CHAPTER 7

GovTech

Emerging Technologies to Disrupt Public Sector Fraud and Corruption

Introduction

How important are emerging technologies in combating corruption?

The broadening and deepening of global digitization of governments and citizens is changing the face of public sector governance and its impact on anti-corruption in both developing and advanced economies. Digital government is moving fast, beyond digitizing paper-based records and transactions. The broad spectrum and increasing sophistication of the use of technology ranging from mobile computing to internet-connected sensors—spanning the internet of things (IoT) and biometric identification—means that digitization is ever more ubiquitous. The increase in digital interactions among officials, citizens, and business within countries and across the globe has had a positive as well as a negative impact. On the one hand, legitimate money can move efficiently, but on the other, illicit gains can be moved quickly across individuals and countries, making it difficult to track.

While digitization as a 'foundational' factor is important, other factors like institutional incentives and capacities and strong leadership are key for enhanced efficiency, improved service delivery and fewer opportunities for corruption. The 2017 World Development Report on Digital Dividends extensively documented that digitization by itself will not change the nature of public services if the institutional incentives and capacities are not in place. Similarly, to be effective, digitization and technology, together with strong institutional mechanisms, can make fraud and corruption more costly and less attractive for perpetrators both inside and outside of government. Use of digital technology with strong leadership can be instrumental in bringing about a wider transformation, including improved service delivery[58] and less opportunities for corrupt practices.[59] This has been demonstrated in the case study of India's Andhra Pradesh (AP) State Digital Transformation Strategy in the past decade. AP's experience shows how the sub-national government was able to disrupt traditionally strong vested interests that resisted change.

The traction that digital technologies may have in reducing fraud and corruption depends on the institutional context. Many political manifestos at the national and sub-national level articulate commitments to anti-corruption and technological innovation. Governments across the world have invested in digitizing government systems, including eProcurement systems.[60] However, any system will only be as good as the practices that complement it. To gain greater traction for addressing fraud and corruption, data needs to be captured, and linked with other data. Mandating the use of the system and validating and analyzing data using Artificial Intelligence (AI) or other methods can prove to be effective. The correct question, therefore, is not whether eProcurement systems can reduce corruption, but rather to investigate whether the institutional environment supports the use of data to detect fraud and corruption (see Box 7.1 on Brazil Court of Accounts). Institutional processes, practices, policies and regulatory regimes will determine whether digital applications are successful (or not) in achieving the desired outcome.

Increasing sophistication and advancement in technical solutions has implications for human resource management in the public sector. Understanding emerging technologies and their application in an institutional context requires specialized skills to assess and apply these technologies, both in the delivery of specific solutions (e.g., procurement data analytics and AI) and to better prioritize solutions. Government officials or public sector specialists typically do not come from a technologist background, or spend much time keeping abreast of the latest technology trends. While reform champions will themselves not need to be technical specialists, they should at the minimum have an understanding of what can be expected from different applications. Any productive discussion in this area will need to carefully align institutional reform with technology terminologies and expertise for domain areas, such as fraud and corruption. Some of these concepts are discussed later in the chapter and listed in Table 7.1.

While available data suggest that higher levels of digital government development are most likely correlated with greater government effectiveness and less corruption, other factors may also be playing a role. While technologies such as the internet, social media, and digital feedback mechanisms may initially heighten perceptions of corruption by exposing corruption, the real issue is whether they lead to change in behaviors to reduce, if not eradicate, corruption in a particular domain. Reporting and disclosure may in its own right not reduce petty bribes, but follow-up actions may.[5] However, given the aggregate nature of these cross-country indicators, measurement is not straightforward, and therefore may confound more general associations between income levels and a general set of governance indicators.[6]

BOX 7.1

Brazil's Tribunal of Accounts Robots

AI can serve as a decision support tool for identifying transactions and payments ex ante that are at a high risk of fraud and corruption. However, this technology can only have an impact if it changes the behavior of relevant government personnel, in this case auditors. The Brazilian Federal Court of Accounts (*Tribunal de Contas da União*, "TCU"), a Brazilian Supreme Audit Institution (SAI), has implemented AI systems since 2015 to analyze the procurement processes of the federal administration. The TCU's acronyms for the systems translate into robot names: Analysis of Bids, Contracts and Public Calls (ALICE)[4]; Analysis of the Dispute in Electronic Bids (ADELE); Integrated Monitoring for Acquisition Control (MONICA); and Guidance System on Facts and Evidence for the Auditor (SOFIA).

