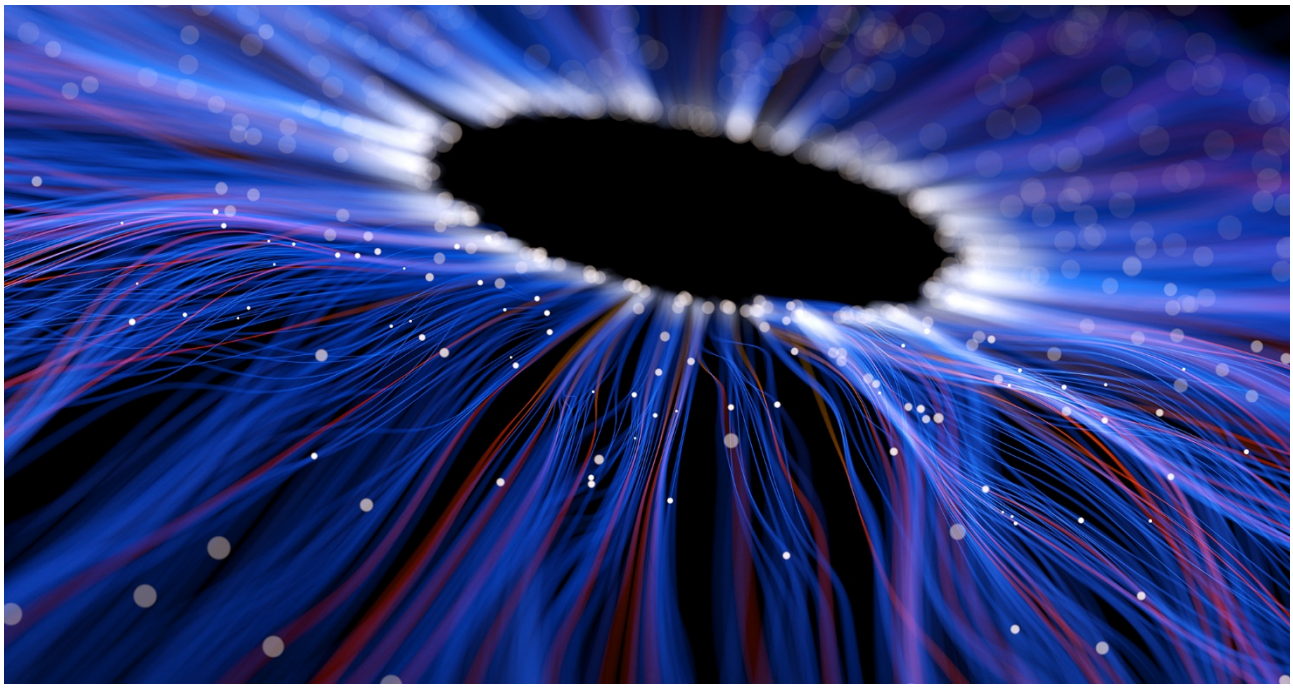
HERBERT SMITH FREEHILLS



Herbert Smith Freehills submission to the Australian Human Rights Commission

Human Rights and Technology Discussion Paper

10 MARCH 2020

HERBERT SMITH FREEHILLS

10 March 2020

Human Rights and Technology Project
Australian Human Rights Commission
Level 3, 175 Pitt Street
Sydney NSW 2000
tech@humanrights.gov.au

Our submission to the Discussion Paper

Herbert Smith Freehills appreciates this opportunity to respond to the Discussion Paper on Human Rights and Technology (the **Discussion Paper**) published by the Australian Human Rights Commission (**AHRC**) in December 2019.

In this submission, we focus on one key proposal, which we consider to be both an urgent priority (given its current prominence in public debate), as well as illustrative of many of the key issues raised and themes covered in the Discussion Paper, particularly in Part B of the Discussion Paper.

Chapter 6 of the Discussion Paper outlines Proposal 11, as follows:

> *The Australian Government should introduce a legal moratorium on the use of facial recognition technology in decision making that has a legal, or similarly significant, effect for individuals, until an appropriate legal framework has been put in place. This legal framework should include robust protections for human rights and should be developed in consultation with expert bodies including the Australian Human Rights Commissioner and the Office of the Australian Information Commissioner.*

We consider it critical that there is a careful and considered assessment of the impacts of the use of facial recognition technology, particularly in the context of decision-making in both the public and private sector.

We also support broader consideration (as part of a collaborative, multi-stakeholder process) of how facial recognition technology — and the data collected, analysed and generated through the use of that technology — can be designed and deployed responsibly.

