This open-access article is distributed under Creative Commons licence CC-BY-NC 4.0.

Bridging the regulatory gaps created by smart and connected technologies in South Africa

B A Townsend,[1] LLM, MST, PhD; **M Botes,**[2] BProc, LLD

[1] *York Law School, University of York, UK; Honorary Research Fellow, University of KwaZulu-Natal, Durban, South Africa*

[2] *SnT Interdisciplinary Centre for Security, Reliability, and Trust, University of Luxembourg; Honorary Research Fellow, University of KwaZulu-Natal, Durban, South Africa*

Corresponding author: *B A Townsend (bev.townsend@york.ac.uk)*

The prevalence of technology-embedded products, services, and cities, described colloquially as 'smart' technologies and 'smart' cities, has seen a spate of unprecedented growth in recent years. South Africa (SA) has not been left behind, with smartphones, smart watches, and smart voice-controlled virtual personal assistants such as Amazon's Alexa now frequently used. But while these technologies hold great promise to revolutionise homes, offices and cities, their adoption poses challenges to individual and collective interests and wellbeing. After demonstrating the legal and ethical difficulties brought about by the introduction of these technologies, this article explores whether SA legislation is sufficiently robust to address these challenges. While the current legislative landscape addresses certain crucial difficulties – such as the safeguarding of personal data by the Protection of Personal Information Act No. 4 of 2013 ('POPIA') – it is suggested that the position regulating other aspects of smart technology adoption is, in large part, fragmented and ill-equipped to deal with some of the more pressing legal and ethical questions. Our contention is that, not dissimilar to the issues arising from artificial intelligence-based technological adoption, the extant legislative and regulatory frameworks do not go far enough in addressing the many concerns emerging from recent novel technological design, development, and deployment. Not only do smart technologies give rise to unique challenges, so does their deployment within the Global South and in South Africa, in particular. We suggest that appropriate and effective regulatory reform measures be undertaken in SA to provide better ethical guidance and policy prescriptions buttressed by rigorous regulatory oversight.

S Afr J Bioethics Law 2023;16(2):e201. https://doi.org/10.7196/SAJBL.2023.v16i2.201

Smart and connected technologies ('smart technologies') have shaped and revolutionised our world and will continue to do so: within our home, workplace, and urban environment. This is achieved by blending traditional goods and services with embodied intelligence, digital technologies, and personal data. However, any imagined transformative future brought about by smart technologies stands to fail where the challenges they present, to both individual and collective rights and interests, are not addressed.

Smart technologies are user products and services embedded with sensing and communication technology that typically connects to the internet and transmits and receives digital data. Applications vary greatly, and include smart homes (voice-controlled virtual assistants, such as Amazon's Alexa and Microsoft's Siri, smart meters, smart light bulbs, smart fridges and smart security cameras), connected cars, smart healthcare (such as patches to allow for the remote reading of health indicators in disease prevention and monitoring, assistance in clinical diagnosis and treatment and smart hospital management), and wearables (such as smart watches, activity monitors and smart glasses). Smart technologies often use sensors, monitors, processors and visual aids or cameras to gather vast quantities of data that are re-laid to a digital platform for use.[1] The aim of such technologies is to optimise service provision, provide proactive support, promote more sustainable behaviour and ultimately, to provide more efficient and effective products and services. Indeed, in many instances, smart technologies provide better products and services than traditional ones.

A related concept is that of a 'smart city'. A smart city is 'the effective integration of physical, digital and human systems in the built environment to deliver a sustainable, prosperous, and inclusive future for its citizens'.[2] The inhabitants of smart cities are referred to as 'smart citizens'.

The use of smart technologies has escalated rapidly in recent years in domains such as industry, business, healthcare, transportation, warfare, surveillance, and security. A Statista Global Consumer Survey conducted in SA in 2020[3] found that 16% of respondents owned a smart home device, with an estimated 12.2 billion smart devices connected worldwide in 2021. It is anticipated that by 2025, the number of connected smart devices will accelerate globally to approximately 27 billion.[3]

With ever-increasing escalation in accessibility, the development and deployment of smart technologies cannot be divorced from important debates involving law, socio-political philosophy and ethics. Accordingly, for SA to keep abreast of such developments and to protect its citizens, certain critical issues must be addressed. In this article, we will share six legal and ethical challenges to such adoption in SA. Thereafter, we will offer observations and recommendations in pragmatically establishing a path forward.

