

The Electronic Harassment Delusion

A 200-year history of researchers, implant practitioners, and tech founders being contacted by people experiencing chip-implant and mind-control delusions

Why this document exists

If you publicly work on, write about, or sell anything that involves placing electronics in or near the human body, including RFID implants, neural interfaces, deep brain stimulators, cochlear implants, or even RFID-tagged pets, sooner or later you will be contacted by someone who is convinced they have already been implanted, against their will, by an unknown party. They will want help to find it, prove it exists, remove it, or jam its signal.

I run Dangerous Things. We make and sell consumer-grade RFID and NFC implants and we host the largest public forum dedicated to the topic. I get these contacts regularly, my staff get them regularly, and the forum admins get them regularly. This document is the historical and clinical context I wish I had been handed years ago, written down so the next person in this position does not have to assemble it from scratch.

This phenomenon is not new, not rare, and not a quirk of any particular era's technology. It has been documented in the medical literature continuously since 1810, and the structure is remarkably stable. Only the imagined hardware and the imagined puppeteers update with the times. Magnetic looms become radio waves become microwaves become microchips become 5G towers become Neuralink. The British government becomes the CIA becomes Freemasons becomes Big Pharma becomes Elon Musk.

This report traces that lineage from the very first documented case to the present day, with particular attention to people in roles like mine, because the inbox I see every week is the same one Delgado got, the same one Mark Gasson got, and the same one every Neuralink press release generates.

Part I: The classical literature (1810 to 1919)

John Haslam and James Tilly Matthews (1810), patient zero

The story begins at Bethlem Royal Hospital (“Bedlam”) in London with John Haslam, the apothecary, and his most extraordinary patient, **James Tilly Matthews**. Matthews was a Welsh tea merchant and amateur peace negotiator who had spent years caught between the British and French governments during the Revolutionary period. By 1797 he was confined to Bedlam after shouting “Treason!” at the Home Secretary from the public gallery of the House of Commons.

Matthews believed a gang of seven operatives, with names like Bill the King, Jack the Schoolmaster, Sir Archy, Augusta, the Glove Woman, Charlotte, and the Middle Man, were tormenting him from a basement near London Wall using a machine he called the **Air Loom**. The Air Loom combined recent advances in pneumatic chemistry with mesmeric “animal magnetism,” producing rays and gases that performed specific operations on him: “Lobster-cracking” (cutting off circulation), “Stomach-skinning,” “Apoplexy-working with the nutmeg grater” (introducing fluids into the skull), “kiteing” (lifting thoughts out of his brain), and “brain-saying” (forcing thoughts in).

Matthews drew detailed engineering schematics of the device. Haslam published these in 1810 as *Illustrations of Madness*, the first book-length case study of a single psychiatric patient in history. It is now considered the original description of paranoid schizophrenia, and Matthews is widely identified as the first person on record to insist his mind was being controlled by a machine.

Mike Jay, who wrote the modern biography of Matthews (*The Air Loom Gang*, later reissued as *The Influencing Machine*), describes Matthews as “patient zero” for everyone who has since had messages beamed at them by intelligence agencies, Masonic lodges, UFOs, dental fillings, mysterious implants, TV sets, or surveillance satellites. The Air Loom was reconstructed as a physical sculpture by artist Rod Dickinson in 2002 from Matthews’ original drawings, and it has been exhibited in Newcastle and at the Prinzhorn Collection in Heidelberg.

The crucial point: Haslam was the first researcher on record to receive what we’d now call a “targeted individual” letter. He spent ten years documenting it, and the result is the foundational text of an entire diagnostic category.

Daniel Paul Schreber and August Strindberg

The 19th century produced two more famous influencing-machine subjects.

Daniel Paul Schreber was a German judge who in 1903 published *Memoirs of My Nervous Illness*, describing in lucid detail his belief that he was being acted upon by “rays” controlled by God and the neurologist Paul Flechsig. Schreber’s memoirs became central to Freud’s 1911 case study of paranoia and remain one of the most-cited primary documents in the psychoanalytic literature.

August Strindberg, the Swedish playwright, documented his own persecutory experiences in *Inferno* (1897), describing electrical machines he believed were being directed at him from neighboring apartments.

Both became reference cases for clinicians dealing with what was beginning to be recognized as a coherent phenomenon rather than a series of isolated curiosities.

Victor Tausk and “On the Origin of the Influencing Machine in Schizophrenia” (1919)

The Viennese psychoanalyst **Victor Tausk** wrote what is generally considered the first formal psychiatric treatment of the phenomenon: a 1919 paper titled *On the Origin of the “Influencing Machine” in Schizophrenia*. Tausk had been a colleague of Freud’s and drew on Schreber, Strindberg, and his own clinical caseload to argue that influencing-machine delusions were a recognizable subtype with predictable features:

- The machine is operated by enemies, often persecutors with specific identities
- It produces sensations attributed to “suggestion by waves, rays, or mysterious forces”
- It can read and broadcast the patient’s thoughts
- It causes motor phenomena and bodily symptoms experienced as imposed from outside
- The patient often elaborates the machine’s mechanism in extensive technical detail

Tausk’s framework remains the basic vocabulary clinicians use today. The phenomenon is now classified under “passivity phenomena” or “delusions of control” in modern diagnostic systems.

