The Law Association OF NEW ZEALAND

Vero Center
Level 18
48 Shortland Street
Auckland City 1010
New Zealand
PO Box 58
1010 Auckland
09 303 5270
thelawassociation.nz

Biometric Processing Privacy Code -

Submissions from The Law Association of New Zealand (TLANZ)Technology and Law Committee and the Employment Law Committee

1. INTRODUCTION

1.1. The Law Association of New Zealand (TLANZ) is an independent membership organisation representing over 7,500 legal professionals nationwide. Dedicated to upholding the highest standards of legal review and policy advocacy, TLANZ actively engages with legislative and regulatory developments that impact New Zealand's legal landscape.

1.2. This submission has been prepared by the TLANZ Technology and Law Committee, with input from the Employment Law Committee, to provide a detailed analysis of the Biometric Processing Privacy Code ("the Code"). The submission focuses on the intersection of biometric technology, privacy rights, and workplace surveillance, ensuring that the regulatory framework aligns with the Privacy Act 2020 and broader ethical and legal principles.

1.3. As biometric technologies become increasingly embedded in both public and private sector operations, it is imperative that their use is lawful, transparent, and proportionate. This submission seeks to refine the Code's provisions, advocating for stronger privacy safeguards, clear limitations on data collection, and protections against potential misuse, particularly in employment and law enforcement contexts.

2. EXECUTIVE SUMMARY

2.1. The TLANZ Technology and Law Committee, with input from the Employment Law Committee, has identified significant concerns with the proposed Biometric Processing Privacy Code. Key issues include the need for clearer safeguards around workplace surveillance, ensuring biometric monitoring remains lawful, proportionate, and transparent, particularly given the inherent power imbalance between employers and employees. The Code must also strengthen Privacy Impact Assessments (PIAs) to protect Pasifika, Asian, African, LGBTQ+, and other minority groups from the risks of racial profiling and biometric bias.

2.2. Additionally, the submission calls for stricter regulations on data retention and secondary use, ensuring that biometric data is stored only for as long as necessary and is not repurposed without explicit legal justification. The rapid advancement of workplace surveillance technologies, such as keystroke tracking and facial recognition, must be addressed to prevent intrusive and unjustified monitoring. The exemptions granted to law enforcement and intelligence agencies should also be narrowed to prevent potential privacy overreach and ensure all biometric processing is subject to appropriate oversight.

2.3. Finally, the Committee strongly recommends bringing employer-provided health and wellbeing applications under the Code's scope, as these apps collect sensitive biometric data that could be misused for performance monitoring or disciplinary actions. These recommendations are essential to ensuring that biometric data processing in New Zealand remains ethical, transparent, and aligned with privacy rights under the Privacy Act 2020.

3. SUBMISSIONS

3.1. Rule 1: Purpose of Collection

3.1.1. The essence of responsible biometric data management lies in ensuring that such data is only collected for "lawful purposes." A "lawful purpose" should be meticulously defined to encapsulate purposes that are legally justifiable under not only the Privacy Act 2020 but also any relevant sector-specific legislation. This purpose must be intrinsically linked to the agency's operational responsibilities, clearly necessary for achieving specific, articulated objectives, and proportional in both scope and impact. Importantly, this definition should ensure alignment with broader societal values, including fairness, equity, and the public interest, thus safeguarding against any potential misuse that could lead to societal discord or inequity.

3.1.2. ***Recommendations:***

3.1.2.1. Define "*Lawful Purpose*" More Clearly**:** Amend the definition to include criteria that ensure the purpose is legally justifiable under New Zealand laws, particularly the Privacy Act 2020. It should also be directly related to the agency's operational responsibilities, necessary for achieving a clearly defined objective, proportional in scope and impact, and consistent with broader societal values including fairness, equity, and public interest.

3.2. Rule 1(3): Privacy Impact Assessments

3.2.1. The stipulation that a privacy impact assessment (PIA) should focus primarily on the "proportionate" nature of biometric processing is too restrictive. Such a narrow focus can lead to an oversight of equally crucial factors like the necessity and effectiveness of the processing activities, potentially leading to a disproportionate emphasis on proportionality over more substantive evaluation metrics.

