LexisNexis Capital Monitor provides parliamentary, political, legislative, regulatory and judicial news and information to its subscribers as soon as it happens. The team is located in the Press Gallery of Parliament House, Canberra.

LexisNexis® Capital Monitor’s editorial team prepares the Advancing Together, Rule of Law Updates and Perspectives from the Asia Pacific bulletin. The team is located in the Press Gallery of Parliament House, Canberra.

Simon Wilkins
Managing Director, Australia

Antoaneta Nina Dimitrova
Product & Content Manager, Capital Monitor

Jenna Allen
Editorial, Capital Monitor

Esther Lam
Social Media and Communications Specialist

Maggie Batacan
Communications Specialist

Michelle Santos
Graphic Designer

LexisNexis partners with the Cook Islands on legislation consolidation project

The challenge of cyber

Why do we need innovation in law?

LexisNexis establishes global foundation to advance the rule of law

Aspects of transparency, appropriateness and proportionality plague new data encryption laws

Why taking a scorched-earth approach to social media companies won’t win the online war on terror

Internet access and the role it plays in civil society activism in the Asia Pacific

Tensions between secrecy and transparency in cyber conflict remain complex yet must be balanced

Disability Discrimination Commissioner Q&A
Hello and welcome to the December 2019 edition of Advancing Together.

Our second half of the year has been as busy as ever and it is always a privilege to share some of the really great projects we have taken part in along the way.

We continued our tradition of embarking upon our annual thought leadership event series. This year’s theme was “Decoding Cybersecurity: Clause & Effect”, with the aim of finding out how cybersecurity and the surging importance of data privacy and the protection of data has affected the legal profession and society at large.

We heard some fascinating insights about what lawyers and cybersecurity experts felt about the current legislative environment, their thoughts on how to best respond to a data breach and also where this space would be going from a legal and practical perspective. It was an extremely interesting discussion and you can read more about our findings in our Roadshow Report [here](#).

We have also celebrated some remarkable achievements in our Rule of Law activities.

In September, we conducted our first-ever business-wide Rule of Law Hackathon as part of our global Rule of Law initiative. Our teams were invited to contribute first-hand to the development of rule of law analytics by creating data-science models to feed into our in-house machine learning teams. It was a huge success and we can’t wait for our next hackathon to take place!

We were also very proud to continue our partnership with the Australian Human Rights Commission team. In August we were thrilled to announce the launch of the Vietnamese version of RightsApp, the world’s first human rights mobile phone app which allows users to quickly and easily search international human rights conventions and legislative instruments. This was a project we had partnered with the Australian Human Rights Commission almost three years ago and it is fantastic to see this mobile application become more readily accessible to the people of Vietnam.

We hope you enjoy this new edition of Advancing Together and we look forward to bringing you more updates about our initiatives and how we can continue to advance the rule of law around the globe.
LexisNexis is delighted to announce winning a tender to partner with the Cook Islands Government to begin consolidation of the South Pacific nation’s legislation.

Led by LexisNexis Executive Director, Myfanwy Wallwork and Executive Manager Jenny Williams, a team of five will travel to the Cook Islands in late January 2020 to undertake the initial scoping, including Operations Manager Katherine Pearson, Legislation Tech Lead Adele Mcatee, and Senior Legal Counsel Kim Nguyen.

Access to an accurate and updated legislative database is an important underpinning of the rule of law.

“In countries like Australia and New Zealand, where legislation is readily available from multiple sources, we can sometimes take this for granted,” LexisNexis Executive Director, Myfanwy Wallwork said.

“It is difficult to imagine the challenges the legal profession and society in general face when even senior members of the judiciary...
or legislative drafting teams do not have absolute clarity over what the law is."

Supporting other countries with similar projects, LexisNexis understands the challenge increases significantly for those without legal training, attempting to go about their daily lives, running businesses, or interacting with government processes.

"Jenny, Kat, Adele and I were all fortunate enough to work on the consolidation of the Laws of Fiji, an 18-month project which resulted in 20 loose-leaf binders comprising 30,000 pages, that provided an authoritative, consolidated version of the country’s legislation for the first time in 31 years," Ms Wallwork said.

Earlier in 2019, another LexisNexis employee, Principal Product Manager Mary Wong, worked with the Office of the Attorney-General on a dedicated website, making the laws freely available to the people of Fiji.

"We are very pleased to have Kim on her first in-country visit to support the rule of law in the Pacific, Ms Wallwork added. Meetings will be held with a variety of people, including the Solicitor-General and senior Crown Law Office team, the Judiciary, Law Society and Legal Aid. The team hopes that by speaking to this wider group, LexisNexis will be better able to support the Cook Island Government in meeting the stated goal of the project to strengthen the rule of law in the country.

Over the medium and long term, this will be done through:

• Strengthened capacity of Cook Islands legal and judicial system;
• Improved access to the laws of the Cook Islands; and
• Strengthened and promoted good governance.

