Intel Security:
Safeguarding
the Future of Digital
Australia in 2025

intel® Security

Table of Contents

(intel) Security

The future of technology is more secure than ever.

In today's world, connected devices are advancing healthcare, transforming business, and evolving social connections in unprecedented ways. That's why security must be ubiquitous – always on and on every device.

That's why Intel Security was formed. We're combining the experience and expertise of McAfee with the performance, innovation, and trust of Intel to deliver secure computing to consumers and businesses worldwide. We want everyone to have the confidence to use technology to its full potential so they achieve their full potential.

The future ahead is ripe with possibilities. Join us on this exciting journey.

Staying Safe in 2025

"With the rapid changes and advancement in technology, security cannot be an afterthought. As we become more reliant on these devices, we need to ensure that we enable a safe future for ourselves at home."

The Future of Home – Sean Duca, Chief Technology Officer, Asia Pacific, McAfee. Part of Intel Security

"The next generation needs a safe place to explore their digital self and find kindred spirits online. Future digital natives need multiple perspectives and sources of feedback to uncover the extraordinary thinker in each of them."

The Future of GenNext – Michelle Dennedy, Chief Privacy Officer, McAfee. Part of Intel Security

"If we have multiple social identities it becomes harder to manage them. It comes back to being able to authenticate who we are, for example, using biometrics."

Future of Social - Michael Sentonas, Vice President & Chief Technology Officer, Security Connected, McAfee. Part of Intel Security

"We need to teach our children principles for staying safe online and the importance of privacy, because they will be connected, regardless."

The Future of Social – Dr. Justin Coulson, Parenting & Relationships Expert and Director, Happy Families

"Technology needs to be able to adapt and understand each individual as a person. All of these changes can make us more secure and more productive."

The Future of Work - Brian David Johnson, Director, Future Casting, Principle Engineer, Intel Corporation

About the Author

Ross Dawson
Futurist, Author and Chairman, Advanced Human Technologies Group

Ross Dawson is globally recognised as a leading futurist, entrepreneur, keynote speaker, strategy advisor and bestselling author. He is Founding Chairman of four companies: international consulting and ventures firm Advanced Human Technologies, futures think-tank Future Exploration Network, events company The Insight Exchange and 3D information interfaces company MultiDimensionCorp.

Strong demand for Ross' expertise has seen him deliver keynote speeches in 27 countries across six continents and consult to leading organisations worldwide such as Ernst & Young, Macquarie Bank, News Corporation, Procter & Gamble and many others.

He is author of books including Living Networks, which foresaw the social networking revolution, the Amazon.com bestseller Developing Knowledge-Based Client Relationships, now out in its second edition, and the acclaimed Getting Results From Crowds. His visual frameworks on the future have been viewed millions of times and appeared in the media in over 30 countries.

Ross has run executive education programs and lectured at numerous academic institutions around the world, including the University of Virginia, Malaysian Directors Academy, Australian Graduate School of Management, Singapore Institute of Management and the Institute of Banking and Finance.

Ross was recently named by Digital Media magazine as one of the 40 biggest players in Australia's digital age.

Previously Ross worked in senior positions in London, Tokyo and Sydney with organisations including Merrill Lynch, NCR and most recently Thomson Financial as Global Director – Capital Markets. He holds a B.Sc (Hons) from Bristol University and a Grad.Dip in Applied Finance from Macquarie University. He has extensive international business experience, and speaks five languages.

Safeguarding the Future of Digital Australia in 2025

Executive Summary

To understand Australia's future we must recognise the enormous impact of digital technologies. They will shape every aspect of our lives, across education, work, business, social interaction, aged care and indeed our very identity as Australians. These developments provide us with tremendous opportunities, yet we must also acknowledge and address the new risks that emerge.

Intel Security's Safeguarding the Future of Digital Australia in 2025 report is intended to provide useful insights into the technology developments we can expect over the coming decade, so that we can together better respond. While we cannot know for sure what will happen, the report's author, futurist Ross Dawson, studied underlying social and technological trends, drew deeply on global research, examined the state of existing technologies, performed interviews with numerous domain experts and analysed the findings to provide relevant perspectives on Australia's future. In addition, we surveyed 1,230 Australians to discover their attitudes on the future of technology which will shape our world in the years to come.

To make the report relevant to the broadest range of Australians, we have covered the Future of Home, the Future of Social, the Future of Work, and the Future of GenNext – our leaders of tomorrow. Each segment begins by describing a day in the life of an Australian in this future world, and then delves deeper into the specifics of what we can expect in 2025. Early indicators have been selected to show how elements of these future worlds already exist today. Finally, and very importantly, we have distilled insights from leading experts on how we can start preparing now to stay safe in the future.

Our intention with this report is to help Australians to understand how the world may change, develop the skills and capabilities necessary in the future, and to keep safe in this brave new world. Moreover, we wish to spark stimulating and useful conversations on the opportunities and challenges we face, and what we can best do today to create the future we want for our children and ourselves.

We hope you find this report useful.

All the best,

Keith Buckley

Managing Director
Australia & New Zealand
McAfee. Part of Intel Security

The Future of Home

Our homes will nurture and protect us, keep us healthy, and may even love us.

