Tracked Into Closeness: Surveillance Intimacy and Location-Sharing in Close Relationships

CLAIRE F. WEIZENEGGER, University of Washington, USA
SEAN A. MUNSON, University of Washington, USA
AUDREY DESJARDINS, University of Washington, USA
JAMES PIERCE, University of Washington, USA

Location-sharing technologies—Apple's Find My, Life360, and AirTags—have become relational infrastructure, normalizing continuous visibility in ways that blur care and surveillance. Through 15 semi-structured interviews with parents, partners, friends, and caregivers in Washington, we examine how location-sharing shifts from situational disclosure into a background condition of the relationship itself. We identify *surveillance intimacy*—a self-reinforcing relational condition in which care motivates sharing, sharing produces closeness, and closeness obligates more sharing. Four dynamics sustain it: relational visibility constituted as care, sharing hardened into relational obligation, moral rationalization as ethical infrastructure, and covert everyday tuning performed disproportionately by those least able to renegotiate openly. We argue that care is not simply a justification for surveillance but a mechanism that helps reproduce it. These findings suggest that design approaches focused only on consent or privacy settings are insufficient to support relational agency in continuous location-sharing.

CCS Concepts: • **Human-centered computing → Empirical studies in collaborative and social computing**; *HCI design and evaluation methods.*

Additional Key Words and Phrases: location sharing; surveillance; privacy; intimacy; consent; relational privacy; family; caregiving; Life360; Find My; AirTags

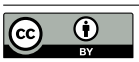
ACM Reference Format:
Claire F. Weizenegger, Sean A. Munson, Audrey Desjardins, and James Pierce. 2027. Tracked Into Closeness: Surveillance Intimacy and Location-Sharing in Close Relationships. *Proc. ACM Hum.-Comput. Interact.* 11, 1, Article GROUP53 (January 2027), 26 pages. https://doi.org/10.1145/3859439

1 Introduction

Location-sharing technologies have become constitutive infrastructure of close relationships. For example, parents can monitor their children's whereabouts as a matter of routine, continuing long after the specific safety concern that prompted sharing has passed. Friends might share location as a token of trust—a quiet signal that the relationship is intimate enough to warrant that kind of access. Some partners maintain continuous mutual visibility not as a choice but as a background condition of being together. In each case, location awareness no longer functions as a discrete act of disclosure.

This shift toward continuous background sharing has outpaced the frameworks through which HCI and CSCW understand location privacy, even those emphasizing practice over thresholds.

Authors' Contact Information: Claire F. Weizenegger, cweiz@uw.edu, University of Washington, Seattle, Washington, USA; Sean A. Munson, smunson@uw.edu, University of Washington, Seattle, Washington, USA; Audrey Desjardins, adesjard@uw.edu, University of Washington, Seattle, Washington, USA; James Pierce, jjpierce@uw.edu, University of Washington, Seattle, Washington, USA.



This work is licensed under a Creative Commons Attribution 4.0 International License.
© 2027 Copyright held by the owner/author(s).
ACM 2573-0142/2027/1-ARTGROUP53
https://doi.org/10.1145/3859439

Palen and Dourish [43] frame privacy as boundary regulation constituted through ever-changing practices of negotiation, not static norms; Nissenbaum's contextual integrity [40, 41] evaluates flows against context-appropriate expectations, requiring specific, identifiable information flows for analysis. McDonald and Forte extend this with "privacy vulnerabilities": power asymmetries shape who constitutes those practices [38]. Yet real-time sharing—often triggered by specific events, like a child's late-night outing—can depart from episodic norms and become infrastructural: no longer a choice but a background feature in how relationships operate.

Cultural observers have begun to name this shift: Hitzig [27] describes location-sharing as a "love language" through which surveillance logic has been internalized into intimate relationships. Yet this account treats the phenomenon as a form of false consciousness—a capitulation to Big Tech's conditioning—rather than examining the relational mechanism through which tracking comes to be experienced as care. Our analysis suggests the dynamic is not imposed from outside relationships but produced through them.