Part II: The brain-stimulation era (1950s to 1970s)

The mid-twentieth century introduced something new: researchers who actually were drilling holes in human skulls and implanting electrodes. This made them irresistible magnets for people experiencing implant delusions, and the volume of correspondence each of them received is part of the historical record.

José Delgado

The example that originally prompted this whole document. **José Manuel Rodríguez Delgado** was a Spanish neurophysiologist at Yale who pioneered radio-controlled “stimoceiver” implants, which were devices that could both record from and electrically stimulate specific brain regions wirelessly. His most famous public demonstration was stopping a charging bull mid-stride in a Spanish bullring in 1963 by triggering a stimulator in its caudate nucleus.

Delgado’s 1969 book *Physical Control of the Mind: Toward a Psychocivilized Society* described implanting electrodes in human patients and noted, somewhat cheerfully, that women patients had taken to wearing decorative hats and wigs to conceal their electrical headgear. The book essentially advertised that this technology existed and was being applied to people, which is why he became, as the Cabinet Magazine piece I read captures, a permanent fixture in the inboxes of people insisting they had been implanted against their will and asking him to remove the devices. He was also sued by people he had never met.

Robert G. Heath

Even more aggressive than Delgado, **Robert Galbraith Heath** founded Tulane University’s Department of Psychiatry and Neurology in 1949 and ran it until 1980. From 1950 onward, Heath implanted electrodes in the brains of psychiatric patients, most of whom were drawn from the back wards of Louisiana state mental hospitals, leaving the electrodes in place for periods ranging from days to years. He targeted the septal region (a pleasure center) and claimed his stimulation could ameliorate schizophrenia, depression, suicidal ideation, and homicidal mania.

Heath’s most notorious experiment was 1970’s “Patient B-19,” a 24-year-old man whom Heath attempted to convert from homosexuality using septal stimulation combined with the introduction of a female sex worker. The work was funded in part by the US military and the CIA, and many of his subjects were African American. Once those facts entered the public record, Heath became a permanent fixture in mind-control narratives.

Heath received the same letters Delgado did, in similar volume, and his Tulane affiliation made him a recurring villain in the literature of the Targeted Individuals movement decades later.

John C. Lilly

Best known today for his work with dolphins and isolation tanks, **John C. Lilly** spent 1946 to 1953 at the University of Pennsylvania developing techniques for safely implanting electrodes in monkey and cat brains. He built a 25-electrode brain-mapping device he called the “bavatron” and proposed scaling up to 1,000 electrodes, a goal that wouldn’t be achieved until BrainGate and Neuralink decades later.

Lilly attended a 1952 meeting at the Ritz-Carlton in Montreal where Donald Hebb proposed sensory deprivation as a tool for making subjects “susceptible to the implantation of new or different ideas,” research that fed directly into MK-Ultra. Lilly was also briefly aware of Ewen Cameron’s “psychic driving” work at McGill, which became the most notorious of the CIA’s mind-control programs.

Lilly’s combination of real electrode implantation, sensory-deprivation work, dolphin-language research, and later open advocacy for psychedelic experience made him a touchstone figure for both legitimate neuroscience and the entire fringe of mind-control belief. His later autobiography openly described being contacted by people convinced they were under remote influence.

Part III: Modern researchers and the post-internet inbox

The invention of the personal homepage and then social media changed the dynamics of this phenomenon completely. Before the internet, a researcher might receive letters from a few dozen people over a career. After the internet, anyone publicly identified with implants or brain interfaces receives this contact at industrial scale. I can attest to that personally, and so can everyone else in this section.

Mark Gasson

In 2009, **Dr. Mark Gasson** of the University of Reading's School of Systems Engineering had an RFID chip implanted in his left hand to access lab doors and operate his cell phone. In 2010, he became the first human deliberately "infected" with a computer virus. He loaded malicious code onto his implant chip, which then propagated to the building's access database when he swiped in. The experiment was designed to highlight security vulnerabilities in the coming generation of implantable medical devices like pacemakers and cochlear implants.

The press coverage was global. Headlines like "First Human Infected With a Computer Virus" guaranteed that Gasson would become one of the most-contacted people in Europe by individuals convinced they too had been infected, except in their case, by something they hadn't consented to. Gasson's affiliation with Kevin Warwick (see below) and his research framing of "human enhancement and the potential risks of implantable devices" placed him squarely in the category of researcher most likely to receive these contacts.