Legal and ethical concerns

Trustworthy smart technologies that are legal, ethical, and technically robust are well positioned to offer significant user advantage. This is well understood.[4] But, to provide any advantage, not only must the public be protected, including those marginalised and most vulnerable in society, but harmful and adverse outcomes must be prevented. While many ethical concerns exist, we consider only, in our estimation, the most pressing. We provide a cursory discussion of issues relating to inclusivity and social justice, personal autonomy, and data privacy, which includes surveillance, and voice, emotion and facial recognition systems. We also consider the manipulation of behaviour using practices such as nudging and dark patterns.

1. Inclusivity, equity and social justice

Smart technologies can improve the individual's quality of life by empowering them, enhancing wellbeing, offering proactive support, and promoting social connectivity and engagement. However, in greatly enhancing connectivity, they paradoxically can lead to increased isolation, especially to the elderly, the youth and the disabled. Research has demonstrated the need to overcome scepticism of smart technology use by members of the public and to ensure that its introduction accounts for individuals' different abilities and appetite for adoption.[5] In addressing the 'digital divide', or the inequities in the distribution of digital connectivity and equipment,[6] the accessibility divide for smart products and services must also be bridged to provide fair, equitable and inclusive products and services. These technologies should be implemented in a way that ensures that the vulnerable and marginalised in society, and often those most in need of such technologies, are not excluded from their use or the debates informing their application.

Fair adoption requires that datasets (used to train, test and validate algorithms upon which smart technologies often rely) are accurate, inclusive, complete and reflective of the wider population. As datasets typically include common-use cases, they may fail to account for under-represented members of society. Data bias and algorithmic injustice can be introduced into the system, which can, in turn, entrench and exacerbate inequality and injustice in society.[7] Although the Protection of Personal Information Act No. 4 of 2013 (POPIA)[8] obligates a party responsible for the collection and processing of data to ensure that personal data are complete, accurate, not misleading and up to date, it does not provide practical benchmark standards for data to adhere to for it to be considered of adequate quality, and leaves that up to the discretion of each responsible party. With regard to medical devices, for example, the Medicines and Related Substances Act No. 101 of 1965 (MRSA)[9] provides that medical devices (including embedded smart technologies) may only be registered for purposes of being commercialised upon 'meet[ing] defined standards of quality, safety, efficacy, and performance',[9] but the reference to quality in this context relates to the safe and efficacious performance of the device itself, and does not address the safety, accuracy or quality of the data that are collected.[10]

Transactions by means of which people acquire technologies that connect them to smart products and smart cities are governed by the Consumer Protection Act No. 68 of 2008 (CPA).[11] The CPA aims to promote a fair and accessible marketplace for these technologies for all by introducing national norms and standards to protect people against discrimination and exploitation.[11] The CPA not only prohibits the supplier of such technological goods from discriminating against a person on any of the grounds set out in the SA Constitution,[12] or in the Promotion of Equality and Prevention of Unfair Discrimination Act,[13] but mandates the supplier to treat consumers equally, by prohibiting the supplier from excluding, granting exclusive access to, assigning priority, supplying a different quality, charging different prices, or targeting particular communities.[14] In theory, equal access, uptake and use of smart technologies should result in wider inclusivity and equity. However, in practice, this is not always the case. Factors such as land governance, level of technology, geopolitical landscape, income levels, the dynamics of increasing rural-urban migration and their complexities may influence the speed and degree of technology uptake and affordability, regardless of legislation providing theoretical fairness and equality.[15]

2. Respecting autonomy

Respecting the autonomy of smart citizens and smart users suggests the users' ability to remain in control and manage the use of the technology, to inform and direct decision-making affecting them and to understand the role these technologies play in their lives. A hyper-connected smart city implicates individual autonomy by the introduction of technologies that may interfere with individuals' choices and control of their lives. An ancillary concern is the risk of over-reliance on technology, or its use as a 'digital crutch'. We need, therefore, to understand the potential for misuse or inappropriate use.

To provide smart citizens with some form of control over their ability to determine their future, they should be active participants in the unfolding of their lives, instead of being used merely for the acquisition of their personal data.[16,17] The functionality of smart cities depends largely on thousands of autonomous and cyber-physical systems that operate in concert to effectively manage densely populated areas. These networks of connected devices ought to be designed to minimise information overload, synchronise the information presented to smart citizens and enhance users' personal autonomy. In addition to individual autonomy, because of the number of developers, manufacturers and operators involved, and the scale upon which such systems operate, it is vital to maintain safe and reliable controls that ensure safe operation of individual systems and safe system interactions with one another.[18]

3. Safeguarding data protection

Smart technologies collect, process, and share personal data with third parties on an unprecedented scale. These vast quantities of personal data – generated by, *inter alia*, the surveillance of persons through the use of video, sensors and monitors, threatens informational privacy. Compliance with data protection laws is therefore paramount. While POPIA provides privacy protection, two provisions within POPIA are worth examining. The first is the so-called 'household activity' exclusion and the second involves automated decision-making.

