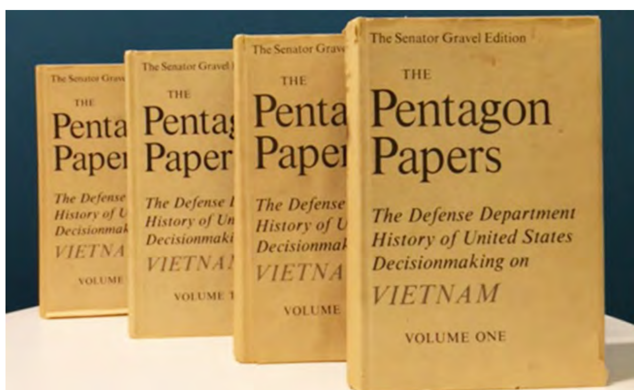
"All that is needed for evil to prosper is for people of good will to do nothing"—Edmund Burke

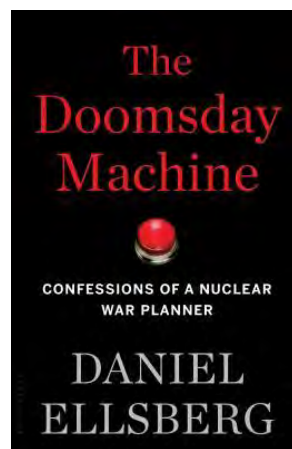
The Whistle

No. 115, July 2023

Newsletter of Whistleblowers Australia (ISSN 2205-0299)

Daniel Ellsberg, 1931–2023, whistleblower extraordinaire





Articles and reviews

Queensland's newest Whistleblower of the Year

A FORENSIC SCIENTIST who raised concerns about the testing of DNA samples from crime scenes at the scandal-plagued Queensland Health Forensic and Scientific Services laboratory has been named the state's latest Whistleblower of the Year.

Queensland Whisteblowers Action Group (QWAG) secretary Greg McMahon praised Alicia Quartermain's actions, which he said were "particularly brave and dutiful to the public interest."

Alicia Quartermain

"The 2022 award has been given to Ms Quartermain for her disclosures about the drop in standards of scientific work … and omitting tests necessary in the investigation of suspected criminal offences," Mr McMahon said.

"What was particularly brave, and dutiful in the public interest, in Ms Quartermain's response to the dismissal by higher management of her concerns, was the initiative she took in undertaking her own successful research and testing of samples and cases that she suspected to have been prematurely dismissed."

He said Ms Quartermain — who gave evidence last year before commissioner Walter Sofronoff KC at an inquiry into the state's forensic DNA testing laboratory — could have been disciplined or charged for trying to expose wrong-doing at the time.

QWAG also announced Queensland Police Union President Ian Leavers was the recipient of the group's 2022 Whistleblower Supporter of the Year Award. The awards — in their 29th year and voted on at QWAG's AGM — recognise the integrity and the courage of whistleblowers, and the contribution of people who have been of outstanding assistance to whistleblowers.

Ian Leavers

"Mr Leavers stated his frustration at the Independent Commission of Inquiry into the Queensland Police Service (QPS) response to domestic and family violence last year, that reform processes in Queensland were based upon government repeatedly calling inquiries and never making any 'meaningful' change," Mr McMahon said.

"He described the situation faced by police as 'working in a broken system', in which the workers were 'being set up to fail'.

"That struck a chord with whistleblowers in Queensland who have endured other broken systems … most recently in justice processes (interference in Archives, Legal Services, Auditor-General, Integrity Commission, the Courts and the Crime and Corruption Commission)."

Mr McMahon said QWAG was "eagerly awaiting the findings" of the Queensland Government's review into the Public Interest Disclosure (PID) Act, which covered the disclosure of information about wrongdoing in the public sector.

The review by retired Supreme Court judge Alan Wilson KC was commissioned following the Coaldrake Review, with the deadline for the final report extended to June 19, 2023.

In a submission, QWAG called for the establishment of a new independent body — a Whistleblower Protection Commission — to oversee and enforce the PID Act and provide support to whistleblowers.

"Whistleblower protection is the outstanding issue that has not been addressed properly in this state since Tony Fitzgerald's watershed inquiry into police corruption in the late 1980s," he said.

QWAG media contact Neil Doorley 0412 393 909

Kudelka J is Richard Boyle's undoing.

Cynthia Kardell

RICHARD BOYLE was a debt collection officer with the Australian Taxation Office (ATO) in Adelaide until he was walked off the premises on 6 September 2017. It would have been shocking to know that they knew what they were doing was wrong, but no less shocking to rue the times he'd given them the benefit of the doubt.

At the time he had screenshots or photographs of taxpayer information on his iPhone together with the audio of conversations he'd recorded covertly at a series of meetings from 19 April 2017. Both came to public notice in April the following year when the Australian Federal Police (AFP) raided his home, seizing his iPhone and computer. It was in the week before he was to appear on the ABC Four Corners news program "Mongrel bunch of bastards." The warrant specifically referred to Four Corners and Fairfax reporter Adele Ferguson and alleged he had illegally taken either originals or copies of taxpayer information, photos of ATO computer screens or emails.

The 23 criminal offences he now faces relate primarily to the information found on his iPhone and computer and ironically, what he didn't do with them.

Boyle remained on special leave until he was dismissed the following May. He submitted three public interest disclosures or PIDs from 12 October 2017 while he was on leave. I don't know the full circumstances surrounding the initial accusation of fraud made against him in November 2016 or its resolution in the following January, although it does seem to have driven his decision to covertly record conversations on his iPhone from April 2017. Boyle says they were to provide a relia-

ble record of what was said, but Kudelka J didn't buy it in her reasons for dismissing his claim for immunity from criminal prosecution on March 27 this year.

Richard Boyle

I think it fair to say that Richard Boyle was wrongly accused of fraudulently accessing taxpayer information in his capacity as a debt collection officer in November 2016. Those screenshots were of information he was required to access in the course of his work, which may explain why the charges were eventually downgraded to a breach of the code of conduct. Significantly, Boyle wasn't sanctioned for stealing them or for hanging on to them, but for continuing to help those tax clients he thought had been wrongly targeted with a garnishee order. Boyle was using the screenshots as an aide-memoire. I call that sensible, and diligent.

Then, in the following February, with no real resolution in sight, the ATO offered him a payout and a statement of service, but without any admissions as to their continuing the "garnishee" scam. Boyle declined, which is why he continued to be a thorn in their side, and why the November 2016 charges were dragged out again in September 2017 as the excuse for walking him off the premises. It's what employers do. You get the pest off the premises and then you do whatever you need to do to keep him there. On my reading, this is when the ATO fully appreciated why Boyle wasn't going to let it be. They understood he had enough evidence to know they weren't interested in shutting the alleged scam down, so he had to go. Simple as that.

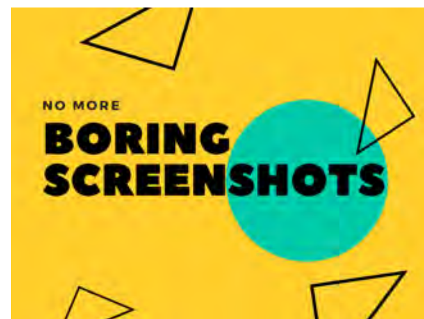
On leave with time on his hands, Boyle sought out a Member of Parliament and the media, as he wanted the "garnishee" scam to be exposed.

