the smartphone is what's actually tabulated.

Hilary Braseth, Vice President:

We have worked exceptionally hard alongside or election officials and independent cybersecurity organizations to develop a very strict post-election audit process

that, for the first time in history, is open to anyone in the public to sign up. Anybody can be part of that audit process, and we encourage anyone to sign up to be an auditor of our pilots. I cannot emphasize that enough. These audits verify that every single ballot submitted using Voatz in those ballots, that voter intent is reflected and that tabulation is accurate. These audits are critical to both involving the community in our innovation process, but also ensuring that every single ballot submitted on our system can be verified independently without compromising the voter's anonymity.

Hilary Braseth, Vice President:

Last, before we dive into questions, I really quickly want to note that we have run more than 50 elections since 2016, including 9 targeted, well-designed governmental election pilots across five states for overseas voters and voters with disabilities. These governmental pilots have all been declared successes by the jurisdictions, and many of the voters who've used the system have shared very valuable feedback about how this voting option made participation accessible for them, and for some, this was the first time in decades.

Hilary Braseth, Vice President:

The reality is that our system, as it's currently designed, actively shuts out citizens from participating in our democracy and we are of the belief that we have to move the needle forward to provide these citizens with an easier way to vote, and in that process, security has always been our number one priority in moving forward with these small, targeted, well-designed pilots so we can learn, iterate, and build, and drive progress. Our hope today is we can have a frank and transparent conversation together and that we can have a chance to respond to the latest news about a report that was written about this morning in The New York Times.

Hilary Braseth, Vice President:

Robert, I'll hand it back to you. I know we have a lot of questions to get through.

Robert Dowling, Moderator:

Great, thanks. Thanks for the background, Hilary. We'll get through these as fast and efficiently as possible. The first set of questions come from Eric Geller, from Politico.

Robert Dowling, Moderator:

Is Voatz concerned about CISAs comment that is looking into MIT's new report on the app's vulnerabilities?

Nimit Sawhney, CEO & Co-founder:

Hi, this is Nimit. I can answer that. So, we are not concerned. We've been collaborating with CISA ever since the discussion about this report started a few days ago, and it's been a very transparent process with them, and we've communicated our feedback to them already throughout the process, so not worried about anything over that.

Robert Dowling, Moderator:

Is the company worried that it will lose contracts due to the research?

Larry Moore, Senior Vice President:

Hi, this is Larry. Of course we are, and we're also concerned that this report will scare off others, but I'm at an event in South Carolina right now and the feedback that we've received as late as this morning, and I mean, everyone who's read this report have had The New York Times article. But as late as this morning, the response has been very gratifying to us.

Robert Dowling, Moderator:

Okay. What evidence does Voatz have that the researchers are motivated by a desire to "thwart the process of innovation and progress for better voting access"? "Disrupt the election process", "sow doubt in the security of our election infrastructure", and "spread fear and confusion".

Larry Moore, Senior Vice President:

Yeah. Let me take that one again. Again, this is Larry Moore. So first of all we are, I was just trying to do this on Google Maps, but we're probably less than two miles away as the crow flies from the MIT Research Lab in Downtown Boston, so we're close. They could have contacted us. Had they invited us over, we had come over on the red line, but they didn't avail themselves of the hacker one program and riffed that in the report, and yet, that would have taken a trivial effort on their part to just confirm the allegations of the jailbroken phones, but they didn't do that.

Larry Moore, Senior Vice President:

The other evidence is the last couple of paragraphs in their report where they say, "Given the severity of failings discussed in the paper," which we dispute, "the lack of transparency," which we also dispute, "the risks of voter privacy and the trivial nature of the attacks, we suggest that any near future plans to use the app for high stakes elections be abandoned." So not a very collaborative environment here, and they use the media attention to, in a pretty aggressive way, to really try to stop this process in these pilots.

Robert Dowling, Moderator:

Thanks. Why did Voatz accuse the researchers of trying to remain anonymous when they put their names on the paper?