Mary Wong, worked with the Office of the Attorney-General on a dedicated website, making the laws freely available to the people of Fiji.

"We are very pleased to have Kim on her first in-country visit to support the rule of law in the Pacific, Ms Wallwork added.

This first visit is essential to not only gather all the materials required related to the current state of the law – principal, subsidiary and amending instruments; operational dates and published, as offline accessibility such as that provided by Lexis Red is crucial when internet connections can be variable on a day-to-day basis. Other aspects will include the order in which the laws are published, for example, a court volume may be useful, as well as operational matters such as future publishing processes. This will ensure that the significant work to be done by the Crown Law Office and LexisNexis for the initial consolidation can be maintained with a plan for regular updating.

Meetings will be held with a variety of people, including the Solicitor-General and senior Crown Law Office team, the Judiciary, Law Society and Legal Aid. The team hopes that by speaking to this wider group, LexisNexis will be able to support the Cook Island Government in meeting the stated goal of the project to strengthen the rule of law in the country.

Over the medium and long term, this will be done through:

• Strengthened capacity of Cook Islands legal and judicial system;
• Improved access to the laws of the Cook Islands; and
• Strengthened and promoted good governance.

Meetings will be held with a variety of people, including the Solicitor-General and senior Crown Law Office team, the Judiciary, Law Society and Legal Aid. The team hopes that by speaking to this wider group, LexisNexis will be able to support the Cook Island Government in meeting the stated goal of the project to strengthen the rule of law in the country.

Over the medium and long term, this will be done through:

• Strengthened capacity of Cook Islands legal and judicial system;
• Improved access to the laws of the Cook Islands; and
• Strengthened and promoted good governance.

Meetings will be held with a variety of people, including the Solicitor-General and senior Crown Law Office team, the Judiciary, Law Society and Legal Aid. The team hopes that by speaking to this wider group, LexisNexis will be able to support the Cook Island Government in meeting the stated goal of the project to strengthen the rule of law in the country.

Over the medium and long term, this will be done through:

• Strengthened capacity of Cook Islands legal and judicial system;
• Improved access to the laws of the Cook Islands; and
• Strengthened and promoted good governance.
A few years ago, when in government, I talked a lot about digital disruption. It’s a term that has lost its weight in the broader narrative around technology, but it is no less relevant today than it was in the early to mid-part of our second decade on the twentieth century.

Digitalisation pervades everything we do, the environment in which we work. In 2011, venture capitalist Marc Andreesen observed that ‘software is eating the world’; if so, the product of this process is not the formation of skin and bone and tissue, like humans, but both unformed and more carefully structured data.

The value of data

Anything that can be quantified can be reduced into data, that in turn may be reformed, transformed and, if repetitive, automated. The reforming of data enables differing processes to be brought together in ways that we would have not normally thought possible. We may also create data that’s of value, and which may also be merged, altered and refined to create more data—and of course data about data. Data does not only attract other data, but itself can be generative, to the point that its provenance is lost. Unused, unreferenced, data can also sit in a block, consuming space and energy—and this is particularly the almost certain fate of the vast amount of unstructured data that cameras and other sensors unthinkingly collect. Estimates suggest that if not used within a month or two, unstructured data is never used.

The value of digitalised data lies in two forms

First, in its utility: the flow of data to meet some immediate or shorter-term need. For example, real-time banking, navigation guidance, health data, conversations with family overseas, networked logistics, more efficient and safer air travel, to name a few.

Second, as a source of truth, of calibration, of reliability: we know what’s in our bank accounts, data collected over decades help inform climate models; and we can replicate designs enabling both mass production and highly engineered parts.

CONTINUED
The vulnerabilities of data

Through technologies that create data, move data, transform data, store data and make it readily available, we have transformed our world in ways that have fundamentally changed our expectations and view of the world. But once our processes, lives, ideas, business operations and actions have been transformed into data, and live in systems, they are vulnerable to attack, contamination, corruption and theft in a way that had not existed before now, or had required action on the physical world.

While the pre-digitalisation world was no Eden, society had developed norms and the means to deal with such incursions. That’s much less the case now. And our thinking and ways of dealing with the vulnerabilities and damage that may be done to data and the technological and social systems that collect, hold, transform, manage and disseminate data now fall under the category of cyber.

The confidentiality, accessibility, and integrity of data and systems

One useful and readily clear way of understanding the challenges cyber poses in our digitalised world is thinking through the confidentiality, accessibility, and integrity of data and systems. Confidentiality is usually associated with national secrets, but applies no less to data that is personal, such as health and financial data or simply locational information; that is privileged, as in lawyer-client, doctor-patient or journalist-source relationships; or that is competitively sensitive, such as intellectual property or business client lists, for example.

Data needs to be accessible and available, for the purpose for which its designed or legitimately needed. When operating real-time sensitive operations, such as an airport, aircraft telemetry, radar and wind data needs to be available all the time, for example. Other data and systems may be less time sensitive, but critical to the functioning of government or other organisations and services, and their unavailability has real cost. The damage wrought by the NotPetya malware, estimated at over $US10 billion, is a case in point.

