Deep Knowledge Analytics
GovTech Division

DEEP
KNOWLEDGE
ANALIYTICS
GOVTECH DIVISION

GovTech Solutions for 2020 Elections: US Case Study

December 2020

www.govtech.global

Table of Contents

CONTACT US

www.govtech.global
info@govtech.global

Introduction

GovTech Division of Deep Knowledge Analytics, a subsidiary of Deep Knowledge Group, is launching the series of quarterly overviews of GovTech and E-Government Technologies used in elections and various types of voting. Our first case study is focusing on the US and its purpose is to analyze GovTech solutions used in the recent US 2020 Presidential election. In the future, DKA will cover other countries and regions and their applications of GovTech solutions.

The purpose of this report is to analyze modern technological tools/concepts used over the course of the past few years in the US election process. As society is rapidly implementing a wide array of digital technologies in almost every aspect, numerous significant issues, such as reliability, trustworthiness, accessibility, are manifesting themselves. The new tools and solutions used for public administration and government election process (generally referred to as "GovTech") are the focus of heated discussions. Such technologies advance and reshape the modern democracy approach.

2020, a year of turmoil, was a rather hard year for digital GovTech solutions as well. The **COVID-19 pandemic**, the **mass protests** (on a global scale), and a number of other contributing events led to the implementation of the new technological solutions. Those technologies, which were not widely accepted previously are now becoming more and more popular due to social distancing measures enacted by governments around the globe.

However, the trend of implementing new tech is not seen everywhere. Despite the fact that the US is a technological leader in multiple domains (mainly in Artificial Intelligence and biotechnological research), the US government is still way behind compared to much smaller countries in terms of introduction of reliable digital solutions.

Overall, the spectrum of technological solutions used for electoral purposes (voting and advertising) in the U.S. and globally is quite large. And this wide array of tools stays behind the digitalization of the electoral process which aims to reduce human mistakes during vote counting. It is also believed that these technologies may have the ability to return the public's trust in the institutions organizing such a socially and politically important event as elections. Big Data Analysis algorithms aim to provide campaigns with insights regarding the best approach to win the people's favor while voting machines replace humans with an objective to increase transparency and to decrease the time needed for the elections to be completed.

However, in reality, based on the US 2020 election, we see that digital technologies do not offer credibility to the political parties and overall political system which was/are using those technologies and e-Government solutions in political campaigns or elections in general. Currently, communication channels such as Twitter and Facebook became active participants in affecting in electoral process. Originally, their algorithms were supposed to be used in spreading the news and ideas about political candidates and increase mobilization of the electorate which could prove helpful when quick political decisions are needed, however latest events clearly demonstrated that these channels can limit the spread of the information by their own discretion.

Executive Summary

- **Advancements in science and engineering are intended to make our lives better and bring more transparency to various aspects of human activities.** While modern technologies provide solutions for multiple administrative problems, they are still not a panacea against unfair practices during elections. **The advancement of the 21st century's GovTech (Government Technologies and E-Governance) solutions is promising in terms of reevaluating our views on modern political administration,** however, the general population is still concerned about them as most attempts to introduce various electronic technologies in the administrative processes (including elections) failed to produce transparency (with few exceptions where the voting technology was rather basic). The problem at hand is that technologies are a 'black box' for a majority of population. For politicians this is not only a 'black box' but also an issue as these technologies may directly influence the election process.
- **With the rise of computing power and the wide usage of smart devices, several threats to the modern democracy came into the spotlight.**
- **In 2016**, during the Presidential election in the United States, Big Data analytics tools and methods were utilized by one of the competing sides to microtarget voters based on the personal data collected from their social media profiles.
- **In 2020**, there was a large number of controversies and doubts related to the electronic voting machines. This clearly demonstrates that technologies became an integral part of the electoral process both as agents which are limits the data transfers and tools aiming to influence the election process.
- **Artificial Intelligence and Blockchain technology have yet to reach the level of maturity needed to execute transparent democratic elections.** At this time, they can only support the electoral process by helping eliminate misinformation and to provide more details about the candidates to the general public.
- **The past few presidential elections in the United States presented a number of concerns regarding the ethical usage of digital data.** The main conclusion that can be derived here is that technologies can be easily used to get ad hoc results or blamed for the failure of modern democratic institutions. People lacking basic scientific understanding still see modern technologies as a 'black box' allowing manipulative techniques to be **u**sed to influence public opinion.
- **Negative sentiments towards GovTech hinder technological initiatives and developments** having the potential to enhance democracy making electoral process more secure and inclusive.
- In 2019, American AI Initiative was created to increase the government's awareness and involvement in AI industry development.
- **After the 2020 election AI may be subject of more attention and regulation by the US government** as well as may lead to the adoption of additional legislation (similar to General Data Protection Regulation in the EU).
- **To prevent manipulations, authorities need to implement new strategies to inform the population** about the use of GovTech. The purpose of this report is to provide information on corresponding policy-making decisions.

GovTech / E-governance Industry in the US 2020

Companies - 30
Investors - 40

DEEP KNOWLEDGE ANALYTICS
GOVTECH DIVISION

Timeline of Key Events: 2016-2020

2016

Big Data Analytics played a crucial role in the US Election and may have been used in a non-transparent way.

2017-2018

The period between elections was an attempt to comprehensively understand new technologies with the potential to disrupt politics across country. There was also a push to describe in detail their ethical use in the electoral process.

2019

In February 11, 2019 American AI Initiative, the AI government body, was established with the purpose to stimulate the technological development and implementation in the field.

2020

US 2020 Presidential Election became a litmus test for the perception of technologies, mainly AI and machine voting. The problem at hand is that technologies are a 'black box' for a majority of population. For politicians this is not only a 'black box' but also an issue as these technologies may directly influence the election process.

2021

Government may aim to increase their level of involvement in Artificial Intelligence development. Establishing AI usage ethics. Establishing Private Data Security regulations.

Trends and Tendencies in the US relations with AI 2020-2021

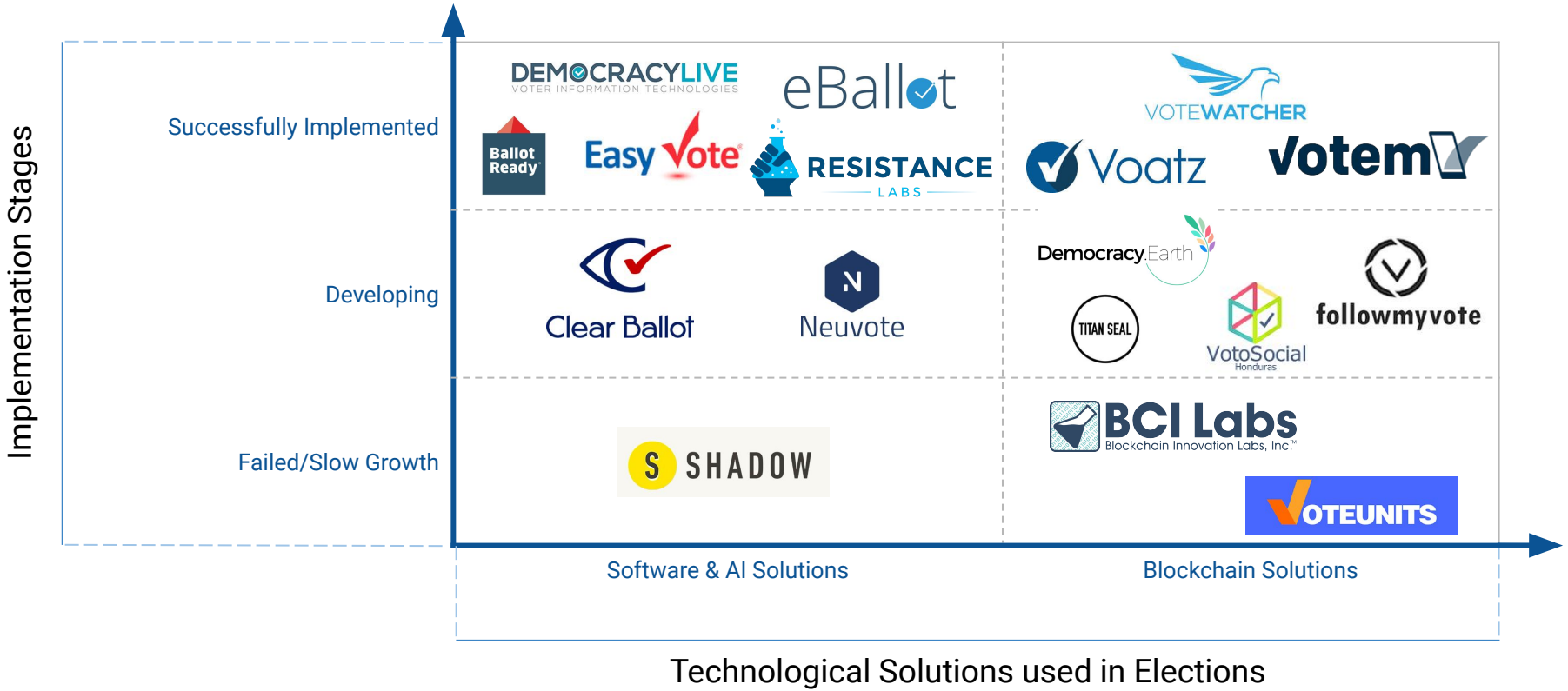
- Increasing of government involvement in AI development and regulation
- Establishing AI ethics
- Establishing Private Data Security regulations

US in 2021

- Increasing cybersecurity prevention mechanisms
- Dealing with China as a competitor and trading partner
- Defining the role of Tech Corporations in US economy

Existing Approaches of GovTech Applications to US Election 2020

Elections Startups and Initiatives in the US



List of Most Promising Startups in GovTech (Elections)

Name	Region	Description
BallotReady	Chicago, Illinois	BallotReady is an online, non-partisan voter guide for local elections. It provides easy-to-digest information about all candidates and referendums on a user's ballot.
Clear Ballot	Boston, Massachusetts	Clear Ballot's browser-based software, used with scanning hardware, scales to election jurisdictions of all sizes and responds directly to the budgetary realities of counties and municipalities.
Democracy Live	Seattle, Washington	Democracy Live is the largest provider of cloud and tablet-based voting technologies in the US It is the only online balloting provider to be certified for electronic ballot delivery in multiple states.
EasyVote	Woodstock, Georgia	EasyVote Solutions delivers a SaaS platform to city, county and state election offices to help manage the process of running elections.
eBallot	Arlington, Virginia	eBallot is an online voting software and services provider that specializes in secure, closed voting events, offering a simple, self-administration platform, all the way up to full service vote management
NeuVote	United States	Neuvote's Mobile Voting System keeps elections combines the best of traditional in-person voting with the accessibility and security of electronic voting into one simple application.
Resistance Labs	Oakland, California	Developer of texting technology designed to support movements and campaigns at critical moments. The company's technology find new ways to use technology to achieve tangible outcomes in areas like voter registration, candidate recruitment, and elections and focuses on experimenting and sharing learning, enabling progressives to appropriately optimize growth and communications strategies.
Shadow Inc.	Denver, Colorado	Shadow Inc is a for-profit technology company contracted by the Iowa Democratic Party to build an app to record and report its caucus results.