A more systematic study of auditors suggests that the solutions have not been mandatory, nor has training for auditors. The designers, however, suggested that this was part of a deliberate strategy. They believe that the auditors don't need to be trained to use the products; if they do, something is wrong. Just as a first-time user doesn't need to be trained to use Netflix. If the solutions use complex algorithms based on machine learning and cognitive processing, what should matter to the auditor are the results and their reliability for each purpose (Chief Data Officer).

Interviews of Audit Managers suggested varying levels of use: ALICE (3/5), followed by SOFIA (2/5), ADELE (1/5) and MONICA (1/5). Most managers were ambivalent about the actual changes or implications the decision support tools brought to their work. Qualitative interviews suggested that many auditors still followed old practices, including a preference for text editors and spreadsheets. While adoption was growing, it was happening at a slow pace.

Source: Neves et. al. (2019)

Use of digital technologies involves both opportunities and challenges

Digital government transitions, coupled with disruptive technological change, offer both opportunities and risks for anti-corruption. Digital investments (e.g., major 5G or shifts to cloud based services)[7] can lead to an increase in complexities and higher scope for corruption, as they might entail new modalities of procurement around notional services and data. Valuable resources, such as spectrum licenses can be a source of significant rents and consequently corruption.[8] Digital realms also bring a new set of public sector vulnerabilities in terms of abuse of office and capturing illicit gains. Digital transaction platforms (including bitcoin stores) can facilitate a rapid or scaled illicit syphoning of resources. On the other hand, digitization can help improve transparency, with near real-time feedback helping expose illicit behavior. Digital workflows and validation can lead to simplification of bureaucratic procedures and limit the discretion of public officials, improving the beneficiary experience and reducing corruption. For example, distributed ledger technologies—commonly known as blockchains (discussed later)—promise to increase the trust in digital registries and transaction data, reducing the scope for records tampering by officials.

Across levels of digital transformation, governments are facing different opportunities and challenges for better leveraging technology. Singapore's government, for example, has demonstrated a strong commitment to addressing fraud and corruption, not only by augmenting the use of technologies, but also by developing in-house technology capabilities in such areas as AI (see Box 7.2). The maturity of Singapore's digital ecosystem, coupled with its integrity institutions, demonstrates how a country can leverage opportunities that new forms of digital data offer, together with technological solutions. However, in a context that is still largely cash based, reliant on paper-based workflows, and where existing systems are not set up to link to each other, options in the short term are quite different. In such an environment, specific technical measures such as linking procurement to enterprise registries, as both systems improve, can prove to be a better solution to detect, for example, rigging patterns in bidding. A relatively underdeveloped digital government ecosystem or institutional context may also provide opportunities for 'leapfrogging' in terms of technology solutions. For example, the use of high-resolution satellite imagery technology platforms to supervise projects in Fragile, Conflict, and Violence (FCV) afflicted states where regular project supervision is not possible (e.g., Afghanistan or Iraq) represents

BOX 7.2

Singapore's SkillsFuture Program and Fraud Detection

Singapore's SkillsFuture program, a several million dollar grant program for training, faced issues of corruption. It was found that fraudulent training providers were signing up fictitious beneficiaries and pocketing the training fees.

Given the importance of the program, Singapore's Government Technology Agency ("GovTech") helped implement an AI machine learning solution to flag anomalous transactions. GovTech is a statutory board of the Singapore government, under the Prime Minister's Office. Since its current establishment in 2016, GovTech has built up strong in-house capabilities for applying technology solutions to government decision-making challenges (in this case Fraud and Corruption Detection), as well as citizen and business facing services.

Beyond the innovative technical solution (unsupervised machine learning to flag training payments that would suggest further human scrutiny), Singapore has introduced additional controls to ensure the integrity of the program. The program involves about 600,000 claims per year. Training recipients must now scan a time sensitive Quick Response (QR) code, which in turn is linked to individual Singpass accounts. SingPass, which stands for Singapore Personal Access, is an authentication system for citizens to transact online with the government. The SingPass mechanism uses a variety of authentication mechanisms, including fingerprint and facial recognition.

