The Economist INTELLIGENCE UNIT

The primacy of privacy

Safeguarding urban intelligence in an age of unease

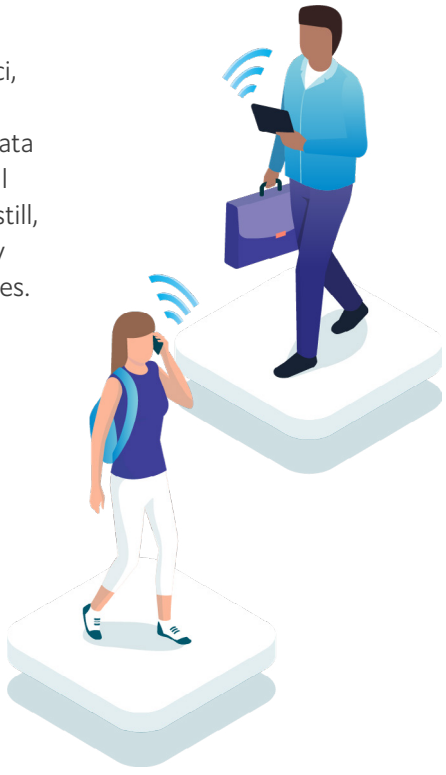
“Smart cities have the potential to become surveillance cities.

Lee Tien, Electronic Frontier Foundation

In October 2018, Ann Cavoukian, the director of privacy for Sidewalk Labs, a subsidiary of Alphabet that is managing a smart-city project in Toronto, resigned after concluding that the project’s data privacy protections were insufficient.[1] The episode underscores the concerns of many that the smart technologies now permeating cities—including Internet of Things (IoT) sensors and powerful machine learning tools that make predictions based on the data they generate—will inevitably compromise citizens’ privacy.

The biggest threat to privacy in cities, according to Joe Cannataci, UN special rapporteur on the right to privacy, is the fact that “people are walking the streets and riding in vehicles giving off data without knowing it.” Sensors embedded in all manner of physical infrastructure are just one source of data collection. More risky still, says Mr Cannataci, are ubiquitous mobile devices which invisibly transmit personal data to IoT sensors and then out to third parties. “Most people have little or no knowledge of this,” he says.

Lee Tien, senior staff attorney and Adams chair for internet rights at the Electronic Frontier Foundation, an advocacy group, similarly warns of the risks posed by fast-growing shared mobility schemes, in which scooter, bicycle or car companies, for example, collect and share user data. “Smart cities have the potential to become surveillance cities,” he says.



[1] In her resignation letter, Ms Cavoukian labelled the project as a “smart city of surveillance”; see Jennings Brown, “Privacy Expert Resigns From Alphabet-Backed Smart City Project Over Surveillance Concerns”, *Gizmodo*, October 23rd 2018.

In nine of the 19 cities, half or more of citizens (82% in Mumbai) are willing to share their personal data in order to obtain smart-city benefits.

An acceptable trade-off?

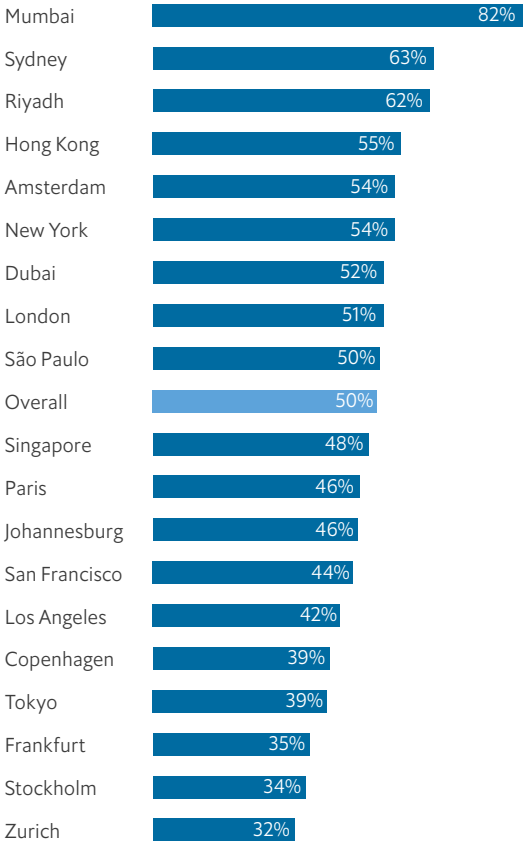
Against this backdrop, it may seem surprising that in a survey of 19 global cities conducted by The Economist Intelligence Unit and sponsored by Nutanix,[2] the majority of citizens appear relatively sanguine about the use of their data in smart cities. Most are ready to share their data if it will help secure improvements to their quality of life that they expect smart-city initiatives to deliver.

In nine of the 19 cities, half or more of citizens (82% in Mumbai) are willing to share their personal data in order to obtain smart-city benefits. But such readiness is not universal: only around one-third of Zurich and Stockholm residents feel as comfortable as their peers in other countries.

Comfort levels about data sharing rise everywhere when citizens are asked about specific smart-city gains. For example, just under three-quarters (74%) of respondents across all cities are happy to allow municipal governments to use their data in order to reduce road and public transport congestion. Almost as many (71%) say the same when the trade-off is lower energy costs (resulting, for example, from smarter energy tariffing). And 70% are ready for their data to be used to help reduce crime. There is some city variance in response rates on all three questions (residents of Copenhagen, Tokyo, Paris, Los Angeles and San Francisco are generally not as relaxed as their peers elsewhere), but majorities are registered in every country without exception.