Data generated in the course of a 'purely personal or household activity' would fall outside of the scope of protection of POPIA as an exclusion afforded by section 6.[19] This exclusion raises difficulties with regard to smart technologies. The brevity of the exclusion presumably intends to exclude those activities conducted by individuals of a personal nature or those activities that generate personal information within household settings. A smart device such as Alexa or Siri (which collects personal information from the recording of a user's voice) or a smart toothbrush (which tallies the number of times it is used per day) operates in the household, generating and collecting personal data. Arguably, at some point the data are transmitted beyond the household and are no longer used strictly or 'purely' for personal or household-related reasons but are shared to other platforms for other commercial or professional (non-household) purposes. Our contention is therefore that manufacturers and deployers of smart devices who determine the purpose and means of processing personal data and are therefore either solely or jointly 'responsible parties' for the purposes of POPIA should not be permitted to invoke the household exclusion even where such collection was part of an application that is personal in nature and used within the home.

The second POPIA provision under discussion is section 71, which relates to activities involving automated decision-making and profiling. While sections 18, 23, 24 and 25 provide for notice, correction and access rights, section 71(1) stipulates explicitly that '… a data subject may not be subject to a decision which results in legal consequences for him … which affects him … to a substantial degree, which is based solely on the basis of the automated processing of personal information intended to provide a profile of such a person including his or her performance at work, or his … credit worthiness, reliability, location, health, personal preferences or conduct' [our emphasis].[20] The words 'based solely' indicate that decisions that are partly human-based and partly automated will not be considered an automated decision for purposes of this section.

Automated decision-making is otherwise permitted only if it is not in the following instances: (*i*) where the decision results in a legal consequence for the data subject, or the decision affects the person to a substantial degree; (*ii*) where the decision is based solely on the basis of the automated processing of personal information; and (*iii*) where the automated processing is intended to provide a profile of the person.

Moreover, section 71(2)(a)(ii) allows such an automated decision to be taken *inter alia* in connection with the conclusion or execution of a contract where 'appropriate measures' have been taken to protect the data subject's legitimate interests, and where in terms of section 71(3)(a) and (b) these measures allow the data subject the opportunity to make representations about a decision, and require a responsible party to provide the data subject with 'sufficient' information about the 'underlying logic' of the automated processing of their information so they can make such a representation.

However, POPIA, while securing information about the underlying logic and computational process involved in the decision-making process, falls short of introducing any explicit 'right to an explanation'. Neither does POPIA mandate that the data subject be informed of the significance or any envisaged consequences to the data subject that may be brought about by the automated decision-making process.[21]

A further concern with data collection and smart technologies is that in voluntarily disclosing personal information about themselves, a person can unwittingly expose the personal information of others: persons who have had no say in the matter and disclosure that can have direct consequences to them.[22] This is illustrated in the Cambridge Analytica controversy, where participants in an online quiz permitting access to their data also allowed access to the data of their friends.[23] Likewise, the disclosure of information by a family member might have significant familial implications on other family members.

An interesting development with regard to inferential data is noted in the CJEU case of OT v Vyriausioji tarnybinės etikos komisija, where the court elected to interpret the European Union General Data Protection Regulation very broadly, by expanding the scope of article 9 and the processing of special category data to include information that may be deduced or inferred from other special categories or 'sensitive' data.[24,25] Information might be inferred, for example, about one's religious beliefs or sexuality based on one's surname, medical data and location data. While POPIA and SA case law make no current allowances for inferential data, information inferred from personal and special category data collected and processed has significant implications not only for those using smart technologies but also to many other artificial intelligence (AI)-related data-driven applications.