Lucy, 79, Ballarat

"Hi Grandma!" Lucy smiled and waved at her grandson as she made her way to the kitchen. "Look. Here's a new truck I made. Do you like it?" the tousled blonde boy asked eagerly. Lucy stepped towards the always-on full-wall video screen to admire the toy her grandson had designed and 3D-printed. After bidding him a wonderful day at school, she said, "Blinds up", allowing a flow of light into the room, and then after thinking for a moment, asked "Where did I leave my glasses?" A pleasant young woman's voice responded, "Your glasses are on your bedside table."

After breakfast Lucy went to the bathroom. "Good morning Lucy! Please take one each of these pills." Lucy duly took her pills then breathed into a sensor.

As Lucy sat down, a large fluffy ball appeared around the corner and came to snuggle up against her ankles, looking up at her with big blinking eyes and purring softly. "Hello Mumu," Lucy said gently, and gave the robotic pet a pat as it wriggled closer.

The highlight of Lucy's week was always her bridge group, where she caught up with her old friends Bridget and Hannah, as well as newcomers to the community and had a chance to exercise her mind. When it was time for Lucy to head to bridge, Lucy said "Please call me a car." After a pause she heard a reply, "Your community driver will be here in 12 minutes."

She pressed the button indicating she was going out to the waiting car. As the house told Lucy her driver was about to arrive, she stopped by the security panel. It showed that the delivery man would be authenticated to enter the house and put groceries in her fridge, with no other permissions. Lucy closed the door and walked outside to the waiting car.

Lucy was in two minds about all the technology in her home. She sometimes found it confusing and overwhelming, but most of it was so easy to use. Most importantly it meant she could stay in her beloved home even though she was alone.

What to expect

Houses at our command

Our voice, gestures and even moods will control our homes, ranging across entertainment systems, lighting, temperature and more.

Controlling our environment

Lighting will match every mood, wallpaper can be changed for every occasion, and rooms (and showers) will adjust temperature to cater for the preferences of the individuals it senses to be present.

Homes keeping us healthy

Sensors in our clothes, chairs and bathrooms will monitor our health and send information as required to doctors. Medicine cabinets will remind us to take our pills and know when we've already taken them. Rich video links together with these sensors will allow 'house visits' from doctors whenever required.

Taking care of the elderly

Household aids and robots will enable seniors to live far longer at home, while always-on full-wall screens will allow distant relatives to monitor how they are and keep engaged. Continuous health monitors and fall alerts will allow instant response and changes in medication when required.

Robots to help and heal

Task-specific robots that vacuum, mop, dust and clean will begin to be supplanted by general-purpose robots that can also tidy and make beds. Robot pets will be increasingly prevalent as they become more emotionally engaging as well as convenient.

Kitchens make life easier

Recipes and video cooking instructions will be available on kitchen benches, matching our target calorie count or nutritional profile. Fridges will monitor the freshness of their contents and can be authorised to make regular orders for staple goods.

Immersed in entertainment

3D TV that does not require glasses and truly immersive virtual reality entertainment will be mainstream and for many will replace classic TV screens. All screens and audio around the home will be linked so content can be played anywhere, and if you wish, follow you from room to room as you walk around.

Intelligent green homes

Houses will monitor energy and water usage, automatically adjust solar panels and blinds, provide suggestions on environmental efficiency, and use sensors to ensure water-friendly flourishing gardens.

What do Australians think?

Australians are divided on the impact robotics and more intelligent technology will have on their quality of life, 44% believe it will make their quality of life worse and 47% believe it will be the same or better.

Currently, 39% of Australians would be comfortable for their wearable technology to transmit personal information to health providers, while 34% would not be comfortable.

Early indicators of the future

"Robots can be used to enable people to remain living at home... this is an emerging smart technology that is rapidly evolving."

Robotics to Enable Older Adults to Remain Living at Home, Journal of Aging Research, 2012

iRobot has sold over 10 million home robots for vacuuming and mopping

iRobot

"Worldwide revenues from shipments of home automation systems will grow at a compound annual growth rate of 33% from US$ 2.3 billion in 2010 to nearly US$ 9.5 billion in 2015"

Berg Insight

There is a 43% reduction in hospitalisations and a 68% reduction in bed days of care in cardiac patients who transmitted daily ECG and blood pressure data

Ambulatory Disease Management in Cardiac Patients, Doede et al. Physikatische Medizin, 2009; 19

BBC is investigating a mood-based interface for accessing TV program

BBC R&D

Expert advice to stay safe

Michael Sentonas
Vice President & Chief Technology Officer, Security Connected, McAfee. Part of Intel Security

"We need to have security built in to products by design, for performance, resilience and security. Some legislation may be required to make this happen. We absolutely should not be building critical infrastructure or using medical devices lacking strong security. We need to understand that as technology may not always work, we need to have fail-safes and backups in place. What happens if your house does not recognise you, or someone attacks the system to deny you access?"

Sean Duca
Chief Technology Officer, Asia Pacific, McAfee. Part of Intel Security

"With the rapid changes and advancement in technology, security cannot be an afterthought. It is very important that home users protect all of their devices and ensure that they operate these devices in the way the manufacturer intended. As we become more reliant on these devices, we need to ensure that we enable a safe future for ourselves at home."

