



Welcome to this week's edition of Defuse News

A weekly briefing for people whose profile attracts attention.

Careless Talk Has Consequences

The gardener, the group chat and the out-of-office

In 1940 the government told people that careless talk cost lives. The point was never that anybody was a traitor. It was that information moves through ordinary conversation, between people who mean no harm at all.

Ask a family today how many people know they are away this summer and you will get a small number. The principal, the office, the staff who need to. Perhaps a dozen.

The real number is very much larger, and almost none of it came from the principal.



💬 The children

The children have told their friends. Not only where, but for how long, when they are back, who is going, and often who else will be there.

They are not being careless. They are doing what everybody their age does, to audiences they have never counted. A group chat of eleven becomes a screenshot in a group chat of ninety without anybody intending it. A family can settle its own posting policy in an afternoon. It has no say in what a friend of a friend does with that screenshot.

The right response is a conversation, not an inquest. If the first one feels like a telling-off there will not be a second.

🏠 The staff

The staff have mentioned it too.

- The relief cleaner tells a friend the family are away until September and it is quiet.
- The gardener tells the man at the yard he has a free run for six weeks.

None of this is disloyal. It is ordinary conversation about work. Notice, though, that neither of them mentioned where the family had gone. **They gave away the dates, which is the more useful half.**

Most household staff have never been told that the family's movements are worth protecting. Once told, most are careful about it. Reprimanding people for something nobody asked them not to do achieves very little.

Then there is everything that leaked while the trip was being arranged:

- the neighbour asked to keep an eye on things,
- the forwarded itinerary,
- the automatic email reply naming the person covering.

Nobody involved is a risk. But the information has travelled through dozens of ordinary exchanges before anyone has thought about who might be listening at the far end of one.



📖 A familiar name at the door

The firms a family uses do not only know its movements. **Their names carry weight at the door, which is a second kind of exposure entirely.**

In February last year a woman knocked at the staff accommodation beside a £105 million house in central London and said a cleaning agency had sent her for a trial shift. She was not known to the staff. She was allowed in, and left later that day. When the occupants returned, jewellery and other property valued at £548,565 was missing. She pleaded guilty at Wood Green Crown Court to that burglary and two others. None of it has been recovered.

According to reporting at the time, the property was under the protection of former royal protection officers.

Nobody forced a door or picked a lock. The name of a trusted supplier, offered confidently to people with no way of checking it, was enough.

That household had been trained by ordinary life to treat a plausible explanation as an explanation, which is what most of us do most days.



One photograph

When John Terry's Oxshott home was burgled in 2017, he had posted a picture from the French Alps telling his followers he was having a few days away skiing with the family.

Sentencing four men to nearly twenty-eight years between them, the judge remarked that it might have been a mistake to post a family photograph showing he was away, and that the house had been deliberately targeted.

- Some £400,000 was taken.
- The gang came back for the safe with an angle grinder.
- It was the noise that woke the housekeeper.

Most families understand that lesson now.

The harder question is what happens when the same information reaches the public without anybody posting anything at all.



The part nobody controls

Everything so far can be influenced. A family can:

- talk to its children,
- brief its staff,
- tighten how it books things.

None of that helps when a photograph runs in a newspaper.

- A principal with faultless discipline is photographed on a beach and the town appears in the caption by the evening.
- Another guest tags the villa.
- A local account posts a yacht in the harbour and a national picks it up within a day.

There is no remedy worth having once that happens. Deleting the original is pointless, since it has already been syndicated and archived, and complaining is slow and draws further attention. The location is public, lawfully, and nobody has done anything wrong.

Three things shift once you assume disclosure rather than hope against it.

1 The location turns out to be the least of it

Knowing a family is in Greece is a curiosity. Knowing they went on the second and are back on the twenty-third is a plan, because duration is what converts information

into opportunity. It gives a window, and a window can be worked at leisure. Which makes the out-of-office a more valuable document than the photograph on the beach. The photograph says they are away now. The auto-reply says until when and helpfully names the person covering. Families worry about the first and set up the second themselves, every summer, without a second thought.

2 The empty house becomes the exposure

At Oxshott the story was on the slopes and the loss was at home.

3 The instruction to the children stops working

"Don't post" collapses once a location is public, because a teenager can see the rule has been overtaken. What survives is narrower:

- not the layout,
- not the gates,
- not who else is staying,
- not the date you come home.

A fourteen-year-old can see the sense in that, which is why it holds.

Secrecy fails all at once. A family that has planned for disclosure loses very little when it comes.

