VERSION 1.0 · NOVEMBER 2026 · OSTERING.COM

Care Assistant Threat Taxonomy

74 threats in nine suits plus the structural hazards, for systems that watch over someone at home. Brett Crawley.



What this is

Systems that monitor a person at home on someone else's behalf, where the person watched over is not the one using the system and may not be able to consent fully or freely: babies and children, older people, people with a disability or long-term illness, and people in mental health care. Covers social alarms and telecare, personal emergency response systems, baby and child monitors, passive ambient monitoring, wearable sensors, camera and audio monitors, and routine or mental-state analytics. Jurisdiction-neutral. Generic platform threats (cloud, CI/CD, email, AI agents) are left to the Software Factory, Elevation of Email Flow and Elevation of Autonomy taxonomies.

Each entry states the threat as a property of a component or a design decision, the principle a sound design follows, and two or three design measures, with mappings to STRIDE, LINDDUN, CAPEC 3.9 and CWE 5.0. Many care threats have no CAPEC or CWE equivalent, and those cells are left empty on purpose. 45 of the 74 entries carry a life-safety consequence.

The ID (EOC-SN-A, EOC-AL-A, EOC-T1) is the card it comes from, with EOC for Elevation of Care and dashes so search engines index each ID as one term. It is a stable identifier, not a severity.

How to use it

1. Draw the system: devices, the home network, the cloud, the watchers' phones, the response chain, and the person watched over. 2. Take one suit and walk every entry against each element it applies to. 3. Record a finding, or "no exposure" with the design decision that defeats it. 4. Adapt the measures to your design; they are the shape of a fix, not a prescription. 5. Finish with the structural hazards, against the design as a whole.

Reading the tables

† **LIFE-SAFETY** marks an entry whose failure can leave someone without help.

STRIDE: **S** spoofing · **T** tampering · **R** repudiation · **I** information disclosure · **D** denial of service · **E** elevation of privilege.

LINDDUN: **L** linking · **I** identifying · **Nr** non-repudiation · **D** detecting · **Dd** data disclosure · **U** unawareness · **Nc** non-compliance.

CAPEC and CWE IDs were checked against MITRE's definition pages (CAPEC 3.9, CWE 5.0) on 2 November 2026; Discouraged and Deprecated CWEs were replaced.

Licence

© 2026 Jonathan Brett Crawley. CC BY-NC-ND 4.0, with additional permissions. Licensed under Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0): you may share the whole taxonomy, unchanged and with credit, for non-commercial purposes. In addition, whether or not the use is commercial, you may use it to threat model systems, including for paying clients; use it internally and for training inside any organisation; and quote individual entries, with credit, in paid courses, reports and talks. Shipping it in a product, such as a tool's built-in library, a printed deck or a reprint for sale, needs written permission.

Credit: “Nobody Asked the Person Being Watched: A Threat Taxonomy for Care Monitoring at Home” by Jonathan Brett Crawley, ostering.com, licensed under CC BY-NC-ND 4.0. Full terms: https://ostering.com/taxonomies/care-assistant/

CONTENTS

Nine suits along the care chain

Four suits follow an alert from the sensor to the responder (Sensing, Interpretation, Alerting, Response). The resident and the care circle are the people at each end. Sight and Sound carries the person straight to the watchers, and Data and Lifecycle threats run under all of it. The structural hazards cut across every suit.

CODE	SUIT	ENTRIES	LIFE-SAFETY	SCOPE
SN	**Sensing**	8	8	Sensors, wearables, radio links, the home unit and the home it sits in
AV	**Sight and Sound**	6	2	Cameras, microphones, talk-back, live streams and recordings
IN	**Interpretation**	7	7	Baselines, rules, models, feedback loops and what counts as an emergency
AL	**Alerting**	7	4	Getting an alert to a person who acts on it
RS	**Response**	7	6	Monitoring centres, responders, entry to the home and the hand-off to emergency services
CC	**Care Circle**	8	4	The watchers: parents, family, friends, paid carers, agencies and clinical teams
RE	**Resident**	8	4	The person watched over (baby, child, older person, person with a disability or in mental health care) and everyone else the sensors see
DA	**Data and Inference**	8	2	What the record reveals, where copies live and how long they last
LC	**Lifecycle**	6	3	Install, claim, moves, resale, death and the end of the service
T	**Structural hazards**	9	5	Properties of the domain that cut across every suit

Reading the mapping line. Each entry ends with one line: STRIDE and LINDDUN categories with their fit, then the CAPEC 3.9 and CWE 5.0 match with the IDs in best-fit order. The rating comes first so it labels the whole list. For example: `STRIDE D (Loose) · LINDDUN None · CAPEC Partial: CAPEC-607 · CWE Partial: CWE-754`.

Fit (STRIDE, LINDDUN): Clean, a facilitator holding that prompt would plausibly ask the question that finds the threat; Loose, a category can be assigned only once you know the threat is there; None, no category applies. **Match** (CAPEC, CWE): Direct, the first ID describes the threat or names the flaw; Partial, only a generic parent or adjacent entry applies; None, nothing in the catalogue names it.

SUIT 01 · SN · 8 THREATS

Sensing

Sensing threats turn a quiet home into a false reassurance: the device, its radio or its power fails or is subverted, and the silence reads as safety.