A recent development is the use of data in foundation and generative models, such as ChatGPT, that use vast quantities of data to pre-train systems by using and linking data at a global level, with direct impact on SA citizens.[26] Of immediate significance is the responsible use of these models and of the lack of transparency underlying the training datasets upon which the Large Language Models (or LLMs) for ChatGPT and its predecessors are trained: datasets that are often not publicly available.[26] The challenge is that models of this sort do not respect geographical borders, and the data used to train the models may be inaccurate, under-representative of certain demographics, biased or not ethically sourced.[27,28]

4. Behavioural manipulation

Smart technologies can introduce manipulative behavioural practices, such as 'nudging' and 'dark patterns', for example. Nudging is a type of behavioural modification used to precisely and effectively target and influence behaviour.[29] While nudging may be used to inform choices, for example, to eat better or exercise more, nudging can also violate individual autonomy and privacy. Nudging is often covert, conducted without the knowledge or consent of the user, and can be a manipulative and coercive interference in human decision-making.[30] An illustration of everyday nudging is the presentation or 'push' of online advertisements based on user internet browsing behaviour. This is particularly problematic if the advertisement algorithms take into account online behaviour that indicates vulnerability, such as searching for terms that suggest a user is disabled, suffers from mental health issues or is dealing with addiction. The added danger is that those being manipulated are often unaware of the 'nudge' or its consequences.[16]

Moreover, the use of 'dark patterns' in interface design poses additional unethical, manipulative, or unreasonably persuasive practices.[31] Dark patterns, also known as 'anti-patterns' or 'deceptive designs', are designed and implemented with the aim of coercing, steering and deceiving users into making decisions without fully considering all the available options or consequences, such as purchasing overpriced products or committing to recurring monthly expenses.[32]

If a person is nudged or manipulated into concluding an electronic transaction only to determine later on that the transaction was not what the person wanted or expected, both the Electronic Communications and Transactions Act No. 25 of 2002 (ECTA)[33] and the CPA[34] provide for 'cooling-off periods' during which a person may cancel a transaction without reason or penalty, including from direct marketing. Interestingly, this consumer safeguard is excluded in the ECTA for some of the most frequently concluded electronic transactions such as 'insurance and reinsurance operations … banking services … supply of foodstuffs, beverages or other goods intended for everyday consumption supplied to the home, residence or workplace of the consumer … the sale of newspapers, periodicals, magazines and books … [and] for the provision of accommodation, transport, catering or leisure services'.[35] Fortunately, the CPA seems to fill the 'cooling-off' period gap left by the ECTA's exclusions,[36] and although the CPA does not specifically provide for direct marketing via electronic means, any method, including mobile device applications, search engine optimisation, pay-pre-click advertising and social media marketing are accepted methods for delivering electronic communication for the purpose of online marketing to customers.[37] But, however valiant these consumer safeguards might be, these measures are only available after the transaction and the behavioural manipulation has taken place, rather than serving to prevent manipulative techniques and technologies from occurring in the first place.

5. Use of facial, voice, and emotional recognition systems

Facial, voice and emotional recognition technologies, including cameras and monitors used for tracking and surveillance purposes, pose challenges to users' privacy, free expression and information security, and to social justice. Due to a lack of specific legislation governing the use of such technologies, the circumstance and conditions under which they might be used should be clarified and regulated. A single set of clear guidelines and standards should be developed, so that those who develop and deploy biometric and surveillance voice and camera systems can be held responsible for their use in a way that is transparent and auditable.

Facial recognition is commonly used in daily activities such as arrival and departure gates at airports, confirming the identity of students attending exams, identifying people banned from entering certain sport stadiums, nightclubs or casinos, and unlocking smart phones.[38] Anticipated applications of facial recognition technologies are premised on the provision of real-time specific and generically described individuals through the smart city's surveillance network.[39] In SA, the implementation of such real-time technologies will be problematic on the basis that the provision of any real-time information to any person, other than the customer of the telecommunication service provider concerned, is prohibited.[40] The only exceptions to the general prohibition on intentionally intercepting or even attempting to intercept[41] indirect communication, which includes visual images,[42] such as the faces of smart city citizens obtained from facial recognition technologies, *in the course of its transmission*, as opposed to real-time transmission, entail interception based on consent of citizens, and law enforcement.[43] Still, to safeguard the privacy and dignity of citizens, and prevent random interceptions for dubious reasons, the exception of law enforcement is only available upon adherence to a number of strict requirements, which involve an interception direction[44] obtained by an authorised person[45] from a designated judge, after having applied for one in writing[46] to prevent a serious offence from being committed[47] or prevent serious bodily harm.[48]

It should be borne in mind, however, that companies have this real-time data and can use it in an aggregated manner to 'track' consumer habits – without disclosing the personal information of the users. This aggregated use of so-called anonymous data is equally powerful and impactful on consumers.[26]