Singapore's digital government development is by all accounts one of the most advanced in the world. The SkillsFuture case highlights not just the applied use of AI, but above all the progressive linkage of different technologies, including foundational biometric identity confirmation technologies.

Source: Goh (2019), Singapore Straits Times (2019), Ko (2020) both a different rationale and realization of technology-supported solutions.

For developing countries seeking to address public sector management challenges, there may be opportunities to leapfrog and deploy new disruptive technologies (DTs) more widely. DTs have, in several instances, enabled better or new ways of doing things (like the shift from chemical to digital photography). They are also associated with lower complexity and costs to address the needs of a wider base of users by improving day-to-day processes. Due to their widespread use of cloud-based platforms, they are also rapidly scalable. Examples of DTs include transport platforms, such as Grab, that combine the use of smartphone, location-referencing/mapping, AI, and financial intermediation innovation to transform a particular service. While biometric technologies to confirm identities are not completely novel, rapid reductions in cost and increases in reliability have made it possible to scale them up in a massive way in such settings as India.[9]

This chapter seeks to highlight areas where digital technology developments can help disrupt fraud and corruption in the public sector. The focus is on the use of more recent technologies, against the wider backdrop of digitization, to promote increased detection of corruption and reduced discretion (or abuse) on the part of public officials and other implicated parties. Through illustrative boxes and cases, the chapter highlights the key contributions of a number of technologies in practice and associated theories of change.

Digital technology disruptions

Digital technology disruptions have been used in the public sector in a number of areas, including for revenue, expenditure, regulation, and financial and physical asset management. Table 7.1 summarizes the range of use-case applications across selected areas of public sector management used to address the associated vulnerabilities. The primary driver for reforms, and consequently more concerted applications, may be driven by efforts to increase taxes, improve the business environment, enhance services, or improve the effectiveness of certain regulatory functions. Framing technology-supported reforms as a public services delivery agenda, rather than in the first instance as an anti-corruption crusade, may also be a more disarming approach in light of the existence of the vested interests benefiting from corruption.

TABLE 7.1 Public Sector Fraud and Corruption Domains

Domains	Addressing Vulnerabilities	Applications
Revenue Mobilization	Reduce tax or customs evasion	eFiling, Risk profiling
Expenditures / Procurements	Reduce expenditure leakages/ efficiencies (wages, recurrent, or capital)	Expenditure risks and risk management
Public Services	Address petty corruption and unresponsive services	Digital services
Regulatory Services Enforcement	Enhance enforcement of environmental standards, zoning,	CCTV Cameras/IoT/satellites/drones for verification
States assets management	Tighten control and oversight over key financial and physical assets	Public property and works registries, public investment management
International Money Laundering /Stolen Asset Recovery	Illicit gains are moved across borders	Stolen asset recovery and re-patriation

Source: World Bank Staff

While digital channels can help improve convenience and lower levels of corruption in many public services (as listed above), the impact will depend on the complementary practices put in place. A study by Okunogbe and Pouliquen[10] in Tajikistan finds that higher risk firms, as categorized by an indicator from the tax authorities, are less likely to use eFiling,[11] as the choice to e-file taxes remains voluntary. The study finds that the impacts of technology, thus limiting discretion on the part of officials, will differ by how that discretion was previously used. If it was used to allow firms to pay lower taxes against a bribe payment to the official, technology may disrupt this equilibrium. If officials were using discretion to correctly monitor firms, the outcome may be different. The study suggests that depending on the degree to which electronic channels are voluntary, and how discretion was used, impacts will be heterogenous. Other benefits of eFiling systems include saving time and the ability to screen data (e.g., for risk profiling) more quickly.

Enhanced technologies may offer opportunities to address information asymmetries in difficult digitization settings, but should preferably be connected to foundational systems. In more extreme data scarce settings, including FCV-affected countries, technologies may serve to mitigate fraud and corruption risks associated with information barriers. Satellite or drone imagery could be useful to validate infrastructure projects where physical supervision is too costly or risky. Enhanced technologies can work to increase detection and reduce discretion (and abuse) with respect to particular risk areas like irregularities in construction. However, some of these techniques may only go so far, as parties colluding towards fraud and corruption learn to neutralize or evade these types of technological measures. "Leapfrog" technologies like satellite imagery are also likely to be most powerful if they can be connected with progressively strengthening "foundational" systems, for example eProcurement systems. Table 7.2 outlines cross-cutting areas of technological change that appear to have an impact on public sector fraud and corruption across the enumerated use-case applications. The past decade has seen rapid changes across a set of cross-cutting technologies. A number of terms, such as big data and AI can refer to very different approaches and use in different settings.