However, in assessing the potential benefits and harms of this technology, and the proposed responses to it (including bans and moratoriums), it is important to consider both the current state of facial recognition technology as well as the likely emergence of, and need for coherent responses to, similarly rights-impacting technologies (or new uses of existing technologies) in the future.

In that context, we caution against a tendency towards reliance on short-term or otherwise reactive responses, including bans and moratoriums, as a 'default' response to such new and emerging technologies, for the reasons set out below.

Proposal 11: Responding to facial recognition technology

What is unique about facial recognition technology?

In the past year alone, facial recognition technology has received significant media attention and calls for specific regulatory interventions including bans and moratoriums. It is important to consider why facial recognition technology has attracted this attention, in contrast to other emerging technologies that may have the same rights-impacting features. This has particularly

been the case in respect of biometric data arising from facial recognition technology then being used in some areas of AI-informed decision making.

This Submission does not attempt to explore the benefits of facial recognition technology. Instead, we believe that the technology has benefits which individuals, industry and government will be eager to obtain and that a balance can be struck between these benefits and human rights.

However, in our view, it is the following interrelated factors that give rise to concerns raised in the Discussion Paper:

- the **specific, sensitive nature of biometric data** (that is, facial images) used as part of facial recognition technology, which is unique to an individual, universally available in respect of each individual, and easily accessible, as well as difficult to change or conceal;
- the associated **privacy considerations**, and in particular the potential for data collected from facial recognition technology to be combined and used with other personal data;
- the **performance and accuracy** of current facial recognition technology where it is used, and the impact that inaccurate results (false positives and false negatives) may have, particularly on marginalised communities, whether or not resulting from development bias or error;
- the potential **ease of collection, scale and ubiquity** of biometric data collected from facial recognition technology, which may become so embedded in daily life as to be difficult to understand and be aware of, much less opt-out of; and
- a broader breakdown of **trust in the technology sector** (the 'techlash') and corresponding concerns that **regulation is not keeping pace with technology**, such that specific regulatory interventions are required. This is a phenomenon that came into public focus last year but can be traced back to widespread concerns about mass government surveillance that have emerged over the last decade.

It is important to note that these factors are not unique to facial recognition technology. Facial images constitute only one type of data that can be used for identification purposes. Significant advances in data storage and data analytics technology mean that the collection and use of biometric information is growing not only in volume but also in variety. For example, biometric information can range from fingerprints and iris patterns to other individually unique identifiers less discernible to the naked eye (for example, heart beats and patterns of human movement).[1] Such identifiers are similarly universal, and are often easily and publicly accessible. In addition, there are a number of other new and emerging technologies (especially applications of AI-informed decision-making) that raise similar issues of performance and accuracy (including the potential for algorithmic bias and discrimination)[2] and of data collection and correlation.

Despite this broader context, many proposals continue to refer to 'facial recognition' in isolation. This narrow focus on facial recognition technology increases the risk that any regulatory responses will be insufficiently comprehensive, coherent or future-proofed.

Current proposals are narrow responses to narrowly defined issues

Internationally, there have been numerous proposals for, and some implementation of, bans and moratoriums on the use of facial recognition technology. In our view, the steps taken to date demonstrate that much of the discussion and regulation (proposed or realised) of facial recognition technology have been reactive and piecemeal in nature, and accordingly too narrow in approach.

---

[1] See e.g. Hug et al., 'Individuals have unique muscle activation signatures as revealed during gait and pedaling' (2019) 127(4) *Journal of Applied Physiology*.

[2] See e.g. Discussion Paper, 87; Neil Vigdor, 'Apple Card Investigated After Gender Discrimination Complaints' *The New York Times* (10 November 2019) https://www.nytimes.com/2019/11/10/business/Apple-credit-card-investigation.html; Ariana Tobin, 'Employers used Facebook to keep women and older workers from seeing job ads. The Federal Government thinks that's illegal' *ProPublica* (24 September, 2019) https://www.propublica.org/article/employers-used-facebook-to-keep-women-and-older-workers-from-seeing-job-ads-the-federal-government-thinks-thats-illegal; Vicki Sentas and Camilla Pandolfini, *Policing Young People in NSW: A Study of the Suspect Targeting Management Plan* (Report, 25 October 2017).

A regulatory patchwork

The current regulatory landscape, as it relates to facial recognition technology, is fragmented geographically as well as in its scope of application, despite much of the technology having cross-border application.