The Gasson case is also instructive because some critics, notably security blogger Graham Cluley, accused him of "the very worst kind of scaremongering," arguing the experiment effectively manufactured legitimacy for fears that bionic devices could be hijacked. This is the recurring tension for any researcher in this space, and it's one I navigate constantly: the work itself, by demonstrating that implants can be compromised, provides ammunition for delusional belief systems.

Kevin Warwick

Professor Kevin Warwick of the University of Reading, Mark Gasson's mentor, is the man dubbed "Captain Cyborg" by *The Register*. In 1998 he had a simple RFID transmitter implanted in his upper arm (Project Cyborg 1.0), and in 2002 he upgraded to a 100-electrode BrainGate-style array surgically wired into his median nerve, which he used to control a robotic hand over the internet

from New York to Reading. His wife Irena had a matching implant, making them the first humans to communicate nervous-system-to-nervous-system electronically.

Warwick has appeared on Conan O'Brien, written manifestos arguing that humans without implants will become a subspecies "like cows," and in 2002 publicly offered to implant a tracking device in an 11-year-old girl as an anti-abduction measure following the Soham murders. The combination of public flamboyance, real implant work, and statements about superintelligent machines coordinating with implanted humans made him a target of contact from people convinced they were already on the receiving end of exactly the technology he was advocating.

Joel and Ian Gold and the Truman Show delusion

In 2002, psychiatrist **Joel Gold** at Bellevue Hospital in New York began noticing patients whose persecutory delusions were structured around the 1998 Peter Weir film *The Truman Show*. They believed their lives were being filmed and broadcast as a reality television show, that their friends and family were paid actors, and that the world around them was a constructed set. He and his brother **Ian Gold**, a philosopher of psychiatry at McGill, coined the term "Truman Show delusion" and, by their account, have been in contact with over a hundred people experiencing the syndrome since then.

Their book *Suspicious Minds: How Culture Shapes Madness* (2014) is essential reading for understanding why the *form* of these delusions tracks the surrounding culture so precisely. The Golds argue that delusions are not arbitrary, but rather reach for whatever the culture provides as the most compelling explanatory framework for the genuine subjective experience of being watched, controlled, or singled out. In the 1940s that framework was radio waves; today it is reality TV, livestreaming, NSA surveillance, and brain implants.

One of Joel Gold's patients traveled to New York City after September 11, 2001, to verify in person that the World Trade Center had really fallen, just to make sure it wasn't a particularly elaborate plot twist in his personal show. Another believed cameras were embedded in everything around him. The Golds describe the syndrome as a contemporary variant of older persecutory and grandiose delusions.

Vaughan Bell

British clinical psychologist **Vaughan Bell**, now at UCL and South London and Maudsley NHS Trust, has done the most rigorous academic work on the online dimension of this phenomenon. His 2006 paper "*Mind control' experiences on the internet: implications for the psychiatric diagnosis of delusions*" sampled web-published mind-control narratives, had three independent psychiatrists blind-rate them, and confirmed that the content was overwhelmingly delusional in nature.

But the more important finding was structural. The people writing these accounts had formed a coherent online community that linked to and reinforced each other. This created a genuine paradox for the DSM, which had traditionally exempted from the definition of “delusion” any belief shared by a person’s “culture or subculture.” Bell’s paper essentially demonstrated that the internet had broken that exemption, because anyone could now find or build a subculture around any belief, no matter how clinically delusional. This is something I think about a lot in the context of running a public forum: the existence of online community is now part of the substrate of these belief systems.

Bell has continued this research thread with collaborators like Nichola Raihani, arguing for a “coalitional” model of paranoia in which persecutory delusions specifically involve fear of harm from organized groups, and in which this is rooted in evolved social cognition gone awry.

Michael Persinger

Michael Persinger at Laurentian University in Sudbury, Ontario, was famous for the “God Helmet,” which was a device that applied weak magnetic fields across the temporal lobes of volunteers in an attempt to induce mystical or sensed-presence experiences. His work on geomagnetic-behavioral correlates and the possibility that human cognition could be covertly affected by Schumann resonances and magnetic activity made him another permanent magnet for these contacts.

Persinger’s research was widely criticized for replication failures and methodological issues, but his public framing of the brain as susceptible to ambient electromagnetic influence guaranteed that he would be cited as expert authority by Targeted Individual communities for decades.

Part IV: The Targeted Individuals movement

Sharon Weinberger and the Washington Post (2007)

Journalist **Sharon Weinberger's** *Washington Post Magazine* cover story "Mind Games" (January 14, 2007) was the first major mainstream media examination of what the affected community called the Targeted Individuals (TI) movement. She interviewed dozens of self-identified TIs who described ringing in the ears, sensations of being touched at a distance, hearing voices, sexual attacks via remote manipulation, and beliefs about government microwave weapons.