Dr Justin Coulson
Parenting & Relationships Expert and Director, Happy Families

"This scenario reinforces the need for parents to engage with their children in discussions of safety – in any environment. And rather than hiding technology from children which some parents still do, we need to expose them to it in appropriate ways to help them become familiar with what will be an everyday occurrence. Children will need to be taught about the technology, and trusted to use it appropriately."

Michelle Dennedy
Chief Privacy Officer, McAfee. Part of Intel Security

"The future for applied technologies, to help seniors in particular, is certainly exciting but we have some thinking to do in advance. In addition to securing data to ensure that our elderly neighbours remain safe and free from fraud, how about thinking about a 'Living Will for Data' to make sure the right people have access to a digital life well lived? Are we ready to face the realities of our genetic history? Will we know when digital help diminishes actual dignity and the right to be silent, is switched off? We have a lot to consider before the future is upon us with data privacy."

Preparing to stay safe in
The Future of Home

What can you do today, and over the next few years, to start preparing to stay safe online in the foreseeable future?

Our expert contributors have recommended some steps individuals and businesses can take to ensure you enjoy the benefits of the digital future, safely and securely.

- As you consider the purchase of new connected technologies and devices for your home, aim to select those with security built in by design. This will help to ensure reliability and your families' personal privacy.

- Educate your family and children that connectivity in home devices means that they transmit information so this data needs to be secure.

- Consider whether you have enough visibility into the data and personal information your smart home is accessing; ask yourself "Where is it being transmitted?" and "Who has access?"

- Make sure you and your family use smart devices in the way the manufacturer recommended with security controls enabled.

- Ensure technology in your smart home guarantees user authentication without jeopardising individual privacy.

- Make sure you've considered what could happen if the home network was compromised or failed; would the kids be able to get in the house, would it be safe?

- Be aware that smart devices have different levels of security based on their intended use. For example, it is unsafe to use an unsecured internet enabled fridge to access your online banking.

- Make sure you monitor what information your applications are accessing in smart devices. Does your favourite gaming app really need to access your contacts?

The Future
of Social

Our reputation, personal opportunities and identity will be shaped by our participation in social media.

Katrina, 32, Surry Hills, NSW

"That looks great on you Katrina!"

Katrina smiled at the warm welcome from her friend Julia and gave her a hug. "When you showed me the dresses, I was sure that the turquoise one would suit you the best. It was really worth letting me have a look on social before you decided!"

As Alana and Noriko joined them for after-work drinks, the women discussed the latest in their social circles. "Did you see that Roger is open life-logging?" asked Julia, referring to the trend of capturing a digital log of every detail of one's life. "TMI", responded Katrina, using the acronym for 'Too Much Information'.

"You know what's good?" said Noriko. "When you know everything about Roger you can see he really is a good guy. You can't find that out on a date. He has a Boyfriend Rep of over 8, so when his girlfriend broke up with him, he wasn't single for long!" "But did you hear what happened to my sister?" Julia asked. "She was too open with her stream, and a gang in Nigeria took over her profile. It was such a mess! She managed to get her money back, but it took ages to convince the U.S. government she was innocent of all the crimes they committed, when she tried to get a visa."

Alana announced she was buying a new car, triggering congratulations and hugs from her friends. "I used peer lending," she said. "The rate was better than from a bank, and several people from my university alumni group said yes straight away!"

Katrina glanced at her screen and showed her friends a map with the location of several of their friends who were nearby. "Hey, a few of the gang are around. Should we invite them along?"

To general nods, she sent out an alert inviting their friends to join them. Katrina changed the small group's status to open, so their friends, and also any friends of their friends who met specific criteria, could see where they were, and come to join them. They pulled up a few more chairs to make space for the extended community.

What to expect

Life-logging and extreme over-sharing

With storage costing almost nothing, some will choose to log every moment of their lives with high quality video, audio and body sensors. Many will feel this is deeply personal information for themselves and perhaps family and friends. Some others will freely share every instant of their lives with whoever is interested, sometimes with devastating consequences.

Authenticating ourselves

Multiple providers will battle to authenticate our online identities, so that we can pay, vote, build our personal reputation, and comment online in our own voice. This authentication must be very closely protected, but can give us power to achieve what we want.

Multiple online identities

In addition to our authenticated identity, many will choose to use other identities. People will want to separate their work and personal lives, and in some cases take on private identities as they engage in other communities.

Industrial identity theft

While, in the main, people will be able to secure their identities through prudent approaches, the value of appropriating individuals' identities will drive sophisticated criminal efforts and result in many finding their names, social media profiles and personal resources are being used by others.

Social media drives our reputation

It won't be something new that our reputation will drive our opportunities, but what will be different is that our reputation will be visible to all. Banks will use social media to determine whether they want to lend to people, and employers will make offers to the newly visible, talented networkers.

Privacy evaporates

The long-term ongoing erosion of individual privacy by companies and governments will result in many relaxing their attitudes to the information held about them, sometimes to their cost. However, institutions will also find that far more information about them will become publicly available.

Financial services become social

Instead of depositing money in a bank we may often choose to lend to a friend or a community of local or like-minded people at a better rate. Some insurance will shift to pools of individuals who trust each other.

Almost all shopping is social

Online social connections will drive all stages of buying, from being exposed to brands and products, through searching among personal networks and communities for opinions, to getting trusted friends' views at the point of purchase.

