Premium Opinion Home / Business

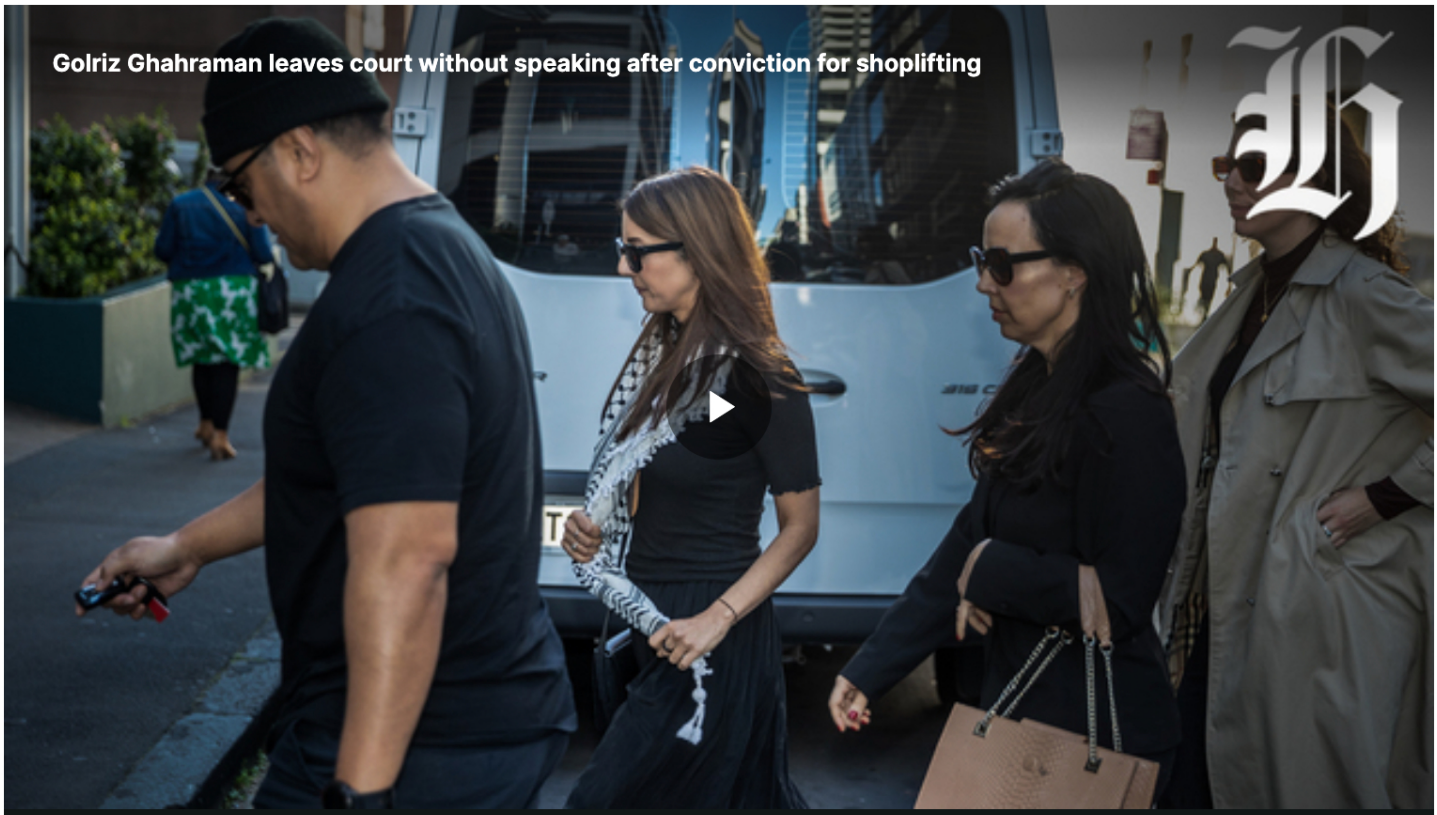
Golriz Ghahraman case brings justice system into the spotlight – Sasha Borissenko

Opinion by

Sasha Borissenko

NZ Herald · 22 Feb, 2025 09:00 PM · 7 mins to read

Freelance journalist who has reported extensively on the law industry



NOW PLAYING • **Golriz Ghahraman leaves court without speaking after conviction for shoplifting**

Judge June Jelas denied the Golriz Ghahraman's request for a discharge without conviction. Video / NZ Herald

THREE KEY FACTS

- **The photo of Golriz Ghahraman being questioned in a supermarket was leaked by a Pak'nSave security guard.**
- **Samoa's minister of police says he was the victim of a similar leak from Pak'nSave to undermine his political position.**

- **Security guards at Pak'nSave Manukau have been accused of trying to extort money out of shoppers, including taking their photographs.**

This month, the *Herald* revealed an image of former MP Golriz Ghahraman, purportedly taken from security camera footage when she was recently accused of shoplifting, had got into the hands of third parties. The key players – the supermarket, the security software company and the police – initially said they didn't know how it got there. The supermarket head, Foodstuffs North Island, then confirmed a security guard was at the heart of the leak. The lack of checks and balances and privacy ramifications have spooked me to my core.