And data and systems need to retain their integrity: they need to be able to be trusted and relied upon, particularly as our society, economy and well-being are increasingly dependent on them.

Most news reporting on cyber tends to focus on the confidentiality aspects—what data were attackers after and were they successful. When data and systems need to be protected, that definitely is of concern.

But in many regards, availability and integrity are of greater, if less apparent concern. That’s often because the realisation and consequences of vulnerabilities, attacks and exploits take time to realise. Our less than ready ability to pre-empt or prevent incursions, damage and personal harm has long-term and systemic consequences: it breeds distrust and fatalism, which extends to our institutions. Consequently, at a time when there is a real need to build systemic, social and economic resilience, governments and organisations find they have less support, and fewer levers, than expected.

For the legal profession, there are a range of consequences

First, legal firms need to ensure the confidentiality, availability and integrity of their own data and systems. They need this to undertake their own with confidence, and to build and retain trust, an increasingly valuable business asset.

Second, legal professionals need to understand the nature and consequences of cyberattacks, infiltration and vulnerabilities. That is the world of both governments and clients, and as our dependencies on data and digital systems continues apace, cyber issues will continue to grow.

Third, governments across the West have shown a disconcerting willingness to seek to legislate the problems away. Cyber, however, is multi-faceted, global, deeply embedded in social, economic, technological systems, driven by a wide range of actors and interests outside national concerns, and not readily tractable to legal recourse. Consequently, much cyber-related legislation will have broader, unintended consequences for individuals, communities and societies.

There is need for a well-informed legal profession, able to grasp the nature of the problem and consequences of poorly considered legislation. And that in turn places the legal profession on the front lines of dealing with cyber in our modern world.
There are some degrees of cynicism when another law firm issues another press release regarding the next step on their innovation pathway. The latest foray into "Blockchain", "Artificial Intelligence", "Design Thinking" and "Smart Contracts" are touted as game changers placing their firm at the forefront of the re-invention of the profession.

The truth is that the profession isn’t being re-invented. Firms are delivering record profits, but with lawyers’ job satisfaction at an all-time low, and declining customer net-promoter scores, something must change.

What is innovation

The “innovation by press release” mantra indicates that firms understand the benefit of innovation and clients are seeking enhanced service delivery. So where are things breaking down?

The inhibiting factor may be a lack of understanding of the term “Innovation” and what it means to be innovative. To innovate is to explore creative ways of improving an existing process as opposed to “invention” which is to create something new. The art of innovation is to focus on self-improvement which in turn provides a richer client experience.

Legal services are transactional in nature, and many law firms see innovation as a single event. “We create something innovative and we charge you for it”. To focus on innovation as a transaction fails to realise the broader opportunity that is presented.

An approach to successful innovation

Law firms are starting to understand that innovation is a mindset that needs to be embedded culturally into the organisation for it deliver real benefit. Lawyers are beginning to open their minds to the opportunity and engage a mix of skills to achieve a tangible outcome.

Streamlining ways for clients to engage with firms may represent a significant opportunity to increase client satisfaction. Importantly, the opportunity to co-create solutions with clients can deliver untold benefits to the client/firm relationship. An exercise
leveraging multidisciplinary skills such as legal, process, user experience, product and technology to create a streamlined solution may result in clients choosing to brief your firm rather than competitors. “If you make it easy for clients to come to you, they will come to you more often” is the hypothesis for this approach.

That’s one example, but the point is that there are some fundamental points law firms should consider when approaching their innovation strategy:

1. Identify a known client pain point. Including clients in this discovery process is critical to obtaining the right perspective.

2. Ascertain multiple options to help mitigate the pain points, before agreeing the right one to take forward. Importantly some of these options may involve simple process changes, rather than complex technology implementations.

3. Ensure a multidisciplinary approach to ideation to broaden the perspective. Don’t be afraid to bring “non-lawyers” into the room.

4. Get the right validation of the solution. Don’t pre-suppose the solution you have created will be well received by everyone. Get feedback and iterate.

5. Ensure you see the most optimal solution through to execution. Too often the focus of events like “hackathons” are restricted to idea generation. The benefit is in the successful implementation of the solution, not the idea.

6. Ensure there is a KPI for the initiative. There should be something measurable to evaluate success to ensure it is delivering value.

Realising the value of innovation

Defining the value of an innovation initiative is something that law firms are starting to grasp as a measure of success. Recognising that clients do not come to law firms for their innovation expertise is an important point. You shouldn’t charge for innovation the same way you charge for legal service delivery, innovation should be seen as a way to enable your customers to more easily do business with you. If you succeed in delivering on this, clients will come to you more readily than go to competitors. This, of course, is the true value of an innovation initiative.

There are several ways firms can provide streamlined services to clients to deliver real value:

1. Matter on-boarding and management services. Make it easy for clients to brief you on a potential matter and allow them to manage budgeting expectations in a transparent manner.

