



InfoGovANZ

HINDSIGHTS & INSIGHTS REPORT

Information governance reflections on 2020 and insights for 2021



Information Governance ANZ

INTRODUCTION



With the benefit of 2020's hindsight, we can now fully appreciate the impact of the year on us as individuals, in the workplace, across nations and globally. We've seen differences in the way governments have responded to the COVID-19 pandemic and the results in managing the pandemic. Similarly, organisations have had to adapt to the changes and, in particular, to faster digital transformation. Robust governance of organisations and of information has never been so important. Increased cyber risks and the importance of access to real-time and accurate data for decision-making, both at the board level and throughout the organisation, are now critical issues.

As we enter 2021, InfoGovANZ reflected via a virtual forum on the key information governance (IG) learnings from 2020 and the insights and actions we must take to leverage opportunities and challenges going forward. This followed our inaugural virtual forum in May 2020, which was our first online event during COVID-19.

Read the report to see how prescient we were in identifying key issues for 2020 [Information Governance + COVID-19 Roundtable Report - InfoGovANZ](#)

I'd like to thank the leading experts who contributed their insights in the 2021 forum: [Sarah Auva'a](#), [Bryn Bowen](#), [Dr. Peter Chapman](#), [Ronke Ekwensi](#), [Dean Gonsowski](#), [Enzo Lisciotto](#), [Aurelie Jacquet](#), [Richard Kessler](#), [Andrew King](#), [Sonya Sherman](#) & [Daimhin Warner](#).

Susan Bennett
Founder & Executive Director

CYBERSECURITY & IG

Dr. Peter Chapman



Peter's insights:

- Massive social and political upheaval across the globe, combined with equally large changes to our standard business processes, created a perfect storm scenario for cybercrime and data breaches by well organised cybercrime gangs, as well as nation-state actors.
- Many are predicting that even post-COVID, we will see knowledge workers increasingly working from home, effectively flipping the concept of 'BYO device' on its head. Organisations now need to be aware of home working environment security as much as BYOD issues.
- The good guys are currently losing the battle for online security - we have seen the rise of 'malware-for-hire', more targeted ransomware attacks and highly sophisticated attacks on the 'supply chain' of software updates (SolarWinds) - demonstrating that not even the experts (FireEye) and 'secure' government agencies are immune from such threats.

Actions for leaders

- Be realistic about cyber-based threats and consider breaches as a question of 'when' and 'what' rather than 'if.' What changes do you need to make, with regard to your core Internet operations and approaches to technical data management, to significantly reduce this threat? (for example, Tim Berners-Lee idea of 'data-pods' and decentralisation).
- Ensure your organisation has really covered the basics of data management (what do we have, where is it, who has access, how is it protected and when do we get rid of it). Given the current state of play, holding onto sensitive data unnecessarily may end up being more damaging than not having access to that data in the first place.



TRUST & INFORMATION

Sarah Auva'a



In the world of data privacy, unfortunately trust and confidence in the way that organisations use data was already low leading into 2020. In New Zealand, [Privacy Commissioner research](#) showed only 32% of people trusted companies with their data in 2018, while [Pew Research Center](#) in the U.S. found that 79% of Americans have concerns about how their data is used, with 81% perceiving the risks of data use outweighing the benefits.

Then add to that the events of 2020 which led to unprecedented levels of sharing, collecting and using sensitive personal information due to COVID-19 and contact tracing, working from home and to the need to control and prevent protests and civil unrest.

Sarah's insights:

- The potential for data sharing to provide benefits to individuals and communities, but also raised questions to consider. Do we share sensitive information about our health status, location and contacts with organisations and governments to help fight COVID-19 and potentially benefit ourselves and others? Do we trust governments to use the information effectively to battle COVID-19 and to keep it safe from potential loss, misuse, or abuse?
- Poorly designed or hastily constructed COVID-19 data collection initiatives (from businesses creating contact registers to organisations attempting to repurpose data sets, such as location data collected for other reasons, to governments failing to consider how contact tracing data may be reused) can not only fail to achieve the desired outcome, but can undermine the confidence of individuals in contact tracing systems more generally.
- Surveillance became a hot topic with employers seeking ways to monitor the performance of millions of people working from home. Invasive surveillance techniques by employers can undermine relationships between employers and employees, and fears of unemployment and a recession helped to subdue employee resistance.
- It's possible for governments to harvest and repurpose personal information in ways that violate human rights, harm people and drive civil unrest, particularly with the assistance of artificial intelligence (AI) and facial recognition technology.