List of Most Promising GovTech (Elections) Blockchain-Based Startups

Name	Region	Description
Blockchain Innovation Labs	Lewes, Delaware	Decentralized and transparent voting applications. Shareholder-style blockchain voting through probabilistic public-key encryption.
Democracy Earth Foundation	Palo Alto, California	Democracy.Earth is building an open-source liquid democracy platform built on blockchain technology that makes governance transparent, auditable and accountable.
Follow My Vote	Lewes, Delaware	Follow My Vote is improving the integrity standards of voting systems used in elections worldwide by developing end-to-end verifiable blockchain voting software.
Titan Seal	Reno, Nevada	Titan Seal puts government records in the Blockchain and ensures trust between the government and the public.
Voatz	Boston, Massachusetts	Voatz is a mobile e-voting platform, secured via smart biometrics, ID verification, and the blockchain for irrefutability.
Votem	Cleveland, Ohio	Votem is a blockchain-based mobile voting platform enabling citizens around the world to easily vote online with unprecedented verifiability, accessibility, security, and transparency.
VoteUnits	United States	Secure Blockchain-based Elections; database of ballot data and results for each ballot scanned, as well as links to every blockchain transaction. Product by Blockchain Technologies Corp.
VoteWatcher	New York	A technology company that is working to make elections even more secure and transparent through the use of blockchain technology
VotoSocial	United States	VotoSocial is an electronic blockchain voting platform for official political elections of all levels including presidential, congressional and city elections; for communities, schools and civil society organizations.

AI and Big Data Analytics in Elections

Description

Big data is a branch of analytics that analyzes and/or systematically extracts information from data sets that are too large or complex to be dealt with by traditional data-processing application software. Data from many cases (more data points) offers much larger statistical power, while data with higher complexity (more features) may lead to a large rate of false discoveries. Big data challenges include data collection, data storage, data analysis, search, sharing, transfer, visualization, querying, updating, information privacy and data source.

Big Data is characterized by six key concepts:

Volume	Variety	Velocity	Veracity	Value	Variability
The amount of data from a large number of sources	Data types - structured, semi-structured, unstructured	The speed at which BD is generated	The degree to which BD can be trusted	The business value of the data collected	The ways in which the BD can be used and formatted

Modern electoral campaigns develop Big Data databases of profiles with detailed information about citizens to help strategic decision-making and to guide their tactical efforts. Although there are multiple claims regarding the huge value of individual consumer data, the most valuable information campaigns acquire comes from the behaviors and direct responses provided by citizens themselves. Campaign data analysts develop predictive models using this information to produce individual-level predictions about citizens' propensity (predictive scores) of exhibiting certain political behaviors, of supporting candidates and initiatives and of changing their opinion conditional on being targeted with campaign interventions.

Examples

- Over the past few years, US elections provided a number of notable examples of Big Data usage. Barack Obama's campaign was one of the first to conduct a large scale political marketing based on numbers' crunching. He hired a 100-strong analytics team to go over tens of terabytes of data using HP Vertica's massively parallel processing, a large database and predictive models constructed with the help of modern statistical languages like R and Strata.
- 8 years later, Donald Trump would implement AI and Big Data analytics on an even bigger scale to score a win against Hillary Clinton. Trump worked together with the British political consultancy company Cambridge Analytica to microtarget voters. The amount of data gathered and processed by the company reached more than 5,000 data points about the behavioral characteristics of American citizens. The team mixed this method with psychological social media polls and surveys to create consumer profiles of the voters. Political data was also used to identify voting patterns. The combination of those approaches helped them target their advertising to the right people at the right time.

Voting Hardware in Elections

Description and examples

One of the most prominent examples of voting hardware are the **voting machines** which are used to record or tally votes. The first voting machines were mechanical but it is increasingly more common to use electronic voting machines. Traditionally, reliability of voting machines was determined by their mechanisms and whether the system tallies votes at each voting location or to central storage. Voting machines differ in various parameters like usability, security, price, speed, accuracy, and public transparency. Some machines could be more or less accessible to voters with different disabilities.

Tallies are very simple in parliamentary systems where just one candidate/ initiative is on the ballot, and these are often tallied by hand. In other more complex political systems where many options are on the same ballot, tallies are often automated (with machines) in order to process the vote faster.

The scope of this report focuses on the use of voting hardware in United States' 2020 election where several types of voting machines were used: touch screens for voters to mark choices, scanners to read paper ballots and scanners to verify signatures on envelopes of absentee ballots.

Examples

Three vendors sell most of the machines used for voting and for counting votes in the US As of September 2016, the American Election Systems & Software (ES&S) served 80 million registered voters, Canadian Dominion Voting Systems - 70 million, American Hart InterCivic - 20 million, and other, smaller companies - less than 4 million each. More companies sell signature verification machines: ES&S, Olympus, Vantage, Pitney Bowes, Runbeck, and Bell & Howell. A Spanish company, Scytl, manages election-reporting websites statewide in 12 US states. Another website management company is VR Systems, active in 8 states.

Election machines are computers, often more than 10 years old, as certification and purchase processes take at least two years and many government offices lack the necessary funds to replace them, resulting in usage of the outdated equipment until it wears out. Like all computers, election machines are subject to multiple errors, many of which have been widely documented.

In some electoral precincts, computers check signatures on postal ballot envelopes to prevent voting falsification. Error rates of computerized signature reviews are not yet published but error rates in signature verification are higher for computers than for human experts.

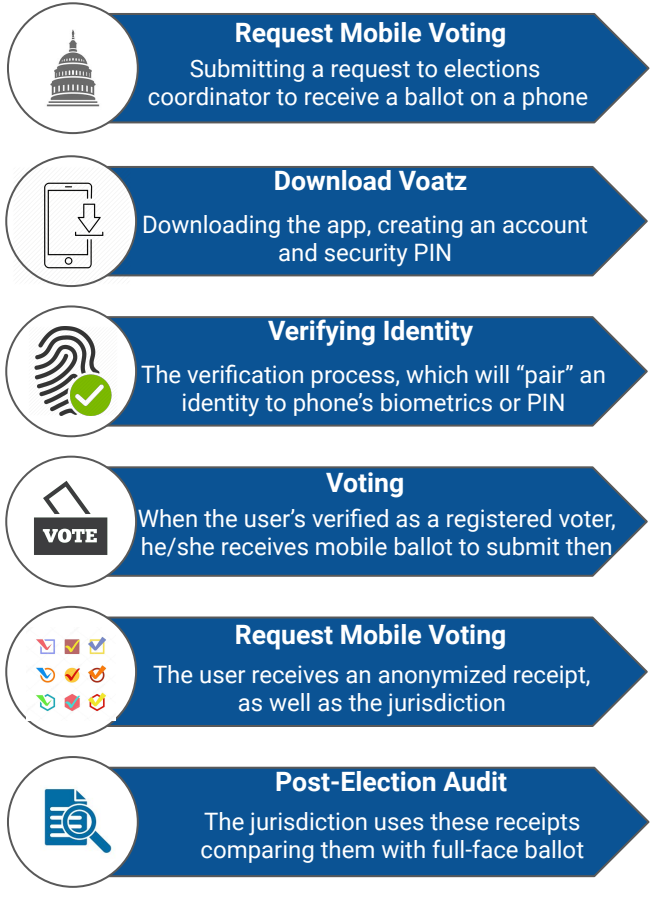
Blockchain in Elections

Description

Many discussions are focused on blockchain-based e-voting systems. Existing challenges and vulnerabilities of the modern electoral process such as cybersecurity, time required for voting, and efficiency are largely debated.

Blockchain-based voting innovations propose a solution based on principles of using coins as votes, using a permissioned blockchain and employing zero-knowledge proofs for secret ballots.

- **Coins as votes** - every registered voter has a public or private key pair created by the voting authority, which the voter then sends to the voting registry. For each public/private key the voter registry saves one coin, which then the user spends on the candidate of his/her choice. At the end of Election Day, each candidate's coins are totaled up and the winner is determined by the maximum number of coins
- **A permissioned blockchain** is another alternative, the main difference of which is the use of a proof-of-authority (POA) consensus algorithm when only approved accounts have the right to vote
- **Transaction secrecy**, also known as zero-knowledge proof, is designed to hide transaction details (i.e., the participants of the transaction and the amount) while still maintaining public verifiability. In other words, the transaction is verifiable and the result of it is publicly available, but sharing the underlying data related to this information is restricted or kept totally secret



Examples

Votem — During Montana 2016 Presidential Election, Votem facilitated absentee ballot delivery serving military and overseas voters and electors with disabilities, supporting approximate 670,000 registered voters in that state. According to the voters' feedback, 99% of them found it convenient to obtain a ballot online, and were satisfied with this method of voting, and would like to repeat an experience again in future elections.

Voatz — During 2018 midterm election in the United States, for the first time in national history West Virginia implemented the option of mobile voting through Voatz blockchain service for those citizens who work or live abroad. The primary goal of the West Virginia Secretary of State was not encompassing many participating voters, but showcasing easy-of-use and secure voting system to increase the overall voter engagement in the future. In general, 144 individuals from 31 countries successfully submitted ballots via the app, and the state officials were satisfied with the experiment results and planned to use it again in 2020 election.

Following that, several states as Denver, Colorado, Utah County, and two counties in the state of Oregon launched pilot projects during municipal elections, and in total 29 counties in 5 states tested Voatz's mobile voting app in official elections with no problems. But technology did not find public support, and many experts still think that blockchain is not an appropriate tool for voting, even after several audits of its systems, which the company stood well. At the beginning of 2020, MIT created a report that highly criticizes blockchain voting, highlighting severe security flaws of Voatz online voting system. Despite Voatz responded that the research is conducted on an outdated version of the app, and also claimed that it has been no successful hacking of the platform yet, for now, the company is available in elections on the pilot basis only.

Smartmatic-Cybernetica — During Utah GOP Presidential Candidate election (March 2016) almost 25,000 voters from 45 countries have used the platform to cast their ballots. Nearly 90% of voters described the online voting experience as good and 82% of them wanted to see online voting implemented nationwide.

There are allegations against Smartmatic of fraud especially in the aftermath of the 2020 US presidential election, by the personal attorney to President Donald Trump, Rudy Giuliani, who asserted the opinion that the company was founded by the former Venezuelan leader Hugo Chávez.

Key Takeaways

Big Data and AI applications	Social Media and Digital participation	Blockchain	Voting Machines
These tools can be well utilized when there is a need for a higher level of engagement and when campaigns and politicians need to gather large amounts of data from the Internet. In some cases, this is quite controversial but still immensely useful in both short and long-term strategy formation.	Politicians around the world are learning that along with traditional mediums such as television and newspapers, they must take advantage of online marketing methods and tools if they wish to compete with their rivals. Over the past decade, we have seen a rise in social media activity by the US presidential candidates, who used social media campaigns to defeat their opponents. However, such activities created strong clashes between the opposing sides.	A recent report from MIT, argues against the idea of blockchain-based e-voting, largely on the basis that it will increase cybersecurity vulnerabilities that are already in place, it will fail to meet the unique requirements of voting in political elections and it will add more problems than it will fix. In essence according to MIT, it is still a very controversial technology and not on the necessary reliable level.	Voting machines which are relatively mature technologically, have an issue with their cost and requirement for regular updates. Unfortunately, many public administration offices still rely on outdated machines, prone to hacker attacks and technical faults. The US Voting machines market is dominated by three companies and their strong lobbying power has the ability to influence the public regulation in that domain.