HCI's empirical literature around location tracking has organized itself around two poles, neither of which describes this shift. The first emphasizes the utility of location tracking for mutual *care*: location-based services support coordination, safety, and reassurance [17, 54, 65]. The second emphasizes harm via *coercion*: the same technologies enable stalking [14], intimate partner surveillance, and a system of coercive dynamics scholars have called tech abuse [22, 36, 61]. This binary—care-motivated versus coercive—treats tracking as categorically distinct, separated by intent, and legible at the ends of a spectrum. Conventional accounts of privacy and surveillance suppose location tracking is contrary to intimacy: controlling, asymmetric, and corrosive of trust [21, 33]. Our findings cut across both. We call this condition *surveillance intimacy*: a self-reinforcing configuration in which care motivates tracking, tracking produces felt closeness, and that closeness in turn obligates further tracking. *Surveillance intimacy* extends prior work on domestic surveillance and family tracking, which emphasizes asymmetric visibility and panoptic dynamics in the home [11], by specifying the relational mechanism through which care and tracking become co-productive across relationship types. It also builds on recent work on privacy silence, which shows that intimate partners often manage privacy boundaries through silence, tacit understandings, and implicit cues [3, 4]. Our work further speaks to research on bystanders and other non-primary users of networked sensing technologies [9, 44, 68]. Researchers typically define these roles by who adopted, configured, or owns a device; we show that people who have opted in and can stop sharing at any time may still feel unable to stop, because stopping can read as a withdrawal of care. We draw on feminist care ethics to theorize this condition. Fisher and Tronto define care as "everything we do to maintain, continue, and repair our world so that we can live in it as well as possible" [19]. In this vision, care is not only a *practice*, the affective and material work of attending to one another, but also a *moral orientation* toward mutual responsibility and relational repair [58, 59]. In close relationships, care is constitutive: it defines what good parenting, trustworthy partnership, and available friendship require. HCI researchers have increasingly examined how digital systems mediate caring relations [30, 62, 63].

Intimacy is the register through which care is felt and recognized. We define intimacy here as the relational condition in which care is enacted, where mutual disclosure of personal information is not only permitted but expected [24]. The relationship between shared awareness and felt closeness has been documented across technologies and relational contexts—from video chat among distant couples [39] to domestic location-awareness devices [15]: knowing someone's whereabouts produces reassurance and connectedness. These studies examine sharing as a choice made within a relationship; we examine arrangements in which visibility has become a condition of the relationship. We ask: how does continuous location-sharing become normalized in close relationships, and what role does care play in making it feel like intimacy rather than surveillance?

Surveillance intimacy sits upstream of tech abuse [61]. We find it in relationships no one would call harmful (e.g., parents granting teens independence via tracking (P8), siblings checking safe arrival (P13)), which may be part of why coercion that develops within them is hard to identify and exit.

We ground this concept in interviews with 15 participants who use location-sharing technologies across diverse close relationships: parents and adolescent children, adult children and aging parents, romantic partners, friends, and caregiving relationships. Through semi-structured interviews, we examined how location-sharing evolves from a deliberate gesture of trust into an expected condition of the relationship; how participants justify ongoing monitoring through expressions of safety, ownership, and love; and how those who feel over-watched manage visibility through covert workarounds rather than open renegotiation, because stopping would mean contesting the care itself. From this analysis, we identify four dynamics through which *surveillance intimacy* takes hold and persists in close relationships:

(1) **Relational visibility as care** — location-sharing enters relationships as an expression of closeness, constituting location data as relational currency: a gesture of trust and a token of availability. Visibility becomes the medium through which intimacy is performed, felt, and recognized;
(2) **Sharing as relational obligation** — once tracking is constituted as care, turning it off reads as withdrawing care. Discomfort remains unarticulated because naming it requires contesting the relationship itself;
(3) **Moral rationalization of surveillance** — when the surveillance dimension becomes hard to ignore, participants resolve the tension by re-invoking care: reframing monitoring as safety, stewardship, and love. This moral work travels from tracker to tracked until both parties inhabit the same frame, making the arrangement self-sustaining;
(4) **Everyday tuning** — those who cannot contest surveillance without contesting the care relationship manage visibility through covert technical workarounds rather than open renegotiation. This labor is ongoing, invisible, and falls most heavily on those with the least power to renegotiate openly.

