Election Data

[Election Data Stored in the Cloud with Amazon Web Services]
[90% of U.S. Voting Systems – Dominion, ES&S, Hart]
[Voting Data- Who Has It?]
[G2M 2021 Multi-Vendor Webinar Schedule]

Forget political parties, candidates, and the controversary of any given election for a moment. Elections and candidates come and go but voter registration databases and voting systems stay. Which companies manage voting systems? What happens to voter registration data, who manages voting, who is accessing voter data between elections? (Is there such a thing as "between elections"?) This newsletter focuses on storage and management of election data.

We send this newsletter to you via Mailjet which does not offer a bookmark feature. If you want to go directly to an article, you can by clicking on the title of the article in the highlights section above, but to do so, you need to view our newsletter directly from our website using this link. I find it more convenient to skip around rather than scrolling through the entire newsletter.

Join us for our January webinar (info next) and check out our entire 2021 webinar schedule at the end of the newsletter.

Thanks, Mike Heumann and the entire G2M Team

Election Data Stored in the Cloud with Amazon Web Services

Forty states, the U.S. Federal Elections Commission, and both the Democratic and Republican party rely on Amazon Web Services for cloud storage of all election data. Amazon Web Services, and its partners, run state and county election websites, store voter registration and ballot data, help provide live election-night results, and facilitates overseas voting by military personnel. Clients include political candidates, civic groups, election offices, and the League of Women Voters. Amazon has three categories of election-related clients: election administrators in states and counties, political campaigns, and election-related non-profits.

AWS does not handle actual voting on election day. Voting machines in most states are not connected to any cloud service.

This stronghold on election data storage services is good news and bad news. The good news is that Amazon's cloud services are more reliable that the outdated systems they have replaced, and security experts believe they are also much harder to hack. For example, in Oregon the state's in-house servers that support election services shut down every time there is a power outage (a surprisingly frequent occurrence as Oregon updates its electric grid). Moving voter registration systems to the cloud fixed that problem.

However, on the bad news side of the equation, with centralized data on a single system, one major breach could be extremely damaging. Chris Vickery, Director of Cyber Risk Research at UpGuard, warns, “It makes Amazon a bigger target” for hackers, “and also increases the challenge of dealing with an insider attack.”

Microsoft Corp's Azure, the biggest rival to AWS, has a sizeable government business and offers some election services but lags Amazon in this arena. Microsoft has software called ElectionGuard that the company says tabulates and secures election results. Amazon, however, does not have a specialized product for hosting and protecting election data. Rather, Amazon's cloud offers a more generalized service that clients can adapt to different needs and industries.

North Carolina chose Amazon Web Services over Microsoft’s Azure to deliver election night results reporting because it “was simple to set up (and) very low in cost,” the State Board of Elections said, saying they previously spent “thousands of dollars” on a similar service. California’s Alameda County paid under $100 a year for citizens to view election night results.

Amazon had 33% percent of the overall cloud market in the second quarter of 2019 followed by Microsoft, according to SRG Research. AWS, officially launched in 2006, generated $25.7 billion in sales in 2018 and is the company’s biggest profit-generator. It was not clear how big the election business is inside AWS.

Tom Burt, Corporate Vice President of Customer Security and Trust at Microsoft, reported targeted cyberattacks on election data in September 2020. These included – 1) Strontium, operating from Russia, attacked more than 200 organizations including political campaigns, advocacy groups, parties and political consultants, 2) Zirconium, operating from China, attacked high-profile individuals associated with the election, including people associated with the Joe Biden for President campaign and prominent leaders in the international affairs community, 3) Phosphorus, operating from Iran, tried to log into President Trump's campaign staff's Microsoft accounts in May and June. The majority of these attacks were detected and stopped by security tools built into Microsoft products.

Greg Miller, co-founder of the OSET Institute, which works with the Department of Homeland Security and Congress on election security, noted that many of Amazon’s partners - such as managed service providers who are tasked with delivering AWS services to customers - do not have the credentials or experience needed in delivering and handling election services.

Three hacks of private information stored on cloud servers provided by AWS. In 2016, Mexico's entire voter database was hacked and made publicly accessible online until discovered by U.S. security researchers. In 2017, a political consultancy firm named Deep Root Analytics had voter information it was gathering for the Republican Party posted online for 12 days due to a server misconfiguration. Last year, Capital One bank had 100 million credit card customers' personal information stolen by a former Amazon employee.

Amazon secures the cloud infrastructure and gives clients suggestions and guidance on how to best safeguard data, but customers are responsible for building their own security protocols to protect whatever they store. “We think (AWS) provides us with the best available level of security,” said Ron Morgan, Chief Deputy County Clerk of Travis County in Texas, one of the largest counties in the state, which uses Amazon’s servers to run its election website. “Is it bullet proof? I don’t know,” he added. “But is it a very, very hard target? Absolutely.”

Fun Fact: To settle a tied race in 2014 for Neptune Beach City Council in Florida, one of the two candidates’ names was drawn from a hat. The winner of that drawing then got to call heads or tails during a coin toss. The winner of that coin toss then chose whether to go first or second in a random drawing of ping-pong balls.