Covers: Sensors, wearables, radio links, the home unit and the home it sits in. Online: https://ostering.com/taxonomies/care-assistant/sensing/

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES
EOC-SN-A †	**Silent Sensor** A sensor that stops reporting (flat battery, fault, removed, knocked off the wall) looks the same as a quiet, normal home, so the event it was there to catch goes unseen. STRIDE D (Loose) · LINDDUN None · CAPEC Partial: CAPEC-607 · CWE Partial: CWE-754	**Treat the absence of data as a signal with its own deadline.**	1. Give every sensor an expected reporting interval and raise a 'sensor quiet' alert at life-safety priority when it is exceeded. 2. Show battery level and last-seen time to the care circle well before failure. 3. Use supervised radio links with heartbeats so the base unit knows a device has gone, not just that it is idle.
EOC-SN-K †	**Lost Line** Mains power, broadband, the cellular network or a legacy phone line fails, or is switched off by the carrier, and the home unit cannot reach anyone. *Seen in: 3G network retirements stranding medical alert systems (United States, 2022)* STRIDE D (Clean) · LINDDUN None · CAPEC None · CWE None	**Every path to help has a backup, and the loss of a path is reported by the far end.**	1. Size battery backup for a stated number of hours and report when running on battery. 2. Use two independent paths (for example broadband and cellular), with the service, not the device, alerting when the device goes quiet. 3. Track carrier network retirements (analogue phone lines, 2G, 3G) against the installed base.
EOC-SN-Q †	**Pendant on the Bedside Table** Wearable buttons, socks and fall detectors work only when worn and charged; people take them off to bathe, sleep or avoid looking frail, babies kick them loose, and that can be exactly when something happens. STRIDE D (Loose) · LINDDUN None · CAPEC None · CWE None	**The system's confidence does not depend on an assumption about the person's behaviour.**	1. Detect and report when a wearable is not being worn or not charging. 2. Use waterproof designs certified for the bathroom. 3. Pair a wearable with ambient sensing where it would otherwise be the only sensor.

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES
EOC-SN-J †	**Unwatched Room** Coverage has gaps by design (bathroom, stairs, garden, garage), and a fall in a gap produces no event while the family assumes the whole home is watched. STRIDE D (Loose) · LINDDUN None · CAPEC None · CWE None	**Make coverage explicit and say what the system cannot see.**	1. Produce a coverage map at installation and show it to the care circle. 2. Raise an alert when the person enters an unmonitored zone and does not come back within a set time. 3. State the limits of coverage in plain words during onboarding and in the app.
EOC-SN-10 †	**Injected Normality** A rogue or cloned sensor joins the network and reports routine activity, masking an absence, a fall or a person who has not moved. STRIDE S, T (Clean) · LINDDUN None · CAPEC Partial: CAPEC-151 · CWE Direct: CWE-290	**Only devices the household enrolled may speak, and every new voice is announced.**	1. Allow joins only inside an explicit, time-limited pairing window opened by an authorised person. 2. Alert the care circle when any device joins outside that window. 3. Corroborate 'all normal' across independent sensors, not only 'something is wrong'.
EOC-SN-9 †	**Jammed Link** Interference or a deliberate jammer blocks the sensor or pendant radio band, so button presses and events never reach the base unit. STRIDE D (Clean) · LINDDUN None · CAPEC Direct: CAPEC-601 · CWE None	**Loss of the radio channel is an event, and the system fails towards alerting.**	1. Detect jamming from noise floor or missed supervision messages and raise a local and remote alert. 2. Use supervised links with a short heartbeat for life-safety devices. 3. Provide a second path (another band, or a wired or cellular fallback) for the trigger devices.
EOC-SN-8 †	**Open Hub on the Home Network** The home unit trusts anything on the local network, and the homes of people who need care have many guests on the Wi-Fi (carers, family, visitors), so its data and controls are open to all of them. STRIDE S, I, E (Clean) · LINDDUN None · CAPEC Partial: CAPEC-115 · CWE Direct: CWE-306	**The home network is untrusted; every local interface authenticates.**	1. Require authentication on every local route by default, with a short explicit allowlist. 2. Pair app and hub with cryptographic proof in both directions. 3. Bind local-only services to loopback and turn off discovery that is not needed.
EOC-SN-7 †	**Hands on the Hub** Someone with a few minutes of physical access (visitor, tradesperson, carer, burglar) unplugs, swaps, boots or carries off the home unit to disable monitoring or read its data. STRIDE T, I, E (Clean) · LINDDUN None · CAPEC Direct: CAPEC-401 · CWE Partial: CWE-1263, CWE-312	**Physical access to the home is expected; the unit resists it and reports it.**	1. Report tamper, power removal and enclosure opening to the service, not only locally. 2. Encrypt stored data with a key held in a hardware secure element. 3. Use verified boot and block unexpected USB input devices.

SUIT 02 · AV · 6 THREATS

Sight and Sound

Sight and sound threats come from cameras, microphones and talk-back: the stream reaches the wrong people, sees too much, or lets a stranger into the room.

Covers: Cameras, microphones, talk-back, live streams and recordings. Online: https://ostering.com/taxonomies/care-assistant/sight-and-sound/

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES
EOC-AV-A †	**A Stranger's Voice** Talk-back lets anyone holding the account, or anyone who has taken it over, speak into the room where a child or vulnerable person is. *Seen in: Stranger speaks to a child through a bedroom camera (Ring, 2019)* `STRIDE S, E (Clean) · LINDDUN None · CAPEC Direct: CAPEC-600 · CWE Partial: CWE-307`	**Speaking into a room is a privileged, announced and recorded action.**	1. Require a fresh, device-bound proof to start talk-back, and resist credential stuffing on the account. 2. Play a chime and light an indicator before any voice comes through. 3. Log every talk-back session and show it to all watchers.
EOC-AV-K †	**Open Stream** Live video and audio can be reached by someone other than the watchers: through a cloud relay that joins devices by an identifier, default credentials, or a stream exposed on the local network. *Seen in: ThroughTek Kalay device impersonation, CVE-2021-28372 (2021); TRENDnet camera feeds posted online, FTC settlement (2013)* `STRIDE I, S (Clean) · LINDDUN Dd (Clean) · CAPEC Direct: CAPEC-634 · CWE Direct: CWE-306`	**A stream reaches only authenticated, authorised viewers, and the relay cannot watch it.**	1. Encrypt streams end to end with keys held only on the watchers' devices. 2. Never treat a device identifier as a credential, and ship no default passwords. 3. Authenticate every local stream endpoint.
EOC-AV-Q	**Clips That Travel** Recordings of a child's or vulnerable person's most private moments are kept in the cloud, shared to family chats or social media, or produced in a dispute, long after anyone needed them. *Seen in: iBaby Monitor M6S alert clips reachable in cloud storage (2020)* `STRIDE I (Loose) · LINDDUN Dd, Nc (Clean) · CAPEC None · CWE Partial: CWE-359`	**Recordings are kept briefly and shared on purpose.**	1. Keep no recording by default, and give saved clips a short retention period. 2. Make sharing a deliberate action with a warning, not a one-tap default. 3. Let the person filmed, or their representative, see and delete clips.