These dynamics have direct implications for design. Prior work on location sharing has largely framed the design problem around disclosure preferences: with whom people want to share, when, and at what granularity [17, 60]. Platforms built on this framing—Apple's ecosystem, Life360, Snap Map—treat location sharing as a legible, manageable preference: a toggle, a permission, a notification when something changes. This legibility model assumes that dissatisfaction with a sharing event will surface as a preference that can be adjusted, and that parties involved have equal standing to adjust. It does not account for arrangements in which visibility has become infrastructural, and normalized into the background, rather than actively maintained and adjusted, or for the relational costs that make withdrawal unspeakable. Prior work notes that continuous sharing becomes entangled with intimacy, so that changes provoke suspicion [49], and examines how perpetrators justify surveillance in abusive relationships [5]. We focus on what comes before abuse—care-normalized tracking in "healthy" relationships, which can supply the relational infrastructure that coercive control later uses.

This paper makes three contributions. First, we develop *surveillance intimacy* as a theoretical concept for HCI that reframes care and control in relational tracking as co-productive rather than competing forces. Second, we document how *surveillance intimacy* operates in parent-child, romantic, friendship, and caregiving relationships, showing that continuous tracking becomes a *relational obligation* rather than a failure of attention or intent. Third, we derive design implications for *relational agency*: because care is the operative force behind *surveillance intimacy*, interventions

limited to consent flows or privacy settings are insufficient to support people in reshaping surveillance without jeopardizing the relationships that depend on it. What is required are sociotechnical systems of care [57] that allow visibility to be renegotiated—*without* that renegotiation reading as a withdrawal of love, loyalty, or support.

2 Related Work

Surveillance intimacy sits at the intersection of three bodies of scholarship: feminist care ethics and its uptake in HCI; theories of intimacy and relational disclosure; and the literature on location-sharing in close relationships, spanning coordination, family surveillance, and technology-mediated abuse. We position our contribution against HCI's privacy frameworks (Section 2.4).

2.1 Care: Practice, Orientation, and Ambivalence

Care is simultaneously a *practice*—the affective and material labor of attending to one another—and a *moral orientation* toward mutual responsibility and relational repair [19, 58, 59]. Fisher and Tronto add that care inherently exceeds duty, signaling relational investment through doing something *extra* [19]. As Berridge et al. show in their study of nursing home surveillance, the same monitoring practices constitute attentive care from one vantage point and control from another—tensions that cannot be resolved by opposing surveillance to intimacy [10].

Within HCI, care has become a key analytical lens for sociotechnical systems [6, 26, 29, 30, 62, 63]. This scholarship establishes that care organizes how people understand their obligations to one another—not merely how they justify them—and that it generates contexts in which surveillance is structurally difficult to separate from support [62]. Where this literature treats care's ambivalence as a design challenge, we show that it is the mechanism that makes location-based surveillance durable and self-reinforcing in close relationships.

2.2 Intimacy, Closeness, and Disclosure

Giddens argues that modern intimacy is not a state that precedes sharing but something disclosure produces and sustains [24]. Altman et al.'s dialectical account provides the structural complement: openness signifies intimacy only against the background of what is ordinarily withheld, with privacy constituted through dynamic cycling between openness and closedness [2]. Continuous location-sharing forecloses that dialectic, replacing oscillation with a fixed state of access previously unavailable outside cohabitation. Once established, withdrawing that access is not adjusting a setting but taking back something that has come to *mean* the relationship [8]. Prior surveillance accounts treat intimacy as the precondition for tracking. We document the reverse: continuous mutual visibility *produces* closeness rather than merely expressing it, transforming exit from a logistical act into a relational one.

2.3 Location-Sharing in Close Relationships

Location-sharing has been examined across a range of close relationships, from early work on voluntary disclosure and coordination [35, 48, 54, 56] to extensive studies of family surveillance [11, 34, 37, 51] and a growing body of research on technology-facilitated abuse [14, 22, 61]. Collectively, this work maps the terrain our study inhabits. What it has not yet provided is a theorized account of the *mechanism* that links care, tracking, and the felt experience of intimacy across these contexts.