In 2019 he was formally charged with 66 counts of stealing in one sense or another. Unsurprisingly, the charges were later reduced to 23, after the ATO told a Senate inquiry that more training was required to ensure garnishees were only ever used as a last resort, not as a fundraiser, because by then the program had been quietly dropped. The implication was that it was all a bit of a storm in a teacup, but they'd sorted things out. My instincts tell me that that explains why the ATO came after him. They realized why the cat was out of the bag. If so, the judge's decision not to make those connections other than to criticize Boyle's conduct left him at a serious disadvantage.

On 20 March this year, Judge Liesl Kudelka (commonly referred to as Kudelka J) in the Supreme Court in Adelaide dismissed Boyle's civil claim for immunity from criminal prosecution under the PID Act. Her reasons were initially suppressed on the application of the Commonwealth Director of Public Prosecutions (CDPP) until 27 March, when a redacted version was made public. I am assuming the CDPP was concerned to ensure its criminal prosecution of Richard Boyle later this year would not be prejudiced in any way, although experience suggests it wasn't as clear-cut as that. Boyle faces the prospect of many years in jail and has lodged an appeal to be heard later this year.

In her judgement, Kudelka J laid out how the PID laws have been designed to confine whistleblowers in what they can do if they are to make a successful claim for protection. Kudelka set the bar pretty high in deciding that "making" a PID "is an important but confined role" … [that] "does not support the concept of a public official holding on to information, whilst conducting their own investigation of that information in order to gather "evidence" of disclosable conduct which then may, or may not, be disclosed." Kudelka J means the "audio" and those "screenshots" on his iPhone.

In other words, you can't gather information and evidence over time and later work out why some of what you've gathered is, after all, surplus to "making" the PID, without risking losing your protection. The idea is that your PID would be seen as "incomplete" because of what you held back, and your reasoning open to the suspicion that you had rigged the evidence for a particular result. Or that you were getting above yourself, by assuming the role of an investigator in making decisions about what was or was not relevant in your view.



If Kudelka J is right, it's clear the PID laws were designed to encourage only largely unsubstantiated beliefs, not well-prepared claims. Ironically, this means claims that can be readily discarded as well-intentioned, but unlikely to be true given the lack of supporting information — claims that don't warrant further reflection, other than by the risk prevention policy wonks. I can see why the relief must be almost palpable as every care is taken to give nothing away, other than that the contents have been noted for future consideration, if the PID maker won't let it rest and gets a bit uppity with it. Like Richard Boyle.

If Kudelka J is right, the PID laws have been remarkably successful, because that is what mostly seems to happen. If you were thinking that those in charge would be interested in doing more to root out wrongs, you'd be horribly disappointed. On Kudelka J's reasoning, the PID laws have been developed to mollify the concerns of those less than compliant, with the bonus of being able to sanction those who would persist. Like Richard Boyle.

I'm guessing he initially thought his superiors would want to stop ATO officers unlawfully issuing dodgy garnishee notices, but he found out he was wrong, as they were in on it.

Kudelka J has got it terribly wrong. You can't require there to be reasonable grounds for making a PID without expecting that the whistleblower is going to try to make a good fist of it and want the other side to do the same. That means gathering up the documents and other evidence you think you need for one reason or another, and checking whether your beliefs stack up before pulling it all together for submission. And then, persisting with its investigation in the face of a worrying lack of diligence from the other side. On Kudelka's reasoning, the PID system is meant to operate like a locked drop box, with no avenue for reply or to contribute further. If so, it's the Honest Government Policy to which only The Juice Media could do justice.

In my observation, if you develop any expectation as to how the system does or should work and you are pro-active in any way, you risk being singled out for special treatment. This special treatment relies on your employer re-casting that same PID as an unauthorized disclosure contrary to the code of conduct or, worse, the criminal law. Because even reminding your so-called "betters" that they are running late with a decision inevitably risks you being tagged as a know-all, and one who is just begging to be pulled down a peg or two. It's worse if you explain why they've got it wrong in deciding not to investigate for reasons that are not, on the available evidence, immediately obvious.

Kudelka J also found the PID Act "does not sanction a public official engaging in a form of 'vigilante justice' prior to making a public interest disclosure" because the "unlawful conduct may range from minor to egregious." In other words, you're not meant to take it up with the boss in the hope he'll blush for shame at being caught out, without risking losing your protection. Why? Well, not because you'd be seen as self-righteous or even vindictive, as the PID law does not deny you protection for enjoying seeing him squirm, but because, apparently, you'd be usurping the investigator's role. Kudelka J says this is way outside of anything the law contemplates and worse, it might all end up in tears if all you achieve is to tip him off to get cracking if he's to cover his tracks and get rid of you. And that, Kudelka J reasons, could come at the price of an investigator not being able to nail him for some truly egregious unlawful conduct. In other words, you are to leave it to the experts, otherwise you'll be blamed for their failures. Is she serious? It seems she is, even though it's clear on the evidence to the Senate, the ATO investigators were never going to investigate Boyle's claims as far back as November 2016. Note that the ATO's reasons for not doing so have been redacted from the decision.

But here's the killer. Kudelka J says, "It is understandable that a public official may feel that they may not be believed if they do not have 'evidence' to 'back up' what they are disclosing". And she accepts that "over time [Boyle] formed the belief that the ATO would not investigate his allegations" and that he "may have been justified in his belief, [but says] it does not follow that s 10(1)(a) (of the PID Act) should be construed to protect public officials in the performance of an investigative role which the PID Act does not contemplate they undertake." That can't be right! Pulling together a PID surely demands that you investigate your own suppositions before you bother anyone with them. Doing otherwise would ensure your PID was automatically earmarked for some policy wonk's in-tray.

By the time the AFP turned up at his door, those screenshots had become stealing offences, along with the audio of conversations he'd recorded covertly at a series of meetings from April 2017. It was one last roll of the dice. You see, those conversations were proof of the garnishee scam being standard ATO policy at the time. So, in theory, Kudelka J was right to worry that all an employer would do is work to cover its tracks once it got the tip-off that it was about to be ousted on national television. That's just what the ATO did. The ATO simply upped the ante every time Boyle failed to take the hint. But Kudelka J didn't see it that way. Kudelka J held Boyle responsible for the ATO's bad faith. He was apparently getting above himself in thinking the PID act did more than provide an opportunity for the ATO to penalise him for not letting it go.

Kudelka J believes that while "on one level" Boyle's argument that what he did was reasonably a part of making a PID may be seen to encourage whistleblowers, "on another level" it would give public officials a "false sense of security." "The test proposed by the Applicant was that public officials [would only be] protected for criminal conduct that reasonably forms part of the process of making a public interest disclosure; the seriousness of the allegation [would need to] be weighed with the relative gravity of conduct and an objective test of reasonableness must be applied." And the fact that the legislation was silent "regarding the limits of the criminal conduct" meant that the test proposed by the Applicant gave public officials "no certainty and little guidance." Kudelka J recognised this construction would be "cold comfort, which may have the effect of discouraging, rather than encouraging, the making of disclosures."

Kudelka J went on, explaining how "the endorsement of some level of criminal conduct to investigate what may be disclosable conduct may discourage the timely disclosure of information that, in the public interest,

should be disclosed. That may in turn undermine the ability of the principal officer to properly investigate a later disclosure." This point might have had more relevance if the ATO had decided to investigate Boyle's claims before escorting him off the premises. But it didn't.

If by endorsing "some level of criminal conduct" she had meant the ATO allowing the alleged scam to run unchecked, then I think she would have been on to something: because the ATO did turn a blind eye in relation to those screenshots when it downgraded its allegations from fraud to a breach of the code of conduct. It did it again by offering a settlement the following year. It only ever investigated Boyle, not the ATO's own fraud, and then only to shut him down. But it didn't deter Boyle, and it rarely does. If anything, pressuring him to give it away only encouraged him to do more. This is why if Boyle's appeal fails, the PID system truly is the Honest Government Policy to which only The Juice Media can do justice.

