Election Technology and Principles: Vendor Landscape

2022

Table of Contents

Introduction

The introduction of electronic technologies into elections can significantly improve elements of election processes. However, there are potential pitfalls and risks to electoral integrity and related public trust in the adoption of electronic technologies. Decisions concerning whether to adopt such electoral technologies are not simply "technical" matters but often should be the subject of open and inclusive public policy discussions. Once inclusive policy deliberations are properly concluded, moving forward typically becomes the responsibility of election officials, though in many countries international assistance agencies and assistance organizations play important roles that can influence technology adoption.

For decades, election management bodies (EMBs) have introduced technology in electoral processes in an attempt to solve problems of access, inequality, inefficiency, and transparency. However, when EMBs adopt various technologies (often by outsourcing to outside vendors various hardware, software and/or related services), the universal principles of democratic elections and the best practices that support them remain applicable. Not only do EMBs need to consider how democratic principles and best practices can be maintained as technologies are introduced, but vendors must ensure these principles are met in tool design and implementation. Other stakeholders, including political parties and citizen and international observers monitoring the process, as well as donors and technical assistance providers supporting the process, should also promote these principles through their work.

This paper is intended to aid professionals advising, implementing or monitoring the application of technology into an election process by helping these actors better understand the vendor space and the potential role that vendors can play in promoting and adopting sound electoral principles. The paper reviews the types of technologies commonly utilized in official election processes, and offers an overview of the "marketplace" of election technology. Additionally, the paper revisits key electoral principles[1] and best practices that vendors – and those managing them – should consider as they identify, design and implement technology solutions, as well as the possible inroads for promoting those principles in the vendor space.

For the purposes of this paper, "vendor" applies to any outside organization, whether a private, public or state-owned enterprise or an external state entity, providing election technology services and goods to an EMB, either at a cost or for free through international aid funding or vendor "donation." This paper is focused on technology that is specific to election processes, rather than broad-use, off-the-shelf hardware or software used by EMBs. This paper does not consider technology used by other electoral actors, including political parties or election observers, as those technologies are not used in official election processes and are not subject to the same obligations under national law or formal international commitments.

[1] This paper builds upon the principles established in the ***General Principles and Guidelines Related to ICTs and Elections*** by the E-ICT Working Group of the Declaration of Principles for International Observation community of practice.

Technology Provided by Vendors

Technologies provided by vendors aid in processes ranging from pre-election planning and staff management to voter registration, and from vote-casting and the tabulation and announcement of results to auditing. Each country utilizes technology in a unique way, as the problems technologies seek to address – as well as the laws governing the process and the technological context – vary significantly from country to country. The following sections describe aspects of today's elections in which technologies are commonly (though certainly not universally) employed.[2]

Voter Registration and Verification

Technologies are widely used to support voter registration, from collecting and verifying voter information, to managing a voter database, to verifying voters at polling stations. This may include the following.

Registration and creation of a voter list

Technologies may be used to collect personal information from potential voters, whether through mobile registration officers, stationary offices, or official websites. At a minimum, voter information, such as name, age and address, may be collected and digitized through direct entry/recording (such as filling an electronic form on a tablet or computer) or optical scan technologies that digitize paper forms. Some countries collect additional personal identifiers from citizens, including signatures or government identity card numbers, or biometric data such as photographs, fingerprints, and/or iris scans.

Depending on the legal and administrative framework, some countries create their voter list from data (informational and/or biometric) collected for a civil registry. In such cases, technologies utilized for the civil registry would be considered electoral technologies.

Voter list data management and data storage

Election management bodies typically utilize technologies, including specialized data management and database software, to compile, verify, and manage a voter list. Software may check for duplications and errors, and in some cases cross-check with other official sources (such as a civil registry) to verify identity documents or voter eligibility. Technology is also used to store the voter list database on a secure platform, whether remote (cloud-based) or local server. In some countries, technologies may be used to make the voter list more accessible and transparent, including look-up tools on the web or social media platforms that allow voters to check their registration, or Application Programming Interfaces (APIs) that provide select partners (such as political parties, the media, civil society organizations and others) access to non-sensitive data on the voter list.

[2] For more details on these specific technologies, see IFES and NDI, Implementing and Overseeing Electronic Voting and Counting Technologies (2013); and NDI Monitoring Electronic Technologies in Electoral Processes (2007).

