



PART 3

Read the text below and answer questions 27–40.

THE PROMISE AND PERIL OF SMART CITIES

A

The term “smart city” is frequently presented as a neutral description of urban modernisation, yet it is less a single model than a contested agenda. In practice, “smartness” encompasses sensors, connectivity, analytics, and automated decision tools that aim to optimise how cities deliver services—from transport scheduling to waste collection and energy management. Proponents frame these systems as a rational response to urban complexity: data can reveal inefficiencies and enable faster, cheaper, and more responsive administration. However, critical urban scholars note that outcomes depend not on hardware alone but on technocratic governance choices: who defines success, which problems are prioritised, and how accountability is enforced. A smart city, therefore, is best understood as a socio-technical arrangement in which technology amplifies institutional capacity when governance is robust, but can deepen existing inequalities or concentrate power when oversight is weak.

B

Many smart-city programmes begin with comparatively uncontroversial applications such as infrastructure monitoring. Roads, bridges, streetlights, and water pipes are expensive to inspect manually, and failures can be disruptive and dangerous. Embedded sensors and networked meters can detect anomalies—pressure drops, unusual vibration, temperature spikes—earlier than routine inspections, allowing predictive maintenance that reduces downtime and repair costs. The attraction is practical: when faults are identified before they become visible crises, services appear more reliable and municipal budgets can be allocated more efficiently. Yet even this “engineering-first” approach raises questions about interoperability and dependence. If monitoring systems are purchased as proprietary packages, cities may find it difficult to integrate new devices later or to compare performance across vendors, creating technical path dependence that shapes long-term procurement.

C

The climate case for smart cities is often anchored in energy optimisation. Smart grids and building-management systems can match supply and demand more precisely, shifting loads away from peak times and identifying inefficiencies that justify retrofits. Sensors and analytics can, for example, adjust heating, cooling, and lighting based on occupancy patterns, while district-level dashboards can highlight where losses are greatest.



Nevertheless, the emissions impact is not automatic and depends partly on how energy is generated. If electricity is produced largely from high-carbon sources, efficiency gains may translate into smaller climate benefits than promised. Moreover, the passage introduces a further complication: efficiency can sometimes stimulate additional consumption, a phenomenon often associated with rebound effects or the Jevons paradox. When energy services become cheaper or more convenient, total use may rise, weakening or even cancelling expected emissions reductions. Thus, smart energy systems can help, but only within a broader policy context that constrains carbon intensity and avoids treating efficiency as a guarantee of decarbonisation.

D

Cybersecurity, by contrast, is a less visible dimension of “smartness” and therefore politically easier to neglect, even though the risks are systemic. As transport signals, utilities, and public-safety communications become connected, the attack surface expands: a compromised network can disrupt mobility, water provision, or emergency response. For this reason, cyber-resilience requires continuous patching, staff expertise, incident planning, and independent auditing—costs that rarely produce ribbon-cutting ceremonies. Some officials may prefer to invest in visible hardware, but the passage argues that this preference is short-sighted: neglect can be expensive when failures occur and trust is damaged. In other words, cybersecurity is not a minor concern compared with the benefits of smart-city infrastructure; it is a foundational requirement for reliability in digitally mediated cities.

E

Transport initiatives illustrate both the convenience and the governance dilemmas of smart-city systems. Adaptive traffic signals and real-time passenger information can reduce uncertainty and improve network efficiency. Integrated ticketing and “mobility-as-a-service” apps are often promoted as a way to combine buses, trains, and shared bicycles into a single user experience. However, these platforms can shift control toward private operators if contracts are poorly designed, particularly when companies manage payment systems, user data, or service integration. The passage notes this risk without claiming that integrated ticketing consistently increases public-transport ridership across cities: it discusses convenience and coordination rather than providing outcome statistics. The core issue is therefore political economy as much as technology—who sets standards, who profits from data, and whether a city retains the capacity to change providers without losing functionality.

F

Smart-city debates become sharper when public safety and surveillance are involved.



Cameras, acoustic sensors, and predictive analytics are often justified as tools that help authorities identify incidents more quickly, coordinate emergency responses, and allocate resources. Yet critics argue that such systems can normalise continuous monitoring and extend surveillance capitalism into public space, especially when data is shared with or processed by commercial partners. Algorithmic bias is a further concern: if datasets reflect existing inequalities in policing or reporting, automated systems may target some groups more than others, reinforcing spatial and social discrimination. The passage recognises that surveillance tools may be used for crime monitoring, but it does not claim that they have reduced crime rates in cities where they have been introduced. Instead, it emphasises the governance dilemma: how to balance legitimate safety aims with civil liberties, transparency, and proportionality.

