FRANKS | OGILVIE
COMMERCIAL & PUBLIC LAW

PO Box 10388
The Terrace
Wellington 6143
New Zealand

14 February 2020

Hon Stuart Nash
Minister of Police
Parliament Buildings
Wellington

MATTER NO:1361.1
OUR CONTACT: Stephen Franks

By email: s.nash@ministers.govt.nz

Dear Minister

DATA SECURITY FAILURE IN THE BUY BACK NOTIFICATION SYSTEM

1. We advise the Council of Licensed Firearm Owners (COLFO). We attach a copy of an affidavit from a licensed firearm owner who saw other people's data when logged in to the notification system in late November/early December 2019.

2. The affidavit is evidence –

   - that not just dealers were able to gain unauthorised access to personal data
   - that more than one person saw this information
   - that Police did not follow up the report of the breach.

3. After lengthy conversations with the person who provided it, we have no reason to consider that it is untruthful.

4. The affidavit giver says that Police heard directly from him/her about the access. So despite evidence that the dealer they acknowledged, was not the only person who had told them they believed they'd wrongly seen personal information, the Police did not try the obvious – offering whistle blower reassurance to learn as much as they could from anyone who offered. Instead they persisted in the course adopted on the first day after the public disclosure, threatening people, trying to discredit COLFO concerns about potential widespread access and rejecting our request for comfort we could pass to potential informants.

5. If the government had treated the privacy of firearms owners as they have ACC claimants, hospital patients, welfare beneficiaries and other recent victims of data privacy lapses, we would by now have a reliable independent report into the incident. Anxious informants would have had assurances to make sure that the independent investigation could get to the bottom of what actually happened. And vows to "ensure it never happens again" would at least have been followed by an explanation of future precautions. We are not sure that firearm owners were favoured even with the empty promises.

Why the affidavit is redacted

6. The affidavit has been redacted to impede identification. To respond to serious concern in the early days after the first disclosure of the data security breach, we offered confidentiality to people who

reported unexpected access to information. A number of people initially made that claim, or were reported to have done so by another lawyer. Nearly all later declined or ceased to communicate after the initial contact. Most simply did not respond to our requests for confirmation. Others had various explanations:

a) a fear of prejudicing a decision on their surrender compensation due;

b) anxiety not to get on the wrong side of the Police, going into an unknown era of Police power in firearms licencing and registration;

c) worry about what they'd heard as Police threats of action against people who had breached the security.

7. That last reason was powerful, despite our advice that if they had not used the information we saw little practical likelihood of a basis for enforcement action.

8. COLFO was willing to work with Police to discover the scale of the breach and to ensure people's information was not misused. We were instructed to assist if we could. Police had made public threats. So it needed Police reassurances that people cooperating would not risk penalties. We asked Police for such reassurance without useful result. Copies of **relevant letters (2) are attached**.

My firm does not lie and did not lie

9. It has been reported to us that you described Franks Ogilvie to at least one MP as having lied about the multiple reports of unsought access to personal data. If that report is true the attached document should elicit an apology. If you did not make such a claim in any form we would appreciate knowing that.

10. I did not lie when I was an MP. My firm does not lie now. It is a very serious charge to make against lawyers. We try hard to avoid giving unwarranted credence to information given to us, that we have been unable to verify. When sources closed up after the data breach disclosure we were hamstrung. But we had been careful to indicate the nature of our instructions and the basis for our advice.

11. We propose to copy this letter to the Commissioner of Police. If you did not make the statement attributed to you, and it was instead made by Police, perhaps those who have been advising the Select Committee, I hope the Commissioner will apologise. We do not lie.

Police threats instead of focus on minimizing risks and reason to worry

12. To our amazement until this week we were never called directly by Police to ask what help we could offer, or to discuss what comfort we could pass on to people who initially claimed to have seen the information of others.

13. Instead of taking natural steps to establish the scale of the problem from those who had first made it public, the first 30 hours of visible Police response after public exposure seem to have been dedicated to public threats and attempts to trivialise the issue. Police reputation damage control seems to have weighed above the interests of those whose information had been seen. If that had been the response of a private company to a Privacy Act breach, the Privacy Commissioner would have been rightly scathing.

14. Your conduct Minister reinforced that strategy and priority. A few hours after the breach became public you attacked this firm by name in a media conference, standing beside the Prime Minister. I have known you well enough over the years for you to give me a call. I would not stand on dignity.