Weinberger noted the structural parallel to alien-abduction narratives: a coherent body of shared experiences, a community of believers, and a stable explanatory framework that, crucially, was anchored to real US military research programs (HAARP, MK-Ultra, microwave hearing effect) that gave the claims a thin veneer of plausibility. She also noted that the Pentagon really had pursued non-lethal weapons that beamed sound into people's heads via the Frey effect, which complicated easy dismissal.

Mike McPhate and the New York Times (2016)

Nine years later, **Mike McPhate's** NYT piece "United States of Paranoia: They See Gangs of Stalkers" (June 10, 2016) estimated, conservatively, that at least 10,000 people in the US identified as Targeted Individuals. The article centered on the "gang stalking" variant, which is the belief that one is being followed and harassed by an organized network of operatives in everyday public spaces, with implants or directed-energy weapons as a frequent component.

McPhate interviewed Lorraine Sheridan and David James, whose 2015 paper in the *Journal of Forensic Psychiatry and Psychology* found that essentially all complaints of "gang stalking" they reviewed appeared to reflect underlying delusional disorder. Sheridan described the online TI communities as "echo chambers" that amplified and entrenched the beliefs.

McPhate himself received threats after publication. The TI community produced multiple lengthy rebuttals accusing him of being a propagandist for the surveillance state.

The mass-violence connection

The TI movement intersects with mass violence more often than is comfortable. Christine Sarteschi's 2018 paper *Mass Murder, Targeted Individuals, and Gang-Stalking* documents at least four cases:

- **Aaron Alexis**, the Washington Navy Yard shooter (2013), left writing about being attacked by extremely low-frequency electromagnetic waves
- **Myron May**, who shot three people at Florida State University (2014), left video describing his belief that he was being gang-stalked
- **Gavin Long**, who killed three Baton Rouge police officers (2016), identified publicly as a TI
- **Jiverly Wong**, the Binghamton shooter (2009), expressed similar beliefs

This is part of why the topic matters operationally for me. A non-trivial fraction of people who arrive at our forum convinced they have non-consensual implants are experiencing genuinely dangerous psychiatric crises.

Part V: The biohacking and body-modification community

My own experience and Dangerous Things

I had an RFID chip implanted in my hand in 2005 to open my office door, gave a TEDx talk about it, wrote *RFID Toys* for Wiley, and, directly because of the volume of contact I received from people wanting to do similar things, founded Dangerous Things to provide vetted hardware and installation guidance. The company exists in part because, after my story went mainstream, one woman who attempted a DIY hack ended up hospitalized.

But I also receive the other category of contact, and have for nearly twenty years now. People email, call, message the forum, and occasionally show up in person, all convinced they have already been implanted, often by employers, ex-partners, the government, hospitals after a routine procedure, or COVID vaccines. The 2020 to 2021 vaccine-microchip conspiracy in particular drove enormous traffic to anyone publicly working with implantable RFID, because the conspiracy specifically claimed Bill Gates was deploying RFID-style trackers via vaccination, and the most visible proof of concept anyone could find on Google was my hand.

The pattern I've talked about publicly is structural and worth restating clearly. RFID does not triangulate location. It does not interact with the nervous system. It does not transmit data without an external reader within centimeters. None of this matters to someone whose belief system has already incorporated the implant; the technical facts are simply absorbed as further evidence of the cover-up.

Lepht Anonym, Grindhouse Wetware, and the broader “grinder” scene

Lepht Anonym (the pseudonymous British biohacker who self-implanted magnets and RFID tags using vodka and a scalpel) and the Pittsburgh-based **Grindhouse Wetware** (Tim Cannon, the Northstar V1 LED implant) are the other public faces of the DIY end of this community. Both have, by their own accounts, received the same flood of contact: requests for help locating implants, removing them, blocking their signals, or proving they exist.

Tattoo and piercing studios that perform magnet implants and NFC injections, including the small network of professional implanters we train and certify through Dangerous Things, are also routinely contacted. The local body-mod studio is, for many people in this category, the closest physical manifestation of the conspiracy they can access.

Why the forum specifically attracts these contacts

The reason the forum specifically attracts these contacts is the same reason Delgado's office did. Dangerous Things is, from the affected person's perspective, a company of experts who would either confirm what's been done to them or be in on it. The forum's existence as a publicly searchable resource on implants makes it an obvious destination after an evening of searching for "how to find a chip in my body."

Part VI: The neural-interface industry

Neuralink, Elon Musk, and the modern flood

The contemporary champion of inbound implant-delusion contact is unquestionably **Elon Musk and Neuralink**. Every press release, every Joe Rogan appearance, every X post about brain-computer interfaces generates a measurable surge of contact directed at the company, at Musk personally, and at any physician affiliated with the program. The company's stated long-term goal of "symbiosis with artificial intelligence" maps directly onto the existing TI cosmology, which makes Neuralink a uniquely powerful source of confirmation for pre-existing delusions.