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES
EOC-AV-J	**The Camera Sees Too Much** The camera and microphone capture far more than the cot or bed: other rooms, the bathroom, other people, the street and conversations nobody meant to share. `STRIDE I (Loose) · LINDDUN Dd, U (Clean) · CAPEC None · CWE Partial: CWE-359`	**Capture only the area and the sound the purpose needs.**	1. Offer privacy masks and a narrow field of view by default. 2. Default to sound-level alerts rather than continuous audio. 3. Show everyone in the home when capture is on.
EOC-AV-10	**Hidden Nanny Cam** The monitor is used to record a nanny, babysitter or paid carer without their knowledge, so the carer becomes the person watched over, with no notice and no rights. `STRIDE None · LINDDUN U, Nc (Clean) · CAPEC None · CWE None`	**Anyone recorded at work is told.**	1. Build an on-device recording indicator that cannot be turned off. 2. Prompt during setup to tell anyone who works in the home. 3. Separate carer-facing views from family recordings.
EOC-AV-9	**Neighbour on the Same Channel** A local radio monitor sends sound or video unencrypted, so anyone nearby with a receiver on the same channel hears or sees the room. `STRIDE I (Clean) · LINDDUN Dd (Clean) · CAPEC Direct: CAPEC-117 · CWE Direct: CWE-319`	**Local radio links are encrypted and paired.**	1. Encrypt the radio link with a key set at pairing. 2. Pair units explicitly instead of joining any receiver on the channel. 3. Warn when an unknown receiver tries to pair.

SUIT 03 · IN · 7 THREATS

Interpretation

Interpretation threats change what counts as an emergency, through drift, feedback, inference or an unauthorised change to the rules.

Covers: Baselines, rules, models, feedback loops and what counts as an emergency. Online: https://ostering.com/taxonomies/care-assistant/interpretation/

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES
EOC-IN-A †	**Model Veto** An inference (a pet, a visitor, 'house empty') is allowed to downgrade or cancel a deterministic life-safety alert. `STRIDE T, D (Loose) · LINDDUN None · CAPEC None · CWE Partial: CWE-807, CWE-1039`	**A model may add information to a life-safety alert, never take it away.**	1. Require a second deterministic signal before any downgrade. 2. Let models annotate an alert rather than change its severity. 3. Log every downgrade and show it to the circle.
EOC-IN-K †	**Rewriting the Emergency** Detection rules, model weights or the set of sensors that feed them can be changed by an unauthenticated or under-privileged caller. `STRIDE T, E (Clean) · LINDDUN None · CAPEC None · CWE Direct: CWE-306, CWE-494`	**Changing what counts as an emergency is a privileged, audited action.**	1. Make rule, model and sensor-scope changes operator-only and audited. 2. Have safety rules read raw sensor state whatever the model's scope says. 3. Load only signed model artefacts.
EOC-IN-Q †	**Learning an Empty House** The model keeps learning while its inputs are broken or partial, and treats the silence as routine. `STRIDE T, D (Loose) · LINDDUN None · CAPEC None · CWE Partial: CWE-636`	**Learning stops when the integrity of the input is unknown.**	1. Check liveness per sensor class, not just for the whole event stream. 2. Make the learning gate fail closed when the watchdog's verdict is stale. 3. Send the watchdog's own heartbeat off the device.
EOC-IN-J †	**Learned Decline** An adaptive baseline re-learns a slow deterioration as the new normal, so the gradual change the product exists to spot never crosses a threshold. `STRIDE T (Loose) · LINDDUN None · CAPEC None · CWE None`	**Compare against a fixed reference as well as the moving one.**	1. Keep an anchor baseline from enrolment, re-confirmed by a person at intervals. 2. Report long-window trends alongside short-window anomalies. 3. Cap how far a baseline may move without review.

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES
EOC-IN-10 †	**Feedback Ratchet** 'False alarm' feedback raises thresholds without validation or decay, so one annoyed or compromised watcher can desensitise detection for good. STRIDE T (Loose) · LINDDUN None · CAPEC None · CWE Partial: CWE-1288	**Feedback is bounded, attributable, reversible and visible.**	1. Accept feedback only for a real, unresolved alert and the feature it named. 2. Cap the effect per watcher and per time window. 3. Decay adjustments on a schedule and show every threshold change to the whole circle.
EOC-IN-9 †	**Alarm Flood** False alerts, accidental or deliberately induced, teach the circle or the responders to dismiss the channel, so the real event is ignored. STRIDE D (Clean) · LINDDUN None · CAPEC Partial: CAPEC-125 · CWE Partial: CWE-770	**The false-alert rate is a safety metric with an owner.**	1. Track false alerts per household with a ceiling that triggers a review. 2. Deduplicate and rate-limit repeated alerts. 3. Treat a sudden burst of alerts from one source as possible manipulation.
EOC-IN-8 †	**Second Occupant** A spouse, live-in carer, lodger, pet or regular visitor confuses detection: their movement masks the resident's fall, or their absence is read as the resident's. STRIDE D (Loose) · LINDDUN None · CAPEC None · CWE None	**Detection knows whose movement it sees, or says that it does not.**	1. Record household composition and offer explicit modes (guest, live-in carer, couple). 2. Fuse per-person signals (a wearable, a phone) with ambient sensing where possible. 3. Show the circle when occupancy is ambiguous and confidence is reduced.

SUIT 04 · AL · 7 THREATS

Alerting

Alerting threats break the last metre: the alert exists but no person sees it, the wrong person sees it, or a fake one arrives.