2. Creation of digital advisors to allow clients to self-serve routine information for such things as contract approval and execution advice, legislative compliance, marketing campaign approvals and data handling and breach advice. These automated tools can allow your firm to be front-of-mind when there is an element of nuance, requiring specialist legal skills.

3. Provide reporting and data tracking for transactional services such as Litigation and M&A projects. Empowering clients to control their project status and spend management creates an increased level of trust between client and firm.

Firms should also seek to create solutions that are re-usable across multiple clients or sectors. For example, “A Marketing Approvals Advisor” is a generically applicable solution. The subtleties of the approval checklist will differ across clients, but the broad approach is the same potentially increasing the value of the solution created.

The way forward

True innovation is an important competitive advantage for any law firm. Recognising that the art of innovation needs to be culturally embedded into the firm and not just sit with an “innovation manager” will help ensure success.

A multidisciplinary approach is an important component of the innovation process to connect pain points to the right outcome. Understanding how to derive value from your innovation initiatives will help determine the investment required, both in terms of money and time.

Those firms that have a strategy incorporating these key elements will better position themselves for the future of legal service delivery.
I am delighted to share news of the LexisNexis Rule of Law Foundation, a not-for-profit entity established in 2019, to further achieve the LexisNexis Legal & Professional mission to advance the rule of law around the world. This new public charity, dedicated to engaging in Rule of Law projects across the globe, will enable leading entities from the legal, judicial, academic, NGO and other sectors to support and implement projects that address one or more of the four rule of law components: equal treatment under the law, transparency of the law, access to legal remedy, and independent judiciaries.

LexisNexis has been strongly committed to advancing the Rule of Law through projects such as the United Nations Global Compact’s Business for the Rule of Law Framework (B4ROL).
More than half of the world’s population lives outside the shelter of the law, struggling for basic human rights. Each of us shares responsibility to bring this percentage down to zero, ensuring vulnerable and disadvantaged populations receive equal treatment within criminal and civil justice systems.

In 2017, the company received the Corporate Leadership Award from Freedom House and its Global Legal Department won the Financial Times Innovative Lawyers Award for advancements in the rule of law. The establishment of the LexisNexis Rule of Law Foundation is an extension of its commitment to build legal infrastructures and solve deep-rooted problems in holistic ways that will achieve more robust outcomes and advance the rule of law.

"Rule of law is foundational to the development of peaceful, equitable and prosperous societies," says Mike Walsh, CEO, LexisNexis Legal & Professional. "Data from the LexisNexis Rule of Law Impact Tracker shows that when the rule of law is strong in a country, other positive social and economic factors within the country are also strong. It is our hope the LexisNexis Rule of Law Foundation will provide the necessary resources and support to shed light on emerging issues critical to advancing the rule of law around the world."

To help accomplish this, the LexisNexis Rule of Law Foundation will include collaborations with organizations to help increase awareness and understanding of the rule of law. LexisNexis announced the Foundation’s first partnership with The Global Investigative Journalism Network (GIJN), an international association of journalism organizations that support the training and sharing of information among investigative and data journalists – even in repressive regimes and marginalized communities. LexisNexis will offer GIJN members access to one of the world’s largest electronic databases and analytic tools for legal, public-records, news and business information.

"We’re thrilled to partner with The Global Investigative Journalism Network and provide their journalists with access to the most comprehensive set of information tools at a discounted rate. More than half of the world’s population lives outside the shelter of the law, struggling for basic human rights. Each of us shares responsibility to bring this percentage down to zero, ensuring vulnerable and disadvantaged populations receive equal treatment within criminal and civil justice systems. Working together with GIJN will allow us to build greater awareness of the rule of law and strengthen watchdog reporting around the world," says Ian McDougall, President of the LexisNexis Rule of Law Foundation.

To learn more about the Rule of Law Foundation, visit www.lexisnexisrolfoundation.org.
LexisNexis® Rule of Law Foundation

is the not-for-profit entity established by LexisNexis Legal & Professional to further achieve its mission in advancing the rule of law around the world.

BUT WE CAN’T DO THIS ALONE.

We need your support and care to help us achieve our purpose.
Visit https://www.lexisnexisROLfoundation.org and be involved.
On 6 December 2018 the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the Bill) passed both houses of the Australian Parliament. This was not without controversy. Digital technologies have enabled many aspects of our professional and social lives. These benefits have also been exploited by criminals in pursuit of their activities and avoiding detection. There were many submissions prior to the Bill being passed and, while most acknowledged the critical importance of law enforcement and national security agencies having appropriate powers to carry out their functions, they questioned aspects of transparency, appropriateness and proportionality.

The survivability of law enforcement agencies depends on the public’s trust and confidence in them. As citizens in a democracy, we give police legitimacy to enforce laws. The public have an existing perception of police based on seeing uniformed officers in a variety of situations. This high-visibility makes people feel safer. How they perform in these situations impacts consumer sentiment, including impressions towards the granting of additional police powers. But how does this translate into the online environment? And what is the broader impact as we spend more and more of our lives online, including social media, e-commerce and as recipients of government services? More broadly there has been a decline in public confidence in the capacity of the government to address public policy concerns in Australia.