3.2.2. ***Recommendations:***

3.2.2.1. Broaden the Scope of PIAs: Extend the mandatory privacy impact assessment to include thorough evaluations of necessity and effectiveness alongside proportionality. This approach will ensure that biometric data is not only used proportionately but is also essential and effective for the intended purposes.

3.2.2.2. Amend Rule 1(3): Modify this rule to require agencies to consider whether the biometric processing is the least intrusive means available to achieve the stated lawful purpose, thereby ensuring that all aspects of Rule 1 are comprehensively addressed.

3.3. Rule 1(3)(c) - Consideration of Impacts on Minority Demographics

3.3.1. The removal of the requirement to consider the impact of biometric processing on *other New Zealand demographic groups* under Rule 1(3)(c) is a significant regression from the previous draft of the Code. This omission weakens the framework's ability to address the full scope of risks posed by biometric technologies, particularly for minority and marginalised communities.

3.3.2. We acknowledge and support the inclusion of provisions requiring an assessment of biometric processing impacts on Māori, recognising the importance of addressing cultural sensitivities and specific risks. However, restricting this consideration exclusively to Māori fails to account for the broader risks that biometric misidentification, algorithmic bias, and systemic discrimination pose to other minority communities. These risks extend beyond Māori and disproportionately affect a range of ethnic and vulnerable groups.

3.3.3. To ensure a comprehensive and equitable approach, the Code must explicitly require the assessment of biometric processing impacts on all vulnerable demographics. While the current draft acknowledges ethnic minorities, it is essential to broaden this scope to include LGBTQ+ individuals, people with disabilities, and other at-risk communities who may face unique privacy risks and potential discrimination as a result of biometric categorisation and processing.

3.3.4. We repeat that there is overwhelming evidence from studies on the effectiveness of common biometric processing tools (e.g. Facial Recognition Technology (FRT)) around the world demonstrate that the heightened risks of misidentification and subsequent flow-on harms are not experienced only by Māori, but also most other ethnic minority groups including Pasifika, Asians, Africans and more. We do not see a good reason why obvious risks to other vulnerable demographics should not be considered where they exist, and we do not think these risks are

not given adequate weight through passing mentions in the draft guide. Noting that the code intends to emphasise the unique risks biometric processing poses to Māori communities due to specific sensitivities in tikanga, we recommend that an additional clause such as the following be added:

3.3.4.1. *1(3)(d) the impacts and effects of biometric processing on any other New Zealand minority demographic group(s).*

3.3.5. We also submit that the justification for this removal is misconceived. The justification provided by the Office of the Privacy Commissioner is that other demographic groups are a part of the privacy risk assessment:

3.3.5.1. *The proportionality assessment focuses on the weighing of benefits against the privacy risk. The requirement to consider any particular impact and effects on specific demographic groups has been removed as it should be part of the organisation's privacy risk assessment.*

3.3.6. However, this reduces the consideration from a mandatory consideration of "cultural impacts and effects", which has a broader and more appropriate scope for an issue as complex as systemic racial profiling. Instead, it is reduced to a privacy risk factor, which is defined in the new draft code as:

3.3.6.1. *any result misidentifies or misclassifies an individual, including where the risk differs based on attributes such as the individual's race, ethnicity, gender, sex, age or disability (whether separately or in combination); (bias)*

3.3.7. This is a reductive approach that takes impacts and effects to a matter of misidentification or misclassification. This does not engage with the research provided as to the wider-ranging complex impacts and effects of racial profiling. It is, therefore, misconceived to have removed and then reduced the scope of the previous mandatory consideration.

3.3.8. ***Recommendations:***

3.3.8.1. Amend Rule 1(3)(c) to ensure that assessments explicitly include the effects of biometric processing on racial, ethnic, gender, and LGBTQ+ communities. This amendment should be accompanied by comprehensive guidelines that aid agencies in understanding and mitigating potential biases and adverse outcomes linked with biometric technologies. Incorporating references to relevant research, including studies on biometric biases impacting the transgender and non-binary communities, is crucial to guide these evaluations effectively.

3.3.8.2. Extended Recommendations for Rule 1(3)(c):

3.3.8.2.1. Expand the assessment requirement to include other minority groups in New Zealand, ensuring that the Code's protections against discriminatory outcomes are inclusive of all communities potentially impacted by biometric technologies. An additional clause could be incorporated to address this:

(d) impacts and effects of biometric processing on any other New Zealand minority group(s).