Covers: Getting an alert to a person who acts on it. Online: https://ostering.com/taxonomies/care-assistant/alerting/

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES
EOC-AL-A †	**Delivered to a Phone, Not a Person** Delivery counts as done when the push service accepts the message, but nobody has seen it: the phone is silenced, asleep in another room, or in a do-not-disturb mode. STRIDE D (Loose) · LINDDUN None · CAPEC None · CWE None	**An alert is complete when a person acknowledges it.**	1. Require acknowledgement for critical alerts. 2. Escalate on a timer to the next watcher, then to a voice call or text message. 3. Use the platform's critical or high-priority alert channel where the platform allows it.
EOC-AL-K †	**Nobody on Call** The whole circle is asleep, travelling or out of signal at once, or the circle is one exhausted person, and nothing notices the gap. STRIDE D (Loose) · LINDDUN None · CAPEC None · CWE None	**Coverage of the circle is monitored like coverage of the sensors.**	1. Keep an on-call rota and warn about gaps in advance. 2. Set a minimum circle size or offer a professional fallback. 3. Tell the account holder when no watcher has been reachable for a set time.
EOC-AL-Q †	**Silent Snooze** One watcher snoozes, pauses or sets 'away', and the others do not know, so alerts are suppressed for everyone. STRIDE D, R (Loose) · LINDDUN None · CAPEC None · CWE None	**Every suppression is visible to every watcher and expires.**	1. Show snooze and away states to all watchers, with who set them and until when. 2. Put a maximum duration on any suppression. 3. Let critical alerts bypass a snooze, or require confirmation from a second watcher.
EOC-AL-J †	**Unmeasured Delay** Nobody has measured how long each failure mode (radio, power, broadband, ingest, relay) takes to reach a person. STRIDE D (Loose) · LINDDUN None · CAPEC None · CWE None	**State a time-to-human for every failure mode, and test it.**	1. Write a target time per failure mode. 2. Run a recurring bench test that injects each fault and measures the time to acknowledgement. 3. Alert the operator when a target is missed.

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES
EOC-AL-10	**Wrong Recipient** Alerts follow stale routing: a removed member, an old phone number, a handed-down handset or a recycled number still receives them. `STRIDE I (Loose) · LINDDUN Dd (Clean) · CAPEC None · CWE Partial: CWE-359`	**Routing is re-verified, not assumed.**	1. Ask watchers to confirm contact details at intervals. 2. Revoke device push tokens when membership changes. 3. Re-verify phone numbers before the first alert after a long gap.
EOC-AL-9	**Counterfeit Alarm** Attackers send messages that look like the service ('Mum's alarm has gone off, tap to view') by text, email or messaging app, to harvest credentials or cause panic. `STRIDE S (Clean) · LINDDUN None · CAPEC Direct: CAPEC-98 · CWE None`	**A watcher can always check a genuine alert in the app.**	1. Never put sign-in links in alerts. 2. Authenticate the sending domain (SPF, DKIM, DMARC) and register SMS sender IDs where the country supports it. 3. Teach watchers to open the app, not the link.
EOC-AL-8	**Lock-Screen Disclosure** Alert text such as 'No movement since 02:10, bathroom' appears on lock screens, watches, car displays and shared tablets, telling whoever is nearby about a person's health and whereabouts. `STRIDE I (Clean) · LINDDUN Dd (Clean) · CAPEC None · CWE Direct: CWE-359`	**Notification content is minimal by default; detail sits behind authentication.**	1. Send generic notification text by default and show detail in the app. 2. Let each watcher choose whether previews appear. 3. Keep names, rooms and locations out of push payloads.

SUIT 05 · RS · 7 THREATS

Response

Response threats sit after the alert: the people and services who act on it, and the access to the home they need. They apply to monitoring centres, clinical teams and responders, and to families who respond themselves.

Covers: Monitoring centres, responders, entry to the home and the hand-off to emergency services. Online: https://ostering.com/taxonomies/care-assistant/response/

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES
EOC-RS-A †	**Centre Down** The monitoring centre or cloud relay is down, overloaded or held by ransomware, and alarms queue unseen. STRIDE D (Clean) · LINDDUN None · CAPEC None · CWE None	**Every alarm has a second place to go.**	1. Fail over to a separate centre or region. 2. Monitor queue depth and age, and alarm on both. 3. Fall back to direct-to-family alerts when the centre cannot answer in time.
EOC-RS-K †	**Keys in the System** Key-safe codes, door codes and entry instructions stored for responders are a way into a vulnerable person's home. STRIDE I, E (Clean) · LINDDUN None · CAPEC None · CWE Partial: CWE-522	**Entry details are secrets with the strictest access, rotation and audit.**	1. Keep entry details in a separate encrypted store and audit every read. 2. Release them only during an active alarm, to the dispatched responder. 3. Prompt a code change after each use and after staff changes.
EOC-RS-Q †	**Trusted Insider** A call handler, responder or support engineer misuses their access to the home, the data or the person. STRIDE E, R (Clean) · LINDDUN None · CAPEC None · CWE Partial: CWE-286	**Responder access is least-privilege, just-in-time and seen by the family.**	1. Run background checks in proportion to the access granted. 2. Grant access per incident, with expiry. 3. Notify the resident and family of each access.
EOC-RS-J †	**Who's at the Door** Someone claiming to be the responder, the installer or the care company calls or arrives at the door to get in or to get information. STRIDE S (Clean) · LINDDUN None · CAPEC Direct: CAPEC-407 · CWE None	**The resident can verify a visitor through the service.**	1. Let the resident or family confirm a visitor in the app or by calling back a known number (named visitor, photo, one-time code). 2. State on the device and in the welcome pack that the service never asks for codes or payment by phone. 3. Notify the circle of every scheduled visit.

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES
EOC-RS-10 †	**Lost in Hand-off** Details are lost or garbled between the system, the call handler and emergency services (address, access, medical notes, language), and help is slower. STRIDE D, T (Loose) · LINDDUN None · CAPEC None · CWE None	**The hand-off is structured and tested end to end.**	1. Pass a structured incident record (verified address, access, contacts) digitally where the emergency service accepts it. 2. Verify the address at install and whenever it changes. 3. Run end-to-end test calls on a schedule.
EOC-RS-9 †	**Wrong Responder** Escalation sends the wrong help: police to a mental health crisis, a stranger to a person with dementia, or an emergency service when a known carer was needed, and the response itself causes harm. STRIDE D (Loose) · LINDDUN None · CAPEC None · CWE None	**Each person has a response plan, chosen with them in advance where possible.**	1. Record a response plan per person: who to contact first, and who not to. 2. Route crises to a specialist team before police where one exists. 3. Capture the person's own preferences while they are well, and honour them.
EOC-RS-8	**Open Microphone** Two-way voice units let the monitoring centre, or anyone who can start a call, listen into the home. STRIDE I (Clean) · LINDDUN Dd (Clean) · CAPEC None · CWE Partial: CWE-306	**Audio opens only for an alarm, with an audible and visible indicator.**	1. Open the speech path only after an alarm or a call the resident starts. 2. Play a tone and light an indicator while audio is open. 3. Audit every audio session.