2.3.1 Coordination, Reassurance, and Relational Maintenance. HCI work establishes that people disclose location selectively to close ties and that mutual visibility supports coordination and peripheral awareness across distance [15, 17, 48, 54]. Schildt et al. show that continuous sharing reshapes awareness and communication patterns within social groups, with location visibility

becoming woven into the ongoing texture of group coordination [48]. This selectivity persists in contemporary platforms, where location access remains an ongoing negotiation over who can see whom and under what relational conditions [20]. Work on mobile app privacy has documented a related dynamic at the individual level: people routinely come to accept data practices they initially experienced as uncomfortable, through a process of gradual normalization that forecloses the reconsideration it appears to invite [50]. Complementing this, large-scale work on continuous location sharing shows that users experience discomfort that escalates from overstepped boundaries to lifestyle-impacting behaviors, even as they continue to use these applications for safety and social convenience [16]. Our findings extend this from individual accommodation and discomfort to relational obligation—drift that is not merely tolerated but morally reinforced through care.

Most of this literature treats sharing as episodic and negotiable; even work on continuous sharing [16] frames discomfort as individual rather than relational. It does not examine what happens when visibility becomes a background condition of the relationship itself rather than a gesture made within it—the shift our study takes as its primary object.

2.3.2 Surveillance, Care, and Control in Families and Beyond. Family surveillance literature documents the tension between parental responsibility and children's emerging privacy interests, and how the care idiom tends to resolve it in favor of visibility [18, 52]. Mavoa et al. find that parents frame tracking as safety rather than surveillance—"it's about safety not snooping"—even as practices extend beyond specific safety concerns [37]. Boesen et al. theorize this as a "domestic panopticon": asymmetric visibility sustained by family care norms, experienced by children as monitoring even when parents experience it as love [11]. Widmer and Albrechtslund show that sustaining this framing requires ongoing moral work—parents develop informal "tracking etiquettes" to keep practices legible as care—yet treat this as an individual struggle of domestication rather than a self-sustaining relational mechanism [64].

Yet none of this work explains why these responses are so durable: what makes care and tracking *co-productive* across relationship types, and what makes continuous visibility difficult to contest even in relationships no one would call harmful. We address these gaps in two ways. First, we move beyond the parent-child dyad to examine how these dynamics manifest across romantic, friendship, intergenerational, and caregiving relationships. Second, we develop *surveillance intimacy* as a theoretical account of the mechanism: care does not merely justify tracking but produces the felt experience of closeness that *obligates* more tracking—a self-reinforcing loop that is structurally upstream of the coercive dynamics the tech-abuse literature documents at the far end of the same continuum. Levy's legal-theoretical account of "intimate surveillance" catalogs surveillance technologies entering romantic and familial relationships and the privacy risks they introduce [32]; where that work asks what surveillance does to intimacy, ours asks what intimacy—through care—does to surveillance. Our use of *surveillance intimacy* is therefore bounded to close relationships where continuous visibility is framed as care, rather than to all instances of intimate surveillance or technology-facilitated abuse.

2.4 Privacy Frameworks: From Boundary Regulation to Structural Power

2.4.1 Boundary Regulation and Contextual Integrity. Palen and Dourish's boundary-regulation framework assumes negotiation precedes or remains available within sharing arrangements; Nissenbaum's contextual integrity assumes flows can be evaluated against stable contextual norms [40, 41]. Vulnerability-centered accounts show that power asymmetries constrain these assumptions [38]; Tang et al. extend this across layered systems where care norms are strongest and where platforms and policy are least able to intervene [55]. Privacy-by-design approaches address this architecturally, embedding boundary controls into the system before sharing begins [46], but

assume that boundaries, once specified, remain stable and exercisable. Continuous background tracking, embedded by default in platforms like Find My and Life360, arrives before negotiation can begin. It obscures the evolving practices Palen and Dourish's framework depends on and eludes contextual integrity's analysis of stable normative contexts. Structural accounts [38, 55] likewise do not address arrangements in which care *is* the mechanism that forecloses negotiation; where tracking is not imposed despite the relationship but through it. Hartzog's concept of obscurity offers a partial bridge: where contextual integrity and boundary regulation assume identifiable flows and available negotiation, obscurity names the privacy resource people rely on when neither is available—the condition of being present but not salient, findable but not interpretable [25]. Our findings suggest that participants navigating *surveillance intimacy* deploy this resource, relying on reduced interpretability rather than formal controls when the relational cost of the latter is too high. Recent work on privacy silence shows that intimate partners often regulate mobile-phone privacy through silence, tacit understandings, and implicit cues rather than explicit negotiation, and that these forms of boundary regulation can sustain trust and intimacy while creating new vulnerabilities [3, 4]. Partners avoid raising privacy concerns because doing so risks being read as mistrust [3]. We find a related dynamic in continuous location sharing, across parent-child, friendship, and caregiving relationships as well as romantic ones. There, location visibility mediates care, closeness, and obligation, so renegotiation risks not only signaling mistrust but unsettling the intimacy that visibility helps sustain.