Voter verification

Some countries use technology to verify voters' identities at polling stations. This may include tablets or computers and software used to check-in a voter. In some countries, this includes electronic verification of voter ID cards or biometric data such as photos or fingerprints. In mail-in voting systems, technologies are commonly used to sort, process and/or verify ballot envelopes (using optical scan or, less commonly, signature verification software).

Voting and Counting Processes

Some countries use technology to distribute ballots and/or cast and record votes – either at a polling place or remotely through mobile devices, the internet, or the postal service. For in-person voting in some countries, voters (or a subset of voters, such as those with disabilities unable to mark a paper ballot) may use a ***ballot marking device (BMD),*** where the voter uses a touch screen or other technology to view the ballot and indicate their choice. Once the voter's choice is indicated, the machine prints a marked paper ballot, which is placed into a ballot box. Some countries use ***optical scanners*** to count votes marked on paper ballots – whether hand-marked at a polling place, printed/marked by a BMD, or mailed by a voter. Other countries use ***direct recording electronic (DRE) devices***, where voters use a touch screen or other technology to indicate their choice and electronically submit their vote. (In line with election integrity principles, DREs should include an auditable, voter-verified paper trail.)

In the last decade, new technologies have emerged to support remote voting through mobile and/or online tools. Some online voting technologies are hybrid, where a ballot is delivered via the internet, marked electronically, printed and returned by mail or other method.[3] By comparison, completely online systems, where voters receive, mark and submit a ballot over the internet, are not widespread in use, and specific applications, methods, and security measures vary. Some systems, like internet voting conducted in Estonia, rely on an "end-to-end" process that links voter/civil registration (often using biometrics), voter verification, and online voting with the aim of mitigating voter fraud. Some systems utilize different forms of enhanced security measures, like encryption or distributed ledgers (such as blockchain), to mitigate the risk of hacking. Despite these measures, voting security experts remain skeptical that current technologies can ensure necessary transparency, secrecy of the vote, and security and accountability measures to hold legally-binding elections that maintain public trust.[4]

[3] Note this hybrid approach (sometimes called "Remote Ballot Delivery") is often utilized where the legal framework does not permit online voting (receiving, marking and submitting a vote over the internet). Some countries use Remote Ballot Delivery to equalize voting access for certain subsets of voters, such as overseas or military voters, or voters with disabilities unable to vote in person.

[4] See https://www.csail.mit.edu/news/mit-experts-no-dont-use-blockchain-vote, https://www.aaas.org/programs/epi-center/internet-online-voting, and https://verifiedvoting.org/the-myth-of-secure-blockchain-voting/.

Results Transmission, Tabulation and Announcement

Technologies are also used to transmit, tabulate and announce election results. This may include transmitting results from polling stations to central tabulation centers or databases, using Unstructured Supplementary Service Data (USSD), text messages sent through short-message systems (SMS), or internet-based systems. These systems sometimes include additional security measures – such as encryption – to mitigate against hacking. Some countries use this technology to rapidly report preliminary results (while legally official results are transmitted on paper forms or other channels), while others rely on technology to transmit official results.

Once official votes are received, technology (such as special software and secure databases) may be used to tally results, confirm winning candidates and/or allocate seats according to the legal framework and electoral system.

In many countries, technologies are often used to display and communicate results. This may include official websites that display aggregate vote totals and winners of races. In many cases, such websites are separate from an election management body's main site and are designed, hosted and maintained by an external vendor. In some elections, aggregated or disaggregated results may be made available to a select audience (such as media) or to the public via an API or other open data mediums.[5]

Core Information Technology and Cybersecurity Services

Increasingly, EMBs seek vendors to provide stand-alone IT services or supplemental cybersecurity services and technologies. Core IT services may include device and network management, secure storage, or data backup either on remote (cloud) or local servers. Cybersecurity security services may include: investigative/forensic services, audit services, cybersecurity engineering services, cybersecurity operations, and/or other services and technologies to check for vulnerabilities.[6] Similarly, EMBs may engage vendors to monitor systems for signs of attack or other problems.