3.3.8.2.2. Inclusive Impact Assessments: Require Privacy Impact Assessments (PIAs) to cover a wider spectrum of demographic groups. This expansion will guarantee that the potential adverse effects of biometric processing are thoroughly understood and mitigated across diverse sectors of society.

3.3.8.2.3. Supportive Guidelines for Implementation: Formulate and embed guidelines to facilitate agencies in conducting these comprehensive impact assessments. These guidelines should be informed by the latest research on biometric biases, particularly those affecting individuals based on gender and sexual orientation, to navigate the complexities of biometric data usage and to forestall discriminatory practices.

3.3.9. By broadening the scope of Rule 1(3)(c), we ensure a more equitable consideration of how biometric technologies affect all sectors of society, especially those at heightened risk of discrimination and bias. This proactive approach not only aligns with principles of fairness and inclusivity but also strengthens the integrity of biometric data usage within New Zealand.

3.4. Rule 3(1)(i): Information on Biometric Data Retention

3.4.1. Rule 3(1)(i) mandates agencies to provide individuals with a summary of the retention period for collected biometric information. This rule underscores the necessity for agencies to have well-defined processes around data collection and retention.

3.4.2. ***Recommendation:***

3.4.2.1. Further strengthen this rule by requiring agencies to detail their retention schedules and disposal procedures in their privacy notices. This would enhance transparency and provide individuals with clearer insights into how long their biometric data is kept and the measures taken to dispose of it securely.

3.5. Exclusions Concerning Law Enforcement

3.5.1. The exclusions provided for law enforcement in Rules 2 and 3 raise questions about their practical implementation and potential to infringe on individual privacy.

3.5.2. Recommendation:

3.5.2.1. Clarify these exclusions to ensure they do not allow for overly broad applications that could undermine privacy rights. Detailed guidelines should be developed to delineate the circumstances under which these exclusions apply, ensuring they are used judiciously and within clearly defined limits.

3.6. Providing Practical Examples:

3.6.1. To aid in the practical application of this rule, the Code should include examples that clearly delineate what constitutes compliant versus non-compliant purposes. For instance:

3.6.1.1. **Compliant Example:** Using facial recognition technology at airports to enhance security measures, where such use is strictly regulated, transparent, and proportionate to the privacy risks involved.

3.6.1.2. **Non-Compliant Example:** Continuous monitoring of employees' biometrics in workplace settings to assess productivity without robust justification tied directly to essential business operations and absent a framework that safeguards employee privacy rights.

3.7. Rule 10 Adjustments

3.7.1. Finally, the provisions under Rule 10 regarding the secondary use of biometric data need to be significantly tightened. The current language allows for the potential repurposing of biometric information beyond its initial collection scope, which could lead to privacy infringements if not strictly controlled. TLA suggests revising this rule to explicitly restrict the use of biometric data to the purposes for which it was initially collected, unless explicit consent is provided or there is a compelling statutory requirement for its reuse.

3.7.2. The need for adjustments in Rule 10 concerning the use of biometric data beyond its initial collection purpose is crucial. Currently, the provisions allow for potential repurposing of biometric data, which could lead to privacy breaches.

3.7.3. ***Recommendation:***

3.7.3.1. Tighten the provisions under Rule 10 to strictly limit the use of biometric information to the purposes for which it was initially collected, except where explicit consent is provided, or a compelling statutory requirement exists.

3.7.4. Rule 10(1) - Clarity on Use of Biometric Information

3.7.4.1. The language used in Rule 10(1) regarding the use of personal information not collected in accordance with Rule 1 is potentially confusing and could lead to unintended interpretations. The distinction between 'personal information' and 'biometric information' needs clarification to ensure consistency throughout the Code.

3.7.4.2. ***Recommendation:***

3.7.4.2.1. Amend Rule 10(1) to clarify that any biometric information not collected in full compliance with Rule 1 cannot be used for any other purpose, aligning this provision with the Privacy Act 2020's principles. This amendment would prevent any misuse of biometric information collected under ambiguous or non-compliant circumstances.

3.7.5. Rule 10(4): Consistency in Rule Applications

3.7.5.1. There is a need to ensure that all rules within the Code consistently apply the principles of necessity and proportionality, especially in contexts where biometric information is used beyond its initial collection scope.