TABLE 7.2 Major Technology Trends for Public Sector Fraud and Corruption

Technology Trends	Examples	Opportunities
Digitization / Core Public Sector Enterprise Systems	FMIS, HRMS, Digital Registries, M&E	Improved process controls and transparency
Big Data	Expansion of data from systems, satellites, smartphones, sensors, Unmanned Aerial Vehicles (UAVs)	Richer feedback and insights from a vast new ecosystem of data
Cloud Computing Platforms	Use of cloud platforms to rapidly scale data integration and analysis	Ability to better leverage conventional core and emerging big data, including AI
Artificial Intelligence/ Machine Learning	Use of automated/deep learning techniques to identify fraud and corruption risks	Ex Ante or Ex Post risk detection (Box 7.1 and Box 7.2)
Biometrics (ID4D)	Unique identification of civil servants and government program beneficiaries	Civil service registry clearing Transfer/ social safety net programs
FinTech	Digital money, wallets	Cashless transactions, transaction tracking
Distributed Ledger Technology/ Blockchains	Trusted data sources and "smart" contracts	Cadasters, next generation e-GP
Internet of Things (IoT)	Use of sensor networks, including visual CCTV for monitoring and control processes	Environmental monitoring, public safety

Big data

The power of big data lies in linking relevant data from a variety of sources (numeric, text, and image data) and breaking data silos. Governments have traditionally relied on collected statistical data, as well as accumulated administrative data. The overarching concept of big data has come to refer to a wealth of new sources that are larger in size, higher in frequency, and often contain quite personalized data.[12] For example, Hlatshwayo et. al.[13] adopt a "big data" approach to measuring corruption based on cross-country news flow indices of corruption (NIC) and anti-corruption (anti-NIC) from over 665 million international news articles. They find that increased reporting on corruption shows some relationship with financial and real sector variables (e.g., stock markets and growth). However, the ability of developing countries, in particular, to implement the requisite data wrangling and analytics may in many cases still prove to be challenging. The term 'data wrangling' refers to the significant effort that is required to bring data together and clean it before meaningful big data analytics or AI can be applied. While data may exist in government, it is often siloed, requiring both technical capabilities and strong institutional leadership for integration, and consequently impact in terms of detection and control.

Greater access to digital data, alongside technology tools, can empower civil society and reform champions in government to detect fraud and corruption. The literature on ICT for better governance has highlighted that leveraging digital channels, including social media, to enhance transparency and feedback helps to flag corruption.[14] The evidence, however, remains patchy.[15] AI is also increasingly viewed as a possible strategy for governments (and civil society) to sift the digital data to gain insights on illicit behavior.[16] In settings such as Brazil, civil society has used data mining opportunities and techniques concerning social media and expenditure records to flag fraudulent behavior by officials and politicians.[17] These initiatives, however, risk remaining at the periphery of how the public sector, and its associated fraud and corruption risks, actually work in the digital area. While significant expectations are placed on transparency and feedback, there is a dearth of robust impact evaluations to confirm the impact of these data and feedback channels.[18]

The use of traditional public administration systems as well as new big data sources requires careful attention to omissions and biases. Conventional public sector enterprise systems relating to counting money, people, assets, and outputs may all be subject to omissions. Even if a civil servant is registered in a database, there is no guarantee that he/she exists. The fact that an eProcurement system records a public works contract is an important step in the journey of digitization. In the context of transactions systems such as FMIS or eProcurement, a key question is whether all transactions are comprehensive, and if not, why certain transactions are not included in these systems.[19] But this is still a long way from linking it to richer big data, such as image verification, or risk pattern analytics of bidding. There may or may not be biases relative to fraud and corruption (e.g., bidders captured in an eProcurement system, or taxpayers in an eFiling system). Despite large investments in IT systems, the systems were not designed necessarily to flag corruption and often do not. Statistical data that is typically collected is representative. But big data sources like India's *I Paid a Bribe* may also only give a partial or biased view of fraud and corruption. While big data—and the related application of Artificial Intelligence-Machine Learning (AI-ML)—can enhance detection and limit discretion abuse, the perseverance and skills to link and clean data will be key.