Other Technology Uses in Elections

Some EMBs procure hardware, software and related services for other processes and needs. These may include:

- Voter education tools, including smart phone apps.
- Special election management software, including tools for candidate registration, campaign finance reporting and monitoring, and other processes.
- Case-management software used for electoral dispute resolution.

---

[5] For more information on Open Data and related principles, see https://openelectiondata.net/en/guide/principles/

[6] Note that testing services are sometimes offered by the manufacturers or developers of that particular election hardware or software. In this case, vendors are testing vulnerabilities for the products they make and maintain, leading to potential conflicts of interest and issues of accountability, transparency and system integrity. For example, see: Voting's Hash Problem: When the System for Verifying the Integrity of Voting Software Lacks Integrity Itself.

- Broad ranging information technology services, including training, maintenance and servicing of EMB internal technologies.
- Technologies related to post-election audits, which may include optical scanners, analytical software or other tools.

Election Tech Marketplace: An Overview of Vendors

As the use of technology in elections expands in scope and extends to new countries, the vendor landscape has evolved in recent years. Several large-scale vendors specialize in the ***supply*** of technologies, by sourcing equipment from different developers or manufacturers, distributing equipment across the country, and servicing those technologies on the ground (often through local affiliates). For the most part, these supply/logistics companies are not addressed in this paper, though the principles discussed below are still applicable to procurement and to the technology solutions they provide.

Instead, this paper focuses on manufacturers, developers and software service providers of election technologies that sell directly to EMBs and other election implementers/donors. Many companies focus on one type of service or product (for example: internet voting systems, or biometric voter registration systems), while an increasing number of companies are providing systems for multiple processes. Some companies promote so-called "end-to-end" solutions that support electronic (often biometric) voter registration, voter verification and electronic voting.

Currently, the vast majority of election technology vendors are privately-owned corporations, with many supplying multiple countries and elections. Many of these companies are incorporated in the United States (US) or Europe, and thus, fall under those legal jurisdictions. In addition, a number of smaller companies based outside of the US and Europe have provided election technologies to EMBs, including several in Latin America, Asia, and Eurasia. Acquisitions and mergers of electoral technology companies have grown increasingly common over the past several years (especially in the US market), expanding the types of technology offered by certain vendors, but also reducing competition in the market, and introducing new security concerns (for example: hacking one major company impacts more elections).[7]

Some government bodies, EMBs or government-owned enterprises in places like Belarus, Brazil, India, Kyrgyzstan, Russia, Switzerland and others, have developed election technologies for their own elections.[8] Some, like India and Russia, have exported that technology to other countries – either at a cost or for free as part of international diplomacy.

[7] Within the US market, the threat of litigation has challenged some competitors entering the market and dissuaded EMBs from dropping older technology as detailed here: https://www.propublica.org/article/the-market-for-voting-machines-is-broken-this-company-has-thrived-in-it. At the same time, merging election technology companies has raised security concerns about hacking risks. See more: https://www.nytimes.com/2018/09/26/magazine/election-security-crisis-midterms.html?searchResultPosition=1.

[8] A small number of sub-national (state) EMBs in the US have built their own technology, primarily for use by overseas and military voters. https://verifiedvoting.org/election-system/in-house-remote-ballot-marking-systems-and-internet-voting-systems/.

While these relatively cheaper options are welcome to many EMBs, these government-owned vendors do not appear to have developed a strong market for their products and services beyond their own countries: such exported technology is often limited to a few pilot cases or national use in only a handful of other countries.

In many countries, domestic corporations sometimes support smaller-scale and simpler technology services, like website support, cybersecurity, simple databases, and, in some cases, results reporting software. Similarly, international election implementers occasionally create small-scale election technology options utilized by EMBs.

Increasingly, social media platforms are playing a greater role as election technology providers by building and deploying voter information and look-up tools. While these platforms are not usually compensated by EMBs for this service, if they expand their role into facilitating other election processes (such as voter registration), their role and technology should fall under the same regulations and principles as paid or donated election technology.

Integrity Principles in Election Technology

As described in Section I, technologies are often deeply entwined in election processes, even those most central to election integrity. Introducing technology (whether hardware, software, or service) into the election process does not remove the need for universal

Elec Tech Start Ups: The on-ramp for new technologies

Holding a much smaller share of the market are election technology "start-ups", which develop and market new products. Oftentimes, start-ups pursue a new technology solution (like internet or mobile voting) rather than trying to compete with more established and hardware-based election technologies (like electronic voting machines or scanners).