Hilary Braseth, Vice President:

I can take this one. So throughout the process of the researchers initially getting in touch with CISA, they decided to remain anonymous throughout that process, and we could have some guesses as to who the researchers were, but even up until publication in The New York Times, they refused to reveal their identity. We are unaware of why they didn't want to reveal their identity. We would have been, as Larry mentioned, happy to have engaged in thoughtful conversation with them and helped them to validate whether or not their approach was sound.

Larry Moore, Senior Vice President:

Yeah, and one of the thing, Hilary, I'll just add to that, they demanded and we exceeded to the demands of having a one on, having a phone call with all of our customers, without us being present, mediated by CISA. Even on that phone call, which happened on Tuesday, a week ago, they did not disclose their own, their identity.

Robert Dowling, Moderator:

If Voatz believes that the research is wrong due to the researchers use of a simulated server, will Voatz let them access its a real server to perform the same analysis?

Nimit Sawhney, CEO & Co-founder:

Hi, this is Nimit here again. I can answer that. Absolutely. We offered that to them as part of our initial response via CISA.

Nimit Sawhney, CEO & Co-founder:

There was no response from researchers. And moreover, we already have this server available. It's to our public bug bounty program. Anybody who wishes to sign up, test that apps over there, against the real server with full functionality, is able to do that. And so that system's already available. They willfully chose not to do it. So absolutely, one of the first things we offered in our responses, why don't you prove all these claims on a real system, and then we can investigate further. But they did not respond to that at all.

Robert Dowling, Moderator:

Thanks Nimit So the next set of questions come from Russell Brandom from The Verge. First question is, I understand from the post that the MIT researchers were testing an outdated version of your software and weren't connected with Voatz servers. However, the post stops short of saying that the vulnerabilities discovered had been patched in recent version. I'm curious if you can speak directly to the status of those vulnerabilities.

Nimit Sawhney, CEO & Co-founder:

Absolutely. So they had whole paper is riddled with holes, if I can use that word. For example, they talk about our use of the blockchain and say, executing a 51 percent attack. That attack is not possible because we do not use a public blockchain. We use a permissioned blockchain based on Hyperledger, and such an attack is not possible on that infrastructure. Similarly, they assume that by defeating the malware and the jailbreak detection on the mobile devices, that they will be able to connect to our server. Because they didn't connect to our server, they did not experience all the checks which happen on the server, which would have prevented them from doing anything.

Nimit Sawhney, CEO & Co-founder:

And then all of their claims are based off that. That because they were able to jailbreak or successfully compromise a client device, that the assumption that device would be able to connect to our server is completely, completely flawed. And so that's the really, really strange thing was, why would they do such a hypothetical analysis when they had a real system to actually test it out?

Nimit Sawhney, CEO & Co-founder:

Similarly, there's another–

Larry Moore, Senior Vice President:

Nimit, a reminder to talk about the first claim on the side channel link.

Nimit Sawhney, CEO & Co-founder:

Yes, I was getting there. So one of the claims they have is, as Larry mentioned, it's called a side channel leak. To drill it down, what it means is as network traffic is passing through while people are using their devices, that by looking at that encrypted network traffic, they can deduce who you are voting for, and then start disrupting that traffic to the disadvantage of the voter. And hypothetically, that may be possible. In a realistic scenario, that's not possible given how our pilots are conducted. Secondly, that issue of a side channel problem was fixed many months ago. So if they had used the newer version of our system, they wouldn't have even seen that. But we want to reiterate that in a real world scenario, exploiting that is extremely, extremely hard. Especially in the case of our pilots where voters are distributed, it's a smaller amount of voters. They're distributed around the world, breaking into network routers, cell towers, isolating individual voters, breaking into their devices... I mean, these are... This is hypothetical scenario. It's not realistic at all.

Larry, is there anything you'd want to add to that?