To sum up this section, the technologies do indeed help with an increase in election transparency and can build an even stronger democratic basis to public decision-making processes. The problem is that most of the current voting technologies are still maturing and lack sufficient test iterations. Some of them are still quite unsafe to use for electoral purposes as they fail to show sufficient reliability and security.
This report aims to provide an overview of the existing problems and offer broad guidelines on how they can be addressed. If and when a secure and ethical usage of technological advancements will be implemented this will result in an enormous efficiency in both public's trust and government efficiency. Once the proper regulations regarding data privacy will be enacted, the potential to create trust between citizens and government officials in a manner never seen before, will finally be realized.

General info about election

The **2020 United States presidential election** was the 59th quadrennial presidential election, held on Tuesday, November 3, 2020. This election clearly demonstrated socio-economic division of the American society and the role of technological giants like Facebook and Google in political life. Generally it could be also said that the 2020 pandemic and unprecedented social unrest have significantly transformed US politics.

The 2020 Presidential election could be considered some of the most controversial in American history and technologies played a significant role in this process.

This election will also determine the country's strategy towards AI development in the following years. The steps which will be made by the new administration will also demonstrate whether US can keep its position as the world's innovation leader. According to the Information Technology and Innovation Foundation (ITIF), a think tank working closely with the American tech industry, states that the US would need to spend additionally more than $100 billion every year, or an increase of around 80% over current spending levels, just to match what it was investing in R&D as a share of the Gross Domestic Product during the 1980s. It's obvious that the US government needs to participate in the development and implementation of the AI industry, as well as regulation of data privacy strategies.

Another issue adding fire to the technological regulation discussion is increasing attention to the activities of Big Tech corporations like Facebook, Google and Twitter which are being questioned by the Congress as well as are subject to antitrust litigation. This shows that the general public finally understood the power of the Internet and social media and is pushing to establish stricter GDPR-like legislation regarding privacy and protection. One thing is becoming clear - the advanced methods and strategies used during and after the election are likely determining who is going to be the winner and who will set the directions in which the future data regulation rules will develop.

There were numerous concerns and problems related to the usage of new tools for election administration purposes - some of them were related to the usage of the voting machines and their failure to create a more transparent electoral process. Due to the fact that in the US the three main election equipment vendors — Election Systems & Software, LLC; Dominion Voting Systems, Inc. and Hart InterCivic, Inc. provide the hardware and software used by 92% of the eligible voting population, **the lack of competition in the election vendor marketplace and weak scrutiny by regulators result in these vendors continuing to produce poor technology** - unreliable and insecure electronic voting machines with the lack of paper ballots or auditability.

Controversies related to Government Technologies in 2016-2020

During the 4 years preceding the US 2020 Presidential election, technologies were in the center of political scandals. During that period (and even before) both parties have been constantly putting the blame for their electoral failures on fault-prone technology.

Media Manipulation

According to a research report by the RAND Corporation, during the 2020 Presidential election convincing evidence of attempts to influence the US election via social media were found. **The main methods of information exploits in social media were determined as bots** that cluster in specific communities, engage both liberal and conservative audiences, and exacerbate political divisions in the United States. The interference efforts are designed using Big Data analytics (networks analytics, text-mining, human qualitative analysis, etc.) in order to understand the different online stakeholder groups, machine learning structure, and building models of the future bots. Even worse - the longer they are used, **the more complex and hard to detect they become.**

Cambridge Analytica Case

Personal data can also be used to target persuadable voters based on their individual psychological characteristics, as in the Cambridge Analytica case. **Using Big Data and machine learning rises major ethical issues and concerns.** The problem with the company's approach is not with the technology itself but with the covert nature of campaigning and the insincerity of political messages.

Lack of regulations

The use of AI techniques in politics is not going away anytime soon, however, policymakers do not fully realize its potential resulting in **regulations and new standards being outpaced by the technology**. More importantly, general public is still vulnerable to manipulation and propaganda, especially during pre-election campaigns due to its tendency to fall for certain extremes.

'Black Box' Problem

Moreover, there is a 'black box' problem: if people don't know how AI comes up with its decisions, they won't trust it. Being a simple user, a person is not able to control the leakage of personal data. The privacy of data is not protected in the US as it is in the European Union.

Parler vs Facebook

This election clearly demonstrated that American society is facing dramatic social, economical and political division. This process translates into changes of technology usage as well. People are turning to alternative social media channels such as Parler or MeWe, which are viewed as neutral platforms without censorship. While Parler is more like Twitter, MeWe attracts Facebook users because it is free of ads and manipulative news feeds and was conceived as a 'privacy-first' platform. This is an outcome of prolonged periods of censorship and purported anti-desinformation measures taken by the social media giants. This shift is just a small reflection of the social, political and economic division within the American society.

Americans' Major Fears Regarding Technologies in 2015 and 2017

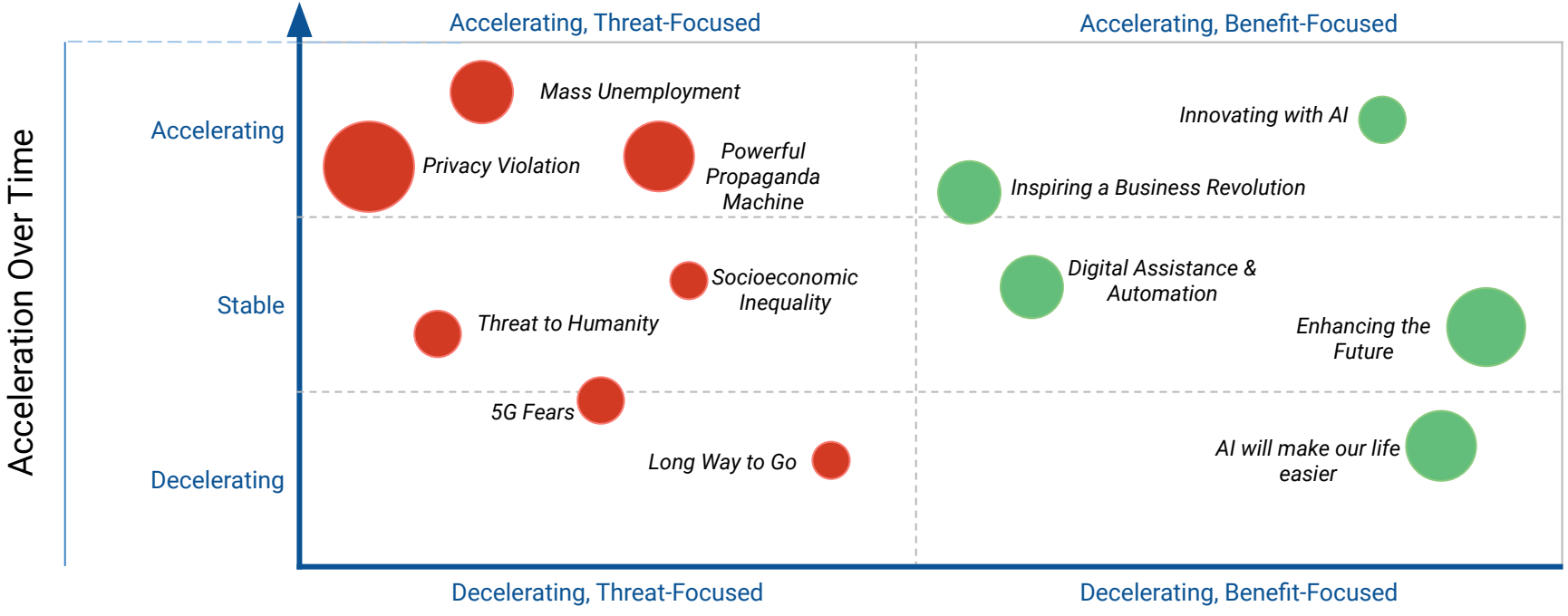
Ranking	Fears	% of Americans are afraid of
1	Cyber terrorism	44.8
2	Corporate tracking of personal data	44.6
3	Government tracking of personal data	41.4
4	Robots replacing workforce	28.9
5	Trusting AI to do work	25.8
6	Robots	23.9
7	AI	22.2
8	Technology I don't understand	19.0

Source: The Chapman University Survey of American Fears, Wave 2 (2015)

Main Concerns about AI:

- Mass Unemployment
- AI Will Destroy Democracy
- AI Capabilities Are Overestimated
- Data Privacy Becomes More Vulnerable
- The Risk of 5G Network
- 'Deep fakes'

Americans' Major Fears Regarding Technologies in 2017



Source: [NARRATIVE ANALYSIS RESEARCH PAPER Artificial Intelligence]

Homeland Security

Big Data in Electoral Campaigns

Big data and Machine learning (ML) transform all aspects of our life, and political campaigns are no exception. By knowing the personal preferences of the voters, candidates can conduct their campaigns in a much more sophisticated way.

Political marketing efforts can now be much more precisely targeted due to the wide variety of digital tools and the huge computing power that can be harnessed through the cloud. With that being said, the ability to analyze vast amounts of data is giving immense power to factions with such resources. Before the dawn of the digital age and the interconnection that the Internet represented, the voter data used by political organizations had only a few data points: home address, voting history, party affiliation, education, marriage status.

However, during the past several years, the amount of detailed information about a single citizen has grown dramatically up to hundreds of data points. Thanks to the Internet, social media, and preference-tracking tools, researchers can now study voter activities on various platforms (social media, news outlets, e-commerce websites, and various forums). The aggregated data of millions of voters is a ripe picking for political campaign marketers and could be used to precisely target the political message to large groups of people.

The United States of America was the first country to apply Big Data marketing techniques commercially before actually using them in political communication. The transfer of marketing practices from the commercial market to electoral campaigns was the result of seeking efficiency when managing activities of political players.

The technologies behind 2020 Presidential election in the US

The use of advanced analytics tools in 2020 US Presidential election was taken one step forward compared to the previous election. The rise of the internet of Things (IoT) and the fifth-generation communication technology (5G) helped to track opinions and activities like never before. Big Data now works in conjunction with AI algorithms crunching through huge amount of both structured and unstructured data. Traditional analytics is giving a way to Deep Learning-powered predictive modeling, massive data exchanges and microtargeting.

Voter data collection

During the past decade, political campaigns have been collecting voters' personal data in their already large databases. The data was gathered mainly through direct-response advertisement which seeks to get contact information and opinion directly from the source. Most of the personal details come from people who already made up their mind regarding which presidential candidate to support. An example given by Technology Review is the Trump campaign app that allows automatic Bluetooth pairing in order to identify the location of the device. While this practice could not be considered entirely ethical, it actually has its logic - voters who download the app have already shown their preference to that specific candidate.

Microtargeting

This method uses the collected vast amount of data which is analysed by organizations in order to try and gather as many insights about particular voter as possible and create a profile encompassing basic demographic data points such as age all the way to relatively subjective phenomena such as personality type.

