Dear CEO and Mayor

I write to you today to express growing concern amongst technology experts, human rights advocates and the general public about the rapid expansion of surveillance technology in public spaces - often those directly managed by local government authorities.

The internet has become inseparable from our daily lives. Yet, every day, there are new cases of digital rights abuse, misuse and misinformation and concentration of power around the world: freedom of expression being censored; personal information, including our movements and communications, monitored, being shared and sold without consent; 'black box' algorithms being used to make unaccountable decisions; and democratic processes and public opinion being undermined.

Technology is developing far more rapidly than we could have predicted just a few decades ago - increases in computer power, access to more sophisticated surveillance systems, data-matching and linked databases and a rise in the use of AI and automated systems have seen many governments expanding their 'public safety' programs and turning to the concept of developing 'smart cities'.

Far from taking advantage of technological leaps to enhance and protect rights, these data-centric projects focus on the constant generation, collection and processing of data, often with a cost for our right to privacy. Indeed, as we place sensors and CCTV cameras all over our streets, buildings and public spaces, we are building a world in which we are constantly subject to surveillance. Here in Australia we are already starting to see these technologies roll out in several cities already, such as Perth, Brisbane and Darwin.

In 2015 the Australian Government announced a national facial recognition system -the National Facial Biometric Matching Capability or simply 'The Capability'- would be implemented. This occurred with absolutely no public consultation or public announcement at the time. This system uses existing identification documents, such as licences and passports, to extract and share biometric information between local, state, territory and national government databases. It is this rapid expansion of data-matching and access to huge troves of data, often without adequate oversight mechanisms, that concerns us. There is no empirical evidence that supports the assertion that blanket surveillance is effective at preventing serious crime and terrorism either domestically or internationally - in fact if anything, these approaches almost always erode rights and diminish freedoms.

The issue of security is often ignored or not prioritised in the design, implementation and maintenance of such smart initiatives. At a time when Australia's federal government is consistently failing to protect centralised, interconnected databases (My Health Record, National Census, Centrelink to list just a few), it is extremely worrying to watch as we are sleep-walking into a world where our cities are becoming vulnerable, and ultimately so are we as individuals, to all types of security threats including breaches, leaks and hacking as well.

info@digitalrightswatch.org.au
PO Box 1426 Fitzroy Nth VIC 3068
digitalrightswatch.org.au
ABN 90 509 129 914

We must ensure that the current models of smart cities are indeed smart for all who inhabit them, with equal weight given to every citizen. Current initiatives often fail to take into consideration issues of poverty, access to technology, access for the less-abled and more generally the issue of gender and how to insure cities are smart for all genders. By failing to do so, these supposedly smart cities are not only failing to address issues they promise to address such as discrimination, exclusion, poor service delivery and safety but they are actually heightening them.

However, there are positive interventions that local government representatives can do to protect residents against this rising trend. In 2018, the Cities for Digital Rights initiative was launched by the three major cities of Barcelona, Amsterdam and New York City with the support of the United Nations Human Settlements Program, with an aim to protect, promote and monitor residents' and visitors' digital rights. Many more local government authorities around the world have since adopted this declaration, including the City of Sydney, with others such as the City of San Francisco recently moving to ban all use of facial recognition software.

Often our local government authorities are the closest democratic institutions to the people, and are best placed to take on the duty of eliminating impediments to harnessing technological opportunities that improve the lives of our constituents, and to providing trustworthy and secure digital services and infrastructures that support communities. It is only through the incorporation of human rights principles such as privacy, freedom of expression, and democracy into digital platforms - starting with locally-controlled digital infrastructures and services - that we will have truly 'smart' cities that are designed for the people.

I invite you to consider adding your city to the growing list of those already signed up to the Cities for Digital Rights initiative, or to progress similar measures through your jurisdiction.

We would also be happy to provide further information or advice.

Thank you
Tim Singleton Norton
Chair - Digital Rights Watch

Further reading:

- Privacy International report 'Smart Cities: Utopian Vision, Dystopian Reality'
- Cities for Digital Rights Declaration
- San Francisco Chronicle - 'San Francisco bans city use of facial recognition surveillance technology'

info@digitalrightswatch.org.au
PO Box 1426 Fitzroy Nth VIC 3068
digitalrightswatch.org.au
ABN 90 509 129 914