As we step into 2021, we are more dependent than ever on digital technology and are creating bigger digital footprints. Data sharing will continue to play a key role in mitigating COVID-19. Not only will contact tracing continue to be a focus, but sharing of immunity and vaccination status information, as well as validation of that status, will become hot privacy topics in 2021. Most people accept that data sharing is inevitable, but people are also looking to their government to make it safer. In [2020, 65% of New Zealanders](#) and [75% of U.S. respondents](#) support additional privacy regulation.



Key questions for leaders

- What would it take to rebuild trust in your organisation to enable safe data sharing to benefit us all?
- What do you think governments and regulators need to do to enhance regulatory frameworks to provide individuals with confidence, autonomy, and safeguards to facilitate data sharing?
- How will your organisation showcase compliance with data and privacy regulations and provide stakeholders with confidence that systems work and companies can be trusted?
- What are you doing or not doing that will impact the trust that individuals are willing to place in you going forward?
- How can you further use privacy enhancing technologies to minimise information collection and impact?

Given what's at stake, 2021 is the year to tackle the question of trust as if our lives depend on it.



UNLOCKING DATA VALUE

Ronke Ekwensi



If there is anything that 2020 taught us, it is companies must have the agility to react to the unpredictable. The COVID-19 pandemic forced companies to address both the monetary and social value of data.

Ronke's insights:

- Value of data in driving digital transformation - the pandemic forced many companies to accelerate their digital transformation strategies. This mostly focused on how use technology to improve customer experience, create new products and significantly deepen understanding of their customers. This requires complete and accurate data that allows organisations to drive transformation initiatives.
- Value of data in driving social good - the era of big data has shifted the traditional data collection paradigm, with more data in the hands of private corporations than government and research organisations.
- Data collected by private and public companies, while valuable for advancing commercial interests, is also valuable for social good. As we move through the COVID-19 pandemic, there are numerous examples of this data malleability, for example, location data is useful for digital contact tracing to arrest the progress of disease spread. In the same way in which companies give away cash through corporate giving programs, they should consider giving away data for social good.
- Importance of good data management and governance - there is a distinction between data management and data governance. Management involves how to make sure data is useful and fit for purpose within an organisation. It includes quality management, metadata capture to accelerate data consumption patterns and other processes, such as security and monitoring. Data governance is more focused on appropriate use and controls (i.e., people and processes). Organisations have to do both in an integrated fashion to ensure that data moves from bits and bytes to useful information that drives decision-making.

Suggestions for leaders

- Shift your focus and don't attempt to "boil the data ocean". Instead, invest in the data that is critical to advancing digital transformation. These investments should focus on data completeness and include external data asset acquisition.
- Consider: (1) assess the value of your data for driving social good and (2) invest in advancing regulatory frameworks that allow you to share data for initiatives that promote societal welfare in ways that balance protection and privacy concerns.
- Your focus on data governance should be multitiered including defining working groups, councils and executive steering committees, that reduce bureaucracy and ensure appropriate escalation to enable timely decision-making. The focus should be on enabling results.



ETHICS & IMPLEMENTING AI RESPONSIBLY

Aurelie Jacquet



In the past few years, there has been a proliferation of AI ethics principles developed by many different actors (e.g., private companies, governments, intergovernmental organisations, civil society, etc.) that has mostly helped with:

- Defining a north star for the adoption and use of the powerful technology that is AI;
- Identifying the level of commitments/expectations of the various actors; and
- Identifying areas of consensus.