Start-ups vending new technologies tend to follow a similar path to break into the elections market. Many will lobby lawmakers, election officials or other decision-makers to promote the need for a new technology and present their solution. Some start-ups will seek out use in informal, non-binding or non-governmental elections (such as trade unions, student elections, etc.) to test and establish use cases for their technologies. Many vendors then seek use in higher profile elections, such as party primaries, regional governmental body elections or use in official government processes, like remote legislative voting or Supreme Court voting utilized during the COVID-19 pandemic.

Once a track record is established, start-ups may promote use in formal, constitutional elections run by EMBs. In these early cases, new technologies are often provided for free or very low cost to EMBs looking to pilot new solutions. Start-up companies, including those selling new technologies or providing services for free, should be held to the same standards and principles of more established vendors, including rigorous testing, feasibility studies, and transparency.

standards of integrity that build public confidence in elections and their outcomes. As explored in depth in ***General Principles and Guidelines Related to ICT and Elections,*** electoral technologies must meet the same principles guiding democratic elections, as prescribed in international, regional and national laws and commitments. This includes: maintaining integrity (including security), the secrecy and equality of the vote, universality, transparency, accountability and public confidence in elections.[9] As discussed in that paper, these principles must be maintained in each step of technology adoption: 1) as the unique and country-specific need for technology is assessed and defined; 2) as the specifications for a technology solution are determined and procured; 3) as an appropriate and competitive vendor is selected; and 4) as the vendor develops, applies, and maintains the tool. As delineated in the paper, ***these principles apply not only to the decision-making and procurement processes of the EMB or other government bodies, but also to the vendors, manufacturers, developers and service providers of electoral technologies and to the products and services they provide.***

The standards discussed in ***General Principles and Guidelines Related to ICTs and Elections*** are highly applicable, extending to clear best practices related to core election technology and its vendors. These considerations can serve as a baseline of industry standards, providing both a set of milestones for vendors to work toward, and a set of measurements for EMBs and others to consider when comparing vendors in a bidding process. In practice, these considerations may include:

1. **Feasibility**. A prominent consideration in assessing technology solutions feasibility: whether or not a technology is suited to a context and can effectively address identified problems. Often, technologies developed for a general context and/or deployed in other countries may not be flexible and/or efficient in solving another country's specific needs or in meeting other specific considerations listed below. Relatedly, testing technologies to ensure basic functionality and security, as well as piloting technologies in real-world conditions to ensure they will work for a country's unique context are critical. Vendors should commit to adapting and testing their technology to ensure its applicability and appropriateness for the specific country context.

2. **EMB Sovereignty and Autonomy.** As the lead implementers of elections, EMBs hold ultimate responsibility for electoral processes and their implementation. This requires EMBs to have a significant ability to decide on solutions, select and oversee vendors, and ultimately troubleshoot and manage technology solutions for longer-term sustainability. On one hand, EMBs should have internal technological capacity (including expert staff) that can assess and advise on technological specifications and selection of tools, as well as troubleshoot problems that arise. On the other hand, technology vendors should provide sufficient training for EMB technology staff and ensure the necessary level of collaboration, transparency and access for the EMB to effectively oversee and manage implementation.

[9] See the Principles and Guidelines paper, p. 2.

3. **Sustainability.** Ideally, vendors should commit to providing sustainable technology solutions that remain feasible, adaptable and accountable over several election cycles. The total cost of ownership (TCO) and lifecycle costs of a technology must be clear to the EMB and made transparent to other electoral stakeholders. Key to sustainability is avoiding "vendor lock," whereby EMBs have no option to change vendors (or technology solutions) without losing control or access to key parts of the election process or data. Cost structures that require "leasing" or "subscription" services (which may be subject to cost increases) to continue access can make technology less sustainable and threaten EMB sovereignty over election processes. This includes predatory pricing for new hardware, software updates or additional services in order to troubleshoot problems, replace or expand equipment, or maintain up-to-date security. Substantive training and collaboration that enhances EMB technology autonomy over time is also key to sustainability.