To start, who knew police could investigate you for "shoplifting" without reaching – or having the opportunity to reach – the checkout? Secondly, I never realised using a grocery-designated tote bag as a basket was not a "thing". There is also a sense of violation, paranoia at worst, realising my former tote/basket practice could've been recorded or flagged in a "Big Brother is watching" fashion.

Finally, in a digital age where civil liberties are rapidly eroding and the extreme far-right gains momentum, this all sits uncomfortably, knowing it's possible that said footage could end up in the hands of those wanting to cause physical harm.

Innocent until proven guilty?

Let's rewind to the police's first official statement: "The shoplifting occurred at the Pak'nSave in Royal Oak on October 12, 2024 …".

Police decided against laying charges for "item taken", valued at $40, referring to the Solicitor-General's Guidelines for Prosecution, which include evidential sufficiency and a public interest test, the statement read.

The term "shoplifting" evokes a judge, jury, and executioner quality, which contradicts the fact no charges were laid. Sure, the statement was amended after input from Ghahraman's lawyer. But not everyone may have the same access to a lawyer. There's also the issue of giving people the benefit of the doubt.

Yet, a police spokesperson told me that in "advising no charges had been filed, there was no inference that an offence was committed". Tell that to 4Chan.

Even if there were charges, you must question how much time, money and resources would be used to establish a case over $40 – especially in this resource-poor economy. (As an aside, the police's media team missed my deadline, citing "capacity issues", ironically.)

In response, the spokesperson said police were "mindful of the individual's privacy. We are not going to comment any further around this".

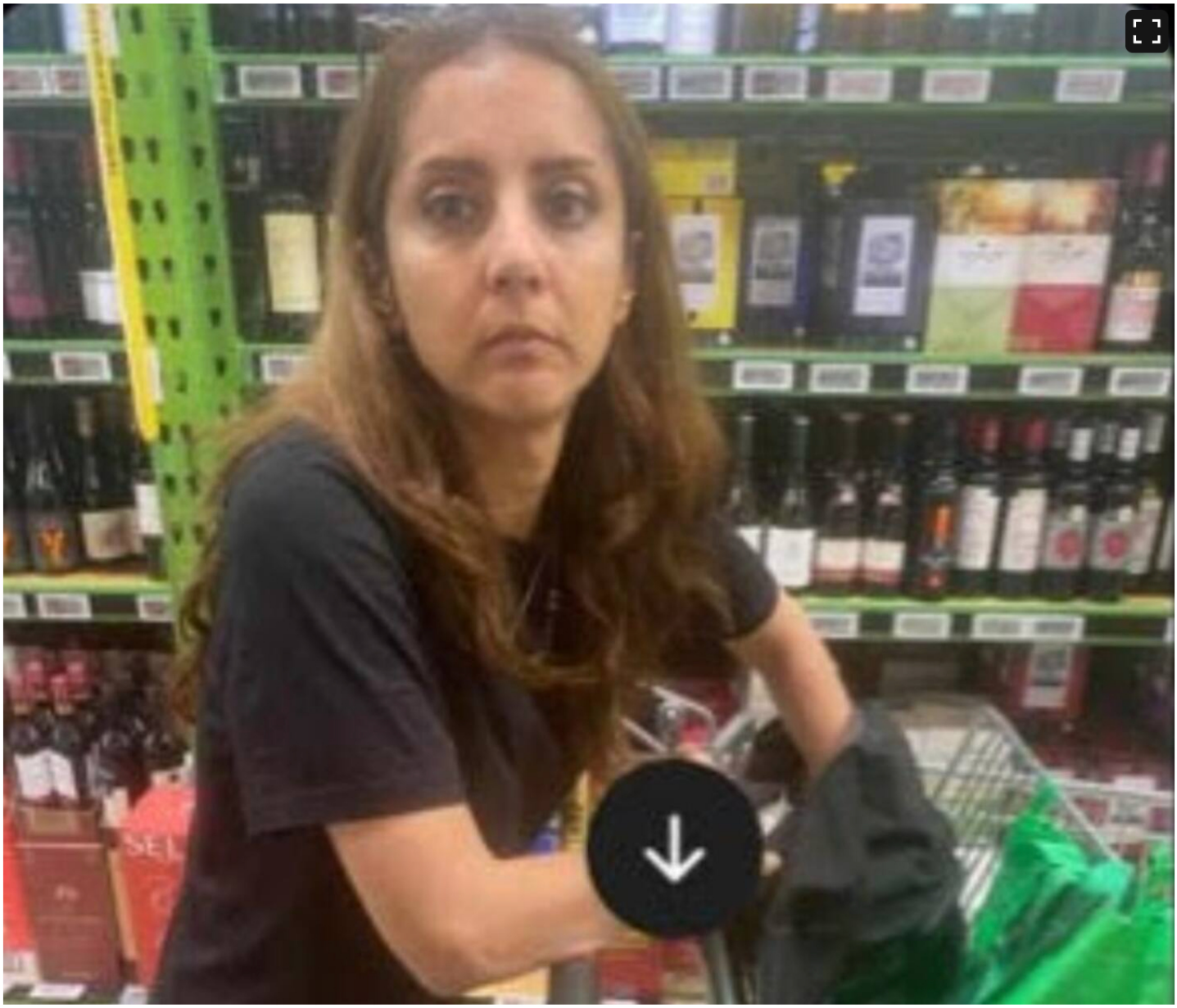
Rule of law – who needs it?!