Larry Moore, Senior Vice President:

Yeah, the... Maybe a little humor on the side channel leak. So despite the fact that we really fixed it, I mean think about what's going on. They have, again, to repeat Nimit, the voters, which there are less than 600 across nine pilots, dispersed around 40 countries. You'd have to gain access to the routers that are located in the cellular providers' networks or at military bases. And just think about how hard that is. The example that they used, it basically looks trivial if you've got one contest and two candidates that have different length names. Bush V Gore for example, would not work.

Larry Moore, Senior Vice President:

And so by looking at gibberish, which is what the encrypted traffic looked like, they claim that you can deduce somewhat easily the identity of the candidates that are being voted for, and then choose to disrupt the traffic back to the server so that the vote would never get registered. That also ignores the guaranteed delivery of messages, and the voter would notice this right away. So, and once again, how did they attack... Attach to the network? They would've seen this.

Robert Dowling, Moderator:

So just to follow up on Russell's question for absolute clarity. He asked, have they been patched? And it sounds like, did they exist? If so, have they been patched? Are they mitigated or otherwise addressed from some server-side protection? I'm curious if you can say why Voatz users should not be worried about the vulnerabilities described in the MIT paper.

Nimit Sawhney, CEO & Co-founder:

Absolutely. So as Larry mentioned earlier, the side channel issue, even though we think it's largely theoretical at this stage, was addressed in one of our versions much newer than the version which the researchers looked at. Regarding the other protection, yes. So their claim of being able to compromise a device and then being able to use that to connect to the network, that would have gotten blocked by server-side protection. And so definitely, there's a lot of the intelligence in the system that relies on the server-side, in the cloud, which they completely missed because they were just looking at one isolated piece of the system. So as far as

Voatz users are concerned, we do not believe that they should be worried at all about these vulnerabilities, which they are highlighted.

Robert Dowling, Moderator:

Good. Okay, thank you. So we're going to go to the next set of questions from Alexander Culafi from TechTarget. The first question is really looking for clarity about what we were just talking about. The researchers' paper said Voatz confirmed the existence of the side channel and PIN entropy vulnerabilities. Is this accurate? I think we've more or less covered it, unless there's anything you want to add there.

Nimit Sawhney, CEO & Co-founder:

I can add something about the PIN entropy. So the system supports PINs of various lengths, various complexities. You can even use external multi-factor devices. But keep in mind, we are focused on accessibility here to make it as convenient as possible for voters without compromising on security. And so the common approach used there is, if you don't have biometrics enabled on your device, if you're not using a fingerprint or a face ID, then you can as a last resort, for accessibility, resort to an eight digit pin. Now an eight digit pin has 100 million permutations. So in order to crack a pin for a pilot voter, firstly you have to get physical access to that voter's device. Then you have to get into that device, run a brute force, it would probably take you two days at the minimum. Destroy the battery, by which time the user would have detected you. And so that's why we feel it's not at all realistic at the moment.

Robert Dowling, Moderator:

Got it. The research paper says Voatz does not actually use blockchain technology to submit votes from a mobile device to the servers. Is this accurate? And if so, then why does Voatz official documentation suggest it does use blockchain for votes submissions?

Nimit Sawhney, CEO & Co-founder:

So this claim is completely inaccurate. Right from our very first election, we have used the Hyperledger based blockchain framework. With every pilot we've enhanced it, made improvements to it, and continued to do so. Our post-election pilots, ever since the third pilot done by then Denver County, have all utilized the blockchain infrastructure to facilitate the forced post-election audit, which citizen auditors have audited. NCC, which is the National Cybersecurity Center, has audited. So this claim is completely baseless. And if they had tried to dig in more into the system, into the reports which are available on our website, they would not have made this claim that we don't use the blockchain.

Robert Dowling, Moderator:

Are there differences between the field-tested version of the Voatz app and the version covered in the HackerOne Bug Bounty program?