Noland Arbaugh, Neuralink's first patient, has himself experienced a related but distinct phenomenon. When threads in his implant retracted weeks after surgery, he describes crying at the prospect of having to have it removed, having "become one" with the device. This is the inverse problem researchers like Frederic Gilbert have begun to write about: legitimate patients who develop intense identification with their implants and experience their removal as a form of trauma.

Frederic Gilbert, Marcello Ienca, and the neuroethics community

Frederic Gilbert (University of Tasmania), **Marcello Ienca** (Technical University of Munich), and a small cohort of neuroethicists studying brain-computer interface trials have documented cases like that of **Rita Leggett**, an Australian epilepsy patient whose experimental NeuroVista implant was forcibly removed in 2013 when the company went bankrupt. Years later she still describes the loss as a form of grief. This work has nothing to do with delusional belief and concerns real implants in real patients, but the ethicists doing it report receiving the standard volume of contact from people convinced they have been implanted without consent.

Cochlear and pacemaker manufacturers

Companies that make cochlear implants, deep brain stimulators, sacral nerve stimulators, and cardiac devices receive these contacts at an industrial scale, mostly funneled through patient support hotlines. The medical literature contains specific case reports of patients developing post-implantation paranoid delusions about their actual devices. For example, a 64-year-old woman developed the conviction that the wires from her sacral nerve stimulator had grown up her spine and were affecting her vision and thoughts, and demanded emergency removal. Her symptoms abated with supportive care after she completed grieving for her recently deceased mother. This is

a useful reminder that even when there is a real implanted device, the delusional content can attach to it secondarily.

Part VII: Recurring patterns

Across two centuries, a stable set of features recurs in essentially every case.

The technology updates with the era. The 1810 version is a magnetic loom in a basement; the 1903 version is rays from God and Dr. Flechsig; the 1950s version is radio waves and the CIA; the 1990s version is microchips in dental fillings; the 2010s version is gang-stalking with directed-energy weapons; the 2020s version is COVID vaccine microchips and 5G. Whatever the most cutting-edge or culturally salient technology is, that becomes the imagined hardware.

The persecutor matches the era's most threatening institution. French Jacobins, then the British government, then communists, then the CIA, then Big Pharma, then Bill Gates, then Elon Musk. The persecutor is whoever the surrounding culture has identified as the most plausible orchestrator of large-scale covert harm.

The phenomenology is remarkably stable. Sensations of being touched, voices in the head, intrusive thoughts experienced as not one's own, motor phenomena attributed to external control, certainty of being singled out, and a strong sense that some technical mechanism explains it all.

Contact-seeking follows a predictable pattern. The affected person eventually identifies someone in the public eye who appears to have authoritative knowledge of the implants in question, whether that's Delgado, Heath, Gasson, Warwick, me, Musk, or Neuralink, and writes, calls, or visits them. The request is almost always one of three things: help finding the implant, help removing it, or public validation that the implants exist and are being used as described.

The internet has industrialized everything. What was once a trickle of letters is now a flood, and the affected person is no longer alone. They enter an online community that confirms their experience, supplies new vocabulary ("V2K" for voice-to-skull, "DEW" for directed-energy weapon), and provides an institutional memory of every researcher and company who could plausibly be the source.

Part VIII: When it's real, tech-enabled stalking and intimate partner surveillance

Everything up to this point has been about people whose beliefs about being electronically tracked are delusional. But the honest version of this story requires a second half, because a substantial and growing number of people genuinely are being electronically tracked by ex-partners, abusers, family members, and occasionally employers, using cheap, legal, widely available consumer technology. Understanding this category is essential for anyone fielding “I think I’m being monitored” contacts, because the two populations look superficially similar and the cost of confusing them runs in both directions: real victims of intimate partner abuse get dismissed as Targeted Individuals, and people in psychiatric crisis get their delusions reinforced by articles about stalkerware.

Stalkerware: commercial spyware marketed for intimate partner abuse

The category name for consumer-grade surveillance software is **stalkerware**, and the industry behind it is substantial. Products with names like mSpy, FlexiSpy, Cocospy, Spyic, Spyzie, pcTattleTale, Cerberus, Mobile Tracker, SpyPhone, TrackView, and LetMeSpy are sold openly online, usually marketed as “parental control” or “employee monitoring” software, but almost entirely used for covert surveillance of romantic partners and ex-partners.

The capabilities are genuinely comprehensive. A typical stalkerware install, once deployed on a target’s phone, can harvest location in near real time, read all SMS and iMessage content, read most messaging app content (WhatsApp, Signal, Telegram, Instagram DMs), log call metadata and sometimes record calls, exfiltrate photos, activate the microphone for ambient audio recording, activate the camera, log keystrokes including passwords, and report browser history. The software is deliberately hidden from the phone’s list of installed applications, and most products advertise their invisibility as a feature.