Cambridge Analytica scandal: 2016 election campaign

In recent years, Cambridge Analytica microtargeting techniques for political campaigns have been highly debated. Mostly, the organization was accused of data misuse by secretly amassing it from millions of Facebook users without their consent and serial involvement in the course of important political events by selling information services based on the insights provided. However, Cambridge Analytica technology is not completely unique, microtargeting has been widely used long before recent high-profile scandals. **The problem with that approach was** not the technology itself but **the covert nature of the campaigning and gathering of consumer data**. Overall, **the events of 2016 have shown how powerful the use and manipulation of data can be.** For this purpose the following strategy was used:

Cambridge Analytica purchased personal data collected through an online app where users took detailed personality/political tests, agreeing to process their personal data up to the personal data of their friends on Facebook. Thus, with 320,000 US voters, about **50 million user data points were gathered.**

The quiz results were then paired with users' Facebook activities such as likes, comments and shares, and with the help of linear regression model **psychological profiles are created.**

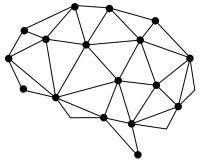
Then those profiles were blended with commercial data and voting histories, revealing "***hidden voter trends and behavioral triggers***".

All this formed a basis for a political campaign targeted in the most individualized way. Using Big Data and machine learning, candidate/party manipulated voters by sending them targeted messages based on predictions about their susceptibility to different arguments.

Unethical use of data by Cambridge Analytica was only half of the problem in the case.

The other half was the problem was the data policy of Facebook which allowed for the unconventional use of personal data by third parties, especially when they can use it for unethical purposes such as targeting tailored but controversial political ads.

Cambridge Analytica case in 2016



Cambridge Analytica

*About **320,000 participants** of personality test and other surveys. Along with **personal data** of participants, **all of friends' data** was collected.*

50 million users database

RAW DATA

BUILDING A MODEL

Participants' Personality + **Participants' Likes**

- ❏ 5-factor OCEAN model
- ❏ Political orientation
- ❏ Demography
- ❏ Facebook data
- ❏ User's preferences
- ❏ User's friends' data

Linear Regression Models

A formula with a coefficient for each like generated for each of the 5 OCEAN model trait

ANALYTICS

Voting Histories

- ❏ Hidden voter trends
- ❏ Behavioral triggers

Commercial Data

PERSONALIZED POLITICAL MESSAGING

- ❏ Customized ads
- ❏ Direct-mail slogans
- ❏ Door-knocking scripts

Computers' Judgements

32 DISTINCT PERSONALITY TYPES DETERMINED

Source: [Computer-based personality judgments are more accurate than those made by humans]

Social Media and the Elections: 2016-2020

2016 campaign brought significant concerns over the technologies used in candidate promotion. Cambridge Analytica and various other Big Data scandals brought that huge issue into the spotlight - social networks provided a very powerful tool to those who were able to harness the data. However, currently, a great knowledge gap exists between the two sides - the majority of Americans who do not understand how their data is used and the organizations processing it.

Technology-related controversies started during the 2016 election campaign when it was found that voting machines could easily be hacked and social media can be used by foreign players to influence public opinion. The result from this was much lower trust and rising concern towards technological advancements.

Several cases of allegations against Facebook:

2012

the US Federal Trade Commission (FTC) charged Facebook with eight separate privacy-related violations, including that the company made deceptive claims about consumers' ability to control the privacy of their personal data. The amount of civil penalty against the company was US$5 bln.

2018

Mark Zuckerberg made his appearance before the Senate on **April 10,** during a five-hour hearing before a joint session of the Commerce and Judiciary committees. The purpose of that meeting was for the senators to understand how Facebook had allowed the profiles of more than 87 million people to be collected by the British political consulting company Cambridge Analytica. This case was just one of many problematic consequences of the rise in the influence of social media.

2019

On **July 24th**, the **United States Government proposed a consent decree** to settle a large number of claims that Facebook had violated a 2012 Federal Trade Commission (FTC) order and the FTC Act by misrepresenting the extent to which their users could control facial-recognition templates and other personal data, misrepresenting the extent to which Facebook made user data available to third parties, not providing the required privacy protection level, and collecting users" phone numbers for security purposes and then the usage of those numbers for digital marketing.

2020

October-November The CEOs of Twitter and Facebook were asked to testify in front of the senate, again, about allegations of anti-conservative bias on their networks. Mark Zuckerberg and Jack Dorsey were called in October to appear at the hearing with the Senate judiciary committee so the senators can evaluate how the companies handled the information regarding the 2020 Presidential election.

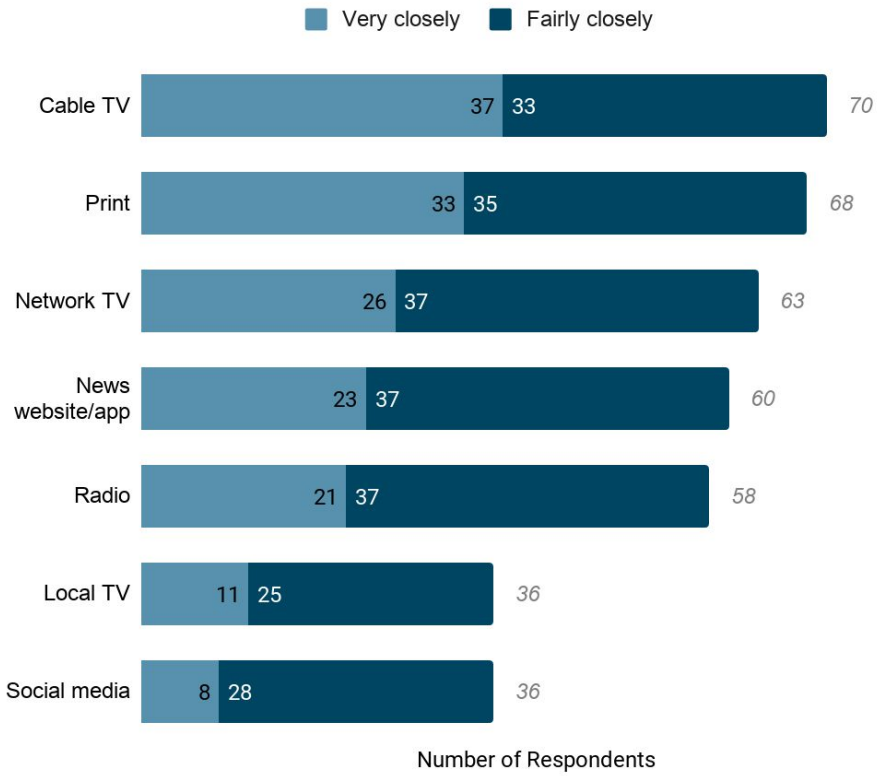
2020 Presidential election

The 2020 Presidential election was the most discussed topic online with two of the largest social media platforms Facebook and Twitter becoming a battleground between political supporters of the Democratic and Republican parties. By virtue of implementing censorship during and after electoral campaign, Facebook and Twitter ceased being neutral actors/ platforms and became agents / participants of the electoral process, triggering hearings related to the repeal of Section 230 of the Communications Decency Act.

Just two hours after a certain controversial story was online, Facebook dispatched a Democratic Party operative who now works for the company — Andy Stone, to announce that the social platform was now reducing the distribution of the article allegedly containing false facts. As a result of the mass disinformation and censorship witnessed in the past few years, fewer and fewer Americans use social media platforms to gather information.

Due to events that unfolded in 2020, many people migrated from the mainstream media platforms (including Facebook and Twitter) and news channels to alternative sources which are perceived as unbiased.

Most common political news sources



Source: Survey of US adults conducted June 4-10, 2020

Social Media Data and Election

Despite the promises made by tech giants such as Facebook and Twitter to maintain neutrality as a platform, many people are convinced that these entities in fact implement censorship.

Facebook	Twitter	YouTube
Changing news submission with 'independent fact-checking' algorithms to suppress "violent publications", "fake news" or posts which **might** contain unverified information.	Candidates will not be able to announce victory until the results are announced.	Prohibiting granular microtargeting of political ads.
Deactivation of certain hashtags related to election results.	Tweets that **may** contain unverified information or misinform will be labelled or removed.	Prohibiting content alleging widespread fraud or errors related to the outcome of the election.
Working with Reuters to provide accurate election results on the night and in the days after the election.	Moreover, Twitter will direct people to resources with accurate, up-to-date information on election status.	Limiting access to the videos claiming 2020 presidential election fraud.
Not accepting new political advertising a week before election day and not showing political advertising from November 3, Election Day, "to reduce opportunities for confusion or abuse".	Candidates will not be able to share tweets calling for interference with the election process.	Displaying fact check information panels, from third party fact checkers together with relevant election-related search results.
Labelling misinformation on voting.		Misleading content about where and how to vote is prohibited

Voting Machines: What technologies were used?

The United States have been considered as one of the main innovators in the electoral system - the country was the first to establish such institutions as the Electoral College and to use new vote counting methods (such as cumulative voting, bucklin voting, Coombs' method, instant runoff voting, and many others). At present, various changes have been implemented, all of them coming from state and county jurisdictions, rather than the Federal government.

A variety of digital voting equipment used by the election offices is the voting machine (a mechanical or electronic voting device used to record or tally votes). The first computer tabulated machines (so-called mechanical lever machine) in the country were used in 1892 in Lockport, New York. By the 1930s, voting machines were used in almost every major American city. That was a major impetus to the development of voting devices and it helped bring new tools and devices to the market very soon after that (tools like optical scanners, punch card voting system and Direct Recording Electronic machines).

1996 was the first time election was conducted over the Internet and that event was considered to be at the cutting edge of the technology at that time. During the 2000 Presidential Election, the first serious malfunctions occured: inaccurate registration lists, unclear ballot designs, high numbers of spoiled ballots. This led to the establishment of high voting systems' standards and the signing of the first legislation (HAVA, 2002) to specifically address voting technology. From 2005, several attempts to hack the voting software for research purposes were conducted, demonstrating hackability and 'backdoors' of the systems. Research found that machines did not meet computer industry security standards, but the leaders of the industry did not react much to those findings.