Nimit Sawhney, CEO & Co-founder:

No, there are not. The only differences, the servers they connect to, the field versions obviously will connect to a production infrastructure when a live election is in progress. The HackerOne applications connect to a replica infrastructure which is identical to the live infrastructure. Just that it's not a live infrastructure. So

you, as a researcher, can request access to test elections if you like. Like many researchers have done, you can request enhanced access where you get... We can provide these special versions of the applications which have less security so you can do more drilling and you know, more kind of under the hood studies as well. And so, but the version available on the bounty program and public production versions are the same. They connect to a different server on the backend.

Robert Dowling, Moderator:

Got it. A Voatz statement said the research team used a flawed approach by constructing hypothetical backend servers, but were the modeled servers used by the research team an accurate representation of Voatz's servers? And if not, how are they different?

Nimit Sawhney, CEO & Co-founder:

They missed a lot of things, so they were not accurate. At best, they were somewhat partial because they could not see all the components.

Nimit Sawhney, CEO & Co-founder:

They could not see all the components. They could not even reverse engineer all the code in the Android app that they looked at. And so they're missing some pieces in the Android app itself. I would say they probably missed 50% of our server architecture information as well, and so that's why we call it really flawed because had they gone through the bug bounty program or collaborated with us through other means, they could have gotten access to the full infrastructure and had a more accurate view of how our system works.

Robert Dowling, Moderator:

Got it. The next set of questions come from Hiawatha Bray from the Boston Globe. Can you confirm that some other states are planning to use the vote software in this year's election? Which states? Also, how many states are using the votes app this year?

Nimit Sawhney, CEO & Co-founder:

Hilary, that's for you.

Hilary Braseth, Vice President:

Yeah, I can take that one. We typically leave any announcements to the jurisdiction. So any new jurisdiction that's going to be using our technology this year, we'll let them make that announcement.

Robert Dowling, Moderator:

How do you get a printout from your smartphone?

Hilary Braseth, Vice President:

So this question might be in reference to what I said in the introductory remarks. As soon, and I was describing kind of the post vote audit trails, so we do have an infographic that delineates and tries to simplify yet still honor the technical process behind the vote system. So if anybody on this call is interested in having a copy of that infographic, please reach out to the organizer of this call and we can get that

to you. But the short of it is that as soon as the voter submits her ballot on her smartphone, three really important things happen.

Hilary Braseth, Vice President:

One, instantly she receives a receipt with all of her selections. This receipt is anonymized, it's password protected, and only she holds the password to see that receipt. The purpose of this receipt is so that the voter can verify her selection, as I reiterate. Simultaneously, what happens at the jurisdiction is an official ballot that is marked with this voter's selections has been formed at the jurisdiction, and on election day two members from the jurisdiction possess the keys to unlock what we call a digital lockbox where they unlock it and print the official ballots for tabulation.

Hilary Braseth, Vice President:

At the close of the election, comparing that digital receipt with the voter's selection that's anonymized with that official ballot, both are signed with an anonymous ID, selection by selection validates that voter intent is reflected in the overall count and to make sure that nothing nefarious happened in the transmission of the voter's vote. Not to get too technical, but the third and last thing that happens, because I mentioned there were three things that happen when a voter submits. The last thing that happens is when a voter submits their ballot, each oval on that ballot passes through that Hyperledger public permissioned blockchain network that Nimit was mentioning, and that serves as the final and third audit piece as an untamperable record in the event that something were to happen to the paper tally. So that digital receipt, the official paper ballot, comparing those two verifies that intent is reflected in the overall count. And then the blockchain record is the overall final audit piece. I hope that clarifies. And again, we have an infographic that delineates this.

Robert Dowling, Moderator:

Thanks Hilary. Aaron Mack from Slate asks, I was wondering if votes had a statement on Mason County deciding not to use the app.

Larry Moore, Senior Vice President:

So I'll take that. I know the auditor there pretty well. So surely this was disappointing to us. He was under intense pressure to back out, but as late as this morning, he indicated he wished he'd stayed in. But I want to put a plug in for the Voatz system, we don't know of another system that in fact could have backed out votes that had already been cast. And that's a real strength of the system. So yes, votes had been submitted in Mason County. And when Paddy McGuire said I need to pull the plug, we were able to back those out and they never counted.