Kudelka J doubled down on her theory saying "The PID Act does not expressly prohibit or endorse the recording of information by a public official to help formulate a public interest disclosure." "The PID Act is silent on this aspect." Again, Boyle only withheld the audio, not the details of what was said in those meetings, as Boyle didn't want to waste anyone's time with the vagaries of his memory. He wanted to show the scam was accepted policy, not the mistake some would've had him believe.

But it was not to be. Kudelka J agreed with the ATO's very narrow and may I say, a tad pompous, even patronising view that "unlawful investigative acts by a public official may delay or undermine the investigative process intended by the PID Act" before dismissing Boyle's claim for immunity. It's laughable really, but the sad truth is Kudelka J wrongly believed the ATO had been planning to investigate itself all along. What Kudelka J doesn't consider is that those screenshots and audio had only ever been seen as a part of his normal work, albeit possibly posing a risk to another's privacy, but never as criminal theft until the ATO realized they were about to be exposed on the ABC's Four Corners program for having egregiously issued garnishees as a type of end-of-year fundraiser. Boyle was doing us a service and Kudelka J, by holding Richard Boyle responsible for his employer's failures, got it wrong when it comes to a contest over what's reasonable.

Cynthia Kardell is president of Whistleblowers Australia.

As a former whistleblower, I'm urging the government to protect Australian whistleblowers

At first the Albanese government did act, dropping the Bernard Collaery case, but no substantial law changes have been made to shield whistleblowers.

Jeff Morris

The Guardian, 24 May 2023

As a prominent former whistleblower, I am contacted by potential whistleblowers on a weekly basis.

Jeff Morris

I was optimistic a year ago when the Australian Labor party entered government. For years, the Coalition government had failed to fix federal whistleblowing law and presided over the prosecutions of four whistleblowers who exposed things like alleged war crimes in Afghanistan, aggressive debt collection and other alleged wrongdoings.

My already pessimistic counsel to those thinking of blowing the whistle had become dire: those who speak up in Australia risking losing everything, all for doing the right thing.

Labor, particularly the attorney general, Mark Dreyfus, promised to change that. I wanted to believe it. At first they did act, dropping the unjust prosecution of Bernard Collaery, who was alleged to have blown the whistle on Australia's morally bankrupt espionage against Timor-Leste. That was a good step forward.

But now, a year since taking government, Labor's whistleblowing report card is looking less rosy. For all Dreyfus's words about the importance of whistleblowing, it is his actions that count. And his actions and omissions do not seem to be those of someone truly committed to protecting and empowering whistleblowers.

First, law reform.

The government promised extensive improvement to the Public Interest Disclosure Act (Pida), enacted by Labor in the final days of the Gillard government. A decade of practical experience had shown the law to be deeply flawed. Dreyfus promised quick passage of initial, technical tweaks followed by a root-and-branch overhaul.

Twelve months on, the Albanese government has not passed any substantial law that strengthens whistleblower protections. The first tranche of reform is stuck in the Senate, with Labor failing to prioritise its passage. The bill has been ready to pass since March, when Labor accepted recommendations from a parliamentary committee to make changes to avoid unintended consequences. It was put to the Senate this month, but squabbling between Labor and the Greens over housing issues saw it held up. It will now not become law until next month at the earliest.

What's a few months, you might say. Every day Australia's whistleblower protection framework remains inadequate, whistleblowers are suffering and wrongdoing is going unchecked. Prospective whistleblowers are staying silent because they know the laws will not protect them. People will face career-ending consequences because these reforms have been held up, not prioritised by the Albanese government.

Next, institutional change.

The single most significant thing the government could do to protect Australian whistleblowers would be to establish a whistleblower protection authority. An independent, well-resourced whistleblowing body would be a game-changer, overseeing and enforcing the law and providing practical guidance to those speaking up.

Australia would join the likes of the US, the Netherlands, Slovakia and Ireland in providing robust institutional support for whistleblowers.

This should be a no-brainer for the government. Such a body was first recommended by a parliamentary committee in the 1990s; Labor then supported the idea in a 2017 bipartisan parliamentary committee report, and the Bill Shorten-led Labor party took the concept to the 2019 election.

It should be core policy. Instead, the government's position has regressed. A whistleblowing authority was included in the crossbench proposal for a national anti-corruption commission; it is nowhere to be found in the Labor version that begins operation in July. From the certainty of those committee proposals and the 2019 election platform, now all we have is a weak commitment to considering the "need" for such a body in a discussion paper to be published sometime this year.

Finally, and most urgently, two Australian whistleblowers remain on trial for doing the right thing and speaking up about alleged government wrongdoing. Richard Boyle blew the whistle on unethical behaviour at the tax office and David McBride exposed allegations of war crimes committed by Australian forces in Afghanistan. In my views, these men are heroes — but right now they face the very real prospect of jail time.

The attorney general can end these prosecutions with the swish of a pen. Instead, they drag on.

McBride will be tried in November — the first Australian to face a jury in relation to alleged war crimes; a whistleblower, not a perpetrator. Boyle thought he was protected by the Pida, but a judge ruled the law was narrower than previously assumed and did not protect him. He is in the process of appealing this decision.

Each case is a stark illustration of the failings in Australia's whistleblowing framework.

The Labor government's inaction — while it talks about the benefits of transparency — is perverse. As I said in a submission to the Senate's recent Pida inquiry, making minor amendments to whistleblowing law while overseeing these prosecutions is fiddling while Rome burns.

For the attorney general, I have a simple message: as a former whistleblower, I know all too well that actions speak louder than words. Drop the pros-

ecutions, fix the law and establish a whistleblower protection authority that will show you are truly on the side of Australia's whistleblowers past, present and future.

Queensland corruption watchdog all bark and no teeth

Des Houghton
Courier Mail, 10 June 2023, p. 66

I THINK we all agree the Crime and Corruption Commission does some fine work in the areas of organised crime.

But the CCC has failed lamentably to uncover wrongdoing in the public service and State Government corporations more generally. Its investigations drag on for months, sometimes years, and come to nothing.

The watchdog has no teeth. Or, more correctly, it rarely sinks in the teeth, despite a lot of barking. When it began as the Crime and Misconduct Commission it was a rottweiler. Now it is a poodle.

I blame the CCC's ludicrous devolution policy, where a valid complaint from a public service whistleblower is referred back to the very department chiefs accused of corruption or wrongdoing or hiding corruption and wrongdoing. So valid allegations of serious misbehaviour are tipped into a deep, dark well from where they are very unlikely to ever again see the light of day.

In his "Let the Sun Shine In" report into the lack of State Government openness and accountability, Peter Coaldrake said the CCC was sometimes ungenerously referred to as Australia Post. This was because it received complaints but quickly passed them on without taking any ownership of investigations.

Back in the workplace investigations can take months, even years and the complainants suffer reprisals.

State Government whistleblowers are often frozen out or paid off.

In a recent case a senior State Government ethical standards unit figure was sent packing with a sizeable payout — but only after agreeing to sign a confidentiality agreement prohibiting him from discussing his grievances.

How often does this happen?

Greg McMahon is an old accountability campaigner who believes he has a solution.

Greg McMahon

McMahon, 73, is secretary of the Queensland Whistleblowers Action Group that last week called for the establishment of an independent body to oversee whistleblower protections and provide a more rigorous assessment of their complaints.