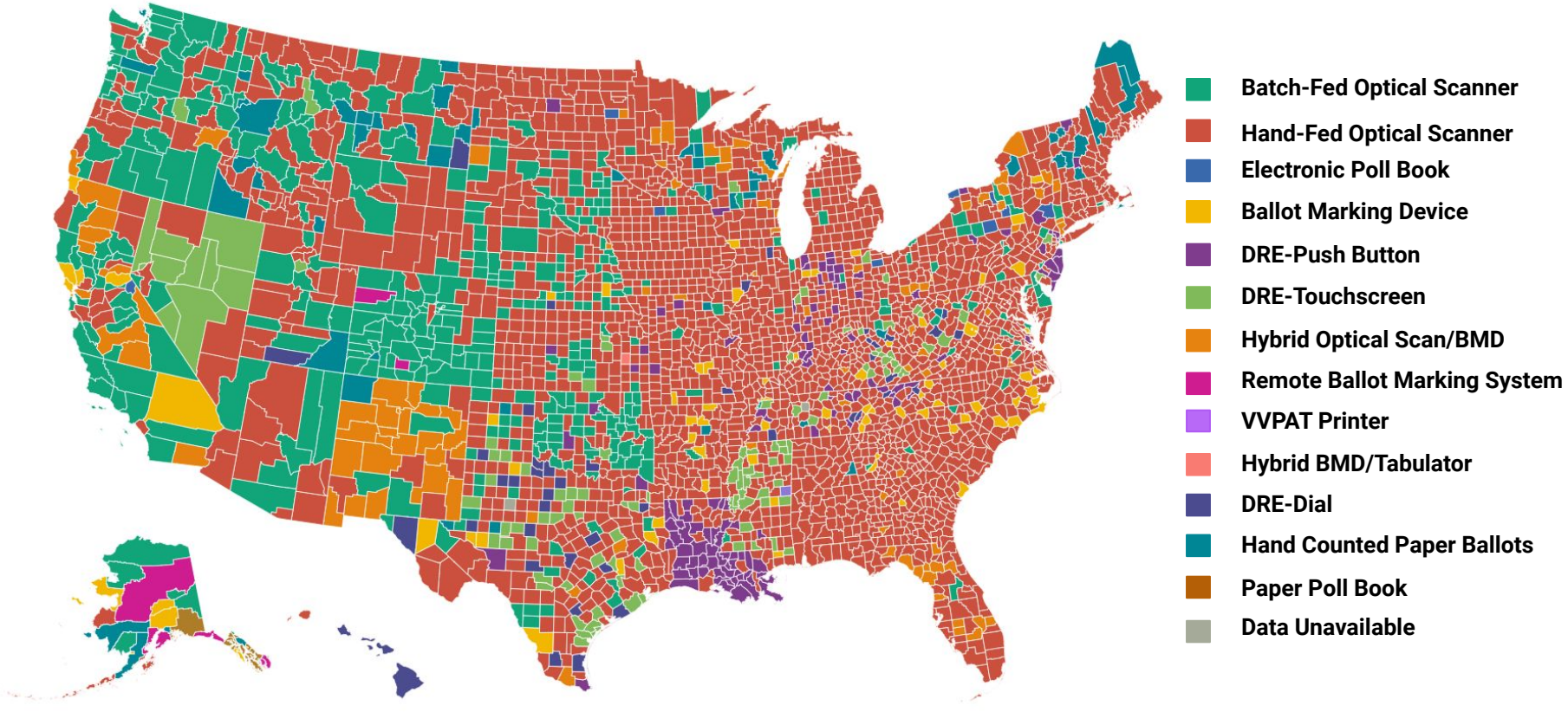
It was considered that the evaluation of computerized voting technology has shown their advantages over the hand vote-tallying and its ability to conduct audits of election processes and ballot recounts. As a way of example, here are some of their advantages over traditional voting systems:

- **Reducing organizational and implementation costs**, as well as the logistical burden associated with the manual paper ballot process
- E-voting technologies **expedite ballot counting**;
- **Improving accessibility** for disabled voters and overseas citizens, increasing the engagement and simplifying voting process;
- The whole **e-voting process is auditable end to end**. It brings an accurate and quick publication of results, with receipt of vote for each vote cast.

However, it is alleged that voting systems were used to get perpetrate election fraud thus raising a lot of concerns regarding their transparency during the 2020 Presidential Election.

Americans feel less confident about the election and more than half of the respondents claimed that the potential election fraud was of major concern.

Distribution of voting machines by equipment type

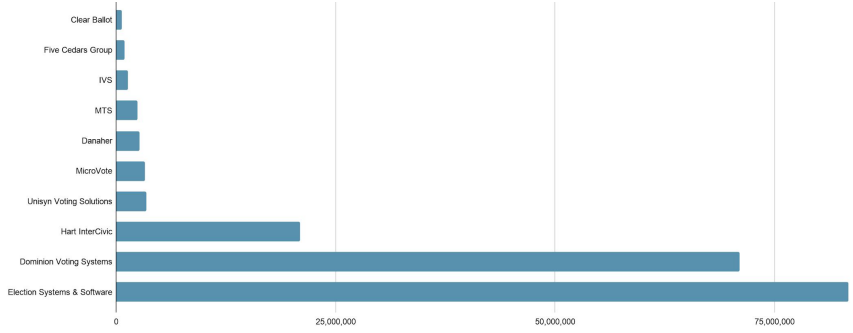


Voting Machines (VM) in the US Electoral Process

In 2002, The Help America Vote Act (HAVA) was enacted with the purpose to perform overarching changes in the country's voting processes and improve the efficiency of the elections. In essence, the law provided financial incentives so the states can meet the new standards and replace the old voting systems.

With the $3.9 billion in funding provided by the program, the voting machines of several large companies were brought into operation. As of today, the following companies provide Voting Machines to the US market:

- Clear Ballot Group, Inc.
- Dominion Voting Systems Corp
- Election Systems & Software, Inc (ES&S)
- Hart InterCivic, Inc.
- MicroVote General Corp.
- Smartmatic USA Corporation
- Unisyn Voting Solutions
- VotingWorks

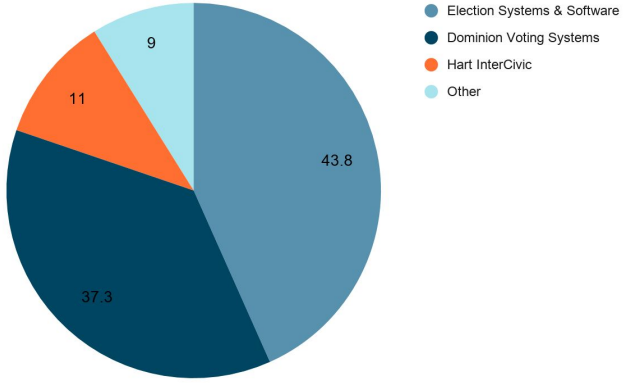


What are the main examples of VM manufacturers on the market?

Dominion - The corporation claims that it is covering around 40% of the US voting machine market. According to the company's internal statistics, it's products are used in 28 states.

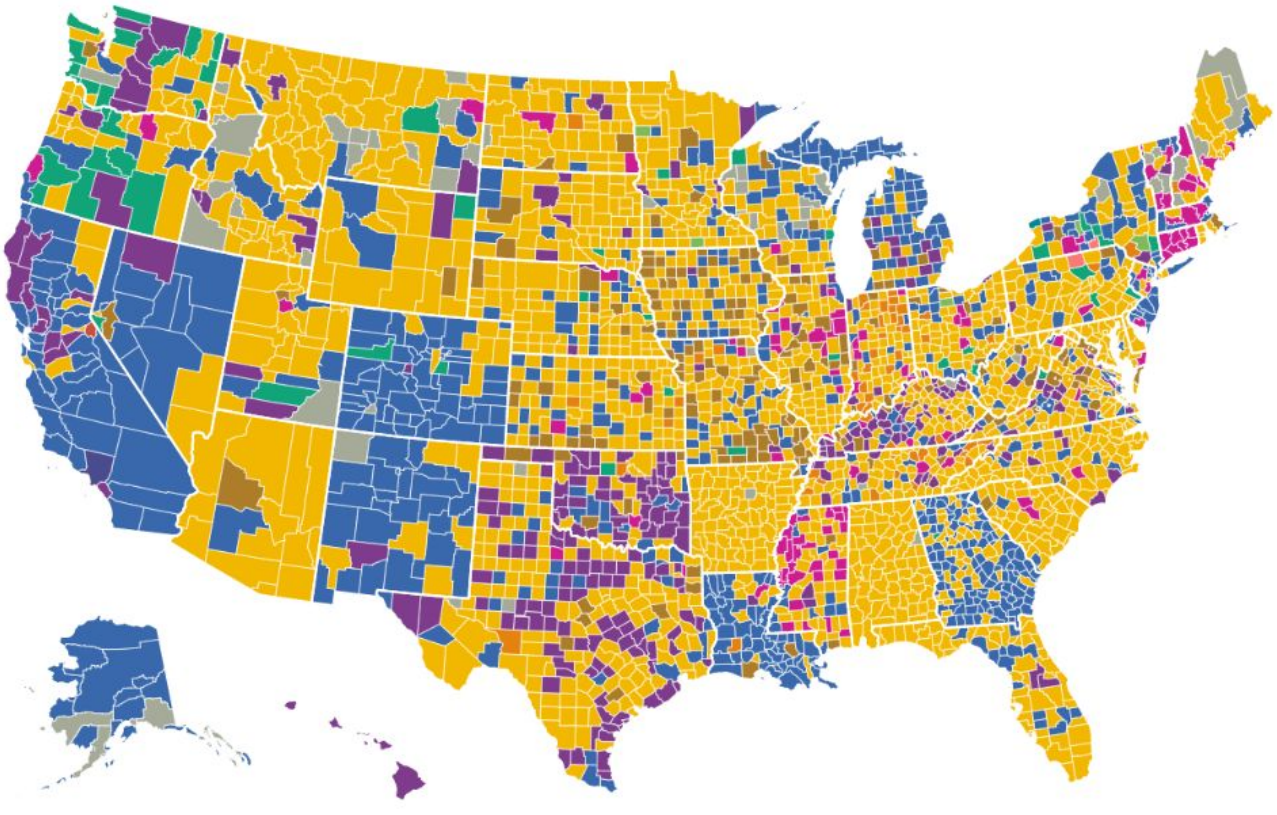
Election Systems & Software (ES&S) - In 2014, ES&S was the largest manufacturer of such type of equipment in the the whole country, claiming having customers in more than 4,500 localities in over 42 states and two US territories.

Hart InterCivic - Their products are used by a large number of government agencies across the entire US.



Source: The Business of Voting: Market Structure and Innovation in the Election Technology Industry

Voting methods and equipment by state



- Clear Ballot
- DFM
- Dominion Voting Systems
- Election Systems & Software
- Hart InterCivic
- KNOWiNK
- MicroVote
- Premier/Diebold (Dominion)
- Not Applicable
- Robis
- Smartmatic/Los Angeles County
- Tenex
- Unisyn Voting Solutions

Source: System Certification Process: Table of Voting Systems

Business of Voting Machines as Part of the Democratic Process

The usage of the voting machines in the electoral campaigns was **quite controversial** from the very beginning. The three companies mentioned in the previous section of the report are actually forming a monopoly in the US, owning a 92% of the market which is valued at about **$300 million**. At the same time, over the past decade and a half the services of these key players were subject to multiple accusations and violation claims.

Lots of discussions revolve around the transparency of investment in the US voting systems industry and regarding the disclosure of shareholders who have at least a 5 percent financial stake in the three companies. An obvious conclusion is that those private entities essentially run the US elections without almost any kind of supervision from government agencies, without transparency, and without sharing information regarding their stakeholders.

The three biggest voting-system manufacturers, (each having powerful lobbies), have the ability to influence local governments' power to purchase machines that are much less secure from the potential fraud standpoint compared to the old-fashioned paper-ballot systems. Moreover, there is the possibility of foreign involvement in US voting systems and for the aforementioned reasons, states now demand safer, auditable and more transparent voting systems. A number of states require testing compliance to federal standards or EAC certification for machines used in their counties. New vendors have a challenging business environment to grow in, as the election machines market remains dominated by several large vendors.

Certification procedures take more than two years, cost more than $1 million and it are required after every system update. In addition, the choice of the voting machine vendor is prone to bias as the largest players have strong lobbyist groups which affect the electoral officials' decision. Those obstacles present almost insurmountable financial challenge to incoming players.

Red Flag reports

2016 US presidential election and Voting Machines replacements in 2018-2019 - Electoral campaigning of 2016 exposed vulnerability of the voting machines due to their outdated hardware and software.