Similar technologies involving voice and emotional recognition capabilities are being experimented with. For instance, a digital system called Vibraimage claims to quantify a person's mental and emotional state by analysing video footage of them, and has already been deployed at the 2014 Sochi Olympic Games,[49] 2018, PyeongChang Winter Olympic Games, 2018 FIFA World Cup in Russia and at major airports in Russia to detect suspect individuals in the crowd.[50] While there is currently no reliable evidence that these technologies are effective (to the contrary, many of the claims made based on these technologies simply seem unprovable), their introduction poses significant challenges to human rights and interests.[51]

6. Smart cities and surveillance

As citizens move around a smart city, sensors are triggered, and their smart devices interact with the smart city infrastructure and network. These collect, store and share data about people's location, habits, and activities. Regardless of the fact that such interaction may streamline service delivery and improve the quality of citizens' lives, significant concerns regarding privacy and security in the context of near constant surveillance needs to be addressed.[52] Major sociolegal changes such as the overturing of Roe v Wade,[53] again criminalising abortion in many states in the USA, triggered renewed interest in the collection and scrutiny of digital surveillance data such as licence plate scanners, biometric databases and phone location tracking services. These measures are currently and actively used to prosecute women in the USA seeking abortion.[54] Instead of improving access to healthcare and healthcare services, surveillance, through smart technologies that track a wide variety of data such as citizens' shopping habits, location, or personal interests communicated through their connected devices, poses serious privacy and security risks.[55] Studies differ as to the extent to which people are concerned about their privacy, with concerns linked to the type of technology and data used, and to whether or not a person's location is identified.[56] Existing modes of governance used in smart cities, the surveillance networks and infrastructure, and the lack of privacy and confidentiality of private communication between citizens have been raised as threats to citizens' fundamental rights.[57] Accounts vary, however, regarding their acceptance: citizens, for example, found the use of surveillance technologies acceptable in areas plagued by crime, such as train stations or public parks, although they were concerned about the collection of personal data more generally.[58]

Gaps in extant law

In combination, regulation, policy development, guidance measures, increased awareness and education can be used to overcome many of the concerns raised by smart technology adoption. POPIA protects personal data and provides a mechanism for addressing data breaches, the CPA and the MRSA provide for product safety regulation, the ECTA provides some safeguards with regard to electronic transactions, and the Regulation of Interception of Communications and Provision of Communication Related Information Act No. 70 of 2002[40-48] prevents the arbitrary interception of location data. However, all measures that assist to some degree or another in addressing certain concerns do not go far enough in addressing the entirety of the unique challenges posed. The current approach is both not comprehensive enough and highly fragmented.

However, in this article we do not advocate a reinvention of the wheel but highlight some of the gaps that arise as a consequence of smart technology adoption. It remains unclear whether the legal and normative issues raised here should be managed by policy prescriptions or are best left to self-regulation and aspirational ethics, rather than enforced through specific regulatory and legislative reform. This needs to be carefully considered within the scope and content of the reformatory process. It is our contention that comprehensive and specific policies and frameworks that go beyond domestic laws of general application, and which are sector- or industry-specific, are required. These could include the development of ethical codes for smart device and smart city development, including ethical risk assessments, safety assurances and audits for fairness and bias.

Currently, various regulatory bodies are mandated to oversee only certain aspects of the smart technological process – the SA Information Regulator with regard to personal information, for example. This means that regulatory frameworks may need to be reviewed to ensure that there is clear responsibility for overseeing *all* aspects of smart technologies, and that no one aspect is left unattended to. Thus, greater co-operation and engagement are called for across all regulatory domains to oversee effective implementation.

Conclusion

Smart technologies applied well, driven by lawful and ethical data and algorithmic use, can promote human wellbeing. For this reason, we support their lawful and ethical innovation and adoption. In light of this and having regard to the discussed ethical and legal issues experienced generally across smart technologies and smart cities, we make the following recommendations.

We suggest the following with regard to further regulatory guidance and development:

(*i*) There should be support and encouragement of products and designs that underpin fairness, equitability and sustainability, and which are grounded in non-exploitative relationships, which includes the establishment of clear responsibility for ethical, value and privacy sensitive interfaces, and in the active implementation of practices of privacy-by-design and by default. We recommend creating frameworks for identifying ethical concerns about fairness and bias and providing guidance on commitments to explainability, transparency, accountability and workable responsibility-attribution models.