McMahon's group is made up of some very interesting ex-cops, academics and others who believe a new agency is needed to navigate a "complex, outdated and inconsistent system."

McMahon says it should have sweeping powers to veto decision-makers in the CCC and the office of the Queensland Ombudsman who chose not to investigate complaints.

McMahon told me he got the idea for a new agency from a similar body set up in America in the late 70s.

The United States Office of Special Counsel is a powerful independent federal investigative and prosecutorial agency specifically designed to protect whistleblowers, and others.

It also has the power to investigate what the CCC will not — abuse of power, gross waste of public funds and gross mismanagement.

McMahon, a retired civil engineer and water expert who worked in state and federal governments, says whistleblowers invariably face reprisals from speaking out.

"Whistleblowers are not protected and quickly forgotten," he said.

"Whistleblowers lose their jobs, their careers and their reputations — and sometimes their marriages. And they suffer financially."

The Whistleblowers Action Group was not seeking judicial powers, McMahon said.

But it should have the power to refer matters to the Chief Justice of the Supreme Court and the Speaker of Parliament to determine whether an investigation was conducted properly, fairly and thoroughly.

"This would add another layer of protection for whistleblowers, who play a vital role in our democracy by maintaining the integrity and accountability of public and private institutions."

The action group's call for an overarching review is timely.

Meanwhile, the Palaszczuk Government's review into the Public Interest Disclosure Act is due any day. The so-called PID covers the disclosure of information about wrongdoing in the public sector and has been roundly criticised by whistleblowers who claimed PID status to no avail.

The review by retired Supreme Court judge Alan Wilson was extended until June 19 because of a flood of submissions. The review of the Act was recommended by Coaldrake in his report.

McMahon said the PID Act should be extended to protect journalists reporting on matters disclosed by whistleblowers.

"The (current) Act facilitates the new-century tactics by entities, administrations, jurisdictions and parliaments to cover up corruption and to silence the disclosures and the whistleblower," he said.

Digital security tips to prevent the cops from ruining your trip abroad

Traveling with a phone and laptop? Here are digital security tips to keep your devices and your data safe from the cops.

Nikita Mazurov

The Intercept, 29 April 2023

Ernest Moret, a foreign rights manager for the French publishing house La Fabrique, boarded a train in Paris bound for London in early April. He was on his way to attend the London Book Fair.

When Moret arrived at St. Pancras station in the United Kingdom, two plainclothes cops who apparently said they were "counter-terrorist police" proceeded to terrorize Monet. They interrogated him for six hours, asking everything from his views on pension reform to wanting him to name "anti-government" authors his company had published, according to the publisher, before proceeding to arrest him for refusing to give up the passwords to his phone and laptop. Following his arrest, Moret was released on bail, though his devices were not returned to him.

The case, while certainly showcasing the United Kingdom's terrifying anti-terror legislation, also highlights the crucial importance of taking operational security seriously when traveling — even when going on seemingly innocuous trips like a two-and-a-half-hour train ride between London and Paris. One never knows what will trigger the authorities to put a damper on your international excursion.

Every trip is unique and, ideally, each would get a custom-tailored threat model: itemizing the risks you foresee, and knowing the steps you can take to avoid them. There are nonetheless some baseline digital security precautions to consider before embarking on any trip.

Travel devices, apps, and accounts

The first digital security rule of traveling is to leave your usual personal devices at home. Go on your trip with "burner" travel devices instead.

Aside from the potential for compromise or seizure by authorities, you also run the gamut of risks ranging from having your devices lost or stolen during your trip. It's typically way less dangerous to just leave your usual devices behind, and to bring along devices you only use when traveling. This doesn't need to be cost prohibitive: You can buy cheap laptops and either inexpensive new phones or refurbished versions of pricier models. (And also get privacy screens for your new phones and laptops, to reduce the information that's visible to any onlookers.)

Your travel devices should not have anything sensitive on them. If you're ever coerced to provide passwords or at risk of otherwise having the devices be taken away from you, you can readily hand over the credentials without compromising anything important.

If you do need access to sensitive information while traveling, store it in a cloud account somewhere using cloud encryption tools like Cryptomator to encrypt the data first. Be sure to then both log out of your cloud account and make sure it's not in your browsing history, as well as uninstall Cryptomator or other encryption apps, and only reinstall them and re-log in to your accounts after you've reached your destination and are away from your port of entry. (Don't login to your accounts while still at the airport or train station.)

Just as you shouldn't bring your usual devices, you also shouldn't bring your usual accounts. Make sure you're logged out of any personal or work accounts which contain sensitive information. If you need to access particular services, use travel accounts you've created for your trip. Make sure the passwords to your travel accounts are different from the passwords to your regular accounts, and check if your password manager has a travel mode which lets you access only particular account credentials while traveling.

Before your trip, do your research to make sure the apps you're planning to use — like your virtual private network and secure chat app of choice — are not banned or blocked in the region you're visiting.

Maintain a line of sight with your devices at all times while traveling. If, for instance, a customs agent or border officer takes your phone or laptop to another room, the safe bet is to consider that device compromised if it's brought back later, and to immediately procure new devices in-region, if possible.

If you're entering a space where it won't be possible to maintain line of sight — like an embassy or other government building where you're told to store devices in a locker prior to entry — put the devices into a tamper-evident bag, which you can buy in bulk online before your trip. While this, of course, won't prevent the devices from being messed with, it will nonetheless give you a ready indication that something may be amiss. Likewise, use tamper-evident bags if ever leaving your devices unattended, like in your hotel room.

Phone numbers

Sensitive information you may have on your devices doesn't just mean documents, photos, or other files. It can also include things like contacts and chat histories. Don't place your contacts in danger by leaving them on your device: Keep them in your encrypted cloud drive until you can access them in a safe location.

Much like you shouldn't bring your usual phone, you also shouldn't bring your normal SIM card. Instead, use a temporary SIM card to avoid the possibility of authorities taking control of your phone number. Depending on which region you're going to, it may make more sense to either buy a temporary SIM card when in-region, or buy one beforehand. The advantage of buying a card at your destination is that it may have a higher chance of working, whereas if you buy one in advance, the claims that vendors make about their cards working in a particular region may or may not pan out.

On the other hand, the region you're traveling to may have draconian identification requirements in order to purchase a SIM. And, if you're waiting to purchase a card at your destination, you won't have phone access while traveling and won't be able to reach an emergency contact number if you encounter difficulties en route.

Heading back

Keep in mind that the travel precautions outlined here don't just apply for your inbound trip, they apply just as much for your return trip back home. You may be questioned either as you're leaving the host country, or as you're arriving back at your local port of entry. Follow all of the same steps of making sure there is nothing sensitive on your devices prior to heading back home.

Taking precautions like obtaining and setting up travel devices and accounts, or establishing a temporary phone number, may all seem like hassles for a standard trip, but the point of undertaking these measures is that they're ultimately less hassle than the repercussions of exposing sensitive information or contacts — or of being interrogated and caged.

What to do before sharing classified documents with your friends online

Nikita Mazurov

The Intercept, 12 April 2023

LET'S SAY you're locked in a heated geopolitical spat with a few of your online friends in a small chatroom, and you happen to be privy to some classified documents that could back up your argument. While it's tempting to snap a photo and share it to prove your point, especially given the appeal of impressing onlookers and instantly placating naysayers, it would behoove you to take a step back and think through the potential repercussions. Even though you may only plan for the documents to be shared among your small group of 20 or so friends, you should assume that copies may trickle out, and in a few weeks, those very same documents could appear on the front pages of international news sites. Thinking of this as an inevitability instead of a remote prospect may help protect you in the face of an ensuing federal investigation.

