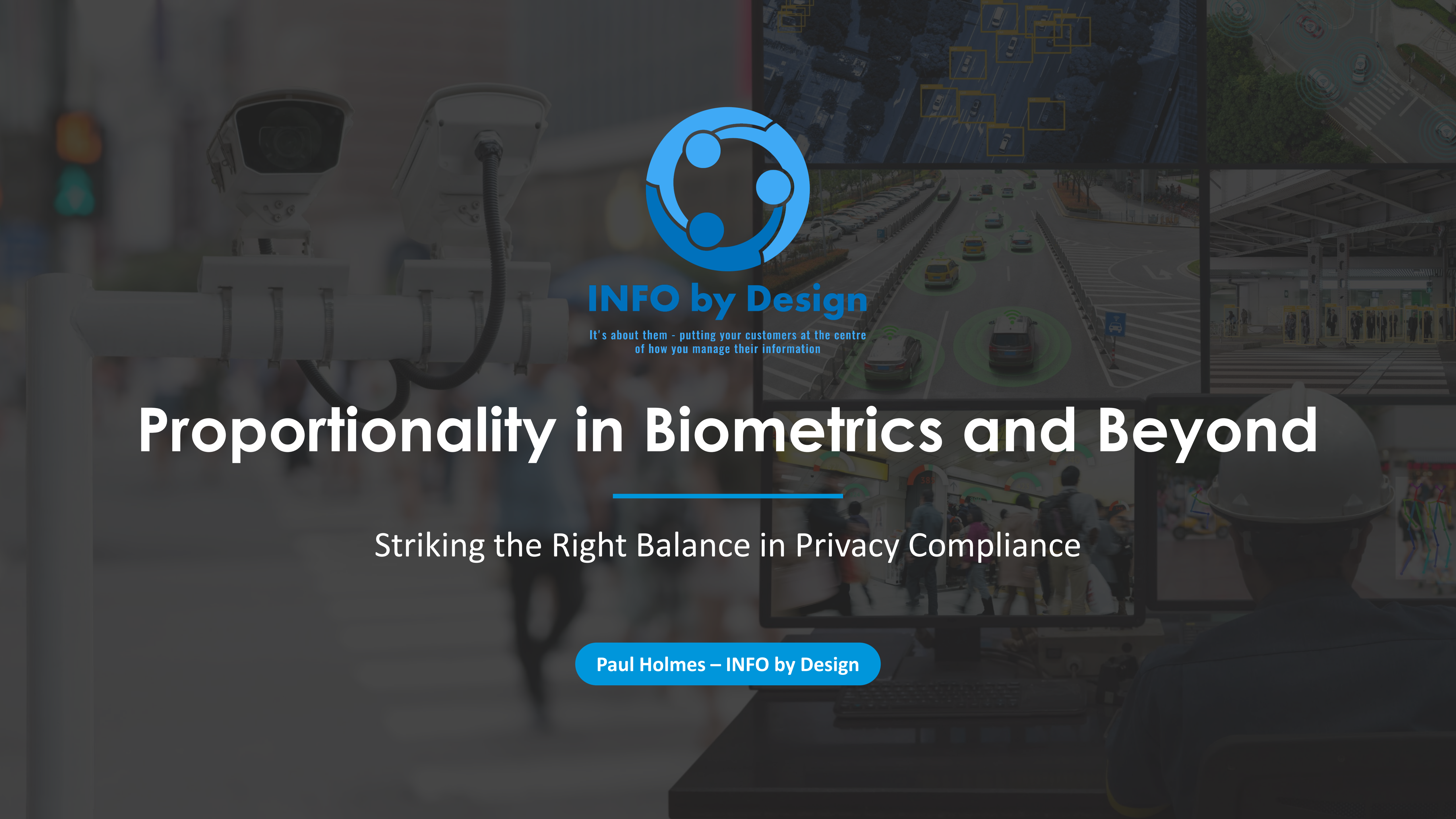

INFO by Design

It's about them - putting your customers at the centre
of how you manage their information

Proportionality in Biometrics and Beyond

Striking the Right Balance in Privacy Compliance

Paul Holmes – INFO by Design

Today’s Objectives

- In today’s webinar I plan to cover the following:
  - Biometrics and privacy in the NZ context.
  - The concepts of necessity and proportionality in relation to biometric processing.
  - How to assess necessity and proportionality and integrate it with existing PIA processes.
  - Provide you with some practical guidance to consider how your agency currently uses biometrics and whether it is proportionate.
  - Answer your questions (time permitting)

Why Focus on Biometrics Now?