In September 2015, the Brennan Center published a report titled "America's Voting Machines at Risk", containing statistics about the United States outdated voting machines. The analysis detailed how these systems were often unauditable, susceptible to malware, frequently difficult to repair, and more prone to failure.

Voting equipment certification process / Concerns about the voting equipment

Voting equipment certification process

The United States Election Assistance Commission (USEAC) operates the American voting system testing and certification program. This program certifies, decertifies and recertifies all hardware and software related to the voting process according to VVSG program and gives accreditation to test laboratories.

The VVSG establishes a set of specifications and requirements against which voting systems can be tested to determine if the systems provide all of the basic functionality, accessibility, and security capabilities required of these systems. In addition, the guidelines provide specific evaluation criteria for the national certification of voting systems.

The EAC's Technical Guidelines Development Committee develops an initial set of recommendations for each VVSG iteration. Then, they are sent to the EAC for review and revision and then published for general comments from the public. These comments are revised and taken into account by the EAC while consulting with NIST in the development of the final release.

The financial transactions between the customers and the voting equipment vendors are shaped by federal and state regulations and standards. While state laws are subject to certain federal constraints, states and local jurisdictions have wide range of freedom when it comes to making decisions regarding the integrity of elections, including the purchase of voting equipment, establishing specific training procedures, implementing testing requirements, and setting standards for certification.

Concerns about the voting equipment

Key issues relating to the safety of the voting equipment include:

- **Supply chain questions:** NBC News found that many parts of ES&S products, including electronics and tablets, were made in China and the Philippines, raising concerns about technology theft or sabotage.
- **Ownership questions:** Vendors do not provide a straightforward answer, even after the US Senator Amy Klobuchar requested such information in her letter. Because companies are privately owned, they are not legally obligated to reveal their ownership or any other details about funding, however, some officials assume potential foreign ownership.
- **Testing questions:** Information on how the testing of voting machines is conducted is closed and testing companies refuse to provide any information on this account to government officials or the public. According to Rebecca Mercuri, a Harvard-affiliated computer scientist, since serious malfunctions were found during the exploitation of the equipment, issues of standards and transparency stay important for the integrity and secure of the whole system.

Early Examples and Problems

Date	System	Description
Nov, 2020	ES&S, Dominion Voting Systems	A failure to properly update software was the reason that in a number of counties, alleged software glitches led to mistakes in vote tabulation for both the Presidential and local races. Errors also caused temporary miscounts in certain locations.
June, 2020	ES&S	The scanner looked in the wrong places on the paper and reported the wrong numbers. It was caught because a popular incumbent got implausibly few votes.
Nov, 2019	ES&S	Because of the weather conditions across New York City ballot scanners malfunctioned: ballots jammed in the machines or multiple ballots went through a scanner at once, hiding all but one.
Oct, 2019	ES&S	The company repackaged the machines (as they passed from a company that stopped making voting equipment seven years ago) and sold them as new technology
Feb, 2019	ES&S	Systems were not properly set up for the high voter turnout the county saw on election day, that brought voting to a standstill at multiple voting sites across the county; some people had voted more than once;
Jan, 2019	Dominion Voting Systems	Systems failed certification due to efficiency issues
Oct, 2018	Hart InterCivic	Vote flipping: a number of people voting on Hart eSlate machines that when they voted straight ticket, it appeared to them that the machine had changed one or more of their selections to a candidate from a different party

Antrim County Case

Background: Antrim County, which usually votes for Republicans was in the center of attention since the initial results on election night demonstrated Biden ahead of Trump by thousands of votes. Officials later determined that there were problems in the reporting of Results and Trump ended up winning in Antrim County by more than 3,700 votes. Even though the fact of election mistake is established, there is a debate about the nature and reasons of the mistake: whether it is a human error or Dominion Voting System mistake, whether it was intentional or not.

Official position: Michigan Secretary of State Jocelyn Benson and Antrim County Clerk Sheryl Guy state that the issue was human error.

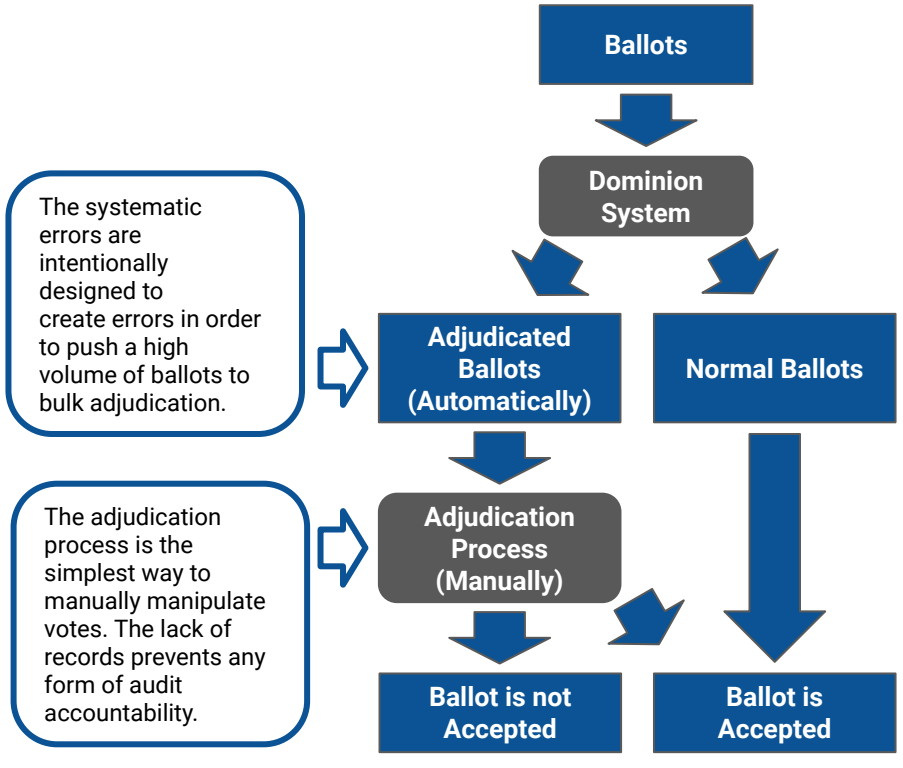
Dominion's statement: There were no software "glitches" that "switched" votes in Antrim County or anywhere else. The errors identified in Antrim County were isolated human errors not involving Dominion.

On December 13th, 2020, Circuit Court Judge Kevin Elsenheimer allowed to publicly release and discuss the report made by the private group and consisting of forensic analysis of tabulators and data in Antrim County.

Antrim Michigan Forensics Report: concludes that the Dominion Voting System is intentionally and purposefully designed with inherent errors to create systemic fraud and influence election results.

The system intentionally generates an enormously high number of ballot errors. The electronic ballots are then transferred for adjudication. The intentional errors lead to bulk adjudication of ballots with no oversight, no transparency, and no audit trail. This may lead to election fraud. Based on the study, the authors conclude that The Dominion Voting System should not be used in Michigan.

Key Points of Antrim Michigan Forensics Report



Timeline of the main events in 2016-2020 // How Digital e-Governance Technologies were Discredited

2016

2016 Presidential Election

Cambridge Analytica and Big Data algorithms used personal data from Social Media to target political campaigns based on individual portraits of voters; this led to raise of mistrust to Facebook and Twitter.

Outdated voting machines were considered easy to hack and falcificate the data.

2017

As Voting Machines were recognized as an easy target, the idea was to replace them.

2018

First testimonials by Mark Zuckerberg in the US Senate.

Voting Machines being replaced by new ones, more advanced and secured.

First cases of Voting Machines not working properly.

Midterm election, accusations of Russian and Chinese interference.

Deepfake technology causes awareness and is being banned or limited by several corporations and states.

National Security Commission on Artificial Intelligence (NSCAI) was created by Federal Government.

2019

The US Justice Department has filed criminal charges against Chinese telecoms giant Huawei and its chief financial officer, for bank fraud, obstruction of justice and theft of technology.

Election Laws are changed and challenged ahead of 2020 voting in several states as the 2016 presidential election proved how narrow victories in battle states could be decisive.

2020

Chief executives of Google, Amazon, Apple and Facebook testify before Congress

2020 Presidential Election

Facebook and Google are directly blamed over their handling of the US election.

Voting Machines are considered insecure and easy to hack.

“Public sentiment against Facebook is a whole lot more negative than public sentiment against Google.”

American AI Initiatives in 2019

Launched on February 11, 2019 by the order of President Donald Trump

One of the main reasons behind the initiative is to **preserve the leadership of the US in the AI** sphere especially with the rapid developments in AI sphere in China

This policy aimed to funnel federal funding and resources toward AI-specific research while also implementing US-led international AI standards. Additionally, the program calls for new research into increasing AI literacy in American workers.

The same year US, jointly with other countries, adopted **OECD AI Recommendation** the first intergovernmental standard for AI and **G20 AI Principles**

American AI Initiative Objectives:

- Promoting sustained investment in AI R&D;
- Enhancing access to federal data, models, and computing resources;
- Reducing barriers to the use of AI technologies;
- Ensuring that technical standards minimize vulnerability to attacks from malicious actors;
- Training American AI researchers;
- Implementing an action plan to protect US economic and national security interests.

The proposed United States AI regulatory principles:

- Ensure Public Engagement;
- Limit Regulatory Overreach;
- Promote Trustworthy AI.

Challenges and criticisms

- The initiative will redirect federal funding and resources towards AI research, however, the program includes no new funding for AI development
- The program is based on free market approach meaning that the government does not directly promote but rather create incentives for AI sphere and its success is still dependent on private initiative

In November, the Congressionally-mandated **National Security Commission on Artificial Intelligence (NSCAI), outlined five lines of effort to help ensure US technological leadership**:

- Invest in AI Research and Development (R&D);
- Apply AI to National Security Missions;
- Train And Recruit AI Talent;
- Protect and Build Upon US Technology Advantages;
- Marshal Global AI Cooperation.

Timeline of the AI initiative in the US

2016

In 2016, **President Barack Obama and the White House Office of Science and Technology Policy (OSTP)** launched a series of workshops and a Subcommittee on Machine Learning and Artificial Intelligence to monitor technological advances and help coordinate federal activity in AI.

National Artificial Intelligence R&D Strategic Plan is developed

2017

In May 2017 the **bipartisan Artificial Intelligence (AI) Caucus** for the 115th Congress is launched

In July 2017, the **Department of Homeland Security** issued a **report titled, "Artificial Intelligence Risk to Critical Infrastructure,"** which analyzed narratives about AI to better understand the perception of benefits and threats from AI adoption.

2018

National Security Commission on Artificial Intelligence (NSCAI) was established "to consider the methods and means necessary to advance the development of Artificial Intelligence, machine learning, and associated technologies to comprehensively address the national security and defense needs of the United States."

The US **Department of Defense** followed up with the release of an **unclassified summary of its own Artificial Intelligence Strategy.**

In May 2018, President Trump and the White House held a **Summit on Artificial Intelligence for American Industry** that included key technology companies.

2019

President Donald Trump issued an Executive Order **launching the American AI Initiative** on February 11, 2019. To facilitate AI R&D, and promote trust, train people for a changing workforce, and protect national interests, security, and values.