Installation usually requires brief physical access to an unlocked device, which, in the intimate-partner abuse context, is trivial. On iPhones, where Apple’s sandboxing makes on-device stalkerware much harder, the equivalent approach is harvesting the target’s iCloud credentials and reading out their cloud-synced data from a web dashboard. The Spyzie/Cocospy/Spyic source-code lineage, for example, was confirmed in 2025 to have compromised at least 4,900 iPhones via iCloud credential abuse.

The scale is not small. Kaspersky's 2023 State of Stalkerware report identified roughly 31,000 users worldwide who were actively being monitored by detected stalkerware on mobile devices in that year alone, across 195 distinct apps. Gen Digital reported a 239% global increase in stalkerware installations between 2020 and 2023. Kaspersky's commissioned survey of 21,000 people across 21 countries found that 12% admitted to installing monitoring software on a partner's phone, and 9% admitted pressuring a partner to install it on themselves. The Canadian study *The Predator in Your Pocket* and the US-based Coalition Against Stalkerware (co-founded by the EFF in 2019) now treat this as a stable and growing category of abuse, not a fringe phenomenon.

The stalkerware industry is also notoriously badly engineered. By one tally, at least 24 separate stalkerware operations have suffered major data breaches since 2017, exposing the surveillance data of millions of victims to the open internet, which is, from a victim's perspective, additional harm on top of the original surveillance.

Hardware trackers: AirTags, Tiles, and the \$29 stalker's toolkit

The launch of the Apple AirTag in April 2021 changed the economics of location stalking overnight. A quarter-sized Bluetooth tracker that piggybacks on Apple's global Find My network, for \$29, with the practical effective range of the entire fleet of iPhones on Earth, is a tool that, prior to 2021, would have been considered covert government hardware.

Vice/Motherboard requested eight months of police records mentioning AirTags from dozens of US police departments in 2022 and received 150 reports. Of those, 50 were women who had received automatic "unknown AirTag traveling with you" notifications; half of those women could name a specific ex-partner, current husband, or boss they suspected had planted the device. The June 2022 murder of Andre Smith in Indianapolis, where his ex-girlfriend Gaylyn Morris allegedly used an AirTag planted in the back of his car to find him before shooting him, was the first high-profile homicide tied to AirTag tracking. A 2022 class-action suit against Apple by two named plaintiffs, both of whom had found AirTags planted by former partners, one sewn into her child's backpack, is still working through the courts.

AirTags are the best-marketed product in the category, but the ecosystem is broader. **Tile**, **Chipolo**, **Samsung SmartTag**, **eufy**, and **Pebblebee** all offer similar Bluetooth trackers, and dedicated GPS trackers with their own cellular modems (often sold as "fleet management" or "teen driver" devices) are available for \$50 to \$200 and will happily report a vehicle's location at one-minute intervals indefinitely. One domestic-violence case in the *Domestic Shelters* reporting involved a victim whose abuser had sewn AirTags into her purse, every jacket she owned, her backpack, her lunch bag, and her car, after having drugged her to use her fingerprint to link them to his phone rather than hers, so the "unknown AirTag" notifications never fired.

Connected cars and the vehicle-surveillance problem

Modern vehicles are themselves surveillance platforms, and this creates a category of abuse that victims frequently cannot identify on their own. A shared-account Tesla will report live location to the original account holder indefinitely after a separation unless the account is explicitly transferred. Many newer cars have factory-installed 360-degree cameras that record whether the car is on or off, with recordings accessible remotely. Aftermarket OBD-II tracking dongles can be plugged into the diagnostic port under the dash in under a minute. Rental cars and leased vehicles sometimes carry undisclosed tracking that the leasing party can access.

Seventeen US states ban non-consensual tracking-device use generally, and an additional nine specifically prohibit tracking in motor vehicles, but enforcement is uneven and victims frequently don't know these statutes exist.

Scale and context

The CDC's 2023/2024 National Intimate Partner and Sexual Violence Survey found that more than 1 in 5 US women, which is 22.5%, or approximately 28.8 million people, have experienced stalking in their lifetimes, and 1 in 20 were stalked in the prior twelve months. Among female stalking victims, 78.3% reported being followed, watched, or spied on; 36.3% reported that the perpetrator used social media specifically to monitor or track them; and 12.6% reported being watched with a hidden camera. Roughly three-quarters of stalking victims know their stalker, and the most common perpetrator-victim relationship is current or former intimate partner.