3.7.5.2. **Recommendation:**

3.7.5.2.1. Modify Rule 10(4) to reflect that all considerations of biometric information use, especially those not initially collected in accordance with Rule 1, must consider the factors outlined in Rule 1(3). This includes not only proportionality but also necessity and the absence of less intrusive alternatives.

3.7.6. Rule 10(5): Concerns Over Exemptions for Security Agencies

3.7.6.1. The potential exemptions granted to intelligence and security agencies, particularly from Rule 10(5), pose significant concerns. The critique that such exemptions could allow for the unrestricted use of biometric classifications by these agencies, even for purposes that might infringe on privacy or lead to racial profiling, is particularly troubling.

3.7.6.2. ***Recommendation:***

3.7.6.2.1. Reevaluate the necessity and scope of these exemptions to ensure they do not facilitate the misuse of biometric data under the guise of national security.

Exemptions should be narrowly tailored, justified by clear evidence of necessity, and subject to stringent oversight.

3.7.7. Rule 10(10) - Exemption for Intelligence and Security Agencies

3.7.7.1. The exemption provided to intelligence and security agencies under Rule 10(10) is concerning. Allowing these agencies to use biometric data for purposes beyond the originally intended scope without stringent checks raises significant privacy and ethical issues.

3.7.7.2. ***Recommendation:***

3.7.7.2.1. Remove the exemptions that allow intelligence and security agencies to use biometric information for secondary purposes not directly related to the original collection intent. Instead, any secondary use should be subject to the same stringent criteria as any other agency, ensuring that all use of biometric data is justifiable, necessary, and proportionate.

3.8. Clarity and Consistency in Rule Applications

3.8.1. Observations regarding the ambiguous language used in the exemptions for intelligence and security agencies highlight an inconsistency that could lead to misinterpretations. The specific rules concerning exemptions need to be articulated with greater precision to prevent any undue broad application that might compromise individual privacy rights.

3.8.2. ***Recommendation***:

3.8.2.1. Standardise the language across the Code to ensure that obligations are clearly mandatory where intended, and address any inconsistencies in rule references, especially those concerning exemptions for intelligence and security agencies. Clear and unambiguous wording is essential for enforceability and compliance.

4. EMPLOYMENT ON THE BIOMETRIC CODE

4.1. Workplace Surveillance

4.1.1. The draft Code's current treatment of biometric processing in workplace surveillance is notably deficient in clarity and specificity. This vagueness could potentially allow for intrusive monitoring practices that disproportionately impinge upon employee privacy. It is imperative that the Code explicitly delineates the acceptable parameters for the use of biometrics in workplace surveillance, stressing that such activities must be directly related to critical business operations and conducted in the least intrusive manner possible. Guidelines should be established to outline acceptable and unacceptable uses, ensuring they are narrowly tailored to protect employee privacy while maintaining necessary security protocols.

4.1.2. From the employment perspective, the focus centers on the regulation of workplace surveillance in the context of biometric processing of employees' personal information. The Code's current provisions on the purpose of collection (Rule 1), manner of collection (Rule 4), and fair use limits (Rule 10) require further clarification to prevent unreasonable intrusions into employees' personal affairs and to ensure fair handling of sensitive biometric data.

4.1.3. Our submissions focus on the issue of workplace surveillance and how this is regulated in relation to biometric processing of employees' personal information.

4.1.4. The Code may not provide sufficient clarity or guidance around the extent to which the collection and use of employees' personal information for biometric processing is an unreasonable intrusion on their personal affairs, taking into account the purpose of collection in Rule 1, the manner of collection in Rule 4, and the fair use limits in Rule 10.

4.1.5. Although the Information Privacy Principles in the Privacy Act 2020 are comparable to the Rules contained in the Code, and also leave issues regarding workplace surveillance largely open to interpretation, the publication of extensive guidance alongside the Code provides a unique opportunity to communicate clarity around biometric processing and workplace surveillance.

4.1.6. Assessments regarding the application of the Privacy Act 2020 to the acceptable collection and use of personal information for workplace surveillance and other scenarios have previously been left to the development of the common law, however, the ever-developing digital methods of surveillance, including the rapid expansion of biometric processing, create a pressing need for further clarity.