SUIT 06 · CC · 8 THREATS

Care Circle

Care-circle threats come from the watchers: misuse by people with legitimate access, disputes between them, and takeover of their accounts.

Covers: The watchers: parents, family, friends, paid carers, agencies and clinical teams. Online: https://ostering.com/taxonomies/care-assistant/care-circle/

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES
EOC-CC-A †	**Ex-Partner Still Watching** After a separation, one parent or partner keeps access to the cameras or app and can still see into the other's home, a serious risk where there has been abuse. `STRIDE E, I (Loose) · LINDDUN Dd (Loose) · CAPEC None · CWE Partial: CWE-286`	**Access ends with the relationship, by a route that does not need the other party's cooperation.**	1. Let any adult in the home see who is watching and remove access through a safety route. 2. Notify the household when a watcher signs in from a new device or location. 3. Offer a safety mode that hides location and occupancy from all watchers.
EOC-CC-K †	**Watching as Control** A watcher uses the monitoring to police or coerce the person rather than keep them safe: a parent of an adult child, a partner, a family member or a service. `STRIDE None · LINDDUN U (Loose) · CAPEC None · CWE None`	**The watched person can see who watches and can push back.**	1. Give the resident a view of every watcher and what each can see. 2. Notify the resident on every enrolment and permission change. 3. Build a safeguarding route into support.
EOC-CC-Q †	**Stolen Watcher** A watcher's session or device is taken over and used remotely to watch the home or to snooze alerts before a burglary. `STRIDE S (Clean) · LINDDUN None · CAPEC Direct: CAPEC-593 · CWE Partial: CWE-1464`	**Sensitive actions need a fresh, device-bound proof.**	1. Bind sessions to the enrolled device. 2. Require step-up for snooze, away and membership changes. 3. Tell the circle when a new device signs in.
EOC-CC-J	**Next Door's Mother** A watcher reaches another household's data by changing an identifier, which matters most on platforms where agencies manage many households. `STRIDE E, I (Clean) · LINDDUN None · CAPEC None · CWE Direct: CWE-639`	**Every request is checked against membership of that household.**	1. Check membership on every read and write. 2. Run an automated sweep across every route as a merge gate. 3. Use identifiers that cannot be guessed.

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES
EOC-CC-10 †	**Family Feud** Family members disagree (separation, estrangement, inheritance), and one adds, removes or locks out the others, or keeps access after falling out. STRIDE E, R (Loose) · LINDDUN None · CAPEC None · CWE Partial: CWE-863	**Membership changes follow a defined authority, not whoever acts first.**	1. Define roles with clear authority (resident, legal representative, primary watcher) at setup. 2. Notify everyone affected by a removal, with a way to contest it. 3. Record who may remove whom.
EOC-CC-9	**Carer Overreach** Agency or private carers given access for their visits keep broad or permanent access to timelines, location and home controls. STRIDE E, I (Clean) · LINDDUN None · CAPEC None · CWE Partial: CWE-286	**Professional access is scoped to visits and expires.**	1. Tie a carer's access to scheduled visits. 2. Show carers tasks, not the full history. 3. Revoke all staff when an agency relationship ends.
EOC-CC-8	**Watched by the Service** A clinical team or care service monitors the person under a care plan, a legal power or a condition of discharge; the person cannot easily refuse, and the data flows to an institution. STRIDE E (Loose) · LINDDUN U, Nc (Clean) · CAPEC None · CWE None	**Required monitoring is bounded by its basis, its end date and what the person can see.**	1. Record the legal or care-plan basis of the monitoring and when it ends. 2. Show the person what is collected and who sees it. 3. Give the person a route to an independent advocate.
EOC-CC-7	**Background Check Hoard** The platform stores carers' background-check identifiers or results, a dataset that is valuable to criminals and harmful to the carers if leaked. STRIDE I, R (Clean) · LINDDUN None · CAPEC None · CWE Partial: CWE-312, CWE-778	**Keep the verification outcome, not the identifier.**	1. Store status and date once verification completes. 2. Purge identifiers after a short window. 3. Audit every decryption.

SUIT 07 · RE · 8 THREATS

Resident

Resident threats concern the person watched over (a baby, a child, an older person, someone with a disability or in mental health care) and everyone else the sensors see: consent, capacity, objection, harm from the watching itself, and being targeted.

Covers: The person watched over (baby, child, older person, person with a disability or in mental health care) and everyone else the sensors see. Online: https://ostering.com/taxonomies/care-assistant/resident/

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES
EOC-RE-A †	**Target List** Data showing that someone is vulnerable (very old, very young, unwell, alone) in waitlists, customer lists, leaked databases, or even the device's box in the recycling, is used to target them or their family with fraud, doorstep crime or worse. STRIDE I (Clean) · LINDDUN L, Dd (Clean) · CAPEC None · CWE Direct: CWE-359	**'Who is vulnerable' is sensitive data in every store.**	1. Protect marketing and waitlist data like customer data. 2. Do not reveal whether an address is registered. 3. Avoid branding on packaging and on the outside of the home.
EOC-RE-K †	**Unplugged on Purpose** The resident switches off, unplugs or hides devices because they do not want to be watched; the system cannot tell objection from failure or attack, so it either ignores it or raises the alarm. STRIDE D (Loose) · LINDDUN U (Loose) · CAPEC None · CWE None	**The resident's objection has a legitimate, visible path.**	1. Give the resident a pause the circle sees as 'paused by resident'. 2. Tell a pause apart from tamper and from failure. 3. Prompt a conversation rather than an escalation.
EOC-RE-Q †	**Watched into Distress** Being monitored harms the person: it can feed paranoid symptoms, strip dignity, break a teenager's trust, or lead the person to disengage from care. STRIDE None · LINDDUN U (Loose) · CAPEC None · CWE None	**Use the least monitoring that meets the need, agreed with the person where possible.**	1. Offer a minimal mode that reports only what the purpose needs. 2. Let the person choose what is shared, where they are able to. 3. Review the effect of the monitoring with the person, not only with the watchers.