What do Australians think?

68% of Australians say they would be concerned if in 2025 young peoples' sense of identity was defined by their online persona and interactions, including 35% who would very concerned.

54% of Australians think it would be unfair for financial credit ratings or job opportunities to be based on our online reputation, while only 20% think this would be fair.

Early indicators of the future

"FICO, which provides the credit scoring used in more than 90% of [U.S.] lenders decisions… is weighing possibilities for incorporating social media."

Wall Street Journal, January 8, 2014

51% of Australians do not read online privacy policies because they are too long (52%), complex (20%) or boring (9%).

Office of the Australian Information Commissioner Community Attitudes to Privacy survey Research Report, October 2013

Over 36% of Australia graduate employers looked at candidates' social media profiles, while 93% of U.S. recruiters are likely to look at their candidates' social media profiles.

Graduate Careers Australia, Jobvite

Children as young as eight (tweens) are swiftly adopting technology, particularly social networking, with 67% revealing they are currently using a social media site and 1 in 4 using Facebook.

McAfee Tweens, Teens & Technology Research, May 2013

"Most Australians have multiple digital identities, managing between five and 50 login and password combinations to conduct their day-to-day online activities."

Australian Communications & Media Authority

Expert advice to stay safe

Dr Justin Coulson
Parenting & Relationships Expert and Director, Happy Families

"Ask your kids questions about what they are sharing, and why. Engage with them (rather than dictate to them) in relation to what they think is appropriate and ask questions that cause them to re-think what they share. They'll become critical of their own TMI [Too Much Information] moments. We need to teach our children principles for staying safe online and the importance of privacy, because they will be connected, regardless."

Sean Duca
Chief Technology Officer, Asia Pacific, McAfee. Part of Intel Security

"It is important for Australians to leverage the privacy controls on social media to ensure they are not compromising their identity and online reputation. Decisions by others will be made based on what we post online, so we need to ensure that oversharing doesn't get away from us. We should track the permissions and authority we give these platforms. Something insignificant we post today could have far greater impact on our digital identity in the future."

Michael Sentonas
Vice President & Chief Technology Officer, Security Connected, McAfee. Part of Intel Security

"If we have multiple social identities it becomes harder to manage them. It comes back to being able to authenticate who we are, for example, using biometrics. We will need to have a trusted identity broker, rather than use a vendor who has a vested interest in tracking your online activity."to use it appropriately."

Brian David Johnson
Director, Future Casting, Principle Engineer, Intel Corporation

"Smartphones, tablets and other new gadgets and gizmos are relatively new in our daily lives and we haven't quite figured out what's socially acceptable and what's not. But it's always important to remember that we are in charge. People get to make the decisions about their technology; technology doesn't get to decide. Just as your family can choose whether they watch TV during dinner or not, so too can you choose how to be social on these new devices."

Preparing to stay safe in
The Future of Social

What can you do today, and over the next few years, to start preparing to stay safe online in the foreseeable future?

Our expert contributors have recommended some steps individuals and businesses can take to ensure you enjoy the benefits of the digital future, safely and securely.

- Use the privacy controls available to you through social networking platforms to minimise the risk to your identity or online reputation.

- Manage your privacy settings, make sure that you are only sharing information with friends and family and check them regularly in case there are any changes.

- Consider using a trusted identity tool to verify that you have secure access to your accounts from a single source.

- Remember the internet is permanent. Assume that once you put information on the site, it stays there forever. Even if you delete the account, you don't know if someone has already printed/copied your text or photos from it.

- Act respectfully and responsibly. Treat people with the same respect online as you would treat them face-to-face.

- Be selective when accepting a friend. Do you really know that their profile is real and not fake? Only "friend" people you know in the real world.

- Exercise caution when clicking on links. Even if they're from friends. Hackers prey on social networks because you are more likely to click on something from your friends. Also be wary of offers with the word "free" or offers that sound too good to be true, as they usually are.

- Until biometrics or future authorisation technologies are available, change your passwords frequently. Choose hard-to-guess passwords that are at least eight characters long and a combination of letters, numbers, and symbols, and change them regularly. Also make sure you use different passwords for each account.

