Unsafe At Any Speed: Take #2

Like most people, I have a cell phone which I use occasionally, only. Most others use them constantly. It's a device that's changed the world, no question. Unhappily, extremists use them as remote triggers for bombs. So ... how would you feel about such a trigger being used to detonate a bomb on a passenger plane high in the sky? Oh, and you're on it....

*

Everybody has a worst nightmare.

Soon we'll all be able to share one more: a passenger jet being blown out of the sky while a terrorist sips his latte in the airport lounge, having just used his cell phone to trigger the onboard bomb.

No doubt you have a mobile, perhaps two. In emergencies, they may be lifesavers; and you can use them anywhere. Well … not quite. There are some places where they are *machina non grata*: doctor's office; church; hospital; library; cinema/theatre; school rooms; petrol/gas stations; all government public galleries; and now while driving. There may be variations in other countries, but the point is clear: mobile phones have a place in our society but not every place should have a mobile phone.

Is there a case to allow use of mobile phones on aircraft? Well, yes. But, in addition to technical problems and the prospect of 'phone rage', there is the overarching fact that the mobile is the most dangerously effective go-to plug-in for extremists when they want to detonate bombs – and soon with the potential of remote detonation on aircraft. Nobody, except the terrorist, wants to see that happen.

Whereas this nightmare has been only vaguely possible, the *probability* of that event is now greater than zero and increasing, because in-flight use of mobile phones will be a reality in 2008 or sooner. And that's a scary prospect considering the fact that, up till end 2006, the probability did not exist.

However, times change and technology with it….

Let's go back to early 2004, first. Business groups in USA, lead by the major airlines, submitted a proposal to the Federal Aviation Administration (FAA), to introduce in-flight use of mobile phones on all passenger aircraft. But, together with the Federal Communications Commission (FCC), the FAA delayed a go-ahead because "the technology could interfere with avionics and onboard electronic gear" thus potentially affecting the safety of the aircraft and passengers. Moreover, it was suggested that existing ground-based cell phone systems also could be adversely affected by transmissions from aircraft.

The debate about interference to aircraft avionics persists. In 2005, a paper from the Institute of Electrical and Electronics Engineers (IEEE) – appropriately entitled *Unsafe at Any Airspeed?* and prepared by four academics – acknowledged that "there is no definitive instance of an air accident known to have been caused by a passenger's use of an electronic device” but strongly advocated curbing the use of cell phones on aircraft in view of the proven record of interference with aircraft avionics. There are no subsequent papers on the topic at IEEE, so it’s reasonable to think that the basic conclusion remains, as stated by the authors: “Our data and the NASA studies suggest to us that there is a clear and present danger: cell phones can render GPS instrument useless for landings.”

By late 2006 things had changed, technically: new technology that addresses the issue of interference to avionics, and which is supplied by two communications companies, OnAir and GSM World, has been introduced and is now undergoing in-flight tests in Europe on selected carriers, and in Australia on QANTAS. Other airlines either showing interest or actually testing the new equipment – called the picocell – include AirBus, Air France, British Midland Airways (BMI), TAP Air Portugal, Ryan Air, and Cathay Pacific. So: while the FAA and FCC in USA still maintain a prohibition on in-flight use, regulatory authorities in Europe and Australasia have obviously decided to allow full use of in-flight mobile phones, provided the testing is satisfactory. On that score, recent news reports from around the world indicate all appears to be going well; an unknown, however, is how effective the picocell is or will be in nullifying any danger to GPS instruments.

Considering the enormous profits to be made by airlines, with expensive in-flight user fees, why are authorities in USA holding out? There has been some limited testing in the USA but, given the recent advances noted above, why *don’t* the FCC and FAA give the green light to US airlines to allow use of in-flight cell phones? That question was posed via email to the media contact at the FCC but remains unanswered.

A bone of contention with many travellers, and not only Americans, is the potential problem of onboard ‘phone rage’: the risk of paying customers getting into disputes with others who tend to talk too loud, too long or both. To some extent, the picocell will handle this problem, but only in an indirect manner: the aircrew can switch off that unit at anytime of their choosing – thus shutting down all portable electronic device (PED) transmissions. In the context of a cell phone bomb trigger, however, phone rage is *a non-issue*.