4.1.7. For example, employers now have the technical know-how to undertake keystroke monitoring of employees, including collecting and analysing personal information about how an employee types, the time taken on a sequence of keys, and the rhythm of keystrokes. Whilst this information may benefit employers, for example by providing additional data to assess an employee's efficiency, the collection and use of such personal information may go beyond what is considered acceptable. Nevertheless, it is difficult to interpret whether the Code envisages that kind of collection and use as legitimate, necessary and proportionate, with such an assessment left instead to the various interpretations of employers and their advisers.

4.1.8. Clarity around the types of biometric information employers can and cannot collect and use is particularly important when considering the inherent power imbalances in employment relationships. This is especially so for vulnerable or less sophisticated employees who may struggle to assert their rights.

4.2. Emerging Surveillance Technologies

4.2.1. Emerging technologies such as keystroke monitoring present new challenges. This technology can provide insights into an employee's efficiency (or other attributes) but also risks overstepping privacy boundaries. The Code should explicitly address the factors to consider when determining, in different contexts, whether monitoring from emerging surveillance technologies are considered a legitimate, necessary, and proportionate use of biometric data in the workplace.

4.3. Need for Clear Guidelines

4.3.1. Given the power imbalances typically present in employment relationships, we recommend the Code clearly outline acceptable biometric practices. This clarity will help protect vulnerable employees from potentially invasive surveillance practices that could affect their employment rights.

4.4. Biometric Data on Fatigue and Alertness

4.4.1. While the collection of biometric data relating to fatigue, alertness, and attention levels may be justified for safety-sensitive roles, extending such practices across the workforce without clear justification could be problematic. The Code should consider explicitly restricting the use of such

data to contexts where there is a direct and legitimate safety concern to protect, or such other context as may be considered appropriate.

4.4.2. The Code prescribes the fair use limits for biometric categorisation, setting out in Rule 10 sub-rule 5, that an agency may not use biometric information in order to produce a result that is health information, personal information relating to a person's personality, mood, emotion, intention or mental state, or a category that is a prohibited ground of discrimination. It then goes on to say that this does not limit the use of biometric information to (attempt to) obtain, infer, or detect, personal information about an individual's state of fatigue, alertness or attention level. However, the ability for employers to use biometric information for those purposes raises additional workplace surveillance issue.

4.4.3. Whilst it may be reasonable for employers to obtain information about fatigue, alertness and attention levels for employees in safety sensitive roles (where the information is clearly tied to the specific business needs and functions of the employee's role), there does not appear to be a legitimate purpose for obtaining that information for employees more generally, particularly if that information was then to be used in performance and/or disciplinary processes. For example, it is difficult to comprehend why an employer would need to know such personal information about an office or retail worker, and collecting those details may be considered unreasonably intrusive.

4.4.4. Although a standard employee who is subject to fatigue, alertness and attention assessments may in theory be protected by the Rule 1 requirement for biometric information to only be collected where it is necessary for a lawful purpose connected with a function or activity of the agency, and proportionate to the likely impacts on individuals, the general statement in Rule 10 sub-rule 6 regarding the broad ability to (attempt to) obtain, infer or detect information about an individual's fatigue, alertness or attention level could nevertheless lead to the greater use of such information, without sufficient scrutiny of its reasonableness.

4.4.5. It would therefore be helpful if the Code and/or the guidance were able to set out more clearly the types of situation in which collecting and using personal information about fatigue, alertness or attention level is acceptable and connected to a function or activity of the agency, compared with the types of situation in which there is no legitimate purpose, the manner of collection is overly intrusive, and/or the privacy risks of collecting and using the information are not proportionate to the benefit.

4.5. Exclusion of Commercial Apps from the Code

4.5.1. The proposed exclusion of certain commercial applications, such as employer-provided health and wellbeing monitoring tools, from the scope of the Biometric Processing Privacy Code ("the Code") raises significant concerns. Although such tools may offer legitimate benefits in terms of employee health and wellness, their potential use for gathering sensitive personal information—including emotional states, personality traits, sleep patterns, and menstrual cycles—poses considerable privacy risks. We therefore recommend that commercial applications remain regulated by the Code.

4.5.2. The Code currently defines biometric categorisation in a way that explicitly excludes "any analytical process that is integrated in a commercial service, including any consumer device, for the purpose of providing the user with" various types of personal information. This particular wording raises concerns about the potential for misuse in workplace surveillance contexts.