One that has bet everything on not being seen loses the lot in an afternoon.



? Questions worth sitting with

- How many people actually know?

Not the number you would guess, but the number you get when you

write them down.

- **Who knows the return date?**

Not who knows the destination, which matters less, but who has been told when the house will be occupied again.

- **Has anybody ever explained to the household staff that the family's movements are worth protecting, or has it simply been assumed?**
- **If somebody arrived tomorrow with a plausible reason and a familiar supplier's name, what would actually happen at the door?**

The point

Families picture the risk as somebody researching them. In practice the information arrives long before anyone goes looking, handed over in fragments by people who care about the family or work for them, none of whom thought they were saying anything of consequence.

You cannot stop that, and it is not worth trying. What you can do is:

- know how far it has gone,
- and decide in advance what it changes.

A name offered at the door is a claim rather than a credential, and so is a photograph, an itinerary and a friendly word at the yard.

The wartime campaign never accused anybody of treachery. It pointed out that information travels, and asked people to notice. Eighty-six years on, that is still most of the advice.

Be hard to find. Even harder to target.



How we help

We advise prominent families and the professionals who act for them on precisely these questions:

- what is already exposed and to whom,
- what a particular trip or destination actually involves,
- and what is worth doing about it.

That includes:

- discreet intelligence checks,
- travel risk assessments,
- and briefing household and estate staff.

Where a house will stand empty for several weeks, we can also arrange residential cover through vetted partners.

✉ **If reading this has raised a question about your own arrangements, do get in touch.**

I overhauled security after Jo Cox's murder. Many MPs are ignoring the basics

In the wake of Ann Widdecombe's death, ex-Scotland Yard detective Philip Grindell says politicians don't take their safety seriously enough



Colin Freeman
Show biography ✓

Published 23 July 2026 2:00pm
BST



Gift this article free

Add us as preferred source



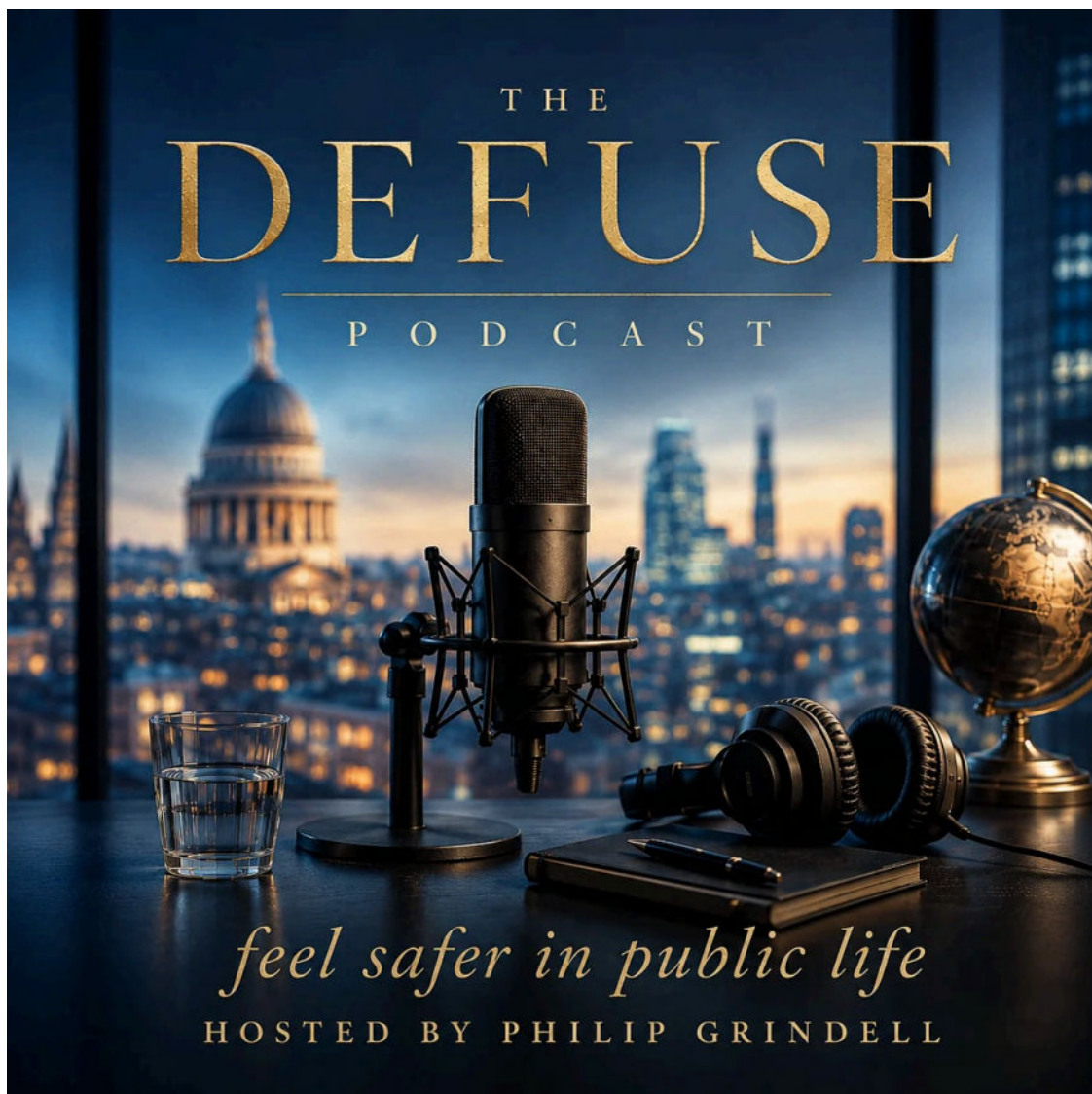
When Prime Minister Andy Burnham pledged a review of MPs' security last week, I sent him a copy of my book, [Personal Threat Management: The practitioner's guide to keeping clients safer](#)