Aurelie's insights:

- When considering a technology such as AI, predicted to add \$15 trillion to the world's economy¹, form a part of our everyday life and is the subject of global governance efforts², identifying areas of consensus is a valuable exercise. In January 2020, to uncover these areas of consensus, the Berkman Klein Center created a visualization tool called 'Principled AI'.³ (As a result of this exercise, they "uncovered eight key thematic trends: privacy, accountability, safety and security, transparency and explainability, fairness and nondiscrimination, human control of technology, professional responsibility, and promotion of human value."⁴)
- There are growing concerns that "principles alone cannot guarantee ethical AI."⁵ In his article, Brent Mittelstadt, Senior Research Fellow at the Oxford Internet Institute, challenges whether ethics principles are appropriate for AI, and explains that "the real work of AI ethics begins now: to translate and implement our lofty principles and, in doing so, to begin to understand the real ethical challenges of AI."⁶
- 2021 is likely to be a year focused on operationalising AI principles, but also a year where we see more often 'AI in court,' reminding us that decisions automated by AI are still subject to existing laws. Even if the AI model used is a black box, organisations still need to demonstrate that the recommendations or decisions made were reasonable and in compliance with the applicable laws. To quote the Australian Human Rights Commission, "*any business should ensure that its decision-making is fair, accurate and avoids bias or discrimination. This proposition should be equally true for decision-making that uses AI systems.*"⁷ The reminder that AI is not lawless came as early as

1 "AI Will Add \$15 Trillion To The World Economy By 2030," Frank Holmes, Forbes, published 25 February 2019, see <https://www.forbes.com/sites/greatspeculations/2019/02/25/ai-will-add-15-trillion-to-the-world-economy-by-2030/?sh=1e08840a1852>

2 "AI & Global Governance: Using International Standards as an Agile Tool for Governance," Peter Cihon, UNU-CPR Centre for Policy Research, published 8 July 2019, see <https://cpr.unu.edu/publications/articles/ai-international-standards.html>

3 "Principled Artificial Intelligence, Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI," Jessica Fjeld, Adam Nagy, Nele Achten, Hannah Hilligoss, Madhulika Srikumar, Berkman Klein Center, published 15 January 2020.

4 Ibid 2

5 "Principles alone cannot guarantee ethical AI," Brent Mittelstadt, Oxford Internet Institute, University of Oxford, Article in Nature Machine Intelligence, published in November 2019, see <https://www.nature.com/articles/s42256-019-0114-4>

6 Ibid 4

7 "Businesses warned AI use risks breaches of anti-discrimination laws," James Eyers, Australian Financial Review, published 24 November 2020, see <https://www.afr.com/technology/businesses-warned-ai-use-risks-breaches-of-anti-discrimination-laws-20201120-p56gjj>



January this year when an Italian court found that Deliveroo's rider-ranking algorithm was in breach of local labour laws as the algorithm would penalise riders who cancelled pre-booked rides less than 24 hours even in circumstances where riders are sick or had to attend to an emergency⁸. This case reemphasises the need for organisations to 'build in compliance,' especially when it can be a costly exercise to retrain machine learning models.

Actions for leaders:

To implement AI responsibly in 2021, while technical requirements, such as data quality and model performance remain essential, focus strongly on broader organisational processes and controls, such as reviewing the adequacy of existing governance processes, embedding dynamic risk management and impact assessments to ensure better oversight of AI, mitigating risks and achieving compliance by design.

⁸ "Italian court rules against "discriminatory" Deliveroo rider-ranking mechanism," Natasha Lomas, published 5 January 2021 Techcrunch, see <https://techcrunch.com/2021/01/04/italian-court-rules-against-discriminatory-deliveroo-rider-ranking-algorithm/>



GLOBAL DATA PRIVACY & ENFORCEMENT

Dean Gonsowski



Dean's insights:

For the last two decades, the U.S. turned a blind eye to data privacy, rejecting its impact as a fundamental human right. The pendulum has swung quickly, with global privacy laws now the norm. Anyone - or any company - who wasn't on board before, got on board in 2020, or at least now recognises the strong consumer and legislative demand for data privacy.

There will be increased enforcement of privacy laws. That was always a question with the California Consumer Privacy Act (CCPA) – how enforcement was going to happen. The California Privacy Rights Act (CPRA) will accelerate the need to become compliant much more quickly as it has a regulatory enforcement arm.