Hence, although electronic interference is still a safety issue, the all-important question remains: how to *prevent* any use of a mobile phone to detonate a bomb. On a train or bus, it’s bad enough that some die; on a plane at 10,000 metres, *everybody* dies. It’s puzzling, too, that neither the FAA nor the FCC have any published comment on the risk of cell phones as remote bomb triggers because the FAA already knew in 2003 that mobile phones and bombs don’t go together. In its corporate *Employee Response to Emergencies* booklet, for example, there is a specific reference that “Transmitting on two-way radios and cell phones in the vicinity of a bomb, suspected bomb, or suspicious package/container, may be hazardous.”

That risk is well known. As early as 2001, a would-be terrorist attempted to blow up the Vietnamese embassy in Bangkok using a mobile phone as “a remote detonation device”, according to an FBI report. It’s also well known that such triggers were used in the Madrid terrorist attack, in London, in Bali and continues in Iraq, Afghanistan, Indonesia, Thailand and other places around the world. In 2005, the Department of

Justice (DOJ) in USA warned, "that terrorists could use cell phones as remote-controlled improvised explosive devices in the air". So everybody who wants to know, knows – especially terrorists, worldwide.

Which brings us to the looming problem….

Given that manual security procedures are not perfect, with anecdotal evidence about journalists and others habitually penetrating security with prohibited objects, how much easier will it be for a suicidal extremist with a mobile phone as part of a small and seemingly innocuous package – for example, a fake new phone purchase, dressed up to look exactly like the real thing? If that doesn't worry you, consider this: there is no guarantee that all luggage is always scanned, searched or opened properly; and technology is still years away from providing a fool-proof electronic solution that includes scanning for explosive devices, if that is *ever* possible. A recent paper about terahertz wave generators, for example, for producing spatial imaging of hidden objects concluded "no imaging or detection technology can reliably find every threat to security."

So, what more can be done to reduce the threat from cell phones as bomb triggers?

Who better to ask than the relevant players? Those most involved are: the mobile phone companies, the telecommunication suppliers, the airlines and other regulatory bodies.

From online website data, it appears that four majors of the cell phone industry are: Sony-Ericsson, Motorola, Vodaphone, and Nokia. They control much of the mobile market, with Nokia being the largest. However, the only publicly available data on security and safety information is in relation to normal phone use; that is, the effects of radio-frequency (RF) waves on the brain and the continued efforts to explore other health hazards. **There is no public information about the misuse of mobile phones as bomb triggers.**

Hence, using email, I asked two questions of each media representative I could find: first, what will the phone company do to *prevent* all future phones from being used as remote bomb triggers; and second, what can be done, if anything, to render the already-installed base of mobile phones totally *ineffective* for use as triggers?

Three of the four replied. Vodaphone sent an automatic reply that completely ignored the questions; it was unsigned, unhelpful and useless. Nokia's was more substantial, being written by a human hand; beyond that, it was composed of unrelated statements such as "mobile operator networks typically have a high level of security, utilizing solutions to prevent viruses and other harmful content from reaching mobile phones"; and it was unsigned. From Sony-Ericsson, Kieleigh Hogan, Partner Support Manager, made a good point: extremists have already and can still use other electronic triggers to destroy aircraft – radio devices and electronic timers, for example; to those I can add infra-red devices such as garage door openers and electro-chemical timers.

Hogan claims that "this is not an issue related to the mobile phone industry as such" but that diverts attention from the core issue: why allow extremists *another* method, one that is the *easiest* of all, and the one almost everybody takes for granted? Why should we actively assist the bad guys in their efforts to, once again, use our technology against us – technology that is just too easy and too pervasive?

Motorola has yet to reply.