Cloud-based platforms

Cloud-based platforms and services provide for on-tap computing,[20] better data management capabilities, and storage capacities. They are not an improvement over traditional hardware deployments that typically entail large fixed costs, but provide a potential mechanism for addressing data fragmentation and silos. Cloud architectures lend themselves to the establishment of Application Programming Interfaces (APIs) that provide real-time integration of data and front-end services. Estonia's X-road is a globally recognized open source data exchange platform that shows in real time if respective agencies are sharing relevant data services. For reformers seeking to break down data silos, for example to cross-reference eProcurement and firm level data, this type of readily available technology can be quite powerful. Rather than requiring prolonged system set-up cycles, the technology allows reformist policy makers to tackle data sharing, along with analytics, in a faster and more agile manner.

Artificial Intelligence (AI) and Machine Learning (ML)

While AI, with adequate digital data foundations, is being increasingly used in a number of areas, its ability to serve as a powerful tool for detecting corruption risks in the public sector rests on a few key factors. First, it should be technically sound and be able to match the right algorithms with requisite data. Second, it should allow flags or triggers to be used manually for further action. And finally, it should be able to decipher, understand and use the information to improve and plug leakages. Successfully bringing these elements together in a public sector setting demands specialized skills, and strong leadership to ensure the linking and rationalizing of the different data systems (e.g., as part of AI-ML applications). The legal and institutional environment for the application of AI tools remains critical in terms of actual impacts for fraud and corruption, particularly to sanction the perpetrators.

Both AI and machine learning have a key role to play in helping to detect fraud and corruption. AI tells the computer what to look for, while machine learning allows the computer to draw out patterns not directly seen by humans. Both approaches should be thought of as decision support for humans, rather than fully automating detection or discretion. There are examples of the use of both with varying degrees of success. For example, when Ukraine's State Audit Service developed 35 risk indicators to help evaluate tenders for closer inspection, fraudulent bidders adapted their behavior to avoid these fixed criteria.[21] The Dozorro system by Transparency International demonstrated that machine learning was a more effective way to flag changing behaviors. Many tax authorities are using digital technologies to make the process of paying taxes easier, while building AI tools for helping detect evasion. The degree to which this combination exists across the functional areas is likely to differ significantly for any given context. A few successful examples are listed below:

Use of AI in detecting corruption in the public sector:

- Mexico's tax authorities identified 1,200 fraudulent companies and 3,500 fraudulent transactions within 3 months of a pilot AI scheme.[22]
- India's Union Finance Ministry Project Insight monitors data from various sources, including social media to detect spending patterns and compares the same data with tax records.
- Brazil's Office of the Comptroller General has developed a system that can rate the probability of any official being corrupt, based on entering a social security number.
- Singapore's AI for fraud detection in the SkillsFuture Program uses unsupervised learning to flag suspicious transactions (Box 2).

Biometrics

Biometrics has enabled identity validation, better targeting and access to services, and, in many countries, improved attendance of public servants. Biometric technologies have to-date focused on such anchors as digital fingerprints, facial recognition, and iris scans.[23] In the public sector, confirming, or more generally cross-linking, identity can help identify ghost workers, target beneficiaries and track transfer payments. While biometric technologies are not new, their cost and versatility has improved significantly. India's Aadhar[24] biometric identity program, launched in 2010, provided unique digital identity to more than 1.2 billion Indians.[25,26] Once a near universal platform of digital IDs is in place, the relative "start-up" costs of verification decrease. In settings where unique digital ID platforms are not yet in place, biometric registration will still need to be conducted on a stand-alone basis. In Sierra Leone, payroll verification and reconciliation exercises using biometrics led to substantial integrity gains through the weeding out of staff wastages. There was a decline in the average civil service payroll bill for 4 years in a row from 2014 to 2017 leading to savings of USD4 million, a significant sum in a small country such as Sierra Leone. The reduced complexity and costs of biometric solutions now also allow biometrics to be deployed in high-risk, FCV settings, such as fraud and corruption associated with refugee aid programs.[27] An impact evaluation by Dhaliwal and Hanna[28] suggests that biometrics helped increase health worker attendance by 15 percent.