Actions for leaders:

From a technology perspective, you need to think differently about how you collect, maintain, minimise and govern your data since the CPRA has an implied data minimisation theme akin to the European Union's General Data Protection Regulation (GDPR).

PRIVACY DEVELOPMENTS IN ANZ

Daimhin Warner



Daimhin's insights:

The evolution in global privacy regulations will continue - since the EU's GDPR, we witnessed the phenomenon of 'GDPR-isation,' the development of myriad privacy laws around the world intended to meet or exceed the high-water mark set by the GDPR. Examples include India's upcoming Personal Data Protection Act, Brazil's General Data Protection Law, and, of course, the UK's GDPR (designed to mirror the EU's GDPR post-Brexit). This explosion of privacy regulations is essential for the maintenance of a functioning global economy, fuelled by the sharing of personal information across borders.



In NZ

- ANZ was no exception - the NZ Privacy Act 2020, which commenced in December 2020, moves NZ further along the regulatory spectrum, introducing mandatory privacy breach notifications, limitations on cross-border data transfers and extraterritorial effects, and providing the NZ Privacy Commissioner with increased enforcement powers. 2021 will be all about the bedding in of this new Act.
- We will see increased enforcement action from the Privacy Commissioner as he flexes his new regulatory muscles - importantly, we will also learn in 2021 if NZ has retained its EU Adequacy status. This coveted status means that organisations in the EU may transfer personal information to NZ organisations in compliance with the GDPR without having to put any other measures (such as Standard Contractual Clauses) in place. This is critical to NZ's rapidly growing community of innovative start-ups and the software as a service (SaaS) products they develop for a global market.

And in Australia

- The Australian Privacy Act 1988 is under review, with lawmakers considering a host of major changes intended to bring the Australian law up to global standards. Possible amendments will include removing the somewhat unbelievable small business and employee exemptions, thereby broadening the reach of the law to cover most, if not all, organisations and individuals in Australia. The review will also reflect on the operation of the mandatory breach notification regime introduced in 2018 to ensure it is meeting its objectives. We can expect an update in the coming months, reflecting submissions received from public and private sector agencies across the country.
- In both Australia and NZ, we are also likely to see further developments in the areas of data portability (referred to this side of the world as the 'consumer data right'), ethics in AI and algorithms, indigenous approaches to privacy (led by efforts to better understand and address Maori data sovereignty in NZ), and the regulation of big tech companies, such as Google and Facebook.

Actions for leaders:

Organisations and the experts supporting them need to learn the new laws and ensure your processes and procedures comply.



ACCOUNTABILITY & IG

Sonya Sherman



Sonya's insights:

At last year's Roundtable, Sonya pointed out three priorities for information governance:

- *Connectivity* - had to do with maintaining business as usual during the shift to digital and remote working. Organisations in 2020 quickly realised that access to reliable information was just as important as access to technology. Rapid digital transformation has been broadly successful in knowledge industries and laggards did a lot of catching up over the past year. But we also saw innovative use of data and technology in sectors that previously relied on in-person interaction. Think about orchestras and choir groups; personal trainers; real estate auctions; Cabinet meetings; and Parliament. Moving forward, we're seeing connectivity transition to creativity, with new types of digital products and services coming into play. This is going to have flow-on effects for information governance and regulation.
- *Sustainability* - ensured the systems and processes put in place last year will help maintain good governance across a remote workforce and a distributed information ecosystem for the longer term. The jury is still out on this one. Rapid transformation in some cases will mean data and information have 'slipped through the cracks.' It's likely some organisations are suffering major challenges with version control, with increased risks of data leakage or data breaches. It's likely we'll never go back to working the way we used to, but this doesn't mean we will all remain working remotely.
- *Accountability* - recognised the critical importance of keeping records during the crisis, even though it may seem more difficult than usual. Last year, Sonya noted that every decision and action would potentially come under scrutiny and we've certainly seen a lot of inquiries already, with, no doubt, more to come. We've also seen the benefits of keeping records, to learn from and adjust our actions through successive virus waves. Accountability will transition to transparency and organisations or governments that communicate very openly with staff or citizens and provide regular, reliable information will build trust that helps them meet their goals. Trust will break down when information is withheld or people have doubts about it.