4.5.3. This definition would appear to leave employer-provided health and wellbeing apps largely unregulated under the Code, despite the fact that these apps may handle deeply personal biometric data relating to emotions, personality, health conditions, sleep patterns, or menstrual

cycles. The current wording indicates that these apps will only be regulated if their "purpose or effect...is to circumvent the application of [the] Code."

4.5.4. While TLANZ acknowledges that such apps will continue to be subject to the general provisions of the Privacy Act 2020, there remains a genuine concern that employers might interpret their explicit exclusion from regulation under the Code as implicit permission to collect and use highly sensitive personal and biometric information through these commercial applications.

4.5.5. Consequently, there is a significant risk that employers may compel employees to utilise these apps to monitor their own health and wellbeing, inadvertently or deliberately providing employers with access to personal data. This scenario poses severe privacy risks, including the possibility that employers could create detailed individual profiles. Such profiles could subsequently be utilised in performance evaluations, medical incapacity assessments, or even to inform decisions that discriminate against employees based on protected characteristics.

4.5.6. Although some of these risks are mitigated by the provision within the Code that it would apply if the apps' purpose or effect is to circumvent regulation, it remains unclear what threshold must be met to determine that such circumvention has occurred. Irrespective of this safeguard, the explicit exclusion for analytical processes integrated within commercial services sends an ambiguous signal suggesting that the use of these health and wellbeing apps in employment contexts is broadly permissible. Given the significant privacy risks associated with these apps, more rigorous regulation should be considered.

4.5.7. In particular, we note a concerning inconsistency between the robust protections provided under the Code against biometric categorisation leading to the collection or use of health-related personal data, and the broad exemption given to commercial analytical processes. The apparent disconnect or ambiguity around secondary uses of health-related biometric information through commercial apps undermines the otherwise strong protections for personal health data provided under existing regulations, such as the Health Information Privacy Code 2020.

4.5.8. We therefore strongly recommend that, instead of exempting these apps from the Code, employer-provided health and wellbeing applications should explicitly fall under the Code's regulatory scope. Employers using such apps should be required to adhere strictly to the same stringent criteria for biometric data processing set out elsewhere within the Code. Specifically, biometric data should only be collected and utilised where clearly justified by necessity, proportionality, and explicit operational purposes.

4.5.9. To achieve this, we propose the Code be amended to remove the exclusion for commercial health and wellbeing applications to ensure they fall within the Code's regulatory scope. Such an amendment would ensure consistency, transparency, and comprehensive protection of employee privacy. This approach aligns directly with the overarching intent of the Biometric Processing Privacy Code, reinforcing its role in safeguarding individual privacy rights and establishing clear, unambiguous guidance on the acceptable use of biometric data within employment settings.

4.5.10. Finally, whilst we appreciate that the reason for the exclusion of certain commercial applications may be to prevent inadvertent breaches of the Code by passive collection of data in an app that is not subsequently viewed or used by anyone other than the user, we recommend utilising alternative wording to address this, rather than by way of a blanket exclusion from the Code which has the potential to unfairly intrude on individuals' privacy rights.

5. CONCLUSION

5.1. The Law Association of New Zealand values the proactive steps taken by the OPC in formulating the Biometric Processing Privacy Code. We believe that with the recommended adjustments, the Code will more effectively protect the privacy rights of individuals while accommodating legitimate uses of biometric technology. We remain committed to collaborating with the OPC and other stakeholders to refine these provisions further.

5.2. We are available to discuss the submissions via Teams if required. Should clarification be required with regards to any matters raised, please contact Moira McFarland, the TLANZ Committee Executive, at Moira.McFarland@thelawassociation.nz if you have any questions.

6. ACKNOWLEDGMENTS

6.1. The Law Association of New Zealand would like to acknowledge the significant contributions of our dedicated members to these submissions. Special thanks to Amy Kingston-Turner, a member of the TLANZ Technology and Law Committee, for leading the subcommittee that drafted this work, alongside her fellow committee members Isaac Lam and Daniel Tran, as well as Moira McFarland from the TLANZ Legal Service Team. We also express our gratitude to William Fussey from the Employment Law Committee for his collaboration and expert insights from the employment perspective on the proposed Code.

Ngā mihi

Lloyd Gallagher
Convenor, TLANZ Technology and Law Committee