Provenance

Thorough investigators will try to establish the provenance of leaked materials from a dual perspective, seeking to ascertain the original points of acquisition and distribution. In other words, the key investigatory questions pertaining to the origins of the leaks are where the leaker obtained the source materials and where they originally shared them.

To establish the point of acquisition, investigators will likely first enumerate all the documents that were leaked, then check via which systems they were originally disseminated, followed by seeing both who had access to the documents and, if access logs permit, who actually viewed them.

What all this means for the budding leaker is that the more documents you share with your friends, the tighter the noose becomes. Consider the probabilities: If you share one document to which 1,000 people had access and that 500 people actually accessed, you're only one of 500 possible primary leakers. But if you share 10 documents — even if hundreds of people opened each one — the pool of people who accessed all 10 is likely significantly smaller.

Keep in mind that access logs may not just be digital — in the form of keeping track of who opened, saved, copied, printed, or otherwise interacted with a file in any way — but also physical, as when a printer produces imperceptible tracking dots. Even if the printer or photocopier doesn't generate specifically designed markings, it may still be possible to identify the device based on minute imperfections that leave a trace.

In the meantime, investigators will be working to ascertain precisely where you originally shared the leaked contents in question. Though images of documents, for instance, may pass through any number of hands, bouncing seemingly endlessly around the social media hall of mirrors, it will likely be possible with meticulous observation to establish the probable point of origin where the materials were first known to have surfaced online. Armed with this information, investigators may file for subpoenas to request any identifying information about the participants in a given online community, including IP addresses. Those will in turn lead to more subpoenas to internet service providers to ascertain the identities of the original uploaders.

It is thus critically important to foresee how events may eventually unfold, perhaps months after your original post, and to take preemptive measures to anonymize your IP address by using tools such as Tor, as well as by posting from a physical location at which you can't easily be identified later and, of course, to which you will never return. An old security adage states that you should not rely on security by obscurity; in other words, you should not fall into the trap of thinking that because you're sharing something in a seemingly private, intimate — albeit virtual — space, your actions are immune from subsequent legal scrutiny. Instead, you must preemptively guard against such scrutiny.

Digital barrels

Much as crime scene investigators, with varying levels of confidence, try to match a particular bullet to a firearm based on unique striations or imperfections imprinted by the gun barrel, so too can investigators attempt to trace a particular photo to a specific camera. Source camera identification deploys a number of forensic measures to link a camera with a photo or video by deducing that camera's unique fingerprint. A corollary is that if multiple photos are found to have the same fingerprint, they can all be said to have come from the same camera.

A smudge or nick on the lens may readily allow an inspector to link two photos together, while other techniques rely on imperfections and singularities in camera mechanisms that are not nearly as perceptible to the lay observer, such as the noise a camera sensor produces or the sensor's unique response to light input, otherwise known as photo-response non-uniformity.

This can quickly become problematic if you opted to take photos or videos of your leaked materials using the same camera you use to post food porn on Instagram. Though the technical minutiae of successful source camera identification forensics can be stymied by factors like low image quality or applied filters, new techniques are being developed to avoid such limitations.

If you're leaking photos or videos, the best practice is to employ a principle of one-time use: to use a camera specifically and solely for the purpose of the leak; be sure not to have used it before and to dispose of it after.

And, of course, when capturing images to share, it would be ideal to keep a tidy and relatively unidentifiable workspace, avoiding extraneous items either along the periphery or even under the document that could corroborate your identity.

In sum, there are any number of methods that investigators may deploy in their efforts to ascertain the source of a leak, from identifying the provenance of the leaked materials, both in terms of their initial acquisition and their subsequent distribution, to identifying the leaker based on links between their camera and other publicly or privately posted images.

Foresight is thus the most effective tool in a leaker's toolkit, along with the expectation that any documents you haphazardly post in your seemingly private chat group may ultimately be seen by thousands.

Man gets life sentence for killing of Georgia whistleblower

Associated Press, 10 April 2023

Brunswick, Georgia (AP) — A Mexican citizen was sentenced Monday to life in a U.S. prison for killing a man who reported him and his brother to authorities for cheating migrant workers out of millions of dollars.

A U.S. District Court judge in Brunswick, Georgia, sentenced 46-year-old Juan Rangel-Rubio nearly six months after a jury convicted him of conspiring to kill a witness and other criminal counts.

According to federal prosecutors, Rangel-Rubio and his brother recruited migrant workers living illegally in the U.S. to work for a tree-trimming business in southeast Georgia, then routed more than $3.5 million of the workers' earnings to their own accounts.

Employee Eliud Montoya filed a complaint with the federal Equal Employment Opportunity Commission and was fatally shot in August 2017 outside his home near Savannah. Prosecutors said Rangel-Rubio pulled the trigger after plotting the killing with his brother, Pablo Rangel-Rubio, and a getaway driver, Higinio Perez-Bravo.

Both co-defendants had previously received prison sentences for conspiring to kill Montoya, a U.S. citizen. Prosecutors said the Rangel-Rubio brothers and Perez-Bravo were all Mexican citizens living in the U.S. illegally when the killing occurred.

Eliud Montoya

"Eliud Montoya was murdered for doing the right thing and revealing Juan Rangel-Rubio's scheme to profit off his use of undocumented workers," Jill E. Steinberg, U.S. attorney for the Southern District of Georgia, said in a news release. "As a result of the diligent efforts of our law enforcement partners, Juan Rangel-Rubio will be held accountable for his despicable crimes."

The whistleblower industrial complex

Alexander I. Platt

Yale Journal on Regulation, volume 40, 2023, pages 688–758

[Look online for the full article and commentaries about it.]

Abstract

Although the whistleblower programs (WBPs) created by Dodd-Frank have received universal acclaim, little is known about how they actually work. In 2021, the Securities and Exchange Commission (SEC) received an average of forty-nine whistleblower tips every workday. Success depends on sifting through this avalanche of tips to determine which ones to investigate. To date, however, the tip-sifting process has been entirely shrouded in secrecy. This article breaks new ground. It offers a rare look inside the WBPs administered by both the SEC and the Commodity Futures Trading Commission (CFTC), shining a bright light on the critical role played by private whistleblower attorneys in the tip-sifting process. Using a new dataset comprised

of information I obtained under the Freedom of Information Act, I find (among other things) that tipsters represented by lawyers appear to significantly outperform unrepresented ones, repeat-player lawyers appear to outperform first-timers, and lawyers who used to work at the SEC appear to outperform just about everybody. The upshot is that the SEC and CFTC have effectively privatized the tip-sifting function at the core of the WBPs. Private lawyers have earned hundreds of millions of dollars in fees from these programs, with a disproportionate share going to a concentrated group of well-connected, repeat players. Unlike traditional plaintiff-side securities attorneys and attorneys who represent clients seeking government payments in many other contexts, private whistleblower lawyers operate free from virtually all public accountability, transparency, or regulation. I highlight significant efficiency and accountability deficits imposed by this private outsourcing program and propose reforms to realign these private actors with the public interest.

Alexander Platt

Four years ago, a whistleblower and I broke North Carolina's ag-gag law. The environment and public health are better for it.

Lisa Sorg

The Pulse, 26 February 2023

NOW THAT the Fourth Circuit Court of Appeals has ruled North Carolina's ag-gag law — as it applies to news-gathering — is unconstitutional, I can tell you that I violated it.

To be clear, I did not trespass, but I checked several of the law's boxes. Likewise, the worker who agreed to document and obtain evidence did so at considerable financial and personal risk, and could also have been fined.