This is the clinically and ethically important point: the base rate of *real* technology-enabled intimate-partner surveillance in the adult population is not small. It is vastly larger than the base rate of psychiatric illness underlying Targeted Individual beliefs. A person who writes to me saying "I think someone is tracking me through my phone" is, on priors, much more likely to be correct than to be delusional.

The crossover problem

The most difficult part of this territory is that the two populations are not cleanly separable and genuinely can contaminate each other. A real victim of stalkerware whose phone appears to know things it shouldn't can, under stress, reach for more exotic explanations. *The Guardian* and others have specifically documented cases of intimate partner abuse victims who came to believe they had been microchipped because the surveillance felt too total to be explained by software alone. Meanwhile, people with genuine persecutory delusions sometimes attach their beliefs to real surveillance products (AirTags, stalkerware, connected-car features) because those products are now part of the culturally available vocabulary for "being watched."

A few practical heuristics for distinguishing the two cases, drawn from domestic-violence advocacy resources and the Coalition Against Stalkerware materials:

- **Named, plausible perpetrator with access.** “My ex-husband, who lived with me until two months ago and knows my Apple ID password” is a very different profile from “the CIA” or “an unidentified gang.” Real stalking almost always has a named perpetrator with a history of controlling behavior.
- **Specific, mechanism-bounded claims.** “I think there might be software on my phone that’s reading my texts” fits the actual capabilities of stalkerware. “They are reading my thoughts through a chip in my tooth” does not fit the capabilities of any known technology.
- **Timeline anchored to a relationship event.** Surveillance that started after a breakup, separation, custody dispute, or restraining order filing is consistent with intimate partner abuse. Surveillance “that has been going on my entire life” or that began without any identifiable triggering event is consistent with psychiatric illness.
- **Device-behavior evidence vs. subjective experience.** Real stalkerware often (not always) produces detectable signs: faster battery drain, phone running warm when idle, unknown apps, unfamiliar iCloud device logins, data-usage spikes. These are verifiable by running a security scan or checking account activity. “I can feel the signal” is not verifiable by anything.
- **Nature of the request.** Real victims usually want help securing their phones, finding a tracker on their vehicle, changing their passwords, or obtaining a restraining order. They rarely want help “removing an implant,” because their model of the problem is correctly placed in their environment, not in their body.

Resources worth knowing about

For anyone running a community where these contacts arrive, it’s worth having a few organizations bookmarked so you can redirect appropriately when the situation seems real rather than delusional:

- **National Domestic Violence Hotline** (US), 24/7 support, including technology-abuse consultation.
- **NNEDV Safety Net Project**, the National Network to End Domestic Violence’s technology-safety program, which publishes practical guidance for victims and advocates.
- **Coalition Against Stalkerware** (stopstalkerware.org), maintains a list of resources and the detection criteria used by major antivirus vendors.
- **Refuge** (UK), has a dedicated Technology-Facilitated Abuse and Economic Empowerment team.
- **Operation Safe Escape**, technical safety planning for people leaving abusive situations.

A useful default response when it's genuinely unclear whether you're dealing with a real stalking victim or someone in psychiatric crisis is to redirect to the domestic violence hotline rather than to a psychiatrist. The hotline is trained to triage both cases, and importantly, a person in psychiatric crisis is not harmed by being routed there, whereas a real abuse victim routed only to a psychiatrist may be failed in ways that materially increase their danger.

Part IX: Practical guidance for community administrators

Almost everything in this section comes from clinicians, journalists who cover the TI community, biohackers who've handled this for years, and my own twenty-year experience running Dangerous Things and the forum. None of it is medical advice; it's harm-reduction guidance. Read this section in conjunction with Part VIII. A non-trivial fraction of the contacts you receive will involve real technology-enabled abuse rather than delusional belief, and the triage problem matters.

Do a quick reality-test before categorizing the contact. The heuristics at the end of Part VIII (named perpetrator, plausible access, mechanism-bounded claims, event-anchored timeline, device-behavior evidence, and the nature of the request) are the fastest way to decide which of the two playbooks applies. If it looks like real stalking, route to domestic-violence resources, not to a psychiatrist.

Don't engage with the technical specifics. Debating whether the device they describe is plausible, offering to scan them, or trying to disprove the implant tends to entrench the belief. The brain is very good at incorporating disconfirming evidence into the conspiracy. Vaughan Bell's research is unambiguous on this point.

Don't agree, either. Validating the belief, even compassionately, provides exactly the confirmation the person was seeking, often makes their distress worse, and can implicate you when their belief system later evolves to include you as a perpetrator.

Acknowledge the distress without endorsing the explanation. "It sounds like what you're experiencing is genuinely awful, and that deserves real medical attention" is a sentence that's both true and useful. The distress is real. The explanation is what's incorrect.

Redirect to a primary care physician, framed as a foreign-body question. "Anything that might be in your tissue is a medical question that needs imaging, and that's not something a forum can help with. Please see your GP and ask for an X-ray or ultrasound." This routes the person toward someone who can actually help, sidesteps the delusional framework, and discourages DIY removal.