Although there are many aspects to focus on, I believe necessity is the most important. Law enforcement and national security agencies have long argued that the Assistance and Access Act (the Act) is necessary as they see, for example, encrypted communications being a part in many investigations involving serious and organised crime. But this alone does not make the law necessary. In the debate during the drafting of the Bill, Australians were never told in any granularity how many investigations did not proceed or were unsuccessful in court due to lack of evidence that would have been available because of access to encrypted communications. Following on from this, Australians should also

CONTINUED

Nigel Phair
Director,
UNSW Canberra Cyber
be informed whether access to encrypted data has been the dominant piece of evidence in a criminal investigation or merely corroborated other avenues of enquiry since the introduction of the Act.

The trade-off between national security and public interest in privacy, security and confidentiality of communications is not new. The narrative before and after the passing of the Act is all about catching criminals and stopping terrorist organisations, even though criminal activity has been diminishing in Australia over the past few decades. And during the debate there was not sufficient time given to the side effects of such legislation.

This legislation is no silver bullet and, indeed, law enforcement should never seek such a thing. Criminals have been obfuscating their communications long before encryption became mainstream. They spoke in code over telephones (or text messages), wrote emails and saved them in draft (without transmitting), and met in person to discuss their criminal pursuits – all to avoid eavesdropping. Every time a technical inhibitor to criminal investigations comes along, we shouldn’t seek to legislate our way out of the problem.

Police have many tools available, particularly metadata (which is very easy to obtain, plentiful in nature, and very powerful) with which to investigate crime.

The Act compels technology companies and communication providers to do certain ‘acts or things’ to enable agencies to access communications, including encrypted communications. This has raised the prospect of unintended consequences arising from weaknesses being built into a device, even though the Act prohibits the introduction of a ‘systemic weakness’ and the implementation or building of decryption capabilities or rendering ‘systemic methods of encryption less effective’. This is confusing to the lay person, especially when they are told encryption is good, for example in e-commerce transactions.

Law enforcement and national security agencies need to do a better job of explaining to the public why these laws were necessary – and not an overreach of police powers. More granular public reporting would build the trust between the public and law enforcement institutions. This should include:

- How many times the legislation was used
- Was the use of the legislation proportional and necessary (for example, were other methods considered, and was the interference caused in the use of the legislation balanced against the investigational outcome) to the crime being investigated?
- What offence was it used to investigate? Were these investigations:
  - In the interests of national security?
  - To detect or prevent serious and organised crime?
  - To safeguard the economic interests of Australia where these interests are relevant to national security?
- What were the court results?
- Was the use of this legislation the sole reason a prosecution was successful?

Importantly the Australian Independent National Security Legislation Monitor has been asked by the Parliamentary Joint Committee on Intelligence and Security to review the operation, effectiveness and implications of amendments made by the Act. This is a public review which will result in a public report being tabled in Parliament in April 2020.

Effective policing demands public trust. Maintaining that trust goes beyond reducing crime, it involves being accountable for how safe communities feel, not just how safe they are.
The terrorist attack in Christchurch on 15 March 2019 has become an online ground zero for governments and social media companies grappling with the weaponisation of the Internet. New Zealand Prime Minister Jacinda Ardern’s Christchurch Call to “eliminate terrorist and violent extremist content online” is as ambitious as it is necessary. But is it actually possible?

Notwithstanding the profit penalty stick the law wields in this game of cyber whack-a-mole, the complexity of the problem lies in the fact that it isn’t technological in nature—it’s societal.

Government expectations versus technological reality

Amendments to the Criminal Code (Sharing of Abhorrent Violent Material) Bill 2019 (the Bill) passed by the Australian Government in April puts internet service providers, hosting and social media companies on notice to both report and takedown abhorrent content within a reasonable amount of time. Certainly, preventing inadvertent online exposure to such material prevents citizens from becoming unwilling virtual eyewitnesses to acts of extreme violence. It also prevents lone-actors and terrorist organisations from leveraging violently extreme content for propaganda of the deed value. These are all good outcomes for civil society.

While the Bill may impact a social media company’s bottom line, the legislation does absolutely nothing to deter the terrorists that create, publish and amplify the content in the first place. From Facebook to Gab to Twitch, we know from terrorist attacks in the past 12 months alone that banishment from mainstream social networks simply migrates users and audiences to more secure and encrypted solutions. Worse still, the way these online spaces are constructed in decentralised peer to peer, distributed, censorship-resistant networks, makes them impervious to takedown.

So, while Government looks for legislative remedies and technological solutions to combat the results of violent extremism,
the people behind the rise of herostratic terrorism remain unchallenged.