Four years ago I received a tip from the worker, who thought wastewater sludge being shipped to a compost facility in Sampson County was making him sick. To get a handle on the story, I needed to verify the shipper, DAK Americas, and the recipient, McGill Compost. And I needed sludge to take to an EPA-certified lab to learn what it contained.

But the worker and I had to defy the state's ag-gag law to find out.

The Private Property Protection Act forbids employees from entering "non-public areas of a workplace" and "without authorization captures or removes the employer's data, paper, records, or any other documents and uses the information to breach the person's duty of loyalty to the employer." That same provision applies to photographs and video.

Yes, the worker did that.

The law applies not just to employees but to "any person who intentionally directs, assists, compensates, or induces another person to violate this section."

I induced. I directed. I assisted. Intentionally.

Had this story turned out differently, both the worker and I could have faced a fine of $5,000 per day, plus legal fees. Moreover, should he be penalized, I felt ethically obliged to cover his fine.

This is what happened. To protect the employee, I'm honoring my original promise to him and keeping his identity and workplace confidential.

After the worker described his illness, I suspected it might be due to his exposure to the sludge. Even if I couldn't establish cause-and-effect, it would still be worth knowing what the sludge contained.

DAK Americas makes plastic resins and discharges a byproduct of that manufacturing — the known carcinogen, 1,4-Dioxane — into the Cape Fear River. I thought it was possible, if not likely that 1,4-Dioxane was also present in the wastewater, a major component of sludge.

The sludge from DAK Americas that was shipped to McGill Environmental. This sample is from the same batch that contained 20,400 parts per billion of 1,4-Dioxane. The colored specks in the sludge are bits of plastic. (File photo: Lisa Sorg)

Day 1: I asked the worker to photograph shipping manifests so I could verify the sender and the recipient of the sludge. Potential fines: $5,000 for his documentation, $5,000 for my "inducing" him to do so.

Day 2: The worker sent me video of sludge in a company truck. Now we're in for another $10,000.

Day 3: Having verified the origin, destination and the existence of the potentially contaminated sludge, I needed to test the material — without trespassing. I asked the worker if he could obtain some, and he agreed.

I delivered four sterile quart-sized mason jars to the worker's home, along with a cooler. The plan was for him to immediately text me after he had filled the jars and packed them in ice. I would drive an hour to a prearranged meeting spot, where he would hand off the cooler and I would rush it to an EPA-certified lab.

Add $10,000 to the previous potential fines, and we're looking at $30,000 — not chump change.

Within 10 days, the lab results arrived via email. The levels of 1,4-Dioxane were so high that I called the technician to see if there had been an error. No error, the technician said.

There really was 20,400 parts per billion of 1,4-Dioxane in the sludge.

The EPA has not set a legally enforceable maximum for 1,4-Dioxane — in sludge, water, soil, or any material — but for context, the agency has established a health advisory level for drinking water supplies. That level is 0.35 parts per billion, which means if the concentrations in the sludge were applied to drinking water, they would have been 57,000 times greater than recommended.

Lisa Sorg

And this sludge was converted into compost and soil builder, to be spread on gardens, farm fields, even playgrounds and soccer fields.

This presented another ethical dilemma. The story wasn't ready for publication yet, but the test results were so alarming that I considered the material to be a possible public health risk. I had no choice but to notify the companies and state regulators of what I had found. That could expose the subterfuge the worker and I had engaged in to get the sludge.

The companies did not respond, but the Division of Waste Management sent investigators to both McGill and DAK Americas. The state found high levels of 1,4-Dioxane in the sludge as well, confirming my testing. There was not 1,4-Dioxane in the finished compost— the state and I independently sampled it — likely because the chemical had evaporated along with the water.

However, the state found toxics in the compost that I had not even tested for: 20 types of PFAS, or perfluorinated compounds, totaling 138 parts per trillion, far above what we now know is hazardous to public health.

Within five months of the story publishing, the Environmental Management Commission approved new rules governing compost facilities.

Previously a loophole in state regulations allowed compost operators and the suppliers of raw materials to operate on a tenuous honor system: Composters didn't have to test for 1,4-Dioxane or any emerging contaminants. And industrial plants didn't have disclose to the composters if those compounds were present in the material they're sending.

Now the state can require those operations to test their "feedstock" — the material that is used to make compost — and their finished product for 1,4-Dioxane.

Because of the worker's bravery, North Carolina has a stronger compost rule. Had he and I been cowed by the ag-gag law and allowed it to chill legitimate news gathering, it's possible the compost rule would have never passed; a known carcinogen could still be entering compost facilities.

The 1,4-Dioxane investigation underscores a brief that the Reporters Committee for Freedom of the Press filed with the federal court: The right to gather information plays a distinctly acute role in journalism. First-hand accounts, buttressed by video evidence, enhance accuracy and credibility in reporting and increase transparency and reader trust, allowing the press "to tell more complete and powerful stories."

The Fourth Circuit's decision is important for journalists. And it's important for whistleblowers.

Whistleblowing: ordeals of civil servants who risked their jobs to expose corruption

Victoria Bamas

Daily Trust, 22 May 2023

A SURVEY published in 2021 shows that the majority of Nigerians perceive corruption as a major problem, but one-quarter of the respondents are unwilling to report any form of corruption.

The survey conducted and published by the African Centre for Media & Information Literacy (AFRICMIL) titled, "Survey on 5 years of whistleblowing policy in Nigeria" also showed that 3 out of 4 respondents have stopped reporting cases of looted funds due to fear of victimisation, believing that authorities do not provide a proper channel to make the report or take action against the suspect.

Whistleblowers in Nigeria often find themselves alone. Image: The ICIR

Weak internal mechanisms

The belief that no action would be taken made a civil servant at the Federal Ministry of Works and Housing (FMWH), Richard Oghenerhoro Martins, look for external recourse. The whistleblowing policy launched in 2016 states that an internal stakeholder can "escalate the matter further" when the issue is not adequately addressed internally.

Martins has repeatedly complained about employment racketeering within the ministry to his superiors but was ignored.

He reported to the then Director of Human Resource Management Isang Iwara, and other superior officers; like the Deputy Director of Appointment Promotion & Discipline, Shehu Aliyu, Assistant Director Bosede Omoniyi, and others, as documents from his lawyers to the ministry show.

Martins briefed his lawyers to send a petition to the Minister of Works and Housing Babatunde Fashola in July 2020, which spurred the setting up of a committee led by a senior official of the ministry, Rufus-Ebegba Immaculata.

Martins said several colleagues intimidated and warned him to stop investigating the prevalence of fake employment in public service, but he was committed to seeing the end to the employment fraud.

The committee, which sat in August and September 2020, found Martins' claims to have merit. They found cases of employment manipulation, violation

of due process and fake employment documentation.

The committee recommended immediate discontinuation of salary payments to the officers with fake letters and their names were forwarded to the Independent Corrupt Practices and Other Related Offences Commission (ICPC) for further investigation.

The ICPC is one of the investigating agencies of the whistleblower policy.

In a twist of fate, the panel also recommended disciplinary action against Martins, citing a breach of the oath of secrecy as contained in the Public Service Rules (PSR).

The report reads that disciplinary action against the petitioner, "Mr Richard Oghenerhoro, over his misconduct, breach of oath of secrecy, unauthorised disclosure of official information and abstraction or copying of official documents without approval as enshrined in the Public Service Rules 030301 (f), 030415, 030416 and 030417 respectively."

The director of press and public relations, FMWH, Blessing Lere-Adams told the ICIR [International Centre for Investigative Reporting] that there is an internal mechanism to deal with reports on corruption without having to involve the office of the minister.

"Whoever has done that [use external mechanism] does not know the public service rule.