With little likelihood of anything further from that quarter, it was time to knock on other doors. On the website for AirBus – in joint venture with OnAir – there's not a shred of information about any technology solution designed to prevent a terrorist using an onboard mobile phone as a remote bomb trigger. Why not? I posed that question to the marketing manager at AirBus responsible for the document containing much of the public information on mobile technology. On the GSM World website – the other supplier of similar technology – it's much the same: there is everything *but* information pertinent to this issue. Hence, the same question was sent. I'm still waiting for replies….

Finally, I searched various agencies in Australia: the Civil Aviation Safety Administration (CASA) website, the Department of Communications, Information Technology and the Arts (DCITA) and the Australian Communications and Media Authority, a sub-department within the former. The result: absolutely no public information on the topic of mobile phones as bomb triggers. I requested further information from the responsible minister, Senator Helen Coonan, but as yet, there has been no reply.

Is it likely that most of these people and organizations are unaware of the risk?

Perish the thought. What's more likely, instead, is that the threat is recognized; the risk is assessed as being low; safety and security procedures are more robust since 9/11 – which they are, despite some upsets and ongoing concerns; and *crucially*, though extremists keep trying to blow up aircraft, nobody has succeeded yet in actualizing our collective nightmare with a cell phone – in colloquial terms, it ain't happened yet on a plane, pilgrim. That's the type of thinking epitomized by security experts such as Bruce Schneier – well-known consultant who often advises the US government and is often interviewed by the media – who essentially sees the benefits of mobile phones as outweighing the risk of attack.

That sort of cost-benefit analysis is familiar: in brutal terms, it means it's okay for some to die so that the rest of us can get on with business. In some areas, they call it 'collateral damage'; but *nobody* ever wants to be part of that damage. However, that *is* a viable frame of reference needed to maintain modern society and business growth: construction deaths occur, yet building continues; mining deaths are often horrendously high, but the diggers keeps digging; policing is dangerous and officers die, but the absence of police is worse; thousands die on the roads, but few will give up their car, and so on. All valid arguments, up to a point, but which break down when we recall that not everybody is in construction, very few want to be miners, only some want to be cops and, unless you're drunk, you tend to have *control* of your car.

But, we're all travellers, of one sort or another, and often at the mercy of providers of all persuasions.

From that perspective and for some time now, it is patently obvious we have all been at greater risk of dying when commuting on buses and trains. Significantly, however, after each attack some people survive to get on a bus or train another day. In the next few months, when in-flight mobile phone use is scheduled to fly, the actual risk of attack may not be too different to that for a bus or train, but *survivability* of any passenger is so unlikely as to be non-existent; which means, in effect, the risk of dying on a plane will soon be greater.

Management of any business includes the eternal need for risk assessment, so what else can be done to reduce that risk?

Well, consider this: some forty years ago, a then little known consumer activist, Ralph Nader, published *Unsafe at Any Speed*, the book that tore the hood off automobile safety in America. In perhaps the first concerted attack on The Big Three automakers – GM, Ford and Chrysler – Mr Nader showed how well established *design faults* were a cause for concern and of passenger death. His book made a big impact: ultimately, the Big Three were obliged to make production changes to improve automobile safety.

There's no time, however, to wait for another book because terrorists have exploited the well established *design flaw/weakness/oversight* – take your pick – of cell phones for years.

And that's why the phone makers must act: first, because of the *increased* risk of death to all travellers and, second, corporate management knows about the problem and published history. It's probably too late to do anything about the millions of existing phones – which, over time, will be replaced anyway – but all new phones should have embedded software – a simple electronic switch – that automatically prevents tampering with its circuitry or operation, preferably to the point of rendering the unit useless and beyond repair.

Considering the growth in air traffic, the market size for cell phones and the enormous profits enjoyed by manufacturers – with uninformed consumers in the middle – the financial risk for airlines, communications providers and the phone companies must be in peril as soon as *one* passenger aircraft is blown to bits. Quite frankly, in these days of uncertainty it's no longer an option, nor very smart, for management to sit on its hands, waiting for *proof* that cell phones are unsafe at any speed.

Meanwhile, the clock is ticking and, like I said, only a terrorist wants to see passengers wake up to live out – and die in – their worst nightmare.