We are also seeing the advantages of sharing data and information to enable contact tracing and to rapidly develop vaccines. It's really important that people can trust systems and processes to maintain data integrity and protect their personal information at this time.

There will be growing awareness of the value IG brings to organisations, government and communities. The pandemic is having a huge impact on the way we live, the environment and global politics. Maintaining accessible records and data about this period in history continues to be vitally important for our future world.



Questions for leaders

- **Connectivity and creativity:** Given the new types of digital products and services coming into play, are you ready for the flow-on effects for information governance and regulation?
- **Sustainability:** You will see sustainability transition to scalability. Will your IG systems and processes support a hybrid workplace, where some people are in the office and others are anywhere else.
- **Have you carried out a reconciliation,** that is, cleared out the redundant, obsolete and trivial (ROT) and duplicates?
- **Accountability and transparency:** Have you got a communications culture that builds trust? Information sharing leads to better business outcomes.

COLLABORATION & IG

Bryn Bowen



Bryn's insights:

- 2020 was certainly a year of acceleration of some long-awaited advances in how technology could be used to improve metadata enrichment and analysis. We saw the knowledge-related workforce become largely virtual, which led to the rise in the deployment of collaboration platforms along with the attendant IG issues, ranging from intra and extra enterprise security considerations to access rights management and the need for proper provisioning to reduce information proliferation.
- We also saw project realignments to reflect shifting priorities brought on by the pandemic, such as accelerated infrastructure moves to the cloud and the already mentioned increased digitisation. We also saw the use of AI enabled technology to mitigate effects of the shifting workforce stance, such as virtual support functions around knowledge workers and vastly improved functionality, like task suggestions in Office 365, empowering the governance of information in a significant way.
- There will be an acceleration of the changes already started in 2020, particularly with added functionality to collaboration replacement tools and the governance considerations and requirements that will need to be put in place.
- For new organisations, there will be an increased level of awareness of the need for IG frameworks, as this becomes more of a foundational necessity due to the virtual workforce. This will also lead to more thoughtful implementation and adoption of technology, with a greater focus on end user needs and overall user experience.
- Virtual workplace collaboration among knowledge workers has grown exponentially due to the restrictions demanded by logical response to the pandemic. Even after the pandemic subsides, significant virtual collaboration will be part of the new normal.

Action for leaders

In order to ensure maximum positive effect and also take advantage of some of the value-added elements of virtual collaboration, a thoughtful, well-guided creation of a proper IG framework is critical.

LEGAL TECHNOLOGY & EDISCOVERY

ADAPTING TO TECHNOLOGY

Andrew King



Andrew's insights:

- For some, the disruption of COVID-19 was the catalyst for change that many resisted for so long. Those that were reluctant to innovate or invest in technology now appreciate why they need to and the value of investing further going forward.
- Overnight, technology became a lifeline as everyone had to work differently - and remotely. Barriers to change quickly disappeared, as many were forced to make changes within weeks that previously may have taken years to implement. Unsurprisingly, many that had not previously innovated or leveraged legal technology struggled, with some battling to even enable their staff to work from home.
- Even though some courts closed, or transitioned virtually with eDiscovery, those that had access to cloud solutions were able to seamlessly conduct eDiscovery, with remote review being possible wherever your location. The experience of COVID-19 has demonstrated how essential it is to have access to your eDiscovery tools, no matter where you are physically located.
- While 2020 reinforced why we need to innovate and leverage technology, the focus for 2021 is how we can go about this. As the pandemic accelerated the rate in which firms have been adopting technology, there is now the opportunity to continue the adoption - and clients will now expect this!
- The volumes and sources of data will continue to evolve, so it is important to adapt with this and not be tied to traditional practices. The adoption of Zoom, Microsoft Teams and other collaboration tools will present new data sources and challenges for the eDiscovery process.