(*ii*) Smart technologies should be categorised in terms of a risk classification. Some smart technologies are at high risk of ethics and rights infringements, while others pose a moderate or lower risk. Categorising their risk will inform any mitigation measures to be implemented. The introduction of a policy-based approach for ethical impact and design can also be considered, including ethical risk assessments, ethical audits tools and the requirement to build sound ethical assurance cases before smart use by the public. More guidance is required in providing specific disclosure and transparency requirements on issues of fairness, social and distributive justice, system trustworthiness, algorithmic bias and fairness, and the assessment and reporting of automated decision-making systems.

(*iii*) We recommend that the issues arising from the use of inferential information, high-risk profiling and manipulative behavioural practices be investigated and addressed. Creating a code of conduct addressing these issues, including the protection of biometric and location data obtained through surveillance technologies to prevent harms as described above, should be considered.

(*iv*) Clarification on the use of voice, facial and emotion recognition systems and the context within which they might be allowable is required.

(*v*) Supporting public engagement in the deployment of technology policy through broad and inclusive public and stakeholder engagement, including users, domain experts, user advocacy groups, developers, designers, ethicists, philosophers, lawyers, community leaders and members of the public to better understand the complexities involved, addressing concerns, and exploring legitimate solutions for legal-ethical smart technology deployment is recommended.

(*vi*) We recommend that system change can be facilitated through greater citizen empowerment though education, beginning at school education level.

As the global South has been mostly excluded from the global conversation, we call for efforts of greater inclusivity and diversity, so that many more previously silenced 'voices' can be heard.[55] We suggest that rather than merely mimicking the regulatory approaches adopted elsewhere in the world, South Africans should play a participatory role in understanding and directing the most appropriate measures for regulation, governance, and oversight – and while this might well include new legislative initiatives, equally it may not. Accordingly, we do not offer any firm commitment to the nature and specificities of the evolving legislative landscape at this stage. We suggest here only that gaps exist, and that policy reform is needed, the subject of which should form part of future work.

Declaration. None.

Acknowledgements. None.

Author contributions. Equal contributions.

Funding. The work by BT was funded by the UKRI project EP/V026747/1 'Trustworthy Autonomous Systems Node in Resilience'. The work by MB has been funded by the Luxembourg National Research Fund (FNR)—IS/14717072 'Deceptive Patterns Online (Decepticon)', the European Union's Horizon 2020 Innovative Training Networks, Legality Attentive Data Scientists (LEADS) under Grant Agreement ID 956562 and REMEDIS Project INTER/FNRS/21/16554939/REMEDIS (Regulatory solutions to MitigatE DISinformation).

Conflicts of interest. None.

1. Lupton D, Pink S, Horst H. Living in, with and beyond the 'smart home': Introduction to the special issue. Convergence 2021;27(5):1147-1154. https://doi.org/10.1177/13548565211052736 w
2. BSI. Smart cities framework. Guide to establishing strategies for smart cities and communities. PAS 181:2014. https://www.bsigroup.com/en-GB/smart-cities/Smart-Cities-Standards-and-Publication/PAS-181-smart-cities-framework/ (accessed 16 September 2022).
3. Kunst A. Smart home device ownership in South Africa 2020. Statista, 2022. https://www.statista.com/forecasts/826546/ownership-of-smart-home-devices-in-south-africa (accessed 30 August 2022).