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES
EOC-RE-J †	**Rights on Paper** The controls the resident must use (pause, objection, transparency view, alarm button, voice prompts) do not work for their sight, hearing, dexterity, memory or language, so their rights exist only on paper. STRIDE None · LINDDUN U (Loose) · CAPEC None · CWE None	**Controls for the resident are designed for the resident.**	1. Test resident-facing controls with people who have the target impairments. 2. Offer a non-app route (a button on the device, a phone call). 3. Meet a recognised accessibility standard for the resident's surfaces.
EOC-RE-10	**Consent Out of Step with Capacity** Consent given once stays in force while the person's capacity changes: declining with dementia, growing as a child gets older, or coming and going with mental illness. STRIDE None · LINDDUN Nc (Loose) · CAPEC None · CWE None	**Consent follows capacity, with a route to a substitute decision-maker and to what the person said while well.**	1. Review consent at intervals and at known milestones (a birthday, a discharge, a diagnosis). 2. Record the legal representative recognised in the person's country, and any advance statement the person made while well. 3. Give the person an objection that pauses processing, and re-confirm with them when capacity returns.
EOC-RE-9	**Enrolled Without Knowing** Family set the resident up without telling them, or tell them in a way they cannot understand. STRIDE None · LINDDUN U (Clean) · CAPEC None · CWE None	**The resident is told in a form they understand, on the device itself.**	1. Put a visible indicator on the device. 2. Explain it in plain language, large print, audio and the resident's own language. 3. Have the resident confirm at installation where they are able to.
EOC-RE-8	**Bystander Data** Co-residents, siblings, visitors, nannies and live-in carers are monitored too, but never consented, are not told, and cannot see or erase their data. STRIDE None · LINDDUN U, Nc (Clean) · CAPEC None · CWE Partial: CWE-359	**Everyone the sensors see is a data subject.**	1. Put a notice on the device and in the home. 2. Record household composition and minimise per-person data. 3. Offer a request route to people who are not account holders.
EOC-RE-7	**Monitoring That Outlives Its Purpose** Monitoring started for a reason (a newborn, a hospital discharge, a bad spell) carries on after the reason has gone: the baby monitor becomes tracking a teenager, and recovery never ends the watching. STRIDE None · LINDDUN Nc, U (Clean) · CAPEC None · CWE None	**Monitoring has an end condition set at the start.**	1. Set a purpose and a review date at setup. 2. Prompt a review at milestones such as a birthday, a discharge or recovery. 3. Hand control to the person as their capacity grows.

SUIT 08 · DA · 8 THREATS

Data and Inference

Data threats concern what the record reveals about a vulnerable person, and where its copies end up.

Covers: What the record reveals, where copies live and how long they last. Online: https://ostering.com/taxonomies/care-assistant/data-and-inference/

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES
EOC-DA-A †	**Routine as Reconnaissance** Activity data shows when the person is alone, asleep or out, which is a burglar's or abuser's timetable. STRIDE I (Clean) · LINDDUN Dd (Clean) · CAPEC None · CWE Direct: CWE-359	**Protect routine data like the keys to the house.**	1. Process on the device and send only minimal derived signals. 2. Encrypt at rest everywhere, including backups and snapshots. 3. Audit who reads it.
EOC-DA-K	**Evidence Against Them** Monitoring data is turned on the person it was meant to protect: in a custody dispute, a compulsory treatment decision, a benefits assessment, an insurance claim or a criminal case. STRIDE I (Loose) · LINDDUN Dd, Nc (Loose) · CAPEC None · CWE None	**Data leaves the care relationship only under declared rules, and the person is told.**	1. Publish when and to whom data is disclosed, and the legal basis needed. 2. Require a formal request, and log every disclosure. 3. Notify the person or their representative of each disclosure unless the law forbids it.
EOC-DA-Q †	**Missing Record** After an injury or death, the family, an inquest, an insurer or the police need the event record, and it is incomplete, editable or already deleted. STRIDE R (Clean) · LINDDUN None · CAPEC Partial: CAPEC-268 · CWE Partial: CWE-778, CWE-732	**Safety-relevant events are tamper-evident and can be preserved on request.**	1. Hash-chain safety event logs. 2. Provide a legal-hold process that suspends deletion. 3. Document an export format.
EOC-DA-J	**Inferred Diagnosis** Routine, phone or sensor data is used to infer conditions or state of mind (infection, cognitive decline, low mood, relapse), creating stigmatising health data nobody supplied. STRIDE I (Loose) · LINDDUN Dd, I (Clean) · CAPEC None · CWE None	**Decide and declare which inferences are made, and protect them as health data.**	1. Keep an inventory of inferences and what each is for. 2. Frame outputs as observations, not diagnoses. 3. Protect inference outputs at the same level as health records.

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES
EOC-DA-10	**Second Purpose** Data is reused for model training, research, insurers or sale without a fresh lawful basis or the resident's knowledge. STRIDE None · LINDDUN Nc (Clean) · CAPEC None · CWE None	**Data is bound to its purpose; new uses need a new opt-in.**	1. Tag data with its purpose at collection. 2. Gate any new use on recorded consent or another lawful basis. 3. Disable ingestion routes for unapproved purposes.
EOC-DA-9	**Frailty Map** Metadata across households (alert frequency, night-time alerts) ranks who is frailest without reading any alert content. STRIDE I (Loose) · LINDDUN L (Clean) · CAPEC None · CWE Direct: CWE-1230	**Minimise delivery metadata and age it out.**	1. Keep per-alert delivery records only briefly. 2. Aggregate to daily counts. 3. Restrict analytics access.
EOC-DA-8	**Erasure That Doesn't** Closing an account removes the account holder but leaves the resident's records, consents and care notes behind. STRIDE None · LINDDUN Nc (Clean) · CAPEC None · CWE Partial: CWE-459	**Erasure covers every subject-linked record in one tested transaction.**	1. Keep an inventory of subject-linked tables. 2. Erase in one transaction. 3. Run a seed, erase and assert test against the schema.
EOC-DA-7	**Copies That Linger** Raw data persists in caches, recorders, snapshots, backups and logs long after the stated retention. STRIDE I (Loose) · LINDDUN Nc (Clean) · CAPEC None · CWE Direct: CWE-459	**One retention schedule per data category, enforced in every copy.**	1. Inventory every store that holds a copy. 2. Enforce retention in each store, including backups. 3. Test retention as code.