The Future
of Work

There will be big winners and losers as collaborative technologies, robots and artificial intelligence transform the nature of work.
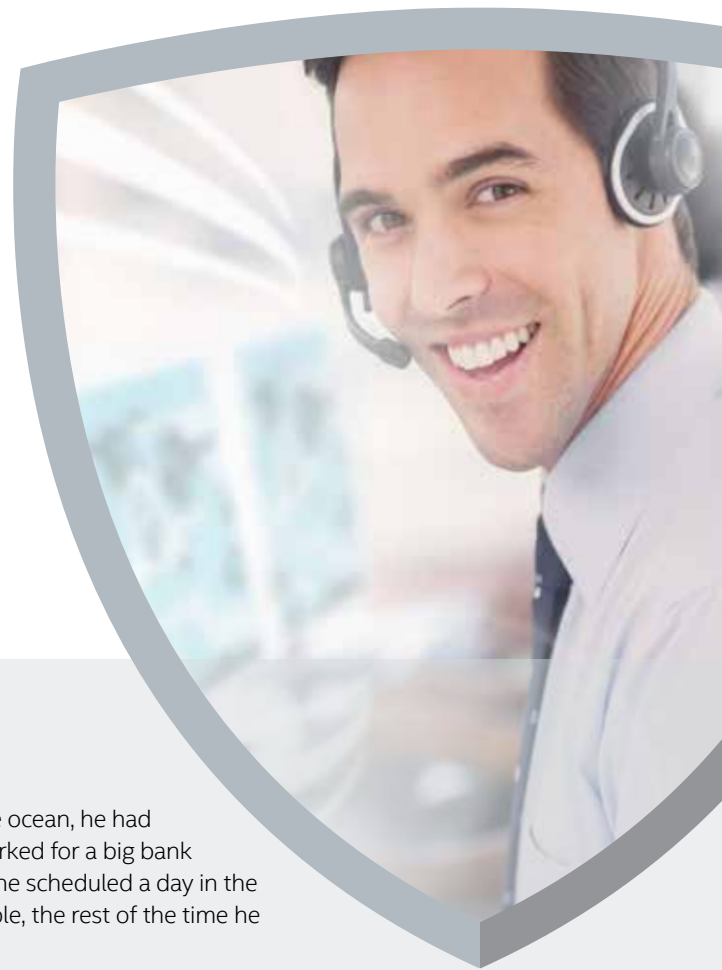
Vinh, 43, Joondalup, WA

Vinh was feeling great. After a run on the beach and quick dip in the ocean, he had walked to work, as he did several times a week. Just because he worked for a big bank didn't mean he needed to battle the traffic every day. Once a week he scheduled a day in the CBD office for meetings and just to wander around chatting to people, the rest of the time he worked at a large local co-working hub or from home.

Many of his colleagues from the bank who lived nearby often worked in the co-working space, where they could spend time with interesting people and have access to advanced technology. The central WA office was a quarter the size it was a decade earlier, while staff numbers were half what they were.

Many jobs had simply disappeared, some to pools of crowd-sourced workers, others essentially taken over by computers that seemed almost human in their ability to make complex decisions. Some of Vinh's former colleagues had done very well with new jobs or working independently, while others had struggled.

"Hi Nathan, what's up? How was Patagonia?" Nathan was a freelancer in the centre who worked when he felt like it, and spent the rest of the time on holidays, usually in exotic places. "It was awesome, thanks! Sorry, gotta run, have to get to the Holodeck for a meeting!"

The tele-conference room they jokingly called the Holodeck didn't use real holograms, but multi-camera setups to capture and project people's images in three dimensions, so that you could almost believe they were in the same room.

Just then Vinh's watch vibrated with a message. He had been identified as the best qualified person to help with a problem in their Auckland office. Vinh sat down at the nearest desk, where the screen immediately displayed the issue. He smiled. He loved the variety of his work, and that his abilities were being used so well. But he also gave a little sigh, because he knew many others, including some of his family, were struggling to get the work they wanted.

What to expect

Almost all work is global

It is not just knowledge work that is being performed remotely; we are seeing everything from surgery to mining machinery operation being routinely completed by people far away. This will create both challenges and opportunities for Australians.

Machines destroy (and create) jobs

Surging capabilities of robots and artificial intelligence will see a range of current jobs supplanted, potentially including driving as well as more process-oriented roles in mining and financial services. However new jobs will rapidly emerge to replace them, focused on the creativity and relationship skills that machines will still lack.

Offices transform

There will still be offices where people work together, though usually more attractive than those of today and designed to facilitate face-to-face communication and collaboration. Play will be a norm in supporting effective work.

Co-working everywhere

Co-working spaces will not just be for the self-employed and entrepreneurs, many suburbs will see open working spaces where people can base themselves to avoid commuting but also get out of the home and have access to sophisticated communication technologies.

An economy of individuals

A rapidly increasing proportion of the population will be self-employed. Individuals will find more work opportunities and flexibility to work independently, and organisations will reshape themselves to draw on extended rather than permanent workforces.

Polarisation of work opportunities

Globalised work and increased automation will drive a polarisation of work, with exceptional possibilities for those with in-demand skills, yet strong downward pressure on wages and opportunities for others. Our collective response to this division will be critical.

Longer working lives

More school-age children will become entrepreneurs, finding opportunities to support excessive spending habits, while the current idea of retirement at 65 or earlier will fade for many, driven by financial need, the desire for mental stimulation, and a more flexible economy.

Value driven through customer data

Organisations' success will be based on the quality of their customer service, driven by their use of rich customer data. Even as work and systems become highly distributed, companies will need to maintain visibility and control to ensure privacy and protect against breaches.

What do Australians think?

46% of Australians would be interested in using technology such as "virtual reality" so they don't have to go into their office or workplace every day, while 23% would be disinterested.

50% of Australians feel comfortable about the rate of technological change and 30% are neutral, while 17% are concerned.

Early indicators of the future

Secular shifts in labour demand have led to a pronounced "polarisation" of job opportunities across occupations, with employment growth concentrated in relatively high-skill, high-wage and in low-skill, low-wage jobs – at the expense of "middle-skill" jobs."

Graduate Careers Australia, Jobvite

Over US$1.5 billion of work has been done on online work marketplaces globally.

Announcements by Odesk, Elance, Freelancer.com

"Since 2000 self-employment has gone up 37% in the UK (compared to a 6% increase in employment)."