4. EU High-Level Expert Group. Ethics Guidelines for Trustworthy AI. European Commission, 2019. https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html (accessed 30 August 2022).
5. Shirani F, Groves C, Henwood K, Pidgeon N, Roberts E. 'I'm the smart meter': Perceptions of smart technology amongst vulnerable consumers. Energy Policy 2020;144:1-29. https://doi.org/10.1016/j.enpol.2020.111637
6. Goodman EP. Smart city ethics. In: Dubber MD, Pasquale F, Das S, eds. The Oxford Handbook of Ethics in AI. London: Oxford Academic, 2020:823-839.
7. Bibri SE. The IoT for smart sustainable cities of the future: An analytical framework for sensor-based big data applications for environmental sustainability. Sustainable Cities Soc 2018;38:230-253. https://doi.org/10.1016/j.scs.2017.12.034
8. South Africa. Protection of Personal Information Act No. 4 of 2013, section 16(1).
9. South Africa. Medicines and Related Substances Act No. 101 of 1965. Section 2B(1)(a).
10. South Africa. Medicines and Related Substances Act No. 101 of 1965. Section 15(3)(a)(iii).
11. South Africa. Consumer Protection Act No. 68 of 2008. Preamble and section 3.
12. Constitution of the Republic of South Africa 1996. Section 9(3).
13. South Africa. Promotion of Equality and Prevention of Unfair Discrimination Act No. 4 of 2000, sections 6 - 9.
14. South Africa. Consumer Protection Act No. 68 of 2008. Sections 8(1)(a) - (g).
15. Yigitcanlar T, Kamruzzaman M, Foth M, Sabatini-Marques J, da Costa E, Ioppolo G. Can cities become smart without being sustainable? A systematic review of the literature. Sustainable Cities Soc 2019;45:348-365. https://doi.org/10.1016/j.scs.2018.11.033
16. Botes WM. Autonomy and the social dilemma of online manipulative behavior. Springer Nature 2023;3:315-323. https://doi.org/10.1007/s43681-022-00157-5
17. Zuboff S. The Age of Surveillance Capitalism. London: Profile Books, 2019.
18. Falco G. Death by AI: Where assured autonomy in smart cities meets the end-to-end argument. Cornell University, 2020. https://doi.org/10.48550/arXiv.2002.11625
19. South Africa. Protection of Personal Information Act No. 4 of 2013. Section 6(1)(a).
20. South Africa. Protection of Personal Information Act No. 4 of 2013. Section 71(1).
21. Townsend BA. Software as a medical device: Critical rights software-based health technologies in South Africa. TSAR 2020;4:747-762.
22. Koerth M. You can't opt out of sharing your data, even if you didn't opt in. FiveThirtyEight, 2018. https://fivethirtyeight.com/features/you-cant-opt-out-of-sharing-your-data-even-if-you-didnt-opt-in/ (accessed 12 August 2022).
23. Carole Cadwalladr C, Graham-Harrison E. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. Guardian, 17 March 2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (accessed 13 August 2022).
24. OT v Vyriausioji tarnybinės etikos komisija C-184/20,ECLI:EU:C:2022:601
25. Cooper MP, O'Shea DS. Special Category Data by Inference: CJEU significantly expands the scope of Article 9 GDPR. Insider Privacy, 2022. https://www.insideprivacy.com/eu-data-protection/special-category-data-by-inference-cjeu-significantly-expands-the-scope-of-article-9-gdpr/ (accessed 12 August 2022).
26. Yigitcanlar T, Kamruzzaman M, Foth M, Sabatini-Marques J, da Costa E, Ioppolo G. Can cities become smart without being sustainable? A systematic review of the literature. Sustainable Cities Soc 2019;45:348-365. https://doi.org/10.1016/j.scs.2018.11.033
27. Van Heek J, Arning K, Ziefle M. How fear of crime affects needs for privacy & safety: Acceptance of surveillance technologies in smart cities. Paper presented at the SMARTGREENS Proceedings of the 5th International Conference on Smart Cities and Green ICT Systems 2016:32-43. http://doi.org/10.5220/0005761900320043
28. Pink S, Gomes A, Zilse R, et al. Automated and connected? Smartphones and automobility through the global south. Appl Mobilities 2021;6(1):54-70. https://doi.org/10.1080/23800127.2018.1505263
29. Thaler RH, Sunstein CR. Nudge: Improving Decisions about Health, Wealth, and Happiness. London: Penguin Books, 2008.
30. Sætra HS. When nudge come to shove: Liberty and nudging in the era of big data. Techn Soc 2019;(59):101-130. https://doi.org/10.1016/j.techsoc.2019.04.006
31. Gray C, Kou Y, Battles B, Hoggatt, J, Toombs A. The dark (patterns) side of UX design. CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems April 2018;534:1-14. https://doi.org/10.1145/3173574.3174108
32. Mathur A, Acar G, Friedman MJ, et al. Dark patterns at scale: Findings from a crawl of 11K shopping websites. Proceedings of the ACM on Human-Computer Interaction 2019;3:1-32. https://doi.org/10.48550/arXiv.1907.07032
33. South Africa. Electronic Communications and Transactions Act No. 25 of 2002 (as amended, 2012). Section 4(1).