"The PSR specifically states if you have a complaint there is a structure you have to follow, so anybody who goes above that should be questioned," the spokesperson said.

When asked what happens when the internal structure is followed and no action is taken, Lere-Adams directed the enquiry to the deputy director Anti-Corruption and Transparency Unit (ACTU), saying he is in the best position to respond.

The head of ACTU, Sonny Inyang, however, said he could not speak to the press as he does not have the clearance to do so, noting that he only deals with the ICPC on issues of whistleblowing and corruption. Lere-Adams, therefore, advised that a letter should be sent to the ministry's permanent secretary. The ICIR sent the letter which was duly acknowledged, but there is no response as at press time.

The Coalition for Whistleblower Protection and Press Freedom (CWPPF), described the action against Martins as "one among numerous cases of violations and stigmatisation of whistleblowers".

"You would think that a government that lays so much emphasis on fighting corruption would be appreciative of citizens who are willing to expose irregularities and corruption in the public interest," the group said.

The shades of violations against whistleblowers

Godwin Onyeacholem has been at the forefront of advocating for the protection of whistleblowers in Nigeria. "It takes a lot of courage to blow the whistle. You need to know what whistleblowers go through," he said. "It's traumatising."

Onyeacholem is the project coordinator for Corruption Anonymous (CORA) an initiative of AFRICMIL working to build public support and confidence in the whistleblowing policy introduced by the Nigerian government in 2016.

CORA, set up in 2017, advocates effective protection for whistleblowers. This makes Onyeacholem the 'go-to guy' whistleblowers call when they face challenges.

"Whistleblowing constricts their lives because of what they are going through," he told the ICIR of his interaction with whistleblowers.

"Friends avoid you. You are alone."

Accountant Joseph Akeju has lived the experience. Before his retirement, he was a lecturer and bursar at Yaba College of Technology, where he was dismissed twice for blowing the whistle.

"You know, it's natural," he said, recalling how family and friends blamed and abandoned him.

He is 70 now, when he spoke to the ICIR.

"Some people were laughing at me; some people were calling me 'Mr Clean'. They were mocking me. They said instead of me to join them and make my own money. Only a few people stood with me," he added in a restrained voice.

Compromised by journalists

Akeju, judging from his experience, said he would not advise anyone to blow the whistle. He also said journalists need to do better with regard to the confidentiality of sources.

Joseph Akeju

"During my time, some of the journalists exposed me to ridicule. They will collect information from me and go and expose me to my boss and tell them I gave them the information," he explained.

Some of the journalists, he said, collected money from his boss. This, he explained, greatly affected him as the school was able to plan to checkmate his moves.

A mass communication lecturer at the University of Nigeria Nsukka, Dr Gerver Verlumun Celestine, described the conduct of journalists who breach the confidentiality of sources as "unethical".

He said such conduct has a far-reaching effect on the source, the journalists, journalism and society.

"If anyone is harassed because he spoke to a journalist in confidence, such a person is likely not to reveal information to journalists again even when such information is needed, the person will be constrained.

"This will affect the development of the society, investigative journalism will be affected, and things that should have been done to help the society will be retarded," Celestine said.

The national secretary for the Nigeria Union of Journalists (NUJ) Shu'aibu Leman Usman, confirmed to the ICIR that the breach of confidentiality of sources "regrettably" happened.

"These things do happen, and they are issues of ethics. sometimes journalists don't play according to the rules. We have instances where journalists

disclosed their sources because they have been enticed with money", he said. He added that journalists needed the cooperation of media owners to curb such occurrences. "Media owners have to stand by journalists and insist that they should not disclose their sources," Usman said.

Compromised by security officials

Since the policy was not in effect in 2008 when Akeju reported irregularities in college funds that were not accounted for, there was no institutional process for whistleblowing. He had to rely heavily on the media to amplify his petition, but that was not the case for an architect Joseph Ameh, who blew the whistle three years after it was launched.

Ameh was head of the physical planning division at the Federal College of Education (Technical) Asaba, when in 2019, he wrote a petition to the ICPC over corrupt practices such as contract inflation and diversion in the institution.

The ICPC reached out to the school for more information and eventually began prosecution.

Ameh had expected some level of protection from the investigating agency.

"In my petition to the ICPC, I wrote my name clearly on it. ICPC was supposed to handle it with diligence, which they did not. They exposed me," he said.

He had expected them to handle it with discreteness and protect his identity when reaching out to the school, but they didn't, he told the ICIR. He received many queries after the ICPC sent a memo to the school requesting documents. That was the start of his travail, which led to the loss of his job, and the collapse of his family.

The whistleblowing policy states that "Its preferable individual puts his/her name and contact to any disclosure" but adds that the person's identity shall be kept confidential to be disclosed only in the circumstances required by law.

That's not the only way the ICPC impacted Ameh.

Ameh said, "When you blow the whistle, you have prepared food for the ICPC officials to eat". By this, he means the ICPC personnel benefit directly by investigating suspects.

He insisted that ICPC officers are corrupt as they use the opportunity for self-aggrandisement.

The officers make money from the suspects in exchange for information, the ICIR gathered. The officers also sometimes give advance notice to suspects and employ delay tactics so that they can cover their tracks.

For instance, Ameh said the ICPC prosecutor on the case whom he called "Barrister Iwoba" visited the college and when he confronted her she told him she went to interview one of the suspects — the registrar.

This, he said, was suspicious because the registrar had already given his statement.

"Somebody that has given his statement to the ICPC in the presence of his lawyers, duly signed and documented by the ICPC, you are telling me you are going to discuss with the person again?," he asked.

He also alleged that statements from the engineer, quantity surveyors 1 & 2 and of the junior architect were not tendered in court. The ICIR could not independently verify this claim.

Ameh's petition had fingered Ignatius Ezoem, Ugbechie Linus and Chukwuka Jonas, former provost, former registrar and former director of works respectively all of whom were taken to court by the ICPC.

Ameh said for the whistleblowing policy to be effective, there must be sanitisation within the commission.

The spokesperson of the ICPC Azuka Ogugua is yet to respond to questions about the corrupt officers at press time despite that she requested the questions be sent to her.

In addition, mails sent to the school — Federal College of Education (Technical) Asaba — current registrar, Rotimi Adepoju and the deputy provost were not responded to at press time. The school has not responded to reminders either. The email bothers on the school's mechanism for reporting corruption and reaction to a court judgement to reinstate Ameh.

"They dismissed me twice, but they reinstated me twice," Akeju the accountant told the ICIR.

The first reinstatement was due to the efforts of the then new rector, who he said was "Dr Mrs Ladipo", who created room for dialogue between his lawyers and the institution.

"I took my case to Federal High Court, Ikoyi. It was after we had been in the court for more than six years that the judge told me I was in the wrong court," the retired accountant explained.

"That was when they referred me to the industrial court."

A major challenge facing whistleblowers is what Onyeacholem described as the "legal abuse syndrome." This arises from the long, winding court battles the whistleblowers have to endure.

"It comes from realising that you are suffering from ethical violation, legal abuse, fraud. The prolonged nature of the justice system makes you go mad," the advocate for whistleblower protection stated.

Godwin Onyeacholem

Why whistleblowers go to court

Whistleblowers end up in court for many reasons-serving as witness for the government or to stop intimidation against them, which can be withholding of salary, suspension or even illegal dismissal from work.

A whistleblower, Sambo Abdullahi, the Nigerian Bulk Electricity Trading (NBET) staff, had to go to court to get the management to pay his suspended salaries.