UK Office for National Statistics

After joining a coworking space 71% of workers report increased creativity, 70% feel healthier and 62% believe their standard of work is higher.

Global Coworking Survey, Deskmag

Social media management company Buffer openly publishes the salaries of its entire staff, while employees share data on their daily activity and sleep patterns with their colleagues.

Buffer blog

Expert advice to stay safe

Michelle Dennedy
Chief Privacy Officer, McAfee. Part of Intel Security

"We're going to need to rethink everything about work. Employers have tried to judge performance on now meaningless correlations of check in and check out times at the office in a world where the most productive work may take place anywhere and anytime. In future, we'll be more results based, not showing up based. Good ideas will come from critical and creative thinkers and fuelled by art and music as well as maths and engineering. These new information sources will continue to evolve which means that how we provision, authenticate and encourage them must also evolve. I can't wait."

Sean Duca
Chief Technology Officer, Asia Pacific, McAfee. Part of Intel Security

"As they increasingly do work remotely they'll be connecting to multiple networks, so employers will need to be sure that we're always connecting to reliable and secure networks. Our devices will continue to be a journal of our lives, so we need to protect this data the same way we would protect data for our employers. As the lines continue to blur between work and personal, this will become as important for individuals as it is for organisations."

Michael Sentonas
Vice President & Chief Technology Officer, Security Connected, McAfee. Part of Intel Security

"We will be able to put sensitive information on a personal device but not give permission to copy, print, or transfer it to other devices. We can control, authenticate, and attach permissions to individual files."

Brian David Johnson
Director, Future Casting, Principle Engineer, Intel Corporation

"The numbers don't lie. We know we will have a lot of young people and people with gray hair. They are going to be spread all over the world and not evenly distributed. Most of these people will remain in the workforce and their connectivity and security is important to their productivity. Technology needs to be able to adapt and understand each individual as a person. If your technology can understand you as an individual, know if you are rushed for time or deep in thought, if you are an introvert or an extrovert, it can adjust how it communicates and interacts with you. All of these changes can make us more secure and more productive."

Preparing to stay safe in
The Future of Work

What can you do today, and over the next few years, to start preparing to stay safe online in the foreseeable future?

Our expert contributors have recommended some steps individuals and businesses can take to ensure you enjoy the benefits of the digital future, safely and securely.

- Remote workers will connect anywhere, at anytime and will need assurance they are connecting to reliable and secure networks.

- Be cognisant that company data will flow freely through employees' mobile devices. Are they secure?

- New information sources will continue to evolve which will change how we provision, authenticate and use them.

- IT managers need to ensure they can answer "Who is on my network, what are they doing and should they have access to specific function or data?"

- Monitoring and responding to activity in real-time across your network will be key to protecting corporate data.

- Multifactor authentication and encryption will continue to play an important role in securing the networks of tomorrow's workplace.

- Data will cross borders constantly and instantly – employers need to think about how they will ensure visibility, control and comply with local and foreign regulations.

- Personal information will be prolific and gathered by companies looking for more ways to target customers. Businesses will need to guarantee privacy and strictly control access to build customer trust.

- Internal IT processes and systems will need to adapt and understand the needs of each individual worker.

The Future
of GenNext

The brains of tomorrow's adults will be networked to technology, transforming how they learn and interact.

Ahmed, 23, Indooroopilly, QLD

Ahmed gave a whoop. One of Australia's largest professional services firms had just sent him a message inviting him to an online interview.

By the end of school he had had enough of formal education, it seemed completely irrelevant and a decade behind the real world. Even though he achieved decent grades he didn't bother to apply to university. He had been doing online courses in data visualisation in his spare time, and immediately found work doing freelance projects for clients around the world.

He didn't earn much to begin with, but over the last few years he had become an expert by spending all his time in online visualisation communities, learning from the best in the world and contributing new techniques he had developed. He felt completely comfortable in these online spaces, though sometimes found it hard to focus on anything for long outside his work.

Ahmed got on the video call with the talent scout. "We know you're the best in your field. We found you through your outstanding community reputation score," she said with a smile. "We know you're the best and we'd like to offer you a job, the terms are up to you."

"Simple," he said. "A maximum of 20 hours per week, you match my usual hourly rate, I can do whatever else I want, and I use my own team on projects." She readily agreed.

Later in the evening he changed into trendy technology-enabled street wear and went out to meet some friends at a club. One member of the group, a stylishly dressed young woman named Grace, had a small, elegant device snugly fitted behind her ear. She noticed Ahmed looking at it and said, "What do you think? It's a MindBox, the latest in thought control devices, and I've decided they're finally good enough now to get it implanted. But what really matters is whether it looks good!"

Ahmed smilingly admired the device. He was happy for now with his intelligent clothing and glasses, which he used for phone calls and accessing information, but he knew he'd want more soon.

What to expect

Next generation brains

Those who have grown up completely immersed in technology will have different neural wiring to the previous generation. We have yet to discover the full implications, but the inclination to multi-task and make connections between ideas will be accentuated.

Technology implants

This generation will be the first to routinely choose to implant technology into their bodies and neural systems. It will be a bold move, but in line with their outlook, and one which could give them a real advantage over those who stick with the bodies and minds with which they were born.