34. South Africa, Consumer Protection Act No. 68 of 2008. Sections 16(3) and 17(2).
35. South Africa. Electronic Communications and Transactions Act No. 25 of 2002 (as amended, 2012). Sections 42(2)(a), (c), (h) and (j).
36. South Africa. Consumer Protection Act No. 68 of 2008. Section 16(1).
37. Hamann B, Papadopoulos S. Direct marketing and spam via electronic communications: An analysis of the regulatory framework in South Africa. De Jure 2014;3:42-62. https://www.dejure.up.ac.za/articles-vol-47-1/papadopoulos-s-hamann-b (accessed 1 September 2022).
38. Sturmer J. Facial recognition: Where is it being used, and how does the technology work? ABC, 2017. http://www.abc.net.au/news/2017-10-05/how-is-facial-recognition-technology-already-being-used/9019526 (accessed 1 September 2022).
39. Nambiar R, Shroff R, Handy S. Smart cities: Challenges and opportunities. 10th International Conference on Communication Systems & Networks (COMSNETS), 2018. https://ieeexplore-ieee-org.proxy.bnl.lu/stamp/stamp.jsp?tp=&arnumber=8328204 (accessed 1 September 2022).
40. South Africa. Regulation of Interception of Communications and Provision of Communication Related Information Act No. 70 of 2002. Section 12.
41. South Africa. Regulation of Interception of Communications and Provision of Communication Related Information Act No. 70 of 2002. Section 2.
42. South Africa. Regulation of Interception of Communications and Provision of Communication Related Information Act No. 70 of 2002. Sections 1(2)(a)(ii) and 1(1).
43. South Africa. Regulation of Interception of Communications and Provision of Communication Related Information Act No. 70 of 2002. Section 3(a).
44. South Africa. Regulation of Interception of Communications and Provision of Communication Related Information Act No. 70 of 2002. Sections 1(1), 16(3) or 18(3)(a).
45. South Africa. Regulation of Interception of Communications and Provision of Communication Related Information Act No. 70 of 2002. Section 1(1).
46. South Africa. Regulation of Interception of Communications and Provision of Communication Related Information Act No. 70 of 2002. Section 16.
47. South Africa. Regulation of Interception of Communications and Provision of Communication Related Information Act No. 70 of 2002. Section 16(5).
48. South Africa. Regulation of Interception of Communications and Provision of Communication Related Information Act No. 70 of 2002. Section 7.
49. Herszenhorn D. Heightened security, visible and invisible, blankets the Olympics. New York Times, 14 February 2014. https://www.nytimes.com/2014/02/14/sports/olympics/heightened-security-visible-and-invisible-blankets-the-olympics.html (accessed 1 September 2022).
50. Government of Japan. 'Suspect detection system' that used digital video and image analysis technology, leads to success at Sochi Olympics (Russia) (in Japanese). JETRO, 2019. https://www.jetro.go.jp/biz/areareports/2019/7235b3bd2d9209d7.html (accessed 1 September 2022).
51. Wright J. Suspect AI: Vibraimage, emotion recognition technology and algorithmic opacity. Sci Technol Soc 2021. https://arxiv.org/ftp/arxiv/papers/2009/2009.00502.pdf (accessed 1 September 2022).
52. Elmaghraby AS, Losavio MM. Cyber security challenges in smart cities: Safety, security and privacy. J Adv Res 2014;5(4):491-497. https://doi.org/10.1016/j.jare.2014.02.006
53. Politico Staff. Read Justice Alito's initial draft abortion opinion which would overturn Roe v. Wade. Supreme Court. Politico, 2022. https://www.politico.com/news/2022/05/02/read-justice-alito-initial-abortion-opinion-overturn-roe-v-wade-pdf-00029504 (accessed 5 September 2022).
54. Sabin S. Digital surveillance in a post-Roe world. Politico, 2022. https://www.politico.com/newsletters/digital-future-daily/2022/05/05/digital-surveillance-in-a-post-roe-world-00030459 (accessed 5 September 2022).
55. Abosaq NH. Impact of privacy issues on smart city services in a model smart city. Int J Adv Computer Sci Applications 2019;10(2):177-185. https://doi.org/10.14569/IJACSA.2019.0100224
56. Van Zoonen L. Privacy concerns in smart cities. Govern Inform Q 2016;33(3):472-480. https://doi.org/10.1016/j.giq.2016.06.004
57. Cho YI. Designing smart cities: Security issues. In: Cortesi A, Chaki N, Saeed K, Wierzchoń S, eds. Computer Information Systems and Industrial Management. Berlin: Springer, 2012.
58. Van Heek J, Arning K, Ziefle M. How fear of crime affects needs for privacy & safety: Acceptance of surveillance technologies in smart cities. Paper presented at the SMARTGREENS Proceedings of the 5th International Conference on Smart Cities and Green ICT Systems 2016:32-43. http://doi.org/10.5220/0005761900320043

Accepted 20 June 2023.