4. **Data Ownership, Accountability and Liability.** As mentioned above, EMBs and vendors should ensure that sensitive electoral data (including voter lists, personally-identifiable information and biometric data, cast votes, tabulated results and seat allocation calculations) remain under the control of the EMB. Data should be collected and stored so it remains subject to the legal jurisdiction of the country and subject to judicial review in the case of electoral dispute proceedings.[10] Further, the country of incorporation of a technology company can be relevant to understand additional liabilities and legal accountability measures. For example, companies may be subject to local laws and regulations that may have positive or negative impacts. On the one-hand, business or privacy regulations in the country where they are incorporated may set higher standards for transparency. On the other hand, some home country governments may apply local laws to gain access to sensitive data –including voters' personally-identifiable data - held by the company.

5. **Transparency and Public Trust.** As with any aspect of the electoral process, transparency is key in the use of election technologies. Procurement processes, product design, source code (whether fully open or provided to select independent reviewers), and contractual arrangements should provide for public transparency, oversight and monitoring of technology products.[11] Beyond the technology itself, transparency about vendors is also important to build public confidence and combat disinformation. In recent elections, bad-faith actors have spread disinformation

[10] See the Principles and Guidelines paper, p. 11

[11] Source codes are sometimes fully public, to build broad confidence. Other times, source code is provided to a select group of independent monitors or auditors. For more information on source code and other technical transparency measures, see NDI Monitoring Electronic Technologies in Electoral Processes (2007); IFES and NDI, Implementing and Overseeing Electronic Voting and Counting Technologies (2013).

Mitigating Technology Risks in Elections

In many cases, technology might help make election administration more efficient and transparent. However, the introduction of technology invites new risks to electoral security and integrity, as well as the rights of individuals. If technologies fail, core voting processes may be impacted, and confidence in elections may irreparably suffer. This is especially true for those processes that are most central to elections and elections confidence: voter registration and verification, voting, counting, tabulation, results management and audits, or technology collecting personally-identifiable voter data. Depending on the type of technology, the processes they automate and the data they involve, a greater level of care and risk mitigation may be necessary.

Potential risks come from all sides: intentional sabotage; poor planning or testing; deficits in budget, training or technology infrastructure; etc. Failure may arise from the technology itself, the vendor, from a supply chain vulnerability, or from an EMB or other implementor. Thus, all key actors – including vendors – have a role in risk mitigation.

The role of EMBs in risk mitigation - EMBs play a primary role in mitigating risks brought by new technologies. In addition to addressing gaps in technology infrastructure and capacity, budgetary shortfalls, or underinvestment in cybersecurity, the EMB should also ensure that: only appropriate tools are adopted; that the entire adoption process (including bidding, selection, testing and certification) is transparent; that redundancies are in place to prevent a breakdown of key electoral processes; and that independent oversight through independent audits and nonpartisan monitoring is ensured.

The role of vendors in risk mitigation - In support of and in addition to EMB policies, vendors are key partners in ensuring proper risk mitigation for election technologies. This includes practicing full transparency around their own vulnerabilities and internal mitigation strategies; committing appropriate resources, openness and accountability in technology design, testing and auditing; and working with EMBs to provide sufficient training and facilitate planned redundancies.

targeting election technology companies and their owners to sow distrust in electoral processes.[12] To demonstrate impartiality, combat disinformation and build public trust in election technologies, details about companies, such as ownership and other financial obligations, and internal due diligence policies, should be made public.[13]

[12] Disinformation was especially at issue in the US, where opaque private equity investments and ownership of US-market companies fed conspiracy theories and sowed significant distrust in election processes.
[13] Some transparency advocates encourage the disclosure of ownership stakes greater than 5% to allow EMBs, decision-makers and the public to be aware of any perceived or real conflicts of interest. In the US, where disinformation about ownership spawned distrust in elections, some federal and state lawmakers began requiring information about election vendor ownership through legislative inquiries and bidding requirements. See https://www.warren.senate.gov/oversight/letters/warren-klobuchar-wyden-and-pocan-investigate-vulnerabilities-and-shortcomings-of-election-technology-industry-with-ties-to-private-equity

Additionally, potential conflicts of interests, security incidents, and other key issues, should be disclosed.