G

These dilemmas converge in the question of data governance. Smart-city programmes commonly involve partnerships between municipalities and technology vendors, raising disputes about data ownership, access, retention, and accountability. If private firms control data formats and analytical tools, cities may become locked into long contracts, losing bargaining power and limiting democratic control over essential systems. Advocates of open standards argue that interoperability and public oversight require clear procurement rules, independent audits, and enforceable constraints on data use. However, the passage stops short of endorsing a single normative solution such as legal resident ownership of all data. Instead, it presents ownership as contested terrain: governments, firms, and communities debate what constitutes legitimate collection, anonymisation, and sharing, and how public value can be protected when data becomes a strategic asset.

H

Equity concerns further complicate the promise of “smart” efficiency. Many digital services assume that residents have reliable internet access, smartphones, and the confidence to navigate online systems. Where the digital divide is substantial, an “online-first” approach can create new barriers to services that were previously accessible through face-to-face contact. Smart investments may also be spatially uneven: pilot projects often concentrate in high-visibility districts—business centres, tourist corridors, affluent neighbourhoods—because they offer political symbolism and easier implementation. This can widen inequality by improving services where they are already relatively strong while leaving neglected areas with ageing infrastructure and fewer opportunities. The passage therefore frames smart-city equity as a distribution question: who benefits, who is excluded, and whether data-driven governance is used to reduce cumulative disadvantage or to cosmetically upgrade already privileged zones.



I

The most persuasive conclusion is that smart cities succeed when technology is treated as a tool within a broader institutional framework rather than as a substitute for it. Data must be interpreted responsibly, agencies must coordinate across silos, and policies must evolve to match new capabilities. Without long-term funding, maintenance plans, and skilled staff, pilot projects degrade into obsolete dashboards and malfunctioning devices. Conversely, where democratic oversight is credible—through transparent procurement, clear rules on surveillance, cyber-resilience planning, and equity targets—digital systems can enhance public value rather than merely expanding technocratic control. The passage therefore emphasises that smartness is not an end state but a governance challenge: the promise of efficiency can be realised only when institutional capacity, accountability, and social legitimacy keep pace with technological ambition.

Questions 27–31

Choose **YES** if the statement agrees with the claims of the writer, choose **NO** if the statement contradicts the claims of the writer, or choose **NOT GIVEN** if it is impossible to say what the writer thinks about this.

27 The writer suggests that energy-efficiency measures in smart cities may fail to cut emissions if they lead to higher overall consumption.

28 The writer regards investment in cybersecurity as less essential than spending on more visible smart-city technology.

29 The writer claims that integrated ticketing systems increase total public-transport ridership in most cities that adopt them.

30 The writer suggests that smart-city surveillance systems have reduced crime rates in the cities where they have been introduced.

31 The writer argues that residents should legally own all data collected by smart-city sensors and platforms.

Questions 32–35

Complete the information below. Choose **NO MORE THAN TWO WORDS** from the text for each answer.

Uses and challenges of smart-city technology

Infrastructure faults can be detected earlier using networked meters together with embedded **32**, while the climate impact of smart energy systems depends partly on how energy is **33** However, governance choices matter: if vendors



control technical standards, cities may become **34** long contracts, and equity may worsen when online-first services assume reliable **35** access.

Questions 36–40

Select the correct answer.

36 What does the writer suggest about the label “smart city”?

- A** It describes a single standardised model used internationally.
- B** It covers many technologies, and outcomes depend on governance and design.
- C** It is mainly used to describe transport systems rather than other services.
- D** It guarantees more equal service provision across neighbourhoods.

37 What governance problem can arise from integrated urban transport platforms?

- A** They may force municipal agencies to operate all payment systems themselves.
- B** They can make coordination between different forms of transport more difficult.
- C** Private providers may gain influence when cities depend on systems and services they control.
- D** They prevent shared transport services from being included in a common platform.

38 What problem can result from biased data used in public-safety systems?

- A** Automated decisions may reproduce existing inequalities in which groups receive greater scrutiny.
- B** Emergency services may become unable to identify incidents quickly enough.
- C** Crime monitoring may become less accurate whenever commercial partners process data.
- D** Authorities may be forced to abandon automated systems entirely.

39 Why can some smart-city initiatives deepen existing inequality?

- A** Digital services are usually introduced first in neighbourhoods with poor internet access.
- B** Online systems reduce the ability of wealthier districts to attract public investment.
- C** Smart investment generally replaces infrastructure in disadvantaged areas before other districts.
- D** Some residents may lack the digital access assumed by services, while investment can favour already prominent areas.

40 According to the writer, what is required for digital systems to create lasting public value?



A Technology companies must take over responsibilities previously held by public agencies.

B Cities must minimise regulation so that new technology can develop more quickly.

C Institutions must be able to coordinate, maintain and govern technological systems with effective oversight.

D Municipalities must avoid working with private technology providers.

Answer Key

27. YES

28. NO

29. NOT GIVEN

30. NOT GIVEN

31. NOT GIVEN

32. sensors

33. generated

34. locked into

35. internet

36. B

37. C

38. A

39. D

40. C