- Biometric systems (e.g. face scanning, voice ID) are increasingly used by government and businesses, raising public concerns about privacy and "creepy" surveillance.
- Without safeguards, biometrics can enable covert identification without consent and are hard to challenge if decisions are wrong. There have been accuracy and bias issues – e.g. facial recognition misidentifying certain ethnic groups.
- The Privacy Commissioner is acting by developing a Biometric Processing Privacy Code to ensure these technologies are used safely and only when justified.
- Global regulations are also placing stricter requirements on the collection and use of biometrics.

What Are Biometrics?

- Biometric Information is personal information based on physical or behavioural traits – e.g. face, fingerprints, iris, voice, gait.
- The information is used in automated processes to recognise or categorise individuals.
- Common Examples:
    - Fingerprint scanners for time recording and building or device access.
    - Facial recognition for security, border protection or photo tagging.
    - Voice authentication in call centres;
- Even behavioural patterns (typing rhythm, gait) can be biometric.

Why Are Biometrics Special?

- Biometric data is usually unique to an individual and hard to change (you can't easily change your face or fingerprint if compromised). It can reveal sensitive attributes (ethnicity, health conditions, etc.) if misused.
- Because of permanence and potential for misuse, biometrics are treated as sensitive personal information in many jurisdictions (e.g. "special category" data under GDPR). NZ's Privacy Commissioner also notes biometrics are particularly sensitive and need careful assessment.
- Use cases range from benign (unlocking your phone) to high-stakes (identifying suspects from CCTV). With greater power comes greater risk – especially if data is stolen or used for unwarranted surveillance.

Ethical Considerations and Public Expectations

Beyond legal compliance	Even if something is legal, ask **“Should we do it?”** Biometrics push boundaries – just because we *can* deploy pervasive identification doesn’t mean we *should*.
Consent and agency	Where possible, give people a choice (consent) to participate in biometric systems. Forcing biometrics on unwilling individuals (especially if not strictly necessary) can be seen as coercive.
Avoiding discrimination	It’s unethical (and likely illegal) if biometric use leads to unfair bias. Ensure your use case does not unfairly target or burden a particular group.
Psychological impact	Consider the **societal and psychological effects** of biometric surveillance. High-surveillance uses are ethically fraught.
Transparency and honesty	Being open about what you’re doing is an ethical duty. Ethical practice means **no secret use of biometrics** on people.
Accountability	Plan for how individuals can challenge, or appeal decisions made by biometric systems. Don’t let the technology’s “mystique” override basic fairness and due process.
Trust and social licence	Ultimately, ethical use of biometrics is about maintaining the **social license** to operate them. By focusing on proportionality, respect, and fairness, you show you deserve the public’s trust.

Doing it right avoids crossing the creepy line.

Biometrics in the Privacy Act

- NZ’s Privacy Act 2020 governs all “personal information” handling by agencies (public and private). Biometrics, being personal information, are covered under the Act and the 13 Privacy Principles.
- There is no special biometric rule (yet). The Act doesn’t have a dedicated “biometric” principle or category – biometric information is treated like any personal information under The IPPs.
- Section 32 of the Act allows the Privacy Commissioner to issue Codes of Practice that modify how the Act applies to specific types of information or activities (e.g. the Health Information Privacy Code, a Credit Reporting Privacy Code, etc.).
- The Privacy Commissioner is currently consulting on a Biometric Processing Privacy Code which will add stricter rules for biometric processing while the rest of the Act still applies.
- The Code is expected to be issued this year.

Draft Biometric Processing Privacy Code – Overview

- A proposed Biometric Processing Privacy Code that will create specific, stricter rules for the collection and use of biometric information in automated systems, supplementing the Act.
- The Privacy Commissioner has noted risks associated with biometric processing like mass surveillance, profiling, bias, and loss of individual control require stronger safeguards.
- The Code will apply to all agencies (public and private) using biometrics for automated identification or categorisation of individuals. It won’t cover purely manual uses, or areas covered by other codes like health information).
- The Code aims to ensure biometrics are used safely, transparently, and only when justified. It modifies key Privacy Act principles, including adding tests for necessity/proportionality, stronger notice, etc.

Key Pillars of the Draft Biometrics Code

Necessity and Proportionality (Rule 1)	Agencies must **only use biometrics if it's necessary for a clear, lawful purpose and is proportionate to the privacy impact**. This means the biometric system should effectively achieve an important goal, with no reasonable less-intrusive alternative available, *and* the benefits outweigh the privacy risks.
Privacy Safeguards	Even if necessary, you must implement **robust safeguards** to minimise privacy risks. Strong safeguards can help tip the balance toward a use being proportionate by reducing risk.
Transparency and Choice (Rule 3)	The Code will require **stronger notice** to individuals when biometrics are collected or used. People should know a biometric system is in operation, why it's used, and ideally have a choice or other way to access a service if they opt out of biometrics
Limitations on High-Risk Uses	Certain intrusive uses of biometrics are heavily restricted or essentially banned. For example, using biometrics to infer sensitive attributes like someone's ethnicity or mood is addressed – the Code puts **boundaries around categorising people by traits like race or health**. In other words, biometric profiling that targets protected characteristics or deeply personal data is generally off-limits.
Upholding Individual Rights	The Code reinforces individuals' rights and promotes **accountability,** requiring agencies to explain and justify their use of biometrics and even publish their proportionality assessment for public transparency, where possible.