6. **Competence, Experience and Capacity.** Recognizing the significance and sensitivity of election technologies, vendors should be deeply committed to conducting necessary due diligence and to delivering a fully successful technology solution. Beyond simple cost, vendors should demonstrate their viability as a company, the reliability of their technology and their level of experience as their technology is considered in a bidding process. Any controversies or history of litigation related to the vendor should also be disclosed and considered to head off potential delivery problems or threats to public confidence in election technologies.

7. **Respect for Human Rights, Security and Privacy.** Broader concerns for human rights, security, and privacy should also be addressed and incorporated into company policies, product design and due diligence.[14] The adoption and design of tools should be inclusive and account for unique risks to and concerns among marginalized communities, as well as broader rights, privacy and election principles–including the secrecy, equality, and universality of the vote. To ensure integrity of the voting process, sufficient security defenses and redundancies should be in place (both within the technology design, by the vendor and by the EMB) to ensure that problems do not derail core election processes or erode public confidence.

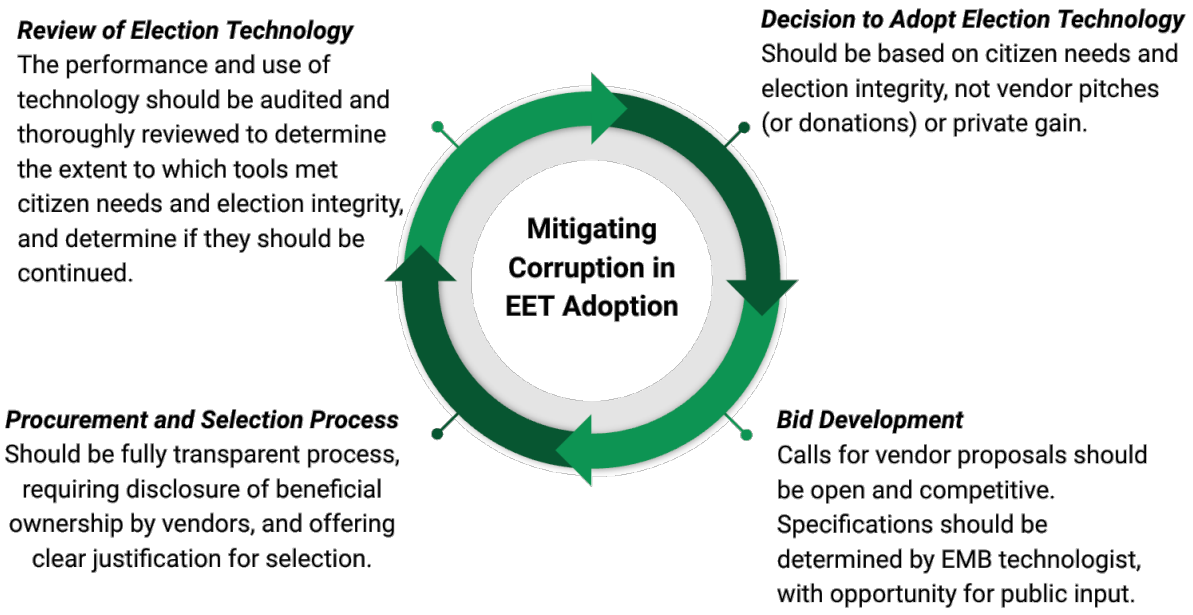
When technologies are used to collect and store voter data – including personal and biometric data – additional measures and principles must be considered. This includes policies and practices that ensure data collection, transmission, storage and protection are secure and at no risk of hacking, misuse or surveillance.

The collection of biometric data – which is vastly more sensitive due to the highly specific and personally-identifiable information retained – demands even higher standards of risk assessment and mitigation, informed consent of how such data will be used, and a greater guarantee of safe data handling and privacy. For example: the use of facial recognition software may be proposed to register and verify voters. However, such software has been abused by governments who, in the name of law and order, use it to surveil the every-day activities of citizens. Use of such sensitive technology in the electoral process demands enhanced oversight, input from citizen rights organizations, as well as privacy and technology experts, to ensure such technology is not abused.