Speaking of privacy, the *Herald* reported police unsuccessfully sought to include the alleged (and ultimately charge-free) incident before Ghahraman's appearance in the High Court in October. Having pleaded guilty to four counts of shoplifting earlier last year, the former MP sought a discharge without conviction, which would improve her chances of obtaining a practising certificate.

Putting aside the nature of the appeal, it's wild police allegedly tried to use unsubstantiated information that could potentially influence a decision. Why else would the information be included? This is one of the reasons we have the Privacy Act.

There's also the Evidence Act. For example, even in the most challenging and horrific cases before the courts, lawyers and police must navigate legislative hurdles to include evidence of past convictions. This refers to the past, not to incidents that, in this case, didn't result in a charge.

In response, the spokesperson said police were "satisfied all staff were notified appropriately and acted responsibly and appropriately [sic] with the information".



Former MP Golriz Ghahraman in an image purported to be from security footage.

Needle in a haystack? Tech's got you covered

This brings me to the fundamental issue – appropriateness, even – of accessing the information in the first place.

In its statement, police said the alleged incident "was reported to police". Yet this is one of 20,000 reports made by Foodstuffs annually.

"We ask our store teams to log every incident of shoplifting into our retail crime reporting platform, which is then made visible to the police who determine what to do next," Foodstuffs told the *Herald's* David Fisher.

It's thus surprising the police spokesperson told me "a police file number was assigned the same day and assessed two days later as part of staff routine screening of shoplifting offending". (See resourcing, above.)

There's a fine line between what's actively reported, mass surveillance, and digging for dirt.

In its defence, Auror – the retail crime reporting platform in question – would not characterise its services as mass surveillance, a spokesperson said. It neither owns nor operates cameras or hardware, which are privately owned and located on private premises.

Instead, the software acts as a database, allowing "retailers to voluntarily share information with police about suspected

crimes and in-store events after they occur". Auror is simply an agent and processes information (that ultimately belongs to the retailer) after the fact.

"Retailers have recorded this information for many years using manual and unsecured processes such as CDs, USBs, and 'walls of shame'."

It's no wonder retailers love it, with 90% of New Zealand's "big-box" retailers reportedly on board. The company is also making waves in the UK, Canada and Australia. Last year, it announced it had partnered with 28 state-level organised crime associations in the US.

Oversight blind spot

So what's the issue? The lack of checks and balances around accessing and using information that's been outsourced and flagged by people other than police.

According to the Auror spokesperson, the information is processed under strict safeguards, and the software is secure and auditable. In this instance, Auror provided audit information to its customers to assist them with their own inquiries.

"[All] users must comply with their own internal operating policies and our terms of use, which requires them to not share information outside the software with unauthorised users."

By default, retailers cannot share information with one another, the spokesperson said.

"However, retailers can choose to share information with one another and do so through sharing agreements separate to the software, but which they can choose to facilitate through the software." Hell on a stick.

Given my tote/basket faux pas, I'd certainly want to know if I've been flagged in a system that could in theory – depending on the sharing agreement – find itself in different hands, and which police reportedly access hundreds of times daily.

The police spokesperson said otherwise: "All police have access to Auror but only a small number of staff will access the Auror retail platform as part of their business role. All police staff are required to complete online training modules on privacy considerations."

Discover more

- 'Sorry': Foodstuffs admits staff leaked photo of ex-MP ...
- 'Obsessed' and 'weird' - Ghahraman critical of police ...
- Image leaked of Ghahraman during Pak'nSave shopping ...
- Ghahraman's $150 shopping incident: Pak'nSave never ...

Yet across the ditch, Australia's privacy watchdog, the Australian Information Commission, launched an investigation following a report exposing the Australian Federal Police's (AFP) use of the software without proper oversight.

Internal AFP emails revealed over 100 police staff used the software to collect data from retailers and integrate police information into the system without agency guidelines.

Auror said the AFP undertook an internal privacy assessment of the software in 2023 and resumed using Auror in mid-2024.

"The OAIC notified Auror in October 2024 that it would not be pursuing an investigation and would not be taking the matter further."

'Say it, forget it, write it, regret it'

Unsurprisingly, we're now seeing cases rolling through the courts questioning whether there is enough oversight. The jury is out in the higher courts, where the District Court reluctantly gave police the go-ahead last year. I'd go on, but criminal judgments were temporarily unavailable on the District Court website – resourcing issues, go figure.

Until then, the police spokesperson said it regularly reviews its use of technology. An unrelated Auror assurance review and audit of its use of third-party automated name plate recognition technology kicked off last year, and results are pending.

However, in the context of the former Green MP, the passing-the-buck nature of investigating the natural justice issues involved in every stage of the supply chain threatens to undermine public confidence in our justice system.