Robert Dowling, Moderator:

Got it. Kevin Collier from NBC asks, I believe Voatz has gone through several independent audits, the results of which it hasn't made public. When you say who each of these auditors are and will you ever make the results public?

Nimit Sawhney, CEO & Co-founder:

I can address that. So many of the audits we've done in the past, as we mentioned earlier, have been under stipulations warranted by the NDA, so we are unable to reveal the names. However, findings have been shared with our customers, and so

there are some audits happening for which information is publicly available. One of them was conducted by the DHS. That's report is available on our website, so if you go into the FAQ section, you'll find a report. And as more public reports are available, we will be sharing them on our website as well.

Robert Dowling, Moderator:

Right. We have one more question that's come in during the call from Rob Right at Tech Target. Voatz took issue with the fact that the researchers wouldn't disclose their identities. But you also offered these same anonymous researchers access to your backend servers? Is that correct?

Nimit Sawhney, CEO & Co-founder:

Yes, we did. When the initial discussions were happening, these are moderated by the team at CISA. We did request the researchers to use our bug bounty system, in which case they can remain anonymous. They don't have to reveal themselves. And prove their claims. Because they didn't actually prove a single one of their claims. It's all hypothetical. And so it's like, okay, why don't you prove this on a real system? And if it's a real problem, other than the side channel one, which we had already previously fixed, if any of the others are real problems, minus the server one. That was a whole sense of hypothesis there, but any of the other issues they highlighted, we would have loved to engage with them but they did not even reply. Larry, you want to add something?

Larry Moore, Senior Vice President:

Yeah. Let me pause for just a second before we go onto any other questions and just talk about the nature of pilots. On innovations in elections, and I think I can say this with a great deal of certainty here, have started with... All innovations in elections have started with pilots, from the time the industry moved from precinct voting to vote centers in early voting, to the time when Washington and Oregon pioneered all vote by mail. These have all started with pilots. And in every single case, security was raised as an issue. And so we see this as a continuum going on. And we're not at all saying that we're ready for universal access or universal adoption, but we feel like we're very responsible starting off with really the two most vulnerable cohorts in the electorate. And that's military and overseas voters, their families and civilians residing abroad as well as voters with disability who have a legal right to access new technology as it's presented to, for example, military and overseas voters.

Larry Moore, Senior Vice President:

So pilots are inherently part of the progress that gets made in elections, which we may agree has been largely a stagnant industry. And these attacks that have been leveled against us this morning really are a continuum of the attacks against this kind of technology that started nearly 18 years ago. And the same arguments are being used. I think the MIT researchers spent a lot of time compiling this report, and I think it would have been a lot better had they collaborated with us instead of attacked us.
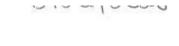
Robert Dowling, Moderator:

Thanks, Larry. And thank you everyone. I know we are past time. You can send follow up questions. We're taking them by email. Give us feedback on the call. And also if you need more information, please reach out. We'll of course let everyone

know if an additional call is necessary and gets scheduled and are happy to
address follow up questions. Thanks for your time and have a great afternoon.

- Democracy · Elections · Events · Press · Technology · US
- No tags

About Voatz

915-2020 Voatz, Inc.

Blog @ Voatz
Chronicles of an Audacious Experiment

13
FEB

Voatz Response to Researchers' Flawed Report

Published by *Voatz* • No comments yet • Permalink

Voatz wishes to acknowledge the enormous effort it must have taken for the team of researchers, until this point anonymous to us, to produce "*The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S Federal Elections*".

Our review of their report found three fundamental flaws with their method of analysis, their untested claims, and their bad faith recommendations.

First, the researchers were analyzing an Android version of the Voatz mobile voting app that was at least 27 versions old at the time of their disclosure and not used in an election. Had the researchers taken the time, like nearly 100 other researchers, to test and verify their claims using the latest version of our platform via our public bug bounty program on HackerOne, they would not have ended up producing a report that asserts claims on the basis of an erroneous method.