[14] See Principles and Guidelines paper, p. 16

Risks for Corruption in the Adoption and Procurement of Electronic Election Technologies

As with any high-cost investment, there remains an increased risk for corruption and undue influence in election resourcing. In fact, there have been several high-profile instances and convictions of bribery by election vendors and corruption by officials. Electoral technology faces this risk throughout its adoption, but this can be mitigated through enhanced transparency, inclusive decision-making and opportunity for public input, and continued accountability and oversight of electoral technology. These principles are key *even when* technology may be donated or provided for free by a vendor.



Principles in Practice: Vendor Regulation, Requirements and Internal Policies

Recognizing the impact that technology can have in the success or failure of election processes, there are growing efforts to bring broader good governance, cybersecurity and human rights principles to the design, manufacturing and procurement of election technology.[15] As the field of election technology grows and evolves, various efforts have emerged to regulate, coordinate and promote best practices among vendors. These approaches can serve as examples and potential inroads for expanding election integrity norms and practices among election technology vendors. These include:

[15] See Principles and Guidelines paper, p. 3

Government regulations

Some governments test and certify election technology from various vendors. A primary example includes the United States, where the Election Assistance Commission, through federally accredited labs, tests and certifies electronic voting machines. Though not required by federal law, the process provides a strong incentive for vendors to meet federal standards and claim official 'certification' when bidding to provide technology for subnational election jurisdictions in the US.

Other governments set regulations that mandate certain human rights and privacy guarantees, transparency requirements or other practices that may apply to companies incorporated in that country or doing business in that country. For example, the European Union's 2018 **General Data Protection Regulation (GDPR)** mandates strict data privacy protections for organizations or companies with a presence in the EU or that handle data about EU citizens (whether or not those entities are based in the EU). These regulations can apply to election technologies used in the EU related to voter registration or verification (including biometric identification). Some technology vendors have responded with new protocols and technological changes to meet these emerging standards, including complying with data collection, storage and privacy measures.[16]

Procurement mandates and standards

Some governments, election bodies, assistance providers, or other actors may set procurement rules that require bidding vendors to abide by certain principles. Government bodies may set recommendations for electoral technologies, like the Council of Europe's Recommendations on Standards for e-Voting. In some cases, donors of election projects have developed their own standards for election technology procurement.

In many cases, procurement requirements are related to broader good-governance and/or cybersecurity principles. In its global procurement practice, which includes a large portion of election technology, the United Nations Development Programme (UNDP), sets qualifications and eligibility requirements for any vendor wishing to bid for contracts. At the same time, all bidding vendors must commit to the United Nation's supplier Code of Conduct, which requires sound labor, human rights, environmental, and anti-corruption/ethical practices.

Vendor Coordination

Recently, as cybersecurity concerns have grown around election technology, government bodies (at the regional, national and sub-national level) have attempted to coordinate various vendors to share information, promote best practices and set higher standards in the market. For example, the United States Cybersecurity and Infrastructure Security Agency (CISA) convenes election technology vendors through the Sector Coordinating Council to share intelligence and coordinate threats to election cybersecurity.

[16] See https://www.biometricupdate.com/202010/genkey-updates-biometric-database-software-to-meet-eu-gdprs-right-to-be-forgotten-requirement

Voluntary Codes of Conduct and Corporate Policies

Independent companies and other entities can voluntarily commit to the UN Global Compact establishing principles on human rights, labor, the environment and anti-corruption, which many election technology vendors have done. Some election technology or election suppliers create and publish their own company-wide codes of conduct to prohibit corrupt, unethical practices. Similarly, some vendors create their own corporate policies, such as prohibiting political donations and maintaining political neutrality.

These examples show the varied approaches – from externally imposed legal and bidding requirements, to voluntary best practice sharing or internal governance – that have influenced how vendors apply election integrity principles to their business and their technology.

Conclusion

As the use of technologies in elections continues to expand, and as the marketplace of technology vendors evolves, the need to adopt guiding principles and best practices is clear. The common principles guiding democratic elections apply not only to election technology, but to the business practices behind their development and implementation. Beyond these principles, there are practical considerations and implications that should be considered, both by EMBs and by vendors themselves. Positively, there are several inroads to promoting standards, principles and good practices among election technology vendors, through regulation and bidding requirements, or through voluntary education and adoption of internal policies. Moving forward, there is room for greater collaboration with vendors–and those engaging vendors for services–to advance democratic principles in election technology.