2.4.2 Primary, Non-Primary, and Adjacent Users. Research on networked sensing has extended privacy analysis beyond device owners to bystanders [1, 31, 45, 66, 68], non-primary users [9, 53, 67], adjacent actors such as co-users and surveilled subjects [44], and incidental users [28]. These categories typically reflect the distribution of power and control at adoption: who purchased, configured, or consented to a device determines who counts as a primary user and who as a bystander, as with the smart home camera owner and the visiting nanny [9]. Continuous location-sharing fits these categories less cleanly. Sharing may or may not be mutual, and even mutual sharing does not mean mutual looking. The technical arrangement also persists long after initial adoption, even as use changes. We return to this in Section 5.1.2.

2.4.3 From Structural Power to Relational Stakes. The literature that most concretely documents what is at stake when privacy negotiation fails comes from technology-facilitated abuse. Freed et al. show that survivors often leave surveillance in place because altering it may alert abusers and escalate harm [22]. Tseng et al. document intimate partner violence (IPV) survivors tolerating invasive monitoring to preserve precarious stability [61]. Together, these studies demonstrate that privacy choices in close relationships are constrained not just by interface design but by the threat of relational and physical consequences—and that asserting a boundary can itself be the dangerous act. Bellini et al. further show how perpetrators of intimate partner surveillance develop narrative justifications that mirror care framings, constructing monitoring as protection rather than control [5].

We extend this insight to relationships not formally recognized as abusive. Building on vulnerability-centered privacy theory and tech-abuse findings, we argue that even in relationships no one would call harmful, continuous location-sharing acquires relational meanings that make withdrawal costly: asserting a boundary risks being read as withdrawing care, trust, or commitment. *Surveillance intimacy* names this condition upstream of abuse and theorizes the mechanism—care—through which such arrangements become durable, whether or not they become coercive.

3 Method

We designed a qualitative interview study to examine how care and intimacy function as conditions through which location-sharing becomes normalized and difficult to exit in close relationships. We chose interviews because the phenomenon we sought to understand—how relational meaning accretes around tracking practices over time—is not legible through behavioral data or survey instruments. It requires participants to reflect on their own practices, narrate the relational contexts in which those practices are embedded, and articulate the tensions and negotiations they navigate. Semi-structured interviews, with their capacity for depth, follow-up, and participant-led elaboration, were well suited to this goal. This study received Institutional Review Board approval. All participants provided informed consent prior to interviews, which lasted 20–90 minutes, and were compensated with $50.

3.1 Interview Design

We designed interviews to move from the concrete to the interpretive. Each session began with participants walking the first author through their current location-tracking tools—which devices and platforms they used, how they were set up, and with whom they shared or monitored location. This grounded the conversation in specific practices before moving to questions about motivation, relational dynamics, and experience. We then invited participants to reflect on how their sharing arrangements had evolved over time; moments of discomfort, ambivalence, or renegotiation; how they thought about safety, trust, and privacy in the context of their relationships; and how they managed visibility when they wanted more privacy than the arrangement provided. The first author conducted all interviews, three in-person and twelve remotely via Zoom. All sessions were audio-recorded with participant consent and transcribed using Temi, a commercial transcription service; audio files were deleted following transcription. Prior to upload, recordings were labeled only with participant IDs, and resulting transcripts were stored on encrypted institutional cloud storage accessible only to the research team. Quotes are lightly edited for readability, removing filler words, false starts, and repetitions; ellipses mark omitted content.

3.2 Recruitment and Participants

We recruited through university channels, Nextdoor, coffee shop flyers, and personal networks, using a two-stage process. First, a screener survey identified participants who actively used location-sharing technologies—including Life360, Find My, AirTags, Tile, smartwatches, or GPS-enabled apps such as Strava—and who shared or monitored location within at least one close relationship. Second, from over 60 screener responses, we purposively invited 28 participants based on relational diversity criteria, seeking variation across relationship types (parent-child, romantic partnership, friendship, caregiving, employment) and tracking roles (those who primarily track others, those primarily tracked, and those in mutual arrangements). Fifteen participants completed interviews; we ended recruitment when the team judged that additional interviews were adding little new interpretive material relative to our research questions.

