A group of experts in Ireland are sounding the alarm about the Minister for Justice's ongoing plans to enable An Garda Síochána's use of Facial Recognition Technology (FRT). However, leading academic and civil society organisations have warned that the risks are too significant. Members of the Oireachtas justice committee, the Green Party and Labour have now also expressed concerns.

Why are experts worried? A primary concern is that FRT is a form of mass surveillance. While criminal procedures permit policing surveillance, this is limited to reasonable suspicion of wrongdoing by individuals. FRT, conversely, has the potential to sweep up in unrestricted ways highly personal data of large numbers of people who are not suspected of crimes.

The use of body-worn cameras with FRT would turn gardai into roaming surveillance units. If allowed, there will be pervasive monitoring of the public without their knowledge or consent. Anyone passing a Garda - or a Garda dog or horse equipped with a body-worn camera - could be potentially scanned, identified, and catalogued in a FRT database. People won't even have to be suspected of a crime or even have communicated with a Garda for the surveillance to take place. This is dystopic.

Other risks are unaddressed. FRT is hardly the silver bullet to social problems of criminality given significant scientific evidence demonstrating accuracy and bias concerns - in research, development, deployment, and decision making. The underlying technologies that make up FRT systems tend to differentiate, target, and experiment on marginalised groups.

Further risks will emerge. This type of data-driven technology, once adopted, can generate new harms at a speed and scale that would have previously been unattainable. The role of FRT in contributing to discrimination and exacerbating existing inequalities would have massive social impacts. For example, ongoing research consistently demonstrates that FRT processes some faces more accurately than others, linked to key characteristics such as skin colour, ethnicity, and gender. This requires regulators to ask whether FRT can be compatible with democracy and beneficial to all of society.

As a mode of mass surveillance, FRT puts people's privacy at risk without due cause as people's images are run through facial recognition software against thousands of images on the low end of the scale. Most systems "rely on large databases containing millions of images, many scraped from social media and other databases without the user's consent". In theory, imagery from any camera, from any period, could be fed into facial recognition software and matched within its database.

Facial pattern recognition is a form of remote biometric recognition which is deemed as high-risk under the European Artificial Intelligence Act. This type of biometric recognition is seen as especially concerning in the context of law enforcement as its misuse could easily lead to human rights abuses. Other recent reports have recommended that remote biometric recognition in public areas needs to be halted until it is proven that the systems comply with privacy and data protection standards.

FRT is also an intrusive technology by virtue of how it operates. The chilling effects to freedom of peaceful assembly and freedom of expression have been seen when law enforcement authorities have previously used FRT to track down protestors by cross referencing CCTV and other video imagery against designated databases. The possibility of applying FRT to contexts other than serious crimes and human trafficking imagery could be very tempting to law enforcement and we could see instances of function creep occur where FRT starts to be used in cases and contexts beyond what was originally stated.

Function creep has been seen in other European countries, such as Austria, where FRT was initially to be used for serious crimes but was later reportedly used by police to identify protestors. The use of technology for a different purpose could also occur if authorities do not receive the correct training. This is a concern that cannot be dismissed in this jurisdiction. An Garda Síochána has been criticised by the Data Protection Commission for not applying data protection law with regard to existing surveillance technologies, while concerns have been raised about the high risk of data breaches by gardaí, and in particular how they handle CCTV, due to a lack of data protection training. Function creep is also a live concern when we have other Government departments using facial image matching software in contexts where marginalised groups are predominantly affected and for systems designed to tackle so-called welfare fraud.

Lastly, the broadscale adoption of FRT by the Gardaí would result in net-widening where the technology contributes to expanding social control over larger populations. Linking back to this idea of mass surveillance, the use of FRT normalises the idea of constantly being watched.

New technologies of surveillance are often offered as the solution to (deeply complex social) problems, as if these problems are 'bugs' that can be 'fixed' through technology. However, we need to think critically and question if the technology is the solution or if it will contribute to creating more social problems and unrest. We must ask: Should policing forces use new surveillance technologies like FRT simply because they are available for purchase?

Interventions from the Oireachtas Justice Committee and political party leaders are therefore very welcome by experts. The concerns are too great to push through a Bill amendment legalising risky policing FRT.

By Dr Ciara Bracken-Roche (Maynooth University School of Law and Criminology), Dr Elizabeth Farries (UCD Center for Digital Policy), Olga Cronin (Irish Council for Civil Liberties)