Richard Arthur pulled a No. 12 ping pong ball out of a bag. Rory Diamond drew a No. 4 ball. Arthur, with the highest number, was named the winner.

HART intercivic

DOMINION VOTING

ES&S ELECTION Systems & Software

90% of U.S. Voting Systems - Dominion, ES&S, Hart

Three companies, Election Systems & Software, Dominion Voting Systems, and Hart InterCivic, account for 90% of the election voting system market.

The U.S. Election Assistance Commission (EAC) provides oversight for voting equipment, but the 30 person agency’s insight is merely recommendations to election voting system companies, not mandatory. They cannot regulate the industry. The EAC distributes the funds

appropriated to states by Congress. The DHS designated election systems "critical infrastructure" but do not regulate or sanction manufacturers if there are problems. Additionally, the election voting system market maintains tight control over access to their software, with an obvious objective of preventing fraud and hacking, but the source code used to design ballots and tabulate votes is proprietrary, also preventing oversight. The Digital Millennium Copyright Act, Section 1201, provides protections for the source code owner from others accessing and viewing the source code.

Dominion has contracts with 19 states and 133 local governements. In 2019, Dominion entered into a 10 year, $107M contract with Georgia for 30k touch screen voting machines and to install a "verified paper ballot" voting system. Dominion has a $52M contract with the state of New Mexico. Michigan has contracts for $31.5M for machines, equipment repair, election services, ballot marketing printers, vote tabulators and ballot boxes, and election and voting machine coding.

Dominion touts the security of their systems by explaining that voting systems are designed and certified by the U.S. government, are designed as closed systems that do not rely on Internet connection, they build their own code and have no tied to other providers, and their systems and software components are submitting to federally-accrediting, third-party test labs which perform code reviews. They explain that there are no means to remotely access voting data and observers can witness each step of the voting process. Additionally, Dominion produces paper records for auditing.

Tom Burt, President and CEO of ES&S, outlined steps ES&S has taken to ensure election security. Additionally, ES&S has asked Congress to pass legislation requiring a paper record for every vote cast

John Poulous, CEO for Dominion Voting Systems, asked Congress to help voting machine providers address cyber threats.

Donald Palmer, a, EAC commissioner, says the $380M for election security approved by Congress in 2018 is being used by most states to replace outdated voting machines and to upgrade cybersecurity services and is critically important to securing election infrastructure.

Matt Blaze, a Georgetown University Law Center professor, believes much of the nation's infrastructure remains vulnerable to attacks ranging from election tampering in local races to "large-scale disruption by national adversaries."

Liz Howard, former Deputy Commission of the Virginia Department of Elections and now counsel at New York University's Brennan Center for Justice, believes there is a need for more federal oversight of election machine vendors, "Election vendors, including voting system vendors, have received little federal or congressional oversight. This would go a long way towards enabling private sector election providers to better prioritize resource allocations in the same economic terms as other enterprise decisions."

Senate Intelligence Committee Chairman, Richard Burr, explains, "We want to make sure that there is a threshold that everybody hits and that when the federal government is looking into intrusions into systems, we don't have to worry about the systems, so having that threshold in that is important."

"If Congress can pass legislation that requires a paper record for every voter and establishes a mandated security testing program for the people making voting machines, the general public's faith in the process of casting a ballot can be restored. That's not just a good thing; it's essential to the future of America."

Tom Burt, President and CEO of ES&S

Voting Data – Who Has It?

Sources of voting data include the Federal Election Commission, the U.S. Census Bureau, National Elections Studies, General Social Survey, CQ Voting & Elections Collection, American National Election Studies, Presidential Election Data (UCSB Repository), Roper Centre United States Elections, U.S. Electoral College, U.S. House of Representatives Historical Election Data, Inter-University Consortium for Political and Social Research, Political Database of the Americans, Gallup Poll, New York Times Polls, and others.

Federal Election Commission - The FEC is the regulatory agency that administers and enforces federal campaign finance law. Its jurisdiction extends to U.S. House, Senate, Vice Presidential and Presidential elections. Data is available regarding funds raised and spent to influence

U.S. Census Bureau – The U.S. Census Bureau operates under Title 13 and 26 of the U.S. Code. Data includes downloadable copies of populations reports and tables for presidential and congressional election year survey results. Population data is collected and used to determine the distribution of Congressional seats to states as mandated by the U.S. Constitution. The data is also used for allocation of community services for elderly, infrastructure, and annual distribution of $675B in federal funds to local, state, and tribal governments. Age search information is used for qualifying for social security, passport applications, and proving relationship in settling estates.

American National Election Studies – ANES is a collaboration of Stanford University and the University of Michigan, with funding by the National Science Foundation. ANES conducts surveys and collects data regarding electoral behavior, political participation, and public opinion, but provides no summary analysis of the data. The data is available for research purposes.