A white rabbit holding a pocket watch

Herostratic Syndrome “has been known for more than two millennia and refers to the killers and arsonists who perpetrate odious attacks for the sake of self-glorification.” In recruiting and radicalising from a platform of contemporary propaganda, “new recruits are bound to reach instant infamous stardom” (Azam & Ferrero, 2017) via livestream, agitprop pieces or mainstream media reporting. We have seen this modus operandi employed by the Islamic State and increasingly, Right Wing terrorists.

Perhaps most disturbingly, these terrorists – who in their own words describe their inevitable death as the price of martyrdom; have an extensive, sympathetic audience ready to watch their exploits.

While Facebook removed the Christchurch terrorists’ video within minutes of being alerted to its presence, people were screen capturing the footage and re-uploading it. Facebook reported that in the first 24 hours they removed 1.5 million videos of the attack globally with more than 1.2 million of those being blocked at upload. That’s 1.5 million people actively, knowingly, attempting to share violently extreme content. The same situation arose just weeks ago (although on a much smaller scale) when the terrorist in Halle, Germany, livestreamed his exploits to gaming platform Twitch, which is owned by Amazon.

It is clear that technological deterrents aren’t preventing terrorist attacks from happening or being livestreamed. In fact, propaganda of the deed continues to play a central role in lone-actor attacks as evidenced through Christchurch inspired right-wing manifestos. While this recent evidence should give Government some pause to consider the practical viability of content takedown expectations versus network capability under crisis (while artificial intelligence and machine learning are rapidly evolving, they aren’t the panacea Government assume them to be, yet) Government instead continues to view legislative remedies and the regulation of digital platforms as broad deterrents.

Technology is not the problem: we have a people problem

Regulating or legislating our way out of this situation doesn’t do anything to disincentivise the accelerationists that seek to hasten change through violently extreme action - because at its core, the problem is not technological - it’s societal.

We are at war with ourselves. While degenerate values are engineered to provoke outrage, online ecosystems remain the messengers of the disaffected. Without unpacking the fractures that exist in our society, and the ways those that would do us harm exploit them to advance their own agendas, we will remain caught in the crossfire of their information war.

While big tech companies may resist the editorial responsibility that comes with being the proverbial messenger under the auspices of free speech framing, their corporate social responsibility to protect their users from harm cannot be ignored. They have an important role to play in making their networks safer for users, more accessible to law enforcement and more noxious to information disorder.

Similarly, Government has a role to play in preventing violent extremism at its source. Until we manage our people problem, herostratic terrorists will continue to find ways to abuse cyber space and technology to further their agendas.

---

The Internet has permeated the world at breakneck pace in the last two decades. Access, however, remains contested, or restricted in certain parts of the globe. As the ‘digital divide’ between developed and developing countries closes, discussions regarding the importance of access to the Internet as a human right have become increasingly commonplace. The Internet plays a significant role in providing individuals with the ability to exercise their right to freedom of opinion – a right guaranteed under article 19 of the Universal Declaration of Human Rights. This is especially the case in nations where the notion of a free and independent media is contested or non-existent. In the case of Indonesia, the total number of Internet users grew by 13% in the last year alone, while the role of the Internet has frequently arisen as a contentious topic in recent years, particularly as the country tackles issues that have posed threats to the stability of the nation.

Concerns related to the use of the Internet in ‘uncivil society’ in Indonesia are not new, with many groups utilising the wide reach of the Internet to disseminate their ideologies. Individuals and civil society organisations have recognised the importance the Internet plays in providing an uncensored platform for social and political debate. This has given the Indonesian State a valid reason to be cautious regarding its use as an unregulated space for the

---


CONTINUED
dissemination of social, political, and religious content.

One example is that of the Moluccan conflict in the late 1990s-early 2000s. Despite its relatively minimal permeation in Indonesia at the time, online groups such as the Forum Komunikasi Ahlu Sunnah wal-Jama’ah (Communication Forum of the Followers of the Sunnah and the Community of the Prophet) or FKAWJ - as well as Christian groups including the Crisis Centre of the Diocese of Ambon and the Massariku Network - used the Internet as a platform to incite and exacerbate sectarian violence between Christians and Muslims in the region. To achieve this, the groups disseminated uncorroborated photos of alleged atrocities and crimes committed by the other side and accompanied them with hateful back-and-forth discourse online. This inevitably served to further deepen the religious divide and create a more challenging environment in which to achieve a political solution.

The role of the Internet in civil society activism has continued to garner greater attention from the Indonesian Government and its re-elected President, Joko Widodo (popularly known as ‘Jokowi’). In the lead-up to the 2017 Jakarta Gubernatorial Elections, incumbent Governor Basuki Tjahaja Purnama (known as ‘Ahok’) was targeted via social media by conservative Islamic opponents. The dissemination of an edited video showed Ahok purportedly committing blasphemy when discussing the Qur’an. The subsequent waves of anti-Christian meme content across social media platforms in reaction to the video created the conditions for a large-scale conservative Muslim movement to materialise. The movement demanded that the Indonesian Government charge Ahok under the nation’s controversial blasphemy laws – a demand that was eventually successful.