Take self-removal risk seriously. The medical literature contains documented cases of psychotic patients self-removing implanted devices with knives, including contraceptive implants and cardiac devices. People who arrive at a body-mod forum convinced they have a hostile implant are at non-trivial risk of attempting their own surgery. The harm-reduction frame ("please don't try to remove anything yourself, see a doctor") is genuinely important.

Don't suggest specific imaging modalities or removal techniques. Even framed as “this is what would prove there's nothing there,” these suggestions can be incorporated into a self-harm plan.

Watch for crisis indicators. Mentions of suicidal ideation, intent to harm others (especially specific named persecutors), recent purchases of weapons or surgical instruments, or detailed plans to confront the persecutors all warrant directing the person to a crisis line and, where appropriate, alerting authorities.

Document and template your responses. If you're getting these regularly, a saved response that says some version of “we cannot help with this, here is why, please see a doctor,” sent kindly, briefly, and without further engagement, saves enormous time and is the best outcome for the person on the other end.

Be aware that some fraction will eventually identify you as a perpetrator. This is the unfortunate occupational hazard. Delgado was sued by people he had never seen. Mike McPhate received threats. Researchers in this space have been physically threatened. It's worth thinking through, in advance, what your response will be if a contact escalates from “help me” to “you're one of them.”

Further reading

The following sources informed this report and are worth reading in full.

Books

- Mike Jay, *The Influencing Machine: James Tilly Matthews and the Air Loom Gang* (Strange Attractor Press, 2012; originally *The Air Loom Gang*, 2003). Foreword by Oliver Sacks. The single best entry point.
- Joel Gold and Ian Gold, *Suspicious Minds: How Culture Shapes Madness* (Free Press, 2014).
- Lone Frank, *The Pleasure Shock: The Rise of Deep Brain Stimulation and Its Forgotten Inventor* (Dutton, 2018), the Robert Heath biography.
- José M. R. Delgado, *Physical Control of the Mind: Toward a Psychocivilized Society* (Harper & Row, 1969). A primary source.
- Daniel Paul Schreber, *Memoirs of My Nervous Illness* (1903; NYRB Classics edition). The other primary source.

Foundational papers

- Victor Tausk, "On the Origin of the 'Influencing Machine' in Schizophrenia" (1919).
- John Haslam, *Illustrations of Madness* (1810). Available via Wellcome Collection.
- Vaughan Bell et al., "'Mind control' experiences on the internet: implications for the psychiatric diagnosis of delusions," *Psychopathology* 39 (2006): 87 to 91.
- Lorraine Sheridan and David James, "Complaints of group-stalking ('gang-stalking'): an exploratory study," *Journal of Forensic Psychiatry and Psychology* 26 (2015): 601 to 623.
- Joel Gold and Ian Gold, "The 'Truman Show' delusion: psychosis in the global village," *Cognitive Neuropsychiatry* (2012).
- Christine M. Sarteschi, "Mass Murder, Targeted Individuals, and Gang-Stalking: Exploring the Connection," *Violence and Gender* 5 (2018): 45 to 54.

Journalism

- Sharon Weinberger, "Mind Games," *Washington Post Magazine*, January 14, 2007.
- Mike McPhate, "United States of Paranoia: They See Gangs of Stalkers," *New York Times*, June 10, 2016.

- Andrew Marantz, “Unreality Star,” *The New Yorker*, September 16, 2013 (on Truman Show delusion).
- The Bartas/Ekman piece on Delgado in *Cabinet Magazine*, issue 2.

On the biohacking side

- My own TEDx SFU talk (2013) and the Dangerous Things forum archives at forum.dangerousthings.com.
- Mark Gasson’s published research on implant security at the University of Reading.

On real tech-enabled stalking and intimate partner surveillance

- Christopher Parsons et al., *The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry* (Citizen Lab, University of Toronto, 2019). The foundational academic study of the stalkerware industry.
- Kaspersky’s annual *State of Stalkerware* reports (2019 to present).
- Zack Whittaker’s ongoing reporting at TechCrunch on stalkerware breaches and exposed consumer surveillance operations.
- The Coalition Against Stalkerware website (stopstalkerware.org) for detection criteria and victim resources.
- The NNEDV Safety Net Project’s published guidance for advocates and survivors on technology-facilitated abuse.
- CDC National Intimate Partner and Sexual Violence Survey (NISVS), 2023/2024 data brief on stalking.
- Joseph Cox’s reporting at Vice/Motherboard on AirTag stalking from police records.

Compiled April 2026 by Amal Graafstra. This report focuses on the Western European and North American documentary tradition; equivalent phenomena exist in every culture but are described in different vocabularies. Cross-cultural comparison would be a useful future addition.