In the United States, bans and moratoriums have been implemented at the local level and proposed at the state and federal level. The United Kingdom and European Union have proposed bans and moratoriums that have ultimately been abandoned. Most proposed bans and moratoriums fail to specify timeframes and goals for when they will be considered to have served their purpose (that is, when appropriate safeguards for use of the technology are deemed to have been established). Significantly, almost all applied only to public sector use of the technology. In general, although bans have been implemented at a local level in the United States, it appears that regulatory responses are moving away from outright bans on the technology. Such proposals have either been entirely abandoned, or regulatory responses have now been accompanied by clear parameters and timeframes within which they will apply.

Although it is critical to respond to the issues raised by facial recognition technology — and indeed other new and emerging technologies — a fragmented and inconsistent approach not only limits the effectiveness of potential regulatory responses but also makes it difficult for potential users to plan for and 'future-proof' the implementation of such technology.

Narrow priorities

As noted in the Discussion Paper, *'a focus on regulating AI as technologies would not be as effective as regulating AI in its context and use'*.[3] We remain concerned that the current approaches to facial recognition technology focus too narrowly on what the technology is, rather than the manner in which it is used and the outcomes achieved by it.

This leads to two problematic outcomes:

1. too little emphasis is placed on whether each technology is effective, fit for purpose or accompanied by appropriate safeguards; and
2. this narrow focus does not allow room to consider the broader contexts in which such technologies (and the data collected by them) will be used.

As noted above, certain biometric data such as facial images is easily accessed and collected, potentially even without the awareness of the subject of that information, and is difficult to alter and conceal. However, the power of this data is amplified when it is combined with other information collected about that person, creating a detailed, highly individualised profile of an individual. Such unique identifying metrics enable surveillance capable of almost literally following an individual around in their day-to-day life.

This ability to connect and consolidate devices, data, systems and networks is core to many forms of new and emerging technologies, not just facial recognition technology. A narrowly targeted ban may not fully address the risks presented by such merging and scaling of data. Further, as a general principle, analysis of the harms and benefits of digital technologies will not necessarily be resolved through regulation of a specific form of technology. Regulation can be more effective when it is technology-agnostic and focused on the impacts of the technology and in particular the way in which it is implemented and used.

Impeding innovation

Our view is that regulation of itself, is not necessarily an impediment to innovation. Indeed, regulation can and has acted as an innovation 'enabler' for industry, helping active participants establish or maintain consistency of operations, legal parameters and a social licence to operate,

[3] Discussion Paper, 144.

and accordingly create an environment for industry to flourish. For this to be the case, however, regulation must be implemented in a way that advances a coherent and holistic global standard.

The imposition of a ban or moratorium on a specific technology is unlikely to further the development of a global standard. Instead, a ban or moratorium will stifle innovation — and, perhaps most importantly, it could have a significant cost to *responsible* innovation.

A ban, or temporary moratorium, in Australia will result in a lost opportunity to test, design, interact and augment the development and use of facial recognition technology and other similar emerging technologies in a variety of contexts. At the same time, this technology will continue to be developed in other jurisdictions, and will ultimately (once any moratorium is lifted) become available to be licensed in Australia. At that point, the technology is likely to have advanced significantly without the benefit of input from Australian governments, experts, consumers and developers.

We support the position in the Discussion Paper that a coordinated and considered response could form part of a greater strategy to enhance Australia's reputation in this respect. That is, such a response could assist in *'developing Australia's reputation for AI that protects human rights and the commercial rights of inventors could help build the nation's competitive edge'*.[4]

Conversely, a ban or moratorium, could result in more than just a missed opportunity for Australian innovation generally. An overly narrow and fragmented approach, ultimately increases the risk of losing a real and present opportunity to set a clear, coherent and comprehensive standard for responding to the challenges of new technologies. We believe Australia is well placed to develop an ecosystem in which innovation is encouraged, while also promoting strong human rights protections and principles of fairness, equality, accountability and transparency.

The path forward

In light of the specific challenges raised by facial recognition and biometric identification technologies (as well as other new and emerging technologies), we think it is appropriate to consider, and seek to implement, a path forward without resort to an outright ban or moratorium focused on a particular type of technology such as facial recognition.

This path forward could take the form of an adaptable framework for the *use* of new and emerging technologies — including facial recognition and other biometric identification technologies — with the potential to significantly impact upon human rights.[5] This framework can, and should, be crafted as part of a collaborative, multi-disciplinary and multi-stakeholder process in order to ensure that the principles under the framework are appropriate, proportionate and contain the necessary safeguards.