In 2019, the Indonesian Government became weary of social media playing a destabilising role in the civil unrest in West Papua. At the height of the unrest in August – September, a decision was made to limit Internet services to the region. The decision was purportedly made on the belief that ‘fake news’ and the spread of rumours were inciting further violence. While this is an understandable concern, the ramifications of limiting Internet access on a large scale should be considered. During a period when violent clashes between protestors, security forces personnel, and pro-Jakarta militias resulted in numerous casualties, many journalists and human rights advocates were unable to send out reports or receive information on the protests. Throttling data connections meant that the Indonesian Government was able...
to control the narrative of the events unfolding on the ground, while increasing the chances of possible human rights violations going unnoticed/unreported. The UN High Commissioner for Human Rights, Michelle Bachelet, commented on the issue, expressing her concern that "Blanket Internet shutdowns are likely to contravene freedom of expression and limiting communications may exacerbate tensions".

In response to ongoing concern about social media and cybersecurity, the creation of the National Cyber Encryption Agency (BSSN) in 2017 aims to tackle issues such as the spread of fake news and hoaxes via fake social media accounts. Along with the creation of new government bodies to address these cybersecurity issues, the Indonesian Government has also attempted to introduce new legislation - known as the Rancangan Undang-undang Keamanan dan Ketahanan Siber (RUU KKS) and the Rancangan Undang-undang Perlindungan Data Pribadi (RUU PDP) - to deal with cybercrime and personal data protection. According to critics the loosely-worded articles within these laws give agencies the ability to censor content that they alone determine to be dangerous or negative without providing clear criteria for what would be considered ‘dangerous’ content.

The new laws would also allow the Government to prosecute individuals posting this content - a move that the Government has already demonstrated they are willing to make after the arrest of a prominent civil activist who used social media to raise funds in support of individuals protesting the reforms in Jakarta.

The introduction of these new laws, along with others attempting to reform Indonesia’s outdated Criminal Code, were immediately resisted by large gatherings of students protesting in major cities throughout the country. Many civil society organisations have also expressed concerns regarding the powers that the new legislations would provide to government agencies. The Southeast Asia Freedom of Expression Network (SAFEnet) also identifies article 14 of the RUU KKS that would enable the Indonesian Government and Internet service providers to cut data connections at their own discretion - allowing the Government to legally justify events like that of West Papua in the future.

While Indonesia’s House of Representatives (Dewan Perwakilan Rakyat or DPR) has officially withdrawn its support for the new laws, it remains highly likely that a new version of the legislation will be considered during Jokowi’s second term.

The recent announcement of Jokowi’s new cabinet (a slew of former police chiefs, military generals, and oligarchs) signals an attempt by the President to appease the more conservative members of Indonesia’s political elite. Perhaps the most controversial is former army general Prabowo Subianto, Jokowi’s rival in the previous two elections and an individual accused of committing multiple human rights violations during his military career, who was appointed as the new Defence Minister.

The clear political concession of Prabowo’s appointment demonstrates a favouring for political power-brokering in order to force through Jokowi’s economy-focused legislative agenda. Unfortunately, protecting citizen’s cyber rights is likely to be pushed aside in the shuffle.

---


For a long time, countries have sought to keep the full breadth of their cyber operations activities under wraps. In his book, The Perfect Weapon, national security reporter for The New York Times, David E. Sanger, revealed the extent of US-Israeli offensive cyber capability by telling the story of Operation Olympic Games. The operation, which was started under President George W. Bush, and eventually given the green light by President Barack Obama, resulted in the development of computer code that caused physical damage to 1,000 to 5,000 Iranian nuclear centrifuges in 2009. The book infuriated the Obama Administration and landed Sanger in a four-year leak investigation conducted by the FBI. Since then, the tensions between secrecy and transparency have become increasingly important and problematic.

The case for secrecy
Among the wide variety of reasons that secrecy surrounding government cyber capabilities and operations has been the historical default, two primary explanations emerge.

First, admitting and publicly owning specific cyber capabilities and actions can render them practically useless. Anonymity of a cyber action complicates attribution and makes it more difficult for the victim to respond. This has obvious and understandable appeal for actors wanting to carry out offensive cyber attacks without consequences. Second, by maintaining the secrecy of their cyber capabilities and activities, the conflict and competition occurring in the cyber domain has remained relatively ungoverned. This has allowed liberal democratic governments to avoid the constraints of codified international norms and rules that exist for conventional conflict. Secrecy also has meant less public accountability for states than their involvement in conventional conflicts would attract. But why do governments view the latitude that comes from secrecy as necessary?

Cyber is relatively cheap to develop and deploy when compared to conventional military forces. It has the potential to be the great equaliser for both state or non-state actors that are normally at
Successful anonymity obviously protects an attacker from retaliation carrying out a cyber attack. Despite this, a preference for secrecy surrounding cyber security often hamstrings the ability of victims to publicly name and shame attackers.