The benefits of more stringent biometric verification criteria must be offset against the risk of errors in excluding genuine beneficiaries from government programs. India's Aadhar program, launched in 2010, covers over 90 percent of the Indian population (available to 'residents'), through a 12-digit ID number linked to specific biometric data, such as iris scans and fingerprints.[29] The scale of India's program makes it unique by global standards, and also a key platform in India's overall emerging digital stack.[30] Its per unit cost of USD1.16 per person also makes it probably the most cost effective on a unit basis globally.[31,32] The program has helped generate huge savings through cleaning up fraud in government social benefits programs. However, Aadhar has also had to address challenges of fraud by its national network of agencies certified to enroll persons into the program.[33] A continuing concern has been that the technology can also generate errors of exclusion. An impact randomized control trial evaluation by Muralidharan et. al.[34] for a subsidized food program in the state of Jharkhand highlights that "attempts to reduce corruption in welfare programs can also generate non-trivial costs in terms of exclusion and inconvenience to genuine beneficiaries."

Financial Technology

Financial Technology (FinTech) innovations have increased the scope and scale for digital payments and are transforming interactions between governments and citizens. Mobile money and payment systems[35] provide convenient means for financial transactions, including for those not served by retail banking systems. The growing prominence of on-line transactions in the private and public sector has increased the need for Know Your Customer (KYC), especially if money or sensitive information changes hands (e.g., transfer payments, access to health records). The standards for KYC usually depend on the type of service and the national context of digital IDs. Effective KYC can significantly reduce the transaction costs (including the reduced need for face-to-face processes) to provide public services, such as transfer payments (e.g., social security, conditional cash transfers, medical reimbursements), while better managing the risks of fraud and corruption through automated processes and AI-ML decision support algorithm applications. Given that most countries lack a universal and unique ID, solutions will need to involve some type of modular approach with respect to program and service design. The financial sector has led developments in predictive analytics, including for credit scoring and assessing potentially fraudulent charges. These techniques are being increasingly used to assess, for example, medical payment claims, as these are a significant part of public sector expenditures in advanced as well as emerging countries.[36]

Blockchains

Blockchains have attracted significant attention as a technological revolution, but the technology is still evolving. Blockchains are in effect a database shared across a public or private computing network.[37,38] Unlike a centralized database, blockchains are in principle less prone to being tampered with by the principal who controls the database. Blockchains rely on decentralized consensus across a number of parties who share the same data. The blockchain can represent stores of value (e.g., BitCoin), indirect representation of value (e.g., land records), or any other form of asset/ownership list. In the public sector, the blockchain can fulfill a number of functions where trust, independence, or conflict of interest may render standard data systems unreliable. This could include elections, records management (including certificates and land titles) and procurement.[39] For example, Andhra Pradesh in India (see case study) is using blockchain systems to maintain land records and streamline vehicle registrations as a solution to rampant corruption and a surge of property disputes.[40] However, blockchains are subject to their own risks, as can be seen from a number of bitcoin thefts, since stakes to a block content can be anonymous, which makes prosecuting illicit behavior challenging.[41] The field of blockchain is a rapidly developing field, with a plethora of different institutional design and technical solutions currently being deployed.

Blockchain technology can support efforts to improve trust in digital government in settings where trust is low. Records are preserved as immutable unless there is a consensus that they can be changed. This can no longer be done by the collusion of corrupt officials as it would need to invoke a wider consensus as there is no single owner. This can have significant impact in areas such as voting, land registries, certificates (marriage, education, or other official attestations, construction permits, civil service rolls, payments, zoning designations, etc.). For example, in Georgia in 2018, 1.5 million land titles were published on a blockchain, with streamlined registration processes and strengthened provision of on-line services.[42] Blockchain technology is still evolving, and the decentralized database structures, especially data, such as images and maps (including historical documents such as scanned deeds and maps), may face challenges in managing large amounts of data.