SUIT 09 · LC · 6 THREATS

Lifecycle

Lifecycle threats arise when the household changes: installation, moves, resale, death and the end of the service.

Covers: Install, claim, moves, resale, death and the end of the service. Online: https://ostering.com/taxonomies/care-assistant/lifecycle/

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES
EOC-LC-A †	**Fleet-Wide Regression** One update breaks detection or connectivity across every home at once. STRIDE D (Loose) · LINDDUN None · CAPEC None · CWE None	**Updates to a safety function roll out in stages behind a safety test.**	1. Run safety regression tests (fall, no-motion, silence) in the release gate. 2. Roll out in stages with health gates and automatic rollback. 3. Watch alert volumes per cohort after each release.
EOC-LC-K †	**Vendor Exit** The provider shuts down, is acquired or ends support, and devices stop alerting, possibly without anyone noticing, or the data passes to a new owner. STRIDE D (Loose) · LINDDUN Nc (Loose) · CAPEC None · CWE None	**Users are told in advance, and devices fail loudly.**	1. Declare a support period. 2. Give notice of end of service and a local-only fallback. 3. Set data transfer terms in advance.
EOC-LC-Q †	**First to Claim** At installation, whoever claims the device first (a neighbour on the Wi-Fi, an installer, a previous owner) becomes its controller. STRIDE S, E (Clean) · LINDDUN None · CAPEC None · CWE Partial: CWE-306	**Claiming proves both possession and entitlement.**	1. Use an out-of-band proof of possession (QR code, Bluetooth pairing, a code inside the box). 2. Check entitlement before binding. 3. Notify the purchaser of every claim.
EOC-LC-J	**After a Death** The system may be first to detect a death, then carries on: alerts and reminders keep coming, nobody controls the account, the record is in limbo and the hub stays on the wall. STRIDE None · LINDDUN Nc (Loose) · CAPEC None · CWE None	**Bereavement is a designed flow.**	1. Provide a verified 'deceased' state that stops alerts and reminders. 2. Define who may act for the account afterwards and on what proof. 3. Decide what is kept, for how long and why (see EOC-DA-Q).

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES
EOC-LC-10	**Second-Hand Device** A resold, handed-down or re-homed device carries the previous household's data or recordings, or still reports to the previous watchers. `STRIDE I (Loose) · LINDDUN Dd (Clean) · CAPEC None · CWE Direct: CWE-1266`	**A change of household is a full reset on both device and service.**	1. Revoke all memberships and tokens on deregistration. 2. Have the service verify that the device was wiped. 3. Refuse a claim on a device with live bindings until they are released.
EOC-LC-9	**Moved Out** The resident moves to hospital, a care home or a relative's home; monitoring carries on in an empty house, or the account and data are left dangling. `STRIDE D (Loose) · LINDDUN Nc (Loose) · CAPEC None · CWE None`	**A change of setting is an explicit state with an end date.**	1. Offer 'in hospital' and 'moved' states that pause alerts and expire. 2. Provide a closure workflow that hands over or erases data. 3. Remind the account holder when a pause outlives its date.

T · 9 HAZARDS

Structural hazards

Structural hazards are properties of the domain, not single faults. Walk them against the whole design after the suits; they usually explain several findings at once.

Covers: Properties of the domain that cut across every suit. Online: https://ostering.com/taxonomies/care-assistant/structural-hazards/

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES
EOC-T1 †	**Silence Reads as Safety** In this domain 'no alert' looks exactly like 'all well'. Any break anywhere in the chain from sensor to person turns into reassurance unless the system proves its own liveness end to end. STRIDE D (Loose) · LINDDUN None · CAPEC None · CWE Partial: CWE-754	**Prove the whole chain is alive, continuously, to someone outside it.**	1. Send end-to-end heartbeats from sensor to acknowledged watcher. 2. Run synthetic test alarms on a schedule. 3. Give every silence a deadline.
EOC-T2	**The Watched Is Not the User** The resident bears the risk, but someone else buys, configures and uses the product, so defaults, consent and the interface serve the buyer. STRIDE None · LINDDUN U (Loose) · CAPEC None · CWE None	**Design every default from the resident's side first.**	1. Write a resident persona into requirements. 2. Review each default for whose interest it serves. 3. Give the resident a voice in support and complaints.
EOC-T3	**Intended Purpose Drift** Marketing copy, app-store text or a new feature (an 'early warning' claim, heart-rate or oxygen readings, a relapse prediction) moves the product from consumer rules into medical-device rules, or back, and its security obligations change with it. *Seen in: FDA warning letter on Owlet Smart Sock (2021), later Dream Sock De Novo clearance (2023)* STRIDE None · LINDDUN Nc (Loose) · CAPEC None · CWE None	**Intended purpose is a controlled design input, reviewed like code.**	1. Write the intended purpose down and gate claims in copy, labels and features against it. 2. Record the regulatory qualification decision for each market. 3. Re-assess when a feature adds a physiological signal or a condition-specific claim.
EOC-T4 †	**Safety–Privacy Inversion** Every privacy control (minimisation, deletion, pause) can cost a missed alert, and every safety control (more sensors, longer retention) costs privacy, and the trade is often made silently on one side. STRIDE None · LINDDUN None · CAPEC None · CWE None	**Make each trade-off explicit and owned by someone.**	1. Record each safety-versus-privacy decision in an ADR, with an owner. 2. Show the resident and circle what each choice gives up. 3. Revisit the decisions when capacity changes.