We consider that at a minimum, such a framework should be guided by core principles of responsible use, as articulated in the Discussion Paper to *'extend beyond legal liability, to include also ethics, fairness and good governance'*.[6] In relation to biometric identification in particular, this means a focus on responsible use at all stages of the technology lifecycle, rather than relying upon models that seek to focus solely on individual control, such as 'notice and consent' processes. Such models are unsuited to technology that may be so embedded in users' daily life as to be difficult to understand and be aware of, much less opt-out of; in particular, these models are likely to place an unfair burden on the individual (rather than the regulator or actor employing the technology) to assess the risks and outcomes of consent to, or use of, the technology.

Notwithstanding the potential for a ban or moratorium to hinder responsible innovation and push the advancement of new technologies into unregulated jurisdictions, there are valid reasons for imposing a moratorium in the immediate term to curb development of facial recognition technology on a temporary basis. We recognise that such action may allow for a cohesive framework to be

[4] Discussion Paper, 133.

[5] This could also align to the proposals contained in the Discussion Paper in relation to the use of such technologies in decision-making where they have a 'legal, or similarly significant, effect for individuals'. See Discussion Paper, 104.

[6] Discussion Paper, 88.

developed and implemented before potentially harmful, or insufficiently rights-protective, practices evolve into accepted norms. In this respect, we agree with the comments in the Discussion Paper that there is a *'sense of urgency regarding the need to establish an expert body to provide proactive policy and legal guidance on rapidly evolving technologies'*.[7] This sense of urgency must be translated into proportionate and careful action.

Any regulatory action, including proposals for a temporary ban or moratorium, will need to be carefully and specifically defined in order to ensure that its application and parameters are clear, its objectives and impacts are measurable, and that it ultimately helps to foster an environment of responsible, rights-compatible use of the technology in Australia and globally. In particular, we suggest that:

- the application and scope of any ban or moratorium must be carefully crafted, having regard to the variety of potential applications of the underlying technologies. This should include appropriate limitations and exclusions, such as personal use of 'FaceID' on an iPhone;
- proposed regulation should remain consistent with and informed by changes in global policy, including having regard to any circumstances where similar proposals are ultimately abandoned in other jurisdictions, either before implementation or where they do not meet their stated goals;
- the design of any domestic regulatory framework should be informed by consideration of international legal standards and standards of responsible business conduct applicable in the private sector, including the UN Guiding Principles on Business and Human Rights and the OECD Guidelines for Multinational Enterprises, as well as relevant industry standards and policies;[8] and
- specific timeframes and goals are set and monitored on an ongoing basis, to ensure the progress of appropriate regulation and allow for the timely adoption (where appropriate) of facial recognition technology. These goals should be pursued as part of a multi-stakeholder engagement and participation approach with an eye towards the development of a cohesive policy framework and the implementation of an appropriate, responsible use model.[9]

We are pleased to provide this submission to the AHRC and would welcome the opportunity to discuss our comments further.

Yours sincerely

[redacted]
Partner
Herbert Smith Freehills
[redacted]

[7] Discussion Paper, 131; In addition, we are in favour of the AHRC Proposal 19 for the establishment of the independent statutory office of an AI Safety Commissioner and its proposed mandate, as set out in the Discussion Paper, 146.

[8] We note the extensive discussion of these matters in Chapter 2 of the Discussion Paper.

[9] For example, the methodology and principles designed by the World Economic Forum's Pilot Project on facial recognition provide several potential characteristics for the implementation of a successful framework on a pilot or proof of concept basis, albeit confined to one specific use case at present. See World Economic Forum, 'A Framework for Respons ble Limits on Facial Recognition: Use Case: Flow Management' (White Paper, February 2020).

About Herbert Smith Freehills

Herbert Smith Freehills is one of the world's leading commercial law firms, bringing the best people together across our 26 offices globally. We are pleased to be a major project partner of the Human Rights and Technology Project of the AHRC, and appreciate the opportunity provided to us to contribute to the Project as members of the Expert Reference Group.

At Herbert Smith Freehills, we believe there is an important role for the private sector, and law firms in particular, to play in considering and implementing frameworks to address the legal, ethical and human rights concerns arising from new and emerging digital technologies.

In our capacity as a trusted professional advisor to a large number and variety of clients, across a wide range of industries and sectors, we have experience supporting our clients to thrive in the digital age and navigate novel technological changes. Herbert Smith Freehills has a number of specialist practice areas that consider the legal and regulatory issues arising in connection with technology and data. These specialists work closely with our business and human rights specialists. This submission was prepared by our cross-practice group, multidisciplinary Digital Law Group who are providing bespoke advice and practical solutions to the opportunities, risks and ethical and regulatory requirements brought on by digital transformation.

These experiences mean that we have a multi-dimensional perspective on the issues raised by new and emerging digital technologies and their impact.

[redacted]

[redacted]