On March 19, 2019, the US federal government **launched AI.gov** to allow easier access to all of the governmental AI initiatives in the process

An updated version of the **National AI R&D Strategic Plan** is released

US, jointly with other countries, adopted **OECD AI Recommendation** and **G20 AI Principles**

2020

In January 2020, **the White House proposed AI regulatory principles for the use of AI in the private sector.**

On February 26, 2020 the **American AI Initiative: Year One Annual Report is released**

In September 2020**, signing of the Declaration of the US and the UK on Cooperation in AI R&D.**

In December 2020, **President Donald Trump** signed Executive Order on Promoting the Use of Trustworthy AI in the Federal Government

General Conclusions and Recommendations

General Conclusions

Some experts consider the 2020 59th quadrennial Presidential election to be among the most important due to their disruptive nature and long-lasting consequences. The events and strategies on regarding technology usage during and after the election suggest that US may face severe turbulences in near future.

For the last 4 years technologies and big online platforms such as Facebook and Google have used consumers' personal data, became battlegrounds of opinions and were used by politicians to win elections. They became active players in the electoral process. The four years preceding 2020 Presidential election showed that the government has little understanding of how personal data is stored and protected.

After election 2020, technological solutions were blamed once more. Voting Machines and Social Media were closely observed by the media outlets and political activists. Facebook and Google faced monitoring from the US Senate.

The main issue of this election was the public distrust towards the electoral procedures and technologies that were used to support the whole process. Unfortunately, this has the ability to ruin the credibility of all technologies used to improve the government's administration efficiency. We consider this to be dangerous for a country dubbed as the most powerful AI nation.

Another important factor here is the great fear of the idea that AI may steal American jobs. The concerns regarding automation technologies, now used by political figures, may hinder the development of AI solutions and more importantly - the implementation of related innovations.

Key points regarding Artificial Intelligence and its usage as a GovTech tool:

The uses of Artificial Intelligence in government are numerous, with the potential to revolutionize almost every aspect of its operations. Hilla Mehr (Harvard Ash Center Technology & Democracy Research Fellow) suggests that six types of government tasks are appropriate for AI applications:

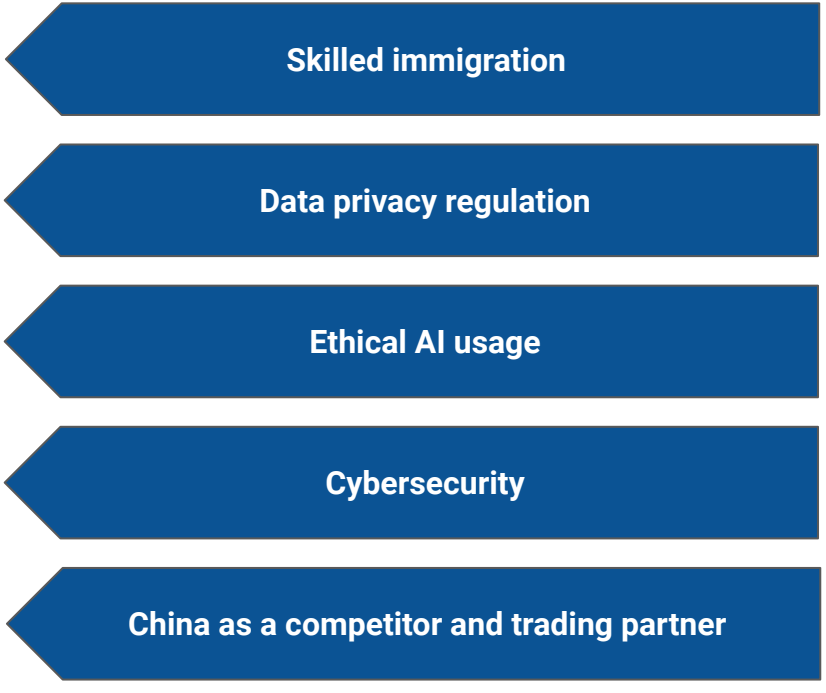
1. **Resource allocation -** Providing insights to where public resources would be spent most efficiently.
2. **With large datasets -** Whenever these are too large and complex for administrators to work on efficiently they can be crunched by AI and when multiple datasets could be combined to provide better insights.
3. **Experts shortage -** including where basic questions could be answered and niche issues can be learned (using tools similar to current commercial chatbots).
4. **Predictable scenario -** historical data allows the administration to create predictive models to improve government response.
5. **Procedural problems -** Repetitive procedures where inputs or/and outputs usually have a binary answer.
6. **Diverse data** - Where data takes a number of various forms (such as visual and linguistic, structured or not) and needs to be summarised and cleaned regularly for better processing.

General Conclusions

In the coming years, we are going to witness the start of a new regulation process in the US. Elections raised suspicion towards several Tech giants and their technologies. The lack of regulation in multiple tech domains sparked numerous debates. As a result, there are critical issues that will need to be resolved by the new Presidential administration:

- Over the past few decades various problems related to Data privacy protection arose. People share through Social media more information about themselves than ever before allowing the aggregation of huge databases of personal information.
- Artificial Intelligence is anticipated to bring the economy automation to a new level. In February, 2019, US has launched the American AI Initiative in order to preserve the US AI leadership in the face of the rising China AI strength.
- Foreign cyber attacks exposed the vulnerabilities in the American electronic government systems and this posed the question regarding national security in the future. The new President must work to strengthen cyber defences.
- The People's Republic of China threatens the super-power position of the US and the new American leader must balance between competing (technology-wise) and partnering with it (in terms of trade).

The problems must be resolved by a new administration:



General Conclusions

- The past decade of local and national elections clearly demonstrated that the US needs much stronger Data Privacy & Protection Regulation in the style of the European Union's General Data Protection Regulation (GDPR) adopted in 2016.
- Various authorities around the world need to help increase the level of trust in new technologies by educating the general public regarding their potential.
- The exponential growth of technological development will have the possibility to transform society in many ways. However, there are multiple challenges, such as: the rising gap between developed and underdeveloped countries and even between the rich and poor people within one society. It is up to the government to step up and provide the necessary directives and regulations in order provide stability and prosperity.
- The Artificial Intelligence (AI) development can be compared to the 19th century Industrial Revolution. It has the power to create new industries, eliminate the old ones and to pervade almost every aspect of our life. Therefore, there is a dire need for transparency and ethics regarding AI research and implementation.
- The future US presidential administration must address a multitude of problems related to the dynamic political environment (both external and internal). The American society is highly divided in the face of the uncertainties in both technological and political perspectives.
- Recent years demonstrated a sharp need for international cooperation in the sphere of AI. It is crucial for US to keep and extend an international collaboration in order to improve the advancement of the field for a greater good.
- During the last several years the EU and the UK implemented several productive initiatives related to the establishment and regulation of AI ethics. International cooperation with leading countries of AI ethics development has the potential to strengthen the democratic institutions of the US.
- Tools and technologies used for government purposes (Big Data Analytics, Online Voting, Artificial Intelligence for Voting Automatization and Anti-Fraud Monitoring, Voting Machines Connected to the Cloud) are still in their relatively primitive stage of development, and their transparency lacks a required level of security.
- The widespread suspicion towards technologies used for government purposes is driving away the much needed investment in the sector. Some of the current solutions are already too old and increasingly fault-prone. A new regulation and information campaigns are required in order to make the people trust them and to allow for the inflow of new investments and ideas in the domain that was hindered due to the virtual monopoly held by several voting machines corporations up until now.

Technologies are Reflecting Social Problems

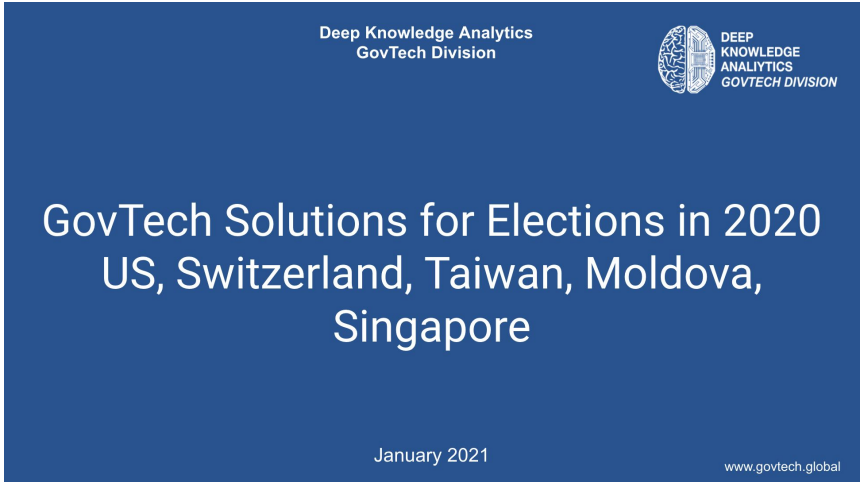
American society today is polarised and exhibits mistrust towards technology solutions used in electoral process, warranting introduction of reliable information services and technologies.

Recent debates regarding unethical or non-transparent use of modern informational technologies by Big Tech companies sparked new demands for such companies and services. A number of companies and start-ups aim to challenge the major players in the field by prioritizing privacy and security, enhancing the interpersonal experiences of users, limiting the personal data gathered from the users, and allowing them access to information banned by the other media channels.

There is a potential trend that innovative media channels would cease this opportunity and challenge media giants and Big Tech companies, bringing diversity and competition to the marketplace which is currently exhibiting a shift towards monopolization.

The image displayed on this page reflects the emerging trend representing a migration of users from previously most popular media platforms and digital technologies to their new rivals in hopes of avoiding censorship.

GovTech Solutions for Elections in 2020 in US, Switzerland, Taiwan, Moldova, Singapore



In this upcoming report we will try to cover to cover Government Technologies (GovTech) used in various countries around the world some of them differing by a number of social and economic parameters. Countries like Moldova and Taiwan, while being on different levels of development, are trying to increase their elections' transparency in a similar way - by automating the process and lowering the chances of man-made mistakes.

Women in Governance 2021

Although women on a high-level public positions are not something new, in 21st century there is a sharp increase in the number of female politicians in leading roles. Many of the high-profile women in that report have been on their public positions for years while others are relative newcomers and this analysis aims to present their profiles in-depth and how they came to be those inspiring figures, that we can see in today's dynamic political environment.