Our 15 participants included women ($n = 12$), men ($n = 2$), and a non-binary participant ($n = 1$), ranging in age from 25 to 74. We collected ethnicity data to reflect on participant positionality and respond to HCI and CSCW critiques of unexamined perspectives [42]; participants included Hispanic, Asian, Native American, Black, and White individuals; most were White. Relationship contexts spanned parent-child dyads (including parents of adolescents and adult children tracking aging parents), romantic partnerships, friendships, and employment-based caregiving. Devices used included Find My, Life360, AirTags, Tile, Apple Watch, and Strava. Table 1 provides a full overview.

Table 1. Participant Overview

ID	Friends	Partner	Family	Role	Gender	Age	Ethnicity	Devices
P1	Yes	No	No	Being tracked	F	25–34	Hispanic	Find My, AirTag, Apple Watch
P2	Yes	Yes	Yes	Mutual	F	25–34	Asian	Find My, AirTag, Life360, Apple Watch
P3	No	Yes	Yes	Tracks others	M	65–74	White	Find My, AirTags
P4	No	Yes	No	Mutual	F	55–64	White	Find My, AirTags
P5	Yes	No	No	Mutual	M	25–34	White	Find My, AirTags
P6	No	No	Yes	Being tracked	F	25–34	White	Find My, AirTag, Apple Watch
P7	Yes	Yes	Yes	Mutual	F	45–54	Hispanic	Find My, Life360, Apple Watch, Strava
P8	No	Yes	Yes	Mutual	F	55–64	White	Find My, Apple Watch, Strava
P9	Yes	Yes	Yes	Mutual	F	45–54	White	Find My, AirTags
P10	Yes	Yes	Yes	Mutual	F	25–34	Asian	Find My, AirTags
P11	Yes	Yes	Yes	Mutual	NB	35–44	Native	Find My, Life360, Apple Watch, Tile
P12	No	Yes	Yes	Mutual	F	35–44	White	Life360, Apple Watch
P13	No	No	Yes	Being tracked	F	25–34	Asian	Life360, Tile
P14	No	Yes	Yes	Mutual	F	35–44	White	Find My, Apple Watch
P15	No	Yes	Yes	Tracks others	M	35–44	Black	Find My, Tile, AirTag

3.3 Data Analysis

We analyzed data following reflexive thematic analysis (RTA) [12, 13], an approach that treats themes not as latent structures waiting to be discovered in the data but as interpretive constructs actively generated by researchers whose positionality and theoretical commitments shape what they notice, how they read, and what they build. Consistent with this approach, we were explicit throughout analysis about the theoretical sensitivities—care, intimacy, relational power, consent—that oriented our attention without predetermining our findings.

The lead author began analysis during data collection, writing reflective memos after each interview that captured initial interpretations, emerging patterns, and questions to pursue in subsequent sessions. This early analytical work shaped the interview design as the study progressed, allowing later interviews to probe more specifically at tensions and dynamics we had noticed in earlier ones. Following transcription of all 15 interviews, the lead author conducted a close reading of the full corpus, generating initial codes directly from the data that captured both semantic content (e.g., in-vivo terms that participants themselves used ("safety," "gotcha")) and latent meaning. We constructed latent codes not from individual statements but by reading across accounts—attending to patterns in what participants normalized, what they struggled to name, and where justifications shifted. This cross-account reading was the primary site at which theoretical constructs such as care-as-mechanism and relational obligation became analytically visible, as no single participant articulated them directly.

The research team collaborated on the construction of the themes through a series of analytical discussions in which the codes were grouped, contested, and refined into broader thematic patterns. Rather than working toward a fixed codebook, this process was iterative and reflexive: early groupings were revisited as later transcripts were analyzed, and the team regularly returned to the data to test whether emerging themes were grounded in the full range of participant accounts or over-represented particular cases. Researcher positionality, including the author team's familiarity with the technologies studied and their own experience of location-sharing in close relationships, was surfaced and discussed as part of this process, as Braun and Clarke's framework requires [12].