Some doubts remain on the question of whether the benefits promised by smart cities outweigh any potential loss of personal privacy. Only a minority accept this premise in several of the aforementioned cities (Frankfurt least of all), but overall 54% of citizens agree.

Figure 1: Private citizens
Proportion of residents willing to share their personal data in exchange for the benefits resulting from smart-city initiatives



Source: The Economist Intelligence Unit

[2] In summer and autumn 2019, The Economist Intelligence Unit surveyed 6,746 citizens and 969 business executives resident in Amsterdam, Copenhagen, Dubai, Frankfurt, Hong Kong, Johannesburg, London, Los Angeles, Mumbai, New York, Paris, Riyadh, San Francisco, São Paulo, Singapore, Stockholm, Sydney, Tokyo and Zurich. The analysis in this article is based on the survey responses of citizens only. For more details on the survey demographics, see http://bit.ly/urbanintelligence

Mr Cannataci is not surprised by citizens' broad willingness to share data despite privacy concerns. "Citizens love the convenience that smart technologies bring, but until recently few have understood the amount of personal data many such technologies gather," he notes. "Thanks to the efforts of legislators and privacy advocates, many citizens are now waking up to it."

"Citizens love the convenience that smart technologies bring, but until recently few have understood the amount of personal data such technologies gather.

Joe Cannataci, UN special rapporteur on the right to privacy

Guardian or big brother?

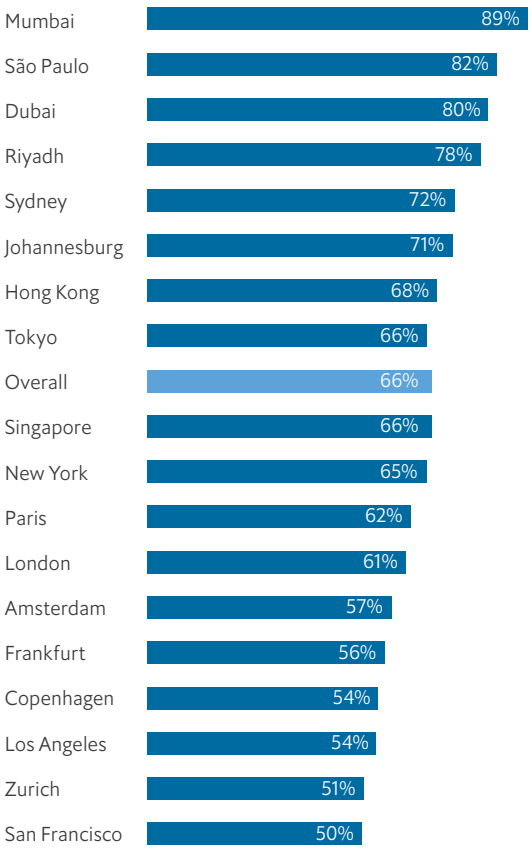
66% of citizens in our survey believe facial recognition technology will do more good than harm when used in fighting crime.

If recent media reports are anything to go by, there is considerable public disquiet in many cities today about one specific perceived risk to personal privacy: the use of facial recognition technology, which San Francisco banned in May 2019.[3] Police in London have also come under heavy criticism in recent months for making arrests while conducting tests of the technology.[4]

Despite these well-publicised developments, most citizens in our survey appear to be as calm about facial recognition technology as they are about sharing data. Two-thirds (66%) overall believe the technology will do more good than harm when used in fighting crime. Emerging-world cities such as Mumbai and São Paulo are more accepting than wealthier ones (with the exception of Sydney)—a finding consistent with the high priority their residents place on the need for smart-city initiatives to help reduce crime, as expressed elsewhere in the survey.

Mr Tien believes these figures would fall if people were fully aware of facial recognition's problems. "It should seriously concern people that this technology often fails," he says. "It's not ready for everyday use yet."

Figure 2: Peek-a-boo
Share of citizens agreeing that the use of facial recognition technology in urban crime prevention will do more good than harm



Source: The Economist Intelligence Unit

[3] Kate Conger, Richard Fausset and Serge F Kovaleski, "San Francisco Bans Facial Recognition Technology", *The New York Times*, May 14th 2019.
[4] Madhumita Murgia, "How London became a test case for using facial recognition in democracies", *Financial Times*, August 1st 2019.

Officials must ensure that their technology partners adhere to privacy at the outset, rather than as an afterthought.

Embedding "privacy by design"

Is the survey respondents' relative optimism about privacy in smart cities illusory? Mr Cannataci believes people's data will always be at risk but that some safeguards can be put in place, provided city authorities educate themselves sufficiently about existing risks and work with technology providers to minimise them. Part of his role as the UN's privacy rapporteur is to guide city officials in such efforts.

Smart technology can act to enhance privacy in cities, says Mr Cannataci. For this to be the case, two elements need to be in place. First, a privacy impact assessment should be conducted of any new technology initiative; this is mandatory, he points out, throughout the European Union (EU) and is used in several other countries. The second element is adherence to "privacy by design", another principle enshrined in EU law, which essentially stipulates that privacy protections should be "baked in" to new technology solutions in their initial design stages.

In the context of smart cities, this means that officials must ensure that their technology partners adhere to privacy at the outset, rather than as an afterthought. The learning curve officials must climb to enable this is steep, and they'll need to ascend it rapidly. But their efforts, says Mr Cannataci, will be well worth it for their fellow citizens.