Considerations for leaders

- With today's proliferation of data volumes in eDiscovery, it is important not to focus solely on the technology itself, but to be smarter in how eDiscovery is approached, together with continuing to refine and improve how you approach the process. This requires considerably more work earlier in the discovery process to prevent the cost and burden from spiralling out of control. The time invested at the outset could save you thousands down the track and lessen the burden.
- Remain curious and open to change and always look at how you can do this better.



THE DATA EXPLOSION & IG

REDUCING EDISCOVERY COSTS

Richard Kessler



While common sense tells us that the overall duplicative data should be *decreasing* in line with the pace of technological advancements, this is not the case. There has been an explosive *growth* in data, which consists of primarily duplicate data rather than uniquely created data, at roughly a ratio of 1:9 and expected to grow to 1:10 in 2021. According to the International Data Corporation (IDC), in 2020 alone, more than 59 zettabytes (ZB) of data was created, captured, copied and consumed in the world.

Richard's insights:

- Despite trends like these, many companies continue to use 'traditional' approaches to eDiscovery and have done little to put in place powerful and effective information governance functions. Although many innovative capabilities within the eDiscovery process have been invented and applied, firms have not yet been able to check their own organisations' explosion of data through the operationalisation of data minimising strategies.
- In addition, many firms simply can't measure their total storage or corresponding actual data requirements because so much data is in the cloud and/or part of their actual supply chain or data supply chain. Although relied on very heavily for day-to-day operations, it is with seemingly minimal financial impact until a data breach occurs or significant costs are involved in a large document production for litigation or regulatory inquiry.

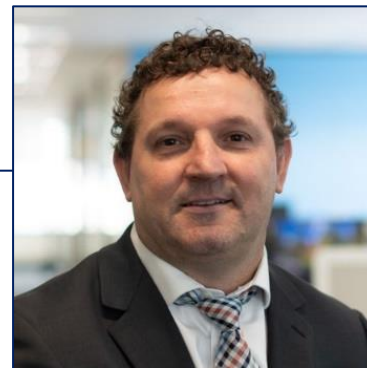
Action for leaders

- Unsustainable growth and proliferation of your data across the supply chain and across a sea of clouds challenges you to identify and protect the most important data and to distinguish your more important assets from your junk. Without knowledge of where to direct investment for protection and reuse, for example, to pivot your business model out of COVID-driven necessity using your data, you are 'flying blind.'
- You need to operationalise information governance and give laser-like focus to critical asset identification to radically simplify and reduce eDiscovery costs and help unlock and unveil your most important data assets for reuse (after de-risking), repurposing, monetisation and other such revenue and value generating activities.
- Start thinking more strategically about data or succumb unwillingly to chaos, potentially exposing critical assets to unnecessary threats and leaving tremendous value untapped.



EDISCOVERY & SECURITY

Enzo Lisciotto



Enzo's insights:

- Working from home has meant that there has been forced changes in the way organisations deal with and manage eDiscovery technology. There has been an increased adoption in cloud-based SaaS eDiscovery solutions, which we saw at Nuix really take-off in 2020, as opposed to the previous hardware-based, on-premise model, and the increase in demand for SaaS solutions will likely continue in 2021. As organisations are looking into or adopting a cloud first approach to their IT data management, the enablement of an eDiscovery cloud SaaS solution for their discovery projects means less internal pressure when managing hardware, storage, backup and disaster recovery for on-premise environments.
- Cloud-based solutions will continue to drive innovation with more engineers and product designers developing solutions to provide greater innovative capabilities around processing of data at lightning speed. Processing speed will support in parallel the ever-growing number of data types needing to be included within eDiscovery cases and the amalgamation of technology products to work seamlessly between multiple solutions.
- Although many hurdles were surmounted in 2020, like data collection remotely as opposed to physical collection and risk of data theft through ransomware, data breach, data leak, etc., COVID-19 will continue to force and accelerate organisations to provide new technology solutions remotely to their employees and/or clients.

Suggestions for leaders

With regard to managing your security risks, outsourcing to cloud-based SaaS eDiscovery solutions will reduce cyber risks, provided appropriate due diligence is carried out to ensure providers have in place best practice cyber management protocols that comply with the relevant laws and standards, such as the Australian government standard, Information Security Registered Assessors Program (iRAP), as well as ISO 27001 of the International Organisation for Standardisation.