Successful anonymity obviously protects an attacker from retaliation carrying out a cyber attack. Despite this, a preference for secrecy surrounding cyber security often hamstrings the ability of victims to publicly name and shame attackers. This exposure, however, is essential to deter future cyber attacks. Even if there is no indictment, attribution often leads to a lackadaisical approach by individuals to their own cyber hygiene and popular opinion sceptical of the cyber policies being created by lawmakers. Without the buy-in of individuals, Australia and many other countries remain relatively easy targets for cyber criminals or the unwelcome actions of other nations.

Conclusion: nuance but necessary
As the cyber domain becomes increasingly important to the ‘real world’ and increasingly a location for contest and competition, and trust in government and large organisations is at a historic low, it has become clear to experts in both the private and public sectors that keeping everything secret will no longer work. Private companies have a duty to shareholders to disclose weaknesses and attacks. And governments must increasingly face concern about the seeming creep of national securitisation and infringements on individual privacy.

Ultimately, effective cyber policy should aim to produce an antibody-like response to a cyber attack within the body of a nation as a whole; neutralising the harmful effects of a threat with constant, unprompted and singular level responses before it becomes a crisis. For this to occur, enough transparency for people to understand the threat-scape is needed to prompt and maintain such a response.

There is often a natural resistance to calls for transparency in national security communities. However, as Sanger noted when remarking on the cyber intrusions that occurred in the Australian Federal Parliament in 2018, “people in the intelligence agencies are going to say ‘but then China is going to discover that we’re watching them,’ and my answer to that is if the Chinese haven’t figured that out by now they wouldn’t be able to attack you in the first place.”

Transparency must be balanced and perhaps even surgical in its precise use, but it is necessary.

Dr Ben Gauntlett commenced as Disability Discrimination Commissioner in May 2019. A barrister prior to commencing his term, Ben holds undergraduate degrees in Law (Hons) and Commerce from the University of Western Australia, and was awarded the Rhodes Scholarship for Western Australia in 2003. He also holds a Master of Laws from New York University and a D.Phil. in Law from the University of Oxford, where he studied as a Rhodes Scholar.


LexisNexis congratulates Dr Gauntlett on his appointment and his vital work in protecting and promoting rights for people with disabilities. We took the opportunity to ask him a few questions about the state of Australian disability law and how we can all work toward positive change in this field.
What is the most significant case to date in Australian disability law?

I do not like to regard one case as more significant than another as for the people who have a disability the result of every case matters. Litigation is time-consuming and expensive and cases are often the result of significant events that cause tremendous angst for the individuals involved. However, the recent decision in Sklavos v Australasian College of Dermatologists [2017] FCAFC 128 has caused some unease in relation to when an employer or education provider is under an obligation to provide reasonable adjustments. The issues raised by Sklavos are probably better dealt with by reforming or amending the Disability Discrimination Act 1992 (Cth).

What piece, or set, of disability law reform would you most like to see in Australia or world-wide?

In Australia, at a Commonwealth level, the Disability Discrimination Act needs to be reviewed in the context of the broader National Disability Strategy and National Disability Agreement. The Disability Discrimination Act is also part of a wider collection of Acts and legislative instruments, which deal with issues such as access to transport or buildings. The reason for review is we need Acts that reflect a modern concept of “disability”, which understands a person’s difficulties may be caused by the environment around them and not any type of medical impairment.

How can the legal profession play a role in ensuring disability discrimination is ended?

I am a strong believer the legal profession should lead by example. This is particularly the case where potentially negative perceptions exist in society that people will not speak out against. Such perceptions exist for people with disabilities in Australia.

The Organisation for Economic Co-operation and Development (OECD) noted in 2011 that Australia ranked 21st out of 29 countries for employment of people with disabilities. A significant aspect of this low ranking within the OECD is the perception of people with disabilities in Australia. Perception of people with disabilities in Australia will only be altered by dealing with the issue at an individual, organisational (e.g. law firm or professional body) and structural level (e.g. legislation). The legal profession needs to assess to the extent it engages with people with disabilities and, if not, why not. The legal profession should target the employment, engagement and inclusion of people with disabilities as part of its diversity strategy.

Any revised approach to diversity needs to involve explicit data collection and training.

What are the most effective actions for positive change that may be made by individuals?

When considering the concept of “diversity” it is important to realise it has a number of elements. For example gender, race, ethnicity, sexual orientation and disability are some aspects of diversity. But disability is a diversity characteristic that some people seek to hide. Part of the reason for this is that people with disabilities may believe they receive no benefit in revealing their disability. When considering the issue of “diversity” in the profession, disability should be explicitly considered. Diversity policies should not be economically-driven. Rather, such policies should seek to acknowledge the inherent characteristics of each individual and the challenges that may be faced. In particular, intersectionality (and the difficulties it poses) should be expressly noted.

Diversity extends to how firms or organisations represent themselves in the media. People with disabilities should be recognised and acknowledged in any publication.