Second, as the researchers admitted, the outdated app was never connected to the Voatz servers, which are hosted on Amazon AWS and Microsoft Azure. This means that they were unable to register, unable to pass the layers of identity checks to impersonate a legitimate voter, unable to receive a legitimate ballot and unable to submit any legitimate votes or change any voter data.

Third, in the absence of trying to access the Voatz servers, the researchers fabricated an imagined version of the Voatz servers, hypothesized how they worked, and then made assumptions about the interactions between the system components that are simply false. This flawed approach invalidates any claims about their ability to compromise the overall system. In short, to make claims about a backend server without any evidence or connection to the server negates any degree of credibility on behalf of the researchers.

The researchers have labeled Voatz as "not transparent". With qualified, collaborative researchers we are very open; we disclose source code and hold lengthy interactive sessions with their architects and engineers. We educate them on the critical demands of election security; they give us feedback and educate us on new best practices based on their practical knowledge of security drawn from other industries.

Voatz has worked for nearly five years to develop a resilient ballot marking system, a system built to respond to unanticipated threats and to distribute updates worldwide with short notice. It incorporates solutions from other industries to address issues around security, identity, accessibility, and auditability.

We want to be clear that all nine of our governmental pilot elections conducted to date, involving less than 600 voters, have been conducted safely and securely with no reported issues. Pilot programs like ours are invaluable. They educate all election stakeholders and push innovation forward in a responsible, transparent way. For nearly two decades, the researchers and the community to which they belong have waged a systematic effort to dismantle any

Search... 🔍

Voatz
@Voatz

Traditionally, college students have voted at one of the lowest rates of any group in the U.S. We've been excited to see this change in recent years as colleges adopt techniques to encourage their students to #vote: lat.ms/2DqYoiU #civicengagement

5:00 pm · February 14, 2020

1,471 followers

:cent Posts

Valentine's Day Myth-Busters
Voatz Open Press Call
inscribed from February 13, 2020
Voatz Response to Researchers' wed Report
Voatz Leads Workshop at ck(H)er413 Hackathon in iherst, MA
The Road to Online Voting

itegories

→ Activism
→ Africa
→ Awards
→ Democracy
→ Elections
— Events
→ India
→ Musings
→ Polls
→ Press
→ Technology
→ UK
→ Uncategorized
→ US

online voting pilots. These attempts effectively choke any meaningful conversation and learnings around the safe integration of technology to improve accessibility and security in our elections. The effect is to deny access to our overseas citizens, deployed military service men and women, their families, and citizens with disabilities.

It is clear that from the theoretical nature of the researchers' approach, the lack of practical evidence backing their claims, their deliberate attempt to remain anonymous prior to publication, and their priority being to find media attention, that the researchers' true aim is to deliberately disrupt the election process, to sow doubt in the security of our election infrastructure, and to spread fear and confusion.

The reality is that continuing our mobile voting pilots holds the best promise to improve accessibility, security and resilience when compared to any of the existing options available to those whose circumstances make it difficult to vote.

Democracy · Elections · Press · Technology · US
No tags

About Voatz

→ World

chives

February 2020
January 2020
December 2019
November 2019
October 2019
July 2019
June 2019
May 2019
April 2019
March 2019
February 2019
January 2019
November 2018
October 2018
September 2018
August 2018
June 2018
May 2018
→ April 2018
→ March 2018
→ February 2018
→ January 2018
→ November 2017
→ September 2017
→ July 2017
→ June 2017
→ March 2017
→ February 2017
→ October 2016
→ September 2016
→ July 2016
→ June 2016
→ May 2016
→ April 2016
→ March 2016
→ January 2016
→ October 2015
→ September 2015
→ August 2015
→ July 2015
→ June 2015
→ May 2015
→ April 2015
→ March 2015

DocuSigned by:

Tanner Ainge

B5F901465FEC43D...

TANNER AINGE
Commission Chair

ATTEST:

DocuSigned by:

Alice Black

2937075D91C74DB...

Deputy Clerk/Auditor