The ‘Necessity’ Test – Only if Required

Why do we **need** a biometric system?	Start with a **specific, lawful purpose** for using biometrics. You must articulate exactly *why* you need a biometric system and what outcome you seek (e.g. enhancing security for X, speeding up Y process). If the purpose is vague or not tied to your functions, it fails at the first hurdle.
Will using biometrics be **effective** in achieving this purpose?	There needs to be a demonstrated **causal link** between the biometric and the outcome. If it’s not effective, or only marginally so, then it’s not truly necessary. For example, using facial recognition to reduce shoplifting – is it proven to significantly deter or catch thieves? If not, its necessity is doubtful.
Can we really say there is **no reasonable alternative**?	Even if effective, you must consider whether a **less privacy-intrusive alternative** can achieve the same result. If yes, then the biometric solution is not necessary. For instance, could a swipe card or PIN code system meet the need instead of fingerprint scanners? If a reasonable non-biometric method exists, the biometric option fails the necessity test.

If a biometric system isn’t clearly necessary, don’t proceed. You should only consider proportionality once you have satisfied the necessity test.

The “Proportionality” Test – Balancing Benefits and Privacy

What are the potential privacy impacts?	Consider risks like data breaches (biometric data theft), function creep (use of data beyond original purpose), surveillance/self-censorship effects on people, accuracy errors and false matches (and their consequences), and bias/discrimination (system less accurate for certain groups). Estimate the severity and likelihood for each risk.
What are the potential benefits?	Benefits may include improved security, fraud prevention, efficiency gains (faster service, less queueing), user convenience, or even societal benefits (e.g. catching criminals). Clarify who benefits: the organisation, the individuals using the system, and/or the wider public.
Balance the benefits and the risks	Are the benefits significant enough to justify the potential privacy intrusions? For the use to be **proportionate**, the positive outcomes should outweigh the negatives. Benefits that directly serve individuals or public interests may carry more weight in this balance than a benefit solely to the organisation’s convenience or profit
What privacy safeguards can we implement?	You can reduce privacy risks by adding safeguards. Re-evaluate the balance after applying mitigations (e.g. strong encryption might reduce breach risk; bias testing and tuning can reduce discrimination risk). If after mitigations the residual risks are low and benefits remain high, the use is more likely proportionate

If the analysis shows that privacy risks would be out of proportion to the benefits, either the system should not be used or further safeguards may be needed.

Privacy Safeguards – Mitigating Risks to Achieve Proportionality

- Consider the following types of safeguards that could be implemented:
  - Data security protections
  - Minimise data collection
  - Define data retention periods and automate deletion
  - Restricting use to original purpose only
  - Bias and accuracy checks
  - Human oversight
  - Transparency measures and choice

Integrating Proportionality into PIAs

- Update your PIA templates to include an assessment of necessity and proportionality.
- Present this as a summary section in the document before you get into the detailed analysis.
- The analysis you undertake throughout your PIA will identify the privacy risks and safeguards that are associated with the system or initiative being assessed.
- Define a periodic review process, based on risk, to ensure the requirements of the draft code are met.
- This will have the added benefit of making your PIAs a living document.
- It can be extracted and published, in full or in summary, as required.
- Also consider publishing all your PIAs for transparency purposes.

Some Practical Steps

- Build an inventory of the collection and use of biometrics in your organisation.
- Develop an internal policy for the collection and use of biometric information.
- Train and raise awareness, particularly in your technology teams.
- Engage stakeholders early and often (both internal and external).
- Monitor legal developments and international trends.
- Build transparency into your systems as a design principle.
- Assume any use of biometrics may be subject to scrutiny and make sure the business is comfortable with it – if you're not willing to tell your customers about it, maybe you shouldn't be doing it.

INFO by Design

It's about them - putting your customers at the centre
of how you manage their information

Questions?

CONTACT US

Feel free to contact me if you would like support or to discuss any of the topics covered today in more detail.

☎	**Phone**	: +64 27 773 7766
✉	**Email**	: paul@infobydesign.co.nz
🌐	**Website**	: https://infobydesign.co.nz