I'd have been happy to talk if you'd asked a staff member to call. So without asking for help from people likely to know best, Police and Ministerial communication denied directly some circumstances we thought we knew and expected to substantiate from direct reports.

Your choice to demonise, instead of seeking cooperation?

15. We consider the Police response, and yours, to be revealing of your government's true priorities in the firearms law changes. I am sure it did not start out as a cynical political stunt. We think many if not most firearms owners understood and would have accepted the intention to ban weapons likely to facilitate terrorist multiple murders. But some senior police and your government have since abused that community unity to make changes that have nothing to do with that risk. You've chosen to exploit the Christchurch massacre. You will be aware of the Islamic Women's National Council submission, asking the government to stop tying your second tranche of law change to the deaths of the 51 people in Christchurch, despite their general support for the Bill.

16. The public wished to see a conspicuous commitment to safety. That wish has been misused to vilify innocent licensed firearms owners. You have seized media opportunities to brand their representatives, our clients, as political enemies. You've tried to transplant and fertilise an alien meme of tribal hatred over gun control. New Zealand was an internationally admired model of Police/citizen collaboration on firearms law. We have a high number of civilian firearms per head, and we had a very low number of criminal firearms injuries and death.

17. If you want chapter and verse on your propagation of US political memes here, we can oblige.

The result, for your firearms registry, and for Police effectiveness

18. The reaction of the Police to the data breach was thoughtless, given the need to for widespread trust if your registry is to work at all. It is supposed to record information that will be a burglar's fantasy shopping guide. Especially after the failure of last year's buy-back, you and the Police should know how important it will be to get broad community consensus that compliance is normal and worthwhile, and safer than non-compliance.

19. So Police should have seized the opportunity of the established data breach to show their top priority was to learn as much as possible about the leak. They should have bent every effort toward minimising the worry of people who had registered the location of many valuable firearms. If that meant making it plain that no one who came forward with information would suffer from that, it would have been a small price to pay, to build trust. Instead you and Police issued threats.

20. Even as late as Monday this week, a Deputy Commissioner declined to give that assurance when pressing us to provide the name of the person whose affidavit accompanies this letter.

21. You and the Privacy Commissioner will recognise that people reasonably place personal and family safety concerns first. If they fear that the registry data is insecure, and could direct criminal attention to them, it is fatuous to disregard a scenario of widespread disobedience to registration demands. The outcome from the registry expenditure could be the same as Canada. After the real priorities of Police and your office were shown in the immediate response to the news of the data leak, too few sensible firearm owner s will trust you, the government, or the Privacy Commissioner

22. Instead your public condemnation aided the Police in trying to discredit people who reported a problem.

Where is the data security and privacy evaluation of the registry?

23. Now you are proceeding with a Bill to create a registry that will be a richer target for deliberate hacking. It is proceeding without any evidence to reassure tens of thousands of New Zealand families facing privacy risks more serious than mere embarrassment. No one appears to have weighed registry costs and risks against benefits. They can't. The benefits or purposes have not been stated.

24. The Privacy Commissioner expressed concern, but did not follow up. The Select Committee's only response to privacy risks is more requirements in the Bill to consult with him.

25. The Privacy Commissioner could not have had the information needed to weigh privacy risks against benefits. There is:

- No statutory statement of purpose for the registry;
- No published specification for data safety
- No other useful statement of the registry purposes (ignoring slogans like "for gun safety")
- No definitive cost information. The only estimates seem unrealistic if the system is to have high protection against penetration, plus wide real-time Police operational access
- No success benchmarks or published assessments of the factors that will determine if it gets enough cooperation to avoid abandonment (like the Canadian one dumped after spending more than $1bn).

26. You know that widespread non-compliance would make the registry useless, if it is not already doomed to operational uselessness by the acknowledged proportion of firearms now outside the law, and of course the sensible 30 day allowance before reporting changes in firearm location. Firearm owners know that data security risks matured last year. No-one denies that thousands did not surrender firearms that should have been in the buy-back – so why should Police who have sacrificed firearm owner trust not expect substantial non-compliance with a more threatening registry?

Yours faithfully
FRANKS OGILVIE

Stephen Franks
Principal
stephen.franks@franksogilvie.co.nz.

cc Mike Bush MNZM
Commissioner of Police
180 Molesworth Street
Thorndon
Wellington

mike.bush@police.govt.nz