Identities forged online

The unbounded nature of online socialisation amplifies human behaviours and the shaping of young identities. Distinctive individuals can find support from like-minded communities anywhere, while bullying can become more extreme. Children will be increasingly precocious, including in their sexual development.

Constant connectivity as a right

There is an expectation that we will be able to be connected at every moment, wherever we are. To be cut off from friends and information will be an affront, to be connected will be the heart of how young people see themselves.

Traditional schools struggle

Schools as we know them today will be highly challenged by connected children, many of whom will learn faster than the pace of the classroom, correctly question teachers, and be intensely frustrated by antiquated approaches and structures. Alternative schooling structures that leapfrog established approaches will gain traction.

Peer recognition over qualifications

Employers will increasingly find and hire talented people by what they actually do and how their peers view their capabilities, tending to view degrees from educational institutions as far less accurate indicators of likely work performance.

Traditional skills fade

Many traditional skills will rapidly erode. Handwriting will almost vanish. Good spelling will become less common though a real advantage. Social skills will be polarised, with some amplifying the scope of their interactions, yet others using connectivity as a crutch to avoid socialising.

Ideals first

The most idealistic generation in human history is growing up and moving into the workforce, certainly believing in their own capabilities but also acting on the principle that we can take effective action today to create a better world tomorrow.

What do Australians think?

47% of Australians would be concerned about online technologies helping children to learn at their own pace, but 27% think it would be positive.

32% of Australians feel safe and secure in the increasingly digital world and 44% are neutral. Only 21% feel unsafe and insecure.

Early indicators of the future

"When people expect to have future access to information, they have lower rates of recall of the information itself and enhanced recall instead for where to access it. The Internet has become a primary form of external or transactive memory, where information is stored collectively outside ourselves."

Google Effects on Memory: Cognitive Consequences of Having Information at Our Fingertips, Betsy et al., Science, 333, 2011

Estonia, France and Costa Rica have declared Internet access to be a basic human right, while in Finland it is a legal requirement that every citizen has access to a broadband connection.

Seventeenth Session Report, United Nations Human Rights Council

At eight years old, cyber bullying is already becoming an issue with 25 per cent saying they have witnessed nasty comments online directed at them or their friend and as a tween gets older and into their teen age years (11-12 years old), 38 per cent said they had been exposed to cyber bullying.

McAfee Tweens, Teens and Technology Report 2013

"[Brain] implants will make the transition from being used exclusively for severe problems such as paralysis, blindness or amnesia to enhancing the performance of healthy or "normal" people. They will be used to improve memory, mental focus (Ritalin without side-effects), perception and mood (bye, Prozac)."

Dr Gary Marcus, professor of psychology, New York University and Dr Christof Koch, chief scientific officer, Allen Institute for Brain Science

"Using a baby aspirin-sized array of electrodes implanted into the brain, early research from the BrainGate team has shown that the neural signals associated with the intent to move a limb can be "decoded" by a computer in real-time and used to operate external devices."

BrainGate Research Team at Brown University, Massachusetts General Hospital, Stanford University, and Providence VA Medical Center

Expert advice to stay safe

Sean Duca
Chief Technology Officer, Asia Pacific, McAfee. Part of Intel Security

"Over the next 10 years, the internet-saavy youth of Australia will take digital connectivity for granted as they grow up. Along with the amazing technological advances they will inherit, and no doubt help to design, we'll also leave a legacy of educating them about the importance of their own privacy and safety online."

Dr Justin Coulson
Parenting & Relationships Expert and Director, Happy Families

"From a developmental perspective, we need to consider at what age it is appropriate to allow this level of potentially intrusive technology into our children's lives. At what point do they have a need and a right to be protected versus connected? Parents also need to know that their children are receiving an education for the future, rather than an education for the past."

Michelle Dennedy
Chief Privacy Officer, McAfee. Part of Intel Security

"We need to define how we measure excellence and move away from the bell curve which allows people to be hidden among the many. The next generation needs a safe place to explore their digital self and find kindred spirits online. Future digital natives need multiple perspectives and sources of feedback to uncover the extraordinary thinker in each of them."

Brian David Johnson
### Director, Future Casting, Principle Engineer, Intel Corporation

"As technology becomes more intelligent and advanced it will be able to do more tasks that humans used to do. One way to future proof for next generations is to highlight tasks that machines will never do. For example, humans are excellent at emotional intelligence, talking to other humans and disparate cognitive synthesis, or as most would call it, creativity."

Preparing to stay safe in The Future of GenNext

What can you do today, and over the next few years, to start preparing to stay safe online in the foreseeable future?

Our expert contributors have recommended some steps individuals and businesses can take to ensure you enjoy the benefits of the digital future, safely and securely.

- Act responsibly when communicating with others online, as well as securing our identity, as this will form a key part on how others interact with you.

- Be aware that as we adopt more wearable or implanted technologies they will be connected and transmiting information. As a result, it is critical we can trust that they have security and privacy built in by design.

- Consider what age is appropriate to allow access to technology platforms for your children.

- Actively discuss the risks and benefits of privacy and connectivity with your children. Decide exactly what is ok and what is not okay with regard to the kind of websites that are appropriate to visit and the chat rooms and internet forums that are appropriate to participate in.