BitCoins

The rise of BitCoins and other cryptocurrencies, initially seen as anonymous ownership of assets, may lead to the strengthening of centralized monitoring for cashless societies over time. The ability of cryptocurrencies to move rapidly across borders, which limits both transparency and accountability regarding ownership of gains, has raised significant concerns that they may be a store of illicit wealth.[43] Its blockchain exchanges could also be used in combination with the traditional financial system to facilitate cross-border money laundering.[44] Countries such as China have clamped down significantly on first generation cryptocurrencies, but are developing their own state-sanctioned digital currencies. This move out of cash and traditional banking systems may in future make traceability easier for authorities, with significant implications for taxation or stolen asset tracking and recovery. For example, China plans to create a national blockchain cryptocurrency that could make traceability easier for the central government and provide greater oversight and scrutiny of transaction records associated with local tax authorities and other government payments. This suggests that blockchain as a technology can be deployed in quite a number of ways, with very different impacts on detection and discretion. Perhaps more than for any of the other technologies reviewed here, both the technology specifics of the application and the institutional context will shape potential outcomes.[45]

Internet of things and other sensor technology

The internet of things (IoT) and other sensor technology are increasingly allowing for richer and more dynamic tracking and feedback. Two main types of sensor technology that generate data are image producing technology (e.g., satellites, CCTV) and local tracking technology (e.g., GPS trackers for vehicles or radio frequency identification (RFID) trackers). These technologies have been available for decades, though with rapid and significant improvements in functionality (higher capabilities coupled with lower cost and complexity of deployment). Combining these technologies with on-line networking (IoT technologies) has enabled opportunities for scaling up the impact in areas such as public asset/infrastructure management and provision of public services (e.g., smart meters for water and electricity). An anecdotal example is tracking down Greek taxpayers who had not declared their pools.[46] Both in the private and increasingly also the public sector, the technology for asset tracking can be used for controlling the illicit use of government assets (e.g., official vehicles) or improving asset inventories (including through the use of embedded RFID asset tracking or QR Code identification).

While different technologies have merit in their own right, the full impact lies in breaking technology silos and implementing interlinked approaches across sectors and services. The intersection of public sector applications (7.1) and more rapidly developing technology applications can work positively, but also adversely, to disrupt the ability of the authorities to detect fraud or circumscribe human discretion so as to reduce the risk of its occurrence. Digital decision support automation,[47] as part of fiduciary oversight, can potentially enable officials to focus on more high-risk activities in unravelling corrupt practices. However, for these applications to have traction they will need to have both ex ante and ex post links to business processes. When viewed through a silo lens, the application and evaluation of digital government transformation technologies will face two major challenges. First, technology silos will need to be broken as silo technology solutions will typically be associated with higher costs, incompatible technologies, and fragmented learning.[48] Second, the biggest impacts from digital technology in government will come from network and critical-mass effects associated with deepening digitization, and increasingly interlinked approaches to detection and business process discretion.

Conclusions and risks

Given the expanse and diverse nature of public sector services, the most productive strategies build on a mix of wider government digitization contexts and intersecting technology developments, rather than focusing excessively on a single technology. Growing digitization in the public sector and societies is a reality and can be used to improve efficiency in delivering public services and plugging leakages. Table 7.3 lists options for navigating through GovTech in the public sector for speedy and more efficient delivery of services with an ultimate aim of addressing leakages and corruption in the system.

In light of rapidly developing technologies, there is a risk that governments over-invest and rely too much on the latest technologies to address deep-seated governance issues in the public sector. As Eaves[49] admonishes, governments should focus on being fast followers, rather than engage in expensive, excessively risky, and ultimately ill-fated explorations of untested technologies. Addressing principal-agent and time-horizon challenges particular to bureaucratic reforms in developing countries, the question is: Where does the line between fast follower and ill-advised technology projects get drawn, especially if reformers are looking to hurdle or "leap-frog"? The key to this dilemma may be to empower reformers with a higher degree of digital technology literacy, as well as to build Technology Innovation Partnerships. These partnerships should be committed to helping national and sub-national governments strike the right balance between more conventional and emerging technology applications. For digitization to be effective, a number of complementary efforts will be required, a few of which are listed below.

Building digital literacy for government leaders: It is important for decision-makers to continuously update their understanding of the type and use of digital technology to guard against the possible pitfalls. Such pitfalls include heavy investment in any one technology, which may be outdated, and vendors selling specific solutions.