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES
EOC-T5 †	**Promised Vigilance** Families check in less because 'the system is watching', or rely on a monitor for sleep safety, while detection has real miss rates and blind spots, so the product replaces the care it was meant to support. STRIDE None · LINDDUN None · CAPEC None · CWE None	**Claims match measured capability, and the limits are stated.**	1. Publish measured detection and miss rates where claims are made. 2. Show limits in the app, not only in the terms. 3. Nudge contact rather than replace it.
EOC-T6 †	**Inside the Walls, Outside the Boundary** The home network, the people who live there and their visitors are all inside the physical perimeter but outside the trust boundary, which the design forgets. STRIDE S, E (Loose) · LINDDUN None · CAPEC None · CWE Partial: CWE-306	**Model the household as several principals, not one.**	1. Draw the household's people as separate actors in the data-flow diagram. 2. Authenticate local interfaces. 3. Assume a visitor has the Wi-Fi password.
EOC-T7	**Many Principals, One Person** The person, parents and co-parents, family, the legal representative, carers, agencies, clinical teams, the provider and the payer all have different rights, and the system does not say whose decision each control is. STRIDE E, R (Loose) · LINDDUN None · CAPEC None · CWE Partial: CWE-862	**Every control names who may operate it and on whose behalf.**	1. Keep a decision-rights matrix for every sensitive action. 2. Record the authority each action was taken under. 3. Change rights when capacity or relationships change.
EOC-T8 †	**Response Is Part of the System** The human response chain (family, monitoring centre, responders, emergency services) is in scope; a perfect detector with an unanswered phone still fails. STRIDE D (Loose) · LINDDUN None · CAPEC None · CWE None	**Threat model the response as well as the technology.**	1. Put the response chain into the data-flow diagram. 2. Set targets for time to a human. 3. Test the response end to end, with people.
EOC-T9	**Capacity Is Not Fixed** The design assumes the person's capacity is fixed, but it declines (dementia), grows (children) or comes and goes (mental illness), so consent, controls and rights are wrong for most of the person's time with the product. STRIDE None · LINDDUN Nc, U (Loose) · CAPEC None · CWE None	**Model capacity as something that changes, and design every right and control for each state.**	1. Draw the capacity states the person can be in, and who decides in each. 2. Attach a review trigger to every state change. 3. Test each control in each state, including the person's own controls.

REFERENCE

Mappings, known cases and licence

CAPEC 3.9	NAME
CAPEC-98	Phishing
CAPEC-115	Authentication Bypass
CAPEC-117	Interception
CAPEC-125	Flooding
CAPEC-151	Identity Spoofing
CAPEC-268	Audit Log Manipulation
CAPEC-401	Physically Hacking Hardware
CAPEC-407	Pretexting
CAPEC-593	Session Hijacking
CAPEC-600	Credential Stuffing
CAPEC-601	Jamming
CAPEC-607	Obstruction
CAPEC-634	Probe Audio and Video Peripherals

CWE 5.0	NAME
CWE-286	Incorrect User Management
CWE-290	Authentication Bypass by Spoofing
CWE-306	Missing Authentication for Critical Function
CWE-307	Improper Restriction of Excessive Authentication Attempts
CWE-312	Cleartext Storage of Sensitive Information
CWE-319	Cleartext Transmission of Sensitive Information
CWE-359	Exposure of Private Personal Information to an Unauthorized Actor
CWE-459	Incomplete Cleanup
CWE-494	Download of Code Without Integrity Check
CWE-522	Insufficiently Protected Credentials
CWE-636	Not Failing Securely ('Failing Open')
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-754	Improper Check for Unusual or Exceptional Conditions
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-778	Insufficient Logging
CWE-807	Reliance on Untrusted Inputs in a Security Decision

CWE 5.0	NAME
CWE-862	Missing Authorization
CWE-863	Incorrect Authorization
CWE-1039	Inadequate Detection or Handling of Adversarial Input Perturbations in Automated Recognition Mechanism
CWE-1230	Exposure of Sensitive Information Through Metadata
CWE-1263	Improper Physical Access Control
CWE-1266	Improper Scrubbing of Sensitive Data from Decommissioned Device
CWE-1288	Improper Validation of Consistency within Input
CWE-1464	Improper Session Invalidation

Known cases

ENTRY	CASE	SOURCE
EOC-SN-K	3G network retirements stranding medical alert systems (United States, 2022)	https://www.phlp.org/en/news/certain-life-alert-systems-will-no-longer-work-following-3g-shutdown
EOC-AV-A	Stranger speaks to a child through a bedroom camera (Ring, 2019)	https://abc7.com/ring-security-cameras-studio-city-hacker-camera-hacked/5750794
EOC-AV-K	ThroughTek Kalay device impersonation, CVE-2021-28372 (2021)	https://cloud.google.com/blog/topics/threat-intelligence/mandiant-discloses-critical-vulnerability-affecting-iot-devices
EOC-AV-K	TRENDnet camera feeds posted online, FTC settlement (2013)	https://search.ftc.gov/news-events/news/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles-ftc-charges-it-failed-protect
EOC-AV-Q	iBaby Monitor M6S alert clips reachable in cloud storage (2020)	https://www.bitdefender.com/en-us/blog/labs/severe-vulnerability-in-ibaby-monitor-m6s-camera-leads-to-remote-access-to-video-storage-bucket
EOC-T3	FDA warning letter on Owlet Smart Sock (2021), later Dream Sock De Novo clearance (2023)	https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/owlet-baby-care-inc-616354-10052021

Licence

© 2026 Jonathan Brett Crawley. CC BY-NC-ND 4.0, with additional permissions. Licensed under Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0): you may share the whole taxonomy, unchanged and with credit, for non-commercial purposes. In addition, whether or not the use is commercial, you may use it to threat model systems, including for paying clients; use it internally and for training inside any organisation; and quote individual entries, with credit, in paid courses, reports and talks. Shipping it in a product, such as a tool's built-in library, a printed deck or a reprint for sale, needs written permission.

Credit: “Nobody Asked the Person Being Watched: A Threat Taxonomy for Care Monitoring at Home” by Jonathan Brett Crawley, ostering.com, licensed under CC BY-NC-ND 4.0.