Presidential Election Data (UCSB Repository) – The American Presidency Project espouses the goal to be recognized as the authoritative, non-partisan on-line source for presidential public documents.

Roper Centre United States Elections - Both the Roper Center and ICPSR provide access to social science data. The Roper Center focuses on public opinion data primarily collected by commercial and media survey organizations, while ICPSR archives broader based social science data from academic or government sources. Public opinion data is a small portion of the ICPSR collection and overlaps only slightly with the Roper Center's collection of polls.

U.S. Electoral College – National Archives - The Office of the Federal Register (OFR) is a part of the National Archives and Records Administration (NARA) and, on behalf of the Archivist of the United States, coordinates certain functions of the Electoral College between the States and Congress. Acting as an intermediary, it reviews the Certificates of Ascertainment and Vote before Congress accepts them as evidence of official State action in preparation for the counting of electoral votes in Congress. In addition to posting them on this website, OFR makes the physical Certificates available for public inspection for one year following the election. After that year, the Certificates become part of the National Archives collection.

U.S. House of Representatives Historical Election Data - Since 1920, the Clerk of the House has collected and published the official vote counts for federal elections from the official sources among the various states and territories.

Inter-University Consortium for Political and Social Research – ICPSR is an international consortium of over 750 academic institutions and research organizations and maintains a data archive of over 250k files of research in social and behavioral sciences. ICPSR maintains and

provides access to a vast archive of social science data for research and instruction (over 14,000 discrete studies/surveys with more than 65,000 datasets). Since 1963, ICPSR has offered training in quantitative methods to facilitate effective data use.

Political Database of the Americans – The PDBA is a project of the Center for Latin American Studies (CLAS) at Georgetown University in collaboration with institutions like the Secretariat for Political Affairs of the Organization of American States and FLACSO-Chile, and also with the support of other organizations and entities in the region. The PDBA offers data regarding institutions and political processes, national constitutions, branches of government, elections, and political constitutional studies. The mission is to contribute to the study, promotion and strengthening of democracy in the hemisphere, through the collection, systematization, dissemination, and exchange of information, data, statistics, and institutions from a political perspective, comparative studies; and other resources relevant to the 35 countries of the region.

Gallup Poll – Gallup is a global analytics firm; Gallup Poll is a division that regularly conducts public opinion polls.

New York Times Poll – A report that outlines and tabulates results of exit polls for presidential elections from 1972 to 1996 and includes demographic data including age, economic status, level of education, gender, geography, marital status, political ideology, race, religion, and voting status.

States have varied requirements on who is eligible to request a voter registration lists, what information the list contains, what information is kept confidential, and how information contained in voter lists may be used. Many states also have specific programs to keep all voter information confidential for certain classes of voters.

For example, California voter data availability is governed by the Cal. Elections Code and Cal. Government Code and allows access to candidates, parties, ballot measure committees, and any person for election, scholarly, journalistic, or political purposes, or for governmental purposes, as determined by the Secretary of State. All voter information is confidential except for those listed that may request lists. Voter data provided includes name, address, telephone number, and political party preference. Specifically prohibited uses of the data includes harassment of any voter or voter household, advertising, solicitation, sale, marketing of products or services, reproduction except for authorized purposes.

Fun Fact: Coin tosses and other games of chance have broken ties in New York, Illinois, Wisconsin, Ohio, Missouri, Washington, Florida, Minnesota and New Hampshire.

South Dakota and Arizona have used card games.

G2M Research Multi-Vendor Webinar Series

Our 2021 webinar schedule is ready! Click on any of the topics to get more information about that specific webinar. Interested in Sponsoring a webinar? Contact G2M for a prospectus.

Our November webinar Implementing NVME™ & NVMe-oF™ for Cloud Service Providers was sponsored by Kioxia (Joel Dedrick), Lightbits (Josh Goldenhar), and Western Digital (Mark Miquelon). View the recording and/or download a PDF of the slides.

2021 Webinars

Jan 26:	Can Your Server Handle The Size of Your SSDs?
Feb 23:	Storage Architectures to Maximize the Performance of HPC Clusters
March 23:	One Year after COVID-19: How Did Storage Architectures Perform for Biotech AI Modeling & What Can We Learn From This?
April 20:	The Race to be Relevant in Autonomous Vehicle Data Storage (both On-Vehicle and Off-Vehicle)
May 18:	Responsive and Efficient Storage Architectures for Social Media
June 15:	It's 2021 - Where Has NVMe-oF™ Progressed To?

July 13:	Computational Storage vs Virtualized Computation/Storage in the Datacenter: “And The Winner Is”?
Aug 17:	AI/ML Storage - Distributed vs Centralized Architectures
Sept 14:	Composable Infrastructure vs Hyper-Converged Infrastructure for Business Intelligence
Oct 12:	Cloud Service Providers: Is Public Cloud, Private Datacenter, or a Hybrid Model Right for You?
Nov 9:	The Radiometry Data Explosion: Can Storage Keep Pace?
Dec 14:	2021 Enterprise Storage Wrap-up Panel Discussion