Abdullahi discovered illegal overpayment running into billions of naira in his organisation and blew the whistle. This led to the suspension of his salary starting in 2017. He filed a suit in 2018, and in 2020, he was still fighting the case.

The ICIR reached out to the spokesperson for Nigeria Judicial Council (NJC), Soji Oye, but his mobile number was not connecting.

A text was sent to that effect. Furthermore, the ICIR reached out to the helpline on the council's website, after some back and forth, the representative confirming that Oye is not available, asked that the questions be sent to the council info mail; this has been done.

As at press time, the council is yet to respond to questions around delayed court cases and how it impacts negatively on whistleblowers and the policy. A reminder was also sent.

SLAPP compromising whistleblowing

"The process of getting this justice also traumatises them due to the insanity of the legal system," said Onyeacholem.

"The organisation might even decide to sue. That's another form of intensifying the punishment. They take you to court for exposing their corruption," he added.

This is known as a Strategic Lawsuit Against Public Participation (SLAPP).

A journalist, Jaafar Jaafar, was at the receiving end of a SLAPP in 2018 after exposing the Governor of Kano state, Abdullahi Ganduje, for collecting a "bribe" and pocketing the currency notes away in his kaftan. The incident has come to be known as "Gandollar."

Jaafar Jaafar

The purpose of a SLAPP is to "intimidate and shut up" whistleblowers, said Onyeacholem.

What many people were not aware of at the launch of the policy is that despite the flamboyant assurance of protection by the then minister of finance, the government placed the burden of fighting corruption in the hands of the public without the requisite legal backing.

The then minister aptly described it as a "stop-gap" initiative until the National Assembly formally passes a law on whistleblowing. It's seven years later and the policy is yet to get the needed backing. This leaves whistleblowers exposed.

PICA — the clipped bird

After blowing the whistle, Joseph Ameh had two court cases to deal with- one in Asaba and the other in Awka, in addition to having to come to Abuja.

The ICPC eventually began prosecution. This meant Ameh appearing in court in Asaba. On the other hand, he was dismissed from work: this meant instituting an illegal dismissal case against the institution at the National Industrial Court in Awka.

Ameh said at some point, he had to travel to Abuja with regard to the petition every fortnight, all bills on him.

"There is no provision to protect the whistleblower. When you blow the whistle, you are on your own," Ameh said.

"Every two to four weeks, I will go to Abuja by night bus. When I am done with them by day, I will take the night [bus] as a cheaper way. Sometimes it requires me to stay back and do some documentation and the entire cost of lodging was on me," he added.

The whistleblowing policy is domiciled with the Ministry of Finance Budget and National Planning and is implemented by the Presidential Initiative on Continuous Audit (PICA). One of the heads of PICA, Johnson Oludare, confirmed to the ICIR the whistleblower bears the financial burden involved.

"If any of our investigating agencies will need him to be in court, maybe as a witness or whatever reasons, I guess he will have to find a way to because when the benefit comes, whatever incidental expenses can be subtracted from it," he said.

By "benefit" Oludare refers to the financial reward a whistleblower is entitled to, anywhere between 2.5 per cent and 5.0 per cent of the total amount recovered.

Oludare said the policy's lack of legal backing means no funding, "If the policy gets legal backing, we can be talking about the funding for the programme, but as it stands today, it's just a policy," he explains.

Joseph Akeju's life came to a standstill after blowing the whistle.

Lack of legal backing compromising whistleblowing

Whistleblowers like Murtala Ibrahim, an internal auditor of the Federal Mortgage Bank of Nigeria, who was punished and later dismissed for exposing malfeasance, are continually subjected to all kinds of punishment for reporting fraud and corrupt practices in their offices.

This is because there is no legal instrument backing it.

A human rights lawyer and senior counsel at Ephesis Lex Attorneys and Solicitors, Abdul Mahmud, described the implementation of the whistleblower's policy as a "dismal failure" due to a lack of a legal framework.

"A policy is a direction of intent, and where it is not backed by law, no effective legal remedy can be derived from it," Mahmud notes.

Onyeacholem, like many other advocates, believes that the duty to blow the whistle can only be enhanced when citizens know that once they blow the whistle, there will not be retaliation, or if there is retaliation, they will be protected.

He added that advocacy to get "whistleblower protection law" is ongoing. A draft bill has been approved by the FEC.

Oludare of PICA confirmed this. He said plans are underway to upgrade it into law. On December 14 last year, the FEC approved the council memo sent to them from the Ministry of Finance. Next is the transmission to the National Assembly, Oludare of PICA said

Relevant stakeholders, investigating security agencies and CSOs are working on getting the policy status upgraded — passed by lawmakers and assented to by the president — before the end of his tenure this May.[1]

"Once we get the law, it will protect me, you or anybody who blows the whistle," Oyeacholem said.

This story is funded by The Centre for Journalism Innovation and Development under the Media Freedom Project through Justice for Journalists Foundation

Whistleblowers Australia contacts

Postal address PO Box U129, Wollongong NSW 2500
Website http://www.whistleblowers.org.au/
Facebook https://www.facebook.com/Whistleblowers-Australia-Inc-172621456093012/

Members of the national committee
http://www.bmartin.cc/dissent/contacts/au_wba/committee.html

Previous issues of *The Whistle*
https://www.bmartin.cc/dissent/contacts/au_wba/whistle.html

New South Wales contact Cynthia Kardell, phone 02 9484 6895, ckardell@iprimus.com.au

Wollongong contact Brian Martin, phone 02 4228 7860.
Website http://www.bmartin.cc/dissent/

Queensland contact Feliks Perera, phone 0410 260 440, feliksfrommarcoola@gmail.com

Queensland Whistleblowers Action Group
Website http://www.whistleblowersqld.com.au
Secretary: Greg McMahon, phone 07 3378 7232

The Whistle
Editor: Brian Martin, bmartin@uow.edu.au
Phone 02 4228 7860
Address: PO Box U129, Wollongong NSW 2500
Thanks to Cynthia Kardell and Lynn Simpson for proofreading.

WBA conference and AGM

Whistleblowers Australia's annual conference will be held in North Parramatta on Saturday 18 November and the annual general meeting on Sunday the 19th. Cynthia will be sending detailed information via email, and there will be a notice in the October Whistle.

Vale Daniel Ellsberg

There have been many stories about Daniel Ellsberg after he died on 16 June. He is probably the world's most famous whistleblower from the pre-digital era. He leaked the Pentagon Papers, a secret history of the Vietnam War, to the media, which were reluctant to publish the story but eventually did. He didn't give up, writing and speaking for decades.

Whistleblowers Australia membership

Membership of WBA involves an annual fee of $25, payable to Whistleblowers Australia. Membership includes an annual subscription to *The Whistle*, and members receive discounts to seminars, invitations to briefings/ discussion groups, plus input into policy and submissions.

To subscribe to *The Whistle* but not join WBA, the annual subscription fee is $25.

The activities of Whistleblowers Australia depend entirely on voluntary work by members and supporters. We value your ideas, time, expertise and involvement. Whistleblowers Australia is funded almost entirely from membership fees, donations and bequests.

Renewing members can make your payment in one of these ways.

1. Pay Whistleblowers Australia Inc by online deposit to NAB Coolum Beach BSB 084 620 Account Number 69841 4626. Use your surname/membership as the reference.

2. Post a cheque made out to Whistleblowers Australia Inc with your name to the Secretary, WBA, PO Box 458 Sydney Markets, Sydney, NSW 2129

3. Pay by credit card using PayPal to account name wba@whistleblowers.org.au. Use your surname/membership as the reference.

New members: http://www.bmartin.cc/dissent/contacts/au_wba/membership.html