First, I asked one of my staff to find his home address. We found it in 20 minutes. That shouldn't be happening.

It's one of the reasons I spoke to Colin Freeman at [The Telegraph](#) this week about why the current debate on protecting politicians keeps missing what matters.

Many of the issues raised in the article apply to private clients and other public figures, complacency being one of them.

[The full article can be read here:](#)



Coming this August

Stop Waiting for the Threat, with Chuck Tobin

Philip is joined by a good friend. Chuck Tobin, President of AT-RISK International, is one of the most influential figures in protective security worldwide: a past President of the [Association of Threat Assessment Professionals](#), current President of the [International Protective Security Board](#), and the man who chaired the ASIS council that published the industry's first standard in executive protection. He is also someone Philip counts as a friend and a mentor, so what follows is two colleagues comparing notes, not an interview with a stranger, on a profession they both want to make better.

Together they take apart some of the industry's most persistent myths. Why 'threat assessment' is framed wrong from the start, teaching people to wait for a threat when the behavioural warning signs appear far earlier. Why the gun is not the answer: almost no attacks on principals have been stopped by a protector drawing a

weapon, and with AI now compressing months of hostile surveillance into a targeting package built in minutes, surveillance detection has overtaken presence as the critical protective effort.

They also get practical, and uncomfortable. The executive with cameras and gates but no plan for the five minutes between calling the police and the police arriving.

The expensive safe room that fails in the first five minutes. The phone that holds your entire life, including the backup codes a thief now controls. And the question almost nobody asks: what harm are you actually exposed to, when reputational, psychological and financial damage are far more likely than physical attack?

A conversation about selling people what they need, rather than what the industry wants to sell them.

Chuck Tobin

Chuck Tobin has served as President of [AT-RISK International](#) since 2003, bringing over 35 years of experience protecting people, property and operations for clients worldwide. He leads complex threat investigations and executive protection risk assessments, and chaired Standards and Guidelines on the ASIS Executive Protection Council, publishing the industry's first standard in executive protection.

He is the current President of the International Protective Security Board, served as President of the Association of Threat Assessment Professionals from 2013 to 2017, and has been a volunteer leader for ATAP since 1999. He is a recipient of the Florida Department of Law Enforcement Commissioner's Medal for his work advancing threat assessment.



Know someone who would benefit from this newsletter?

Please send it to them.

Most people receive their first warning sign long before they receive any advice on what to do about it.



Subscribe to Defuse News defuseglobal.com/newsletter

- ✓ Free to subscribe
- ✓ Delivered every Monday morning
- ✓ Unsubscribe at any time

Philip Grindell MSc CSyP

Founder & CEO, Defuse Global

Author of [Personal Threat Management: The Practitioner's Guide to Keeping Clients Safer](#)

If anything in this newsletter has caused you to think, you may benefit from our help.
Contact us at info@defuseglobal.com

Defuse Ltd, 124 City Road, Old Street, London EC1V 2NX, United Kingdom, +44 02072930932

[Unsubscribe](#) [Manage preferences](#)