- Don't forget technology is an enabler, but it cannot replace human functions such as creativity and emotional intelligence.

- Understand that online interactions and reputation will play a significant role in how upcoming generations of digital natives perceive themselves.

- Help teach your kids not to reveal personal information online. They should be suspicious of anyone who asks for your personal information online and never share your home address, phone number, or other personal identifying information.

- Remind your children and family members that people met online are strangers and may not be who they say they are.
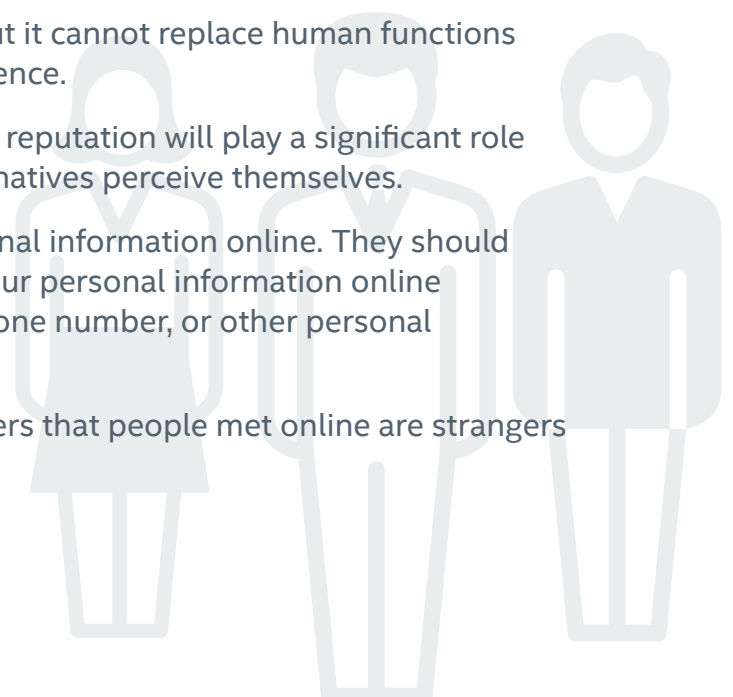
About the contributors

Michael Sentonas
Vice President & Chief Technology Officer, Security Connected, McAfee. Part of Intel Security

Michael Sentonas has over 18 years experience in the IT industry, focusing on internet security solutions with past roles including software development, security research and consulting and management. Michael is a key champion for driving the integrated security architectures and platforms that have propelled McAfee and Intel Security into a leadership position as the largest dedicated security provider in the world.

Michelle Dennedy
Chief Privacy Officer, McAfee. Part of Intel Security

Michelle is responsible for creating a privacy practice that is focused on quality and excellence in McAfee's policies, products, procedures and governance efforts. Her team is a staunch supporter of McAfee's outreach efforts to educate and protect children, families and communities in the Digital Age. Michelle recently published The Privacy Engineers' Manifesto: Getting from Policy to Code to QA to Value, a framework for businesses to put customer privacy at the heart of their operations.

Sean Duca
Chief Technology Officer, Asia Pacific, McAfee. Part of Intel Security

Sean Duca is responsible for driving McAfee's solution strategy and technology vision throughout Asia Pacific. With more than 16 years of experience in the IT industry, Sean is passionate about helping organisations improve security postures and align security strategically with business initiatives.

Dr Justin Coulson
Parenting & Relationships Expert and Director, Happy Families

Dr Justin Coulson is an author, speaker, blogger, columnist, and media commentator. He writes and speaks about parenting and has a PhD in psychology at the University of Wollongong (2012). Justin has authored several peer-reviewed journal articles and is also the author of several chapters in edited scholarly books about positive psychology and parenting. Justin has worked as a reviewer for the Australian Government's Raising Children Network, and also provides advice to the Alannah and Madeline Foundation and Life Education for their cyber safety school programs.

Brian David Johnson
Director, Future Casting, Principle Engineer, Intel Corporation

As a futurist at Intel Corporation, his charter is to develop an actionable vision for computing in 2020. His work is called "future casting" – using ethnographic field studies, technology research, trend data, and even science fiction to provide Intel with a pragmatic vision of consumers and computing. Along with reinventing TV, Johnson has been pioneering development in artificial intelligence, robotics, and using science fiction as a design tool. He speaks and writes extensively about future technologies in articles and scientific papers as well as science fiction short stories and novels.

Final thoughts

The future is what we make it.

The intention of this report is to show where the evolution of a highly digital, connected world could take Australians. This helps us to understand how we can best act today to create the future we desire.

Technology has the power to enrich the everyone's life. To transform how we live and work. But as technology becomes more deeply integrated into daily life, security must be more deeply integrated into technology. Things such as wearable and implantable technologies provide exciting opportunities, but only if security is built in from the beginning. It's one thing to have our computers crash and our online movements tracked, but it's quite another if it involves our physical well-being.

This is the challenge we face. A safer world is one where security is ubiquitous and integrated. It's a world where we don't have to choose to add security to our devices and technologies, because security and privacy are already built in. It's a world not filled with the failures of technology, but rather all of the great things that are possible – because that technology is secure.

Please use this report as a starting point to help you think about the future, and what you can do to create a happy, prosperous future for you, your family and your community.

The Intel Security Team