Increasingly adopting and operationalizing a digital government platforms lens: The opportunities and risks for technology in the public sector must be set against the broader context of digitization within and outside the country. Rather than see these investments as stand-alone cases, they should be treated as a portfolio and platform building set of efforts. Some initial investments will result in higher returns only after more cross-cutting technologies are yielding dividends.

TABLE 7.3 Navigating GovTech for Public Sector Fraud and Corruption

Prioritization and Sequencing	Dimensions/Questions
Functional or Foundation Prioritizations	Deliver use-case centric applications (AI, big data, data integration), versus emphasizing foundational platforms (Digitization, ID, connectivity)
Conventional or Disruptive Technologies	Improve legacy systems (e.g., traditional database design) or seize new models (cloud, blockchain)
Detection or Discretion Focus	Stress decision support tools for detection, versus changing business processes to reduce discretion with high-risk fraud and corruption abuse
Public or Private Data Foundations	Leverage traditional administrative data (e.g., civil service registries, procurement, targeted statistical data collection) or draw on private sector/interest data (big data, satellites)
Digital and Analogue Complements	Emphasize digital solutions (e.g., detection) or analogue complements (e.g., willingness to prosecute)
Performance "versus" fraud-corruption metrics	Stress performance outcomes (tax, services), while framing fraud and corruption as barriers to achieving these objectives.

Investing adequately for broader digital disruptions: Most digital disruptions stem from improving public services rather than eradicating fraud and corruption. The most successful activities will therefore depend on a wider set of functional and foundational efforts and resourcing. Strong cost-benefit appraisals will help strengthen the design and implementation of these efforts. While benefits may be framed in terms of losses averted (e.g., so many dollars in ghost worker salaries saved), wider metrics are likely to be particularly material (e.g., health services improved, revenues raised equitably).

Addressing privacy concerns: The literature on the use of AI in the US justice system illustrates this concern.[50] If algorithms are used to flag firms or individuals for fraud and corruption risks, care must be taken to filter for any adverse bias.[51] For example, firms that have come out of the "digital shadows" by registering on eProcurement systems may be more exposed. These transitions therefore need to be managed, including by strengthening the incentives for firms or individuals to participate in the digital ecosystem. Conversely, safeguards need to be put in place to ensure that digital data is not abused to illicitly target particular firms or individuals.

Adopting a prudent approach to digital technology investments both for public service delivery improvements and addressing corruption: It is well-recognized that ICT is no silver bullet to address poor public sector governance. Implementing technological solutions in the context of government bureaucracies rife with inertia and vested interests can be challenging. The roll-out of the latest ICT systems, including those supported by development partners, may be seen as potentially solving the problem, but this is not necessarily the case. Given the traditional investment project lifecycle of 3-4 years, sustainability could be at risk under the next political cycle or administration unless the reform context or commitment is truly enabling. What is essential is that for any country to adopt new technology or 'leapfrog', the corresponding analog complements must be in place. While the current wave of disruptive technologies brings a variety of new tools to address old problems, one needs to guard against catching up with the latest technology. In some cases, they may indeed be game-changing, but care must be taken that the next must-have technology does not become an excuse to address persistent challenges, such as poor service delivery and fraud and corruption. These issues should not wait for new technology before they are addressed.

ANNEX 1 Selected Tech Glossary

Digital Transformation	Broadly refers to instances where the ways of working of an organization (including government) are fundamentally changed due to the application of new workflows and data use.
Disruptive Technologies	Typically used to refer to innovations that have upstaged market incumbents (e.g., Uber and the taxi industry) by offering more convenient and scalable solutions. In terms of governments, key aspects would include reduced complexity and costs for a user, along with requisite capabilities to address a particular need or wholly new process.
GovTech	The World Bank's GovTech initiative is focused on three core aspects, as follows: (i) designing human-centered services that are simple, transparent, and universally accessible; (ii) engaging citizens to increase participation, foster transparency and accountability and build trust; and (iii) transforming core government operations to bring the public sector into the 21st century.[52]
Cloud Services	On-demand availability of computer system resources, especially data storage and computing power, which does not require direct active management by the user or fixed hardware outlays.
Blockchains	A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network.[53]
API	Application Programming Interface is a communications protocol, allowing for example targeted and dynamic data exchanges across government.