IT'S A WRAP! 7 INFORMATION GOVERNANCE TAKEAWAYS FOR 2021

Susan Bennett

Given the expected ongoing complex and uncertain operating environment in 2021, robust information governance is needed to provide a system for the effective control and management of information assets to enable access to real-time and accurate information, as well as optimise data assets and value-generating activities while minimising risks.

This will enable the optimum:

- **Board oversight with access to real-time information and data for decision-making** - COVID-19 highlighted the need for access to real-time information for decision-making, notwithstanding ongoing complexity of operating environments.
- **Integration of information security and regulatory compliance** - a holistic strategic IG framework is needed to govern and effectively align data, information, compliance and technology together with policies, processes and people.
- **Data optimisation through complete and accurate data** - organisations need to be focused in investing in the data that is critical to advancing digital transformation and driving transformation initiatives.

7 Information Governance takeaways for 2021

1. **Implementation of AI responsibly** - governance processes must adequately embed dynamic risk management and impact assessments to ensure better oversight of AI technology and properly mitigate risks to achieve compliance by design.
2. **Cybersecurity will continue to be a significant challenge with increasingly sophisticated attacks on organisations** - working from anywhere has increased cybersecurity risks and ensuring employees have regular cyber and privacy training is essential to creating and maintaining a culture of data privacy, data protection and security with full compliance of policies and procedures.
3. **The explosion of data being collected and generated by organisations, together with the relentless nature of cyberattacks, will continue to pose substantial risks to organisations, particularly in the event of a data breach** - it is essential that information be governed through its lifecycle - collection, protection and use, security, archive and disposal. In 2021, the combination of regulations, data volumes and the increasing focus on understanding what data to optimise and what is ROT will lead to an increased understanding and action in secure disposal to minimise organisational risks.
4. **Development of new technologies, particularly those that enable increased collaboration, will continue to rise and create efficiencies with work productivity** - be mindful that they also present information governance challenges and are already resulting in rising eDiscovery costs in legal proceedings.
5. **Organisations and law firms will need to be smarter in how eDiscovery is approached** - investing in earlier strategic work in the discovery process to prevent the cost and burden spiralling out of control.



6. **Working from anywhere has highlighted the importance of physical interaction for incidental learning, mentoring and social interaction** - this requires careful planning for future workplace design and governance of systems and people.
7. **Changing privacy regulations will continue toward the EU's GDPR standard** - in addition to the review of Australia's Privacy Act 1988 (submissions received in response to the Issues Paper are [available here](#)) and New Zealand's updated Privacy Act coming into force on 1 December, the following has occurred so far in 2021:
 - China's Civil Code took effect on 1 January providing a statutory right of privacy for individuals and establishing data protection principles
 - Indonesia's Personal Data Protection Bill was submitted to the House of Representatives
 - Singapore's Amendments to the Personal Data Protection Act (PDPA) took effect on 1 February, with accompanying regulations published on 29 January 2021 - strengthens organisational accountability and consumer protection while enabling organisations to use personal data for innovation
 - India's Personal Data Protection Bill 2019 is expected to be tabled in an upcoming parliamentary committee budget session.

The sped up digital transformation of 2020 gave us an insight to the workplace of the future and the importance of robust information governance and both online and physical connectivity.



Moving into 2021, InfoGovANZ calls on information governance professionals working across the information, data, regulatory and technology facets to step up and ensure that systems and governance in their organisations are adequate, integrated and enable information assets to be maximized while risks are minimized.



About InfoGovANZ

Join InfoGovANZ to tap into the latest developments and global thinking across the sphere of information governance. Comprised of leading international multi-disciplinary professionals, join [HERE](#) to grow your network and stay on top of global innovation and best practice to ensure you're best placed as a leader to step up to drive the delivery of better outcomes for your organisation by minimising risk and maximising the value of the information held.

Contact:

P +61 2 8226 8546

E infogovanz@infogovanz.com

W <https://www.infogovanz.com>

InfoGovANZ SUPPORTERS

GOLD PARTNERS



SILVER PARTNERS



EDUCATION SUPPORTER