Data Sources

1. Denmark, Korea and Estonia Top the 2020 UN E-Government Ranking. Retrieved: Dec 9
2. The Rise of GovTech: How Technology Is Transforming Government. Retrieved: Dec 9
3. 8 Voting Technology Startups That Are Advancing Democratic Voting Infrastructure. Retrieved: Dec 9
4. Driving Political Campaigns with Artificial Intelligence Technologies. Retrieved: Dec 9
5. Voting in social networks. Retrieved: Dec 9
6. 5 Measures to Harden Election Technology. Retrieved: Dec 9
7. Internet Voting Technologies and Civic Participation: The Users' Perspective. Retrieved: Dec 9
8. Going from Bad to Worse: From Internet Voting to Blockchain Voting. Retrieved: Dec 9
9. Big Data Analytics On-Premises, in the Cloud, or on Hadoop | Vertica. Retrieved: Dec 11
10. Case study - Montana 2016 Presidential election. Retrieved: Dec 9
11. ShiftState Security - Senator Ron Wyden. Retrieved: Dec 9
12. US Pioneers Blockchain Election Voting With West Virginia Mobile Trial. Retrieved: Dec 9
13. WV's Secure Mobile Voting Application. Retrieved: Dec 9
14. UNDER THE HOOD: The West Virginia Mobile Voting Pilot. Retrieved: Dec 9
15. US: Denver to Use Mobile Voting Blockchain Platform Aimed at Overseas Voters in Elections. Retrieved: Dec 9
16. Utah County Becomes 3rd US Jurisdiction to Launch Blockchain Voting. Retrieved: Dec 9
17. Two More US Jurisdictions Launch Blockchain-Based Mobile Voting. Retrieved: Dec 9
18. The US will have digital voting sooner than you might expect. Retrieved: Dec 9
19. Utah 2016: World's first government election using blockchain technology. Retrieved: Dec 9
20. How President Obama's campaign used big data to rally individual voters. Retrieved: Dec 9
21. Computational Methods for Handwritten Questioned (2010). Retrieved: Dec 9
22. US election results: Five reasons Biden won. Retrieved: Dec 9
23. Ranking Members Klobuchar, Warner, Reed, and Peters Press Election Equipment Manufacturers on Security. Retrieved: Dec 9
24. Data Firm Says 'Secret Sauce' Aided Trump; Many Scoff. Retrieved: Dec 9
25. How does Big Data influence elections and electoral campaigns? Retrieved: Dec 9
26. Digital Political Marketing. Retrieved: Dec 9
27. How political campaigns use your data. Retrieved: Dec 9
28. How Obama Used Big Data to Lock Up His Reelection in 2012. Retrieved: Dec 9
29. The technology that powers the 2020 campaigns, explained. Retrieved: Dec 9
30. United States of America v. Facebook, Inc. Retrieved: Dec 9
31. US Elections in Search 2020. Retrieved: Dec 9
32. Facebook and Twitter Cross a Line Far More Dangerous Than What They Censor. Retrieved: Dec 9
33. 7 benefits of electronic voting - Civiciti. Retrieved: Dec 9
34. The Help America Vote Act (HAVA). Retrieved: Dec 9
35. How Will the US Combat Election Day Cyberwarfare? With Paper. Retrieved: Dec 9
36. Foreign Interference in the 2020 Election. Retrieved: Dec 9
37. Facebook Moves to Limit Election Chaos in November. Retrieved: Dec 9
38. Expanding our policies to further protect the civic conversation. Retrieved: Dec 9
39. Social Media Could Determine The Outcome Of The 2020 Election. Retrieved: Dec 9
40. Facebook announces plan to stop political ads after 3 November. Retrieved: Dec 9
41. Twitter Safety in Twitter: "We placed a public interest notice on…" Retrieved: Dec 9
42. Electoral Systems in the United States. Retrieved: Dec 9
43. US Patent 415,549. Retrieved: Dec 9
44. US Patent 395,782. Retrieved: Dec 9
45. US Patent 3,793,505. Retrieved: Dec 9
46. Historical Timeline: Electronic Voting Machines and Related Voting Technology. Retrieved: Dec 9
47. Glossary - Voting Machines - ProCon.org. Retrieved: Dec 9
48. The Graphic Truth: Americans' growing mistrust of elections. Retrieved: Dec 9
49. Effective Use of Computing Technology in Vote-Tallying. Retrieved: Dec 9
50. Challenging the Norms and Standards of Election Administration: Electronic Voting. Retrieved: Dec 9
51. The next-generation bots interfering with the US election. Retrieved: Dec 11
52. Terrifying technology tops list of American fears. Retrieved: Dec 9
53. NARRATIVE ANALYSIS Artificial Intelligence July 2017. Retrieved: Dec 9

Data Sources

54. The Real AI Threat to Democracy. Unprecedented challenges and new opportunities. Retrieved: Dec 11
55. Artificial intelligence can save democracy, unless it destroys it first. Retrieved: Dec 11
56. A legislative comparison: US vs. EU on data privacy. Retrieved: Dec 11
57. Don't Trust Artificial Intelligence? Time To Open The AI 'Black Box'. Retrieved: Dec 11
58. US Elections in Search 2020 | Google Trends. Retrieved: Dec 11
59. Twitter and Facebook Contend With Concerns Over Election Interference, Censorship. Retrieved: Dec 11
60. Americans Who Mainly Get Their News on Social Media Are Less Engaged, Less Knowledgeable. Retrieved: Dec 11
61. Experts: Disinformation poses greatest threat to the election. Retrieved: Dec 11
62. Supporting the 2020 US election. Retrieved: Dec 11
63. An update on our political ads policy | Google Ads. Retrieved: Dec 11
64. Private Equity Controls the Gatekeepers of American Democracy. Retrieved: Dec 11
65. State officials demand voting system vendors reveal owners after Russian hacks and investments. Retrieved: Dec 11
66. Private companies should not be running our elections, law professor says. Retrieved: Dec 11
67. State Requirements and the Federal Voting System Testing and Certification Program. Retrieved: Dec 11
68. America's Voting Machines at Risk. Retrieved: Dec 11
69. Testing & Certification Program Manual | US Election Assistance Commission. Retrieved: Dec 11
70. Certified Voting Systems | US Election Assistance Commission. Retrieved: Dec 11
71. Withdrawn Or Decertified Systems | US Election Assistance Commission. Retrieved: Dec 11
72. Voluntary Voting System Guidelines | US Election Assistance Commission. Retrieved: Dec 11
73. Voting System Testing LAP | US Election Assistance Commission. Retrieved: Dec 11
74. The Technical Guidelines Development Committee | US Election Assistance Commission. Retrieved: Dec 11
75. Chinese parts, hidden ownership, growing scrutiny: Inside America's biggest maker of voting machines. Retrieved: Dec 11
76. Who Owns Our Voting Machines? Retrieved: Dec 11
77. Who Tests Voting Machines? The New York Times. Retrieved: Dec 11
78. Posts falsify ties between election tech firm and Democrats. Retrieved: Dec 11
79. Concern from candidates, officials as error creates delay in release of returns; Dixon leads in Baltimore mayoral count. Retrieved: Dec 11
80. What Went Wrong at New York City Polling Places? It Was Something in the Air. Literally. Retrieved: Dec 11
81. The Market for Voting Machines Is Broken. This Company Has Thrived in It. Retrieved: Dec 11
82. Johnson County to change election equipment before May Primary. Retrieved: Dec 11
83. Inspection of the Dominion Voting Systems' Democracy Suite 5.5 conducted on January 16 and 17, 2019. Retrieved: Dec 11
84. Election Advisory No. 2018-35 Voting on Hart eSlate machines. Retrieved: Dec 11
85. NSCAI Interim Report for Congress 2019. Retrieved: Dec 11
86. The National Artificial Intelligence Research And Development Strategic Plan. Retrieved: Dec 11
87. Artificial Intelligence for the American People. Retrieved: Dec 11
88. Executive Order on Maintaining American Leadership in Artificial Intelligence. Retrieved: Dec 11
89. The National Artificial Intelligence Research And Development Strategic Plan: 2019 Update. Retrieved: Dec 11
90. OECD Principles on AI. Retrieved: Dec 11
91. G20 Ministerial Statement on Trade and Digital Economy. Retrieved: Dec 11
92. American Artificial Intelligence Initiative Year One Annual Report. Retrieved: Dec 11
93. Declaration of the United States of America and the United Kingdom of Great Britain and Northern Ireland on Cooperation in Artificial Intelligence Research and Development: A Shared Vision for Driving Technological Breakthroughs in Artificial Intelligence. Retrieved: Dec 11
94. Promoting the Use of Trustworthy Artificial Intelligence in Government. Retrieved: Dec 11
95. Artificial Intelligence for Citizen Services and Government. Retrieved: Dec 11

DISCLAIMER

The information and analysis provided in this document were prepared by GovTech Division of Deep Knowledge Analytics (DKA). The sources of information contained herein are deemed reliable by DKA, however, DKA makes no representations regarding to the accuracy or completeness of such information. Though the information herein is believed to be reliable and has been obtained from public sources believed to be reliable, we make no representation as to its accuracy or completeness. Hyperlinks to third-party websites in this report are provided for reader convenience only. Opinions, estimates and analyses in this report reflect the opinions of DKA as of the date of this report. DKA has no obligation to update, modify or amend this report or to otherwise notify readers in the event that any topic, opinion, estimate, forecast or analysis set forth herein changes or subsequently becomes inaccurate. This report is provided for informational purposes only, it may contain errors and is subject to revision.

CONTACT US

www.govtech.global
info@govtech.global

Deep Knowledge Analytics
GovTech Division

DEEP KNOWLEDGE ANALIYTICS
GOVTECH DIVISION

GovTech Solutions for Elections in 2020 US, Switzerland, Taiwan, Moldova, Singapore

January 2021

www.govtech.global

Deep Knowledge Analytics
GovTech Division

DEEP
KNOWLEDGE
ANALIYTICS
GOVTECH DIVISION

Women in Governance 2021

February 2021

www.govtech.global

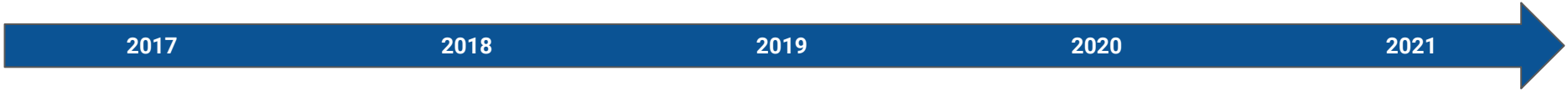
Trends and Tendencies in the US relations with AI

A long period of concerns and criticism against technologies currently used during the election process such as VM and Big Data Analytics as well as the ones used by Big Tech companies during which the American public is starting to slowly sympathize with the idea of centralized regulation regarding data privacy and AI R&D.

The US was one of the last countries to establish a government authority, responsible for the regulation and stimulation of AI research and development activities. The American AI Initiative has the purpose to focus the resources of the Federal Government in support of AI innovation, increase the level of national security and improve efficiencies on all levels of the economy.

No matter who will win the 2020 US Presidential elections, both parties are going to request the large internet companies to change their current policies and practices concerning personal data protection. Such cases may create precedents and in 2021 this may lead to the establishment of central authority (akin to European Union's GDPR).

In 2020 the implementation of the California Consumer Privacy Act (CCPA) brought the requirement for businesses to disclose personal information gathered about consumers. The next most anticipated step is the US Congress to pass a specific federal data privacy legislation, and if this happens, it will form the first-ever federal privacy standard which will provide stability for business entities operating with large consumer data sets.



Technologies are Reflecting Social Problems

American society today is polarised and exhibits mistrust towards technology solutions used in electoral process, warranting introduction of reliable information services and technologies.

Recent debates regarding unethical or non-transparent use of modern informational technologies by Big Tech companies sparked new demands for such companies and services. A number of companies and start-ups aim to challenge the major players in the field by prioritizing privacy and security, enhancing the interpersonal experiences of users, limiting the personal data gathered from the users, and allowing them access to information banned by the other media channels.

There is a potential trend that innovative media channels would cease this opportunity and challenge media giants and Big Tech companies, bringing diversity and competition to the marketplace which is currently exhibiting a shift towards monopolization.

The image displayed on this page reflects the emerging trend representing a migration of users from previously most popular media platforms and digital technologies to their new rivals in hopes of avoiding censorship.