Final themes were developed through extended analytical memos in which the research team elaborated the interpretive claim each theme made, identified the evidence that supported it, and noted cases that complicated or qualified it. The four dynamics that organize our findings—relational visibility as care, sharing as relational obligation, moral rationalization, and everyday tuning—were the result of this process: analytically distinct but sequentially related expressions of the *surveillance intimacy* condition we theorize.

3.4 Limitations

This study captures rich individual accounts but is limited to single-sided perspectives: we interviewed one participant per relationship, a design choice we made to create a safe reflective space for each participant, and to avoid the relational strain that could arise from interviewing multiple members of the same dyad. Two participants were married to each other; however, we interviewed them separately. This approach preserves candor but precludes direct comparison of how the same arrangement is experienced by both parties—a limitation that matters most given our theoretical interest in how the care frame is inhabited differently by trackers and tracked. Future work should examine these dynamics through dyadic or longitudinal designs that can track how relational meaning around location-sharing evolves, and how care framings shift as relationships and life circumstances change. We return to the theoretical implications of these constraints, and to questions of scope and transferability, in Section 5.3.

4 Findings

Location-sharing produces and sustains closeness: the felt sense of knowing where someone is, even across distance. Intimacy emerges from this act of access—lowering one's privacy guard to let another "in"—both expressing and creating relational bonds. Care provides the moral logic that makes this feel natural and obligatory, transforming location-sharing into an act of attending to one another.

Together, these processes constitute *surveillance intimacy*: a relational condition in which care motivates sharing, sharing produces intimacy, and intimacy in turn normalizes tracking as something other than surveillance. The four dynamics we identify instantiate this logic: relational visibility as care (Section 4.1), sharing as relational obligation (Section 4.2), moral rationalization (Section 4.3), and everyday tuning (Section 4.4). We use *surveillance intimacy* to describe arrangements in which care is invoked to initiate, justify, and sustain continuous visibility in otherwise non-abusive relationships.

4.1 Relational Visibility: Tracking as an Expression of Closeness

Among participants, location-sharing entered their close relationships through two pathways: as a deliberate gesture of trust and closeness, or as a practical response to a specific need, such as a trip or safety concern. Over time, location visibility took on a relational layer, becoming the medium through which participants performed care and felt intimacy.

4.1.1 Location Sharing as Relational Currency. For some participants, the initial act of sharing location was itself a relational gesture. P5 framed it as an act of vulnerability and reciprocity: *"I'm happy to give it to the people I trust… hopefully one day I can be someone that they trust."* Someone, as he put it, *"has to go first."* The language of going first—of making yourself visible before the other person has—positions location-sharing as an offering that constitutes closeness rather than following from it. P10 articulated how sustained sharing deepened relational trust over time:

> After having someone's location for a long time…it feels like we just have this development of trust…to be able to look at someone's location at all times is super intimate.

P1, by contrast, did not share with her partner, and was explicit that this was not about distrust: "*it's not that I don't love [my partner], it's not that I don't trust [him], but… in terms of a rapid response person who I know is gonna be on their phone, that man is not it.*" Her location went instead to the friends she had relied on while single. The contrast is telling: sharing can signal intimacy performed through visibility, trusting the other person with both the information and its interpretation, but the people entrusted with one's location need not be the closest; they are the ones who will respond.

For other participants, sharing began instrumentally—not as a gesture of closeness but as a practical response to a specific situation—and acquired relational meaning only afterward. P1 described this drift among friends: sharing that began for a date, a trip, or getting home after a night out became the friend group's background default. "*There's an event that we're both going to, or like a trip... let's share location. And then we just never turned it off.*" What began as a practical measure became—without explicit negotiation—a form of ongoing care woven into friendship groups. This drift from purposive to ambient sharing, in which arrangements begun for specific reasons persist beyond their occasion, echoes work on mobile privacy [50]. P5 described the same instrumental start ("*in the earlier days it was more so out of convenience... useful for that moment*") but converted it by choice rather than by drift, deciding friend by friend whether to share indefinitely: "*is this someone that I trust to have my location all the time? And if it is, then I really don't mind sharing indefinitely.*" Arrangements that began for purely instrumental reasons took on the moral weight of care once participants linked them to being looked after, which made them difficult to opt out of. We explore this obligation and its moral rationalizations in more detail in Sections 4.2 and 4.3.

4.1.2 Ambient Presence and the Feeling of Togetherness. For many participants, the relational value of location-sharing was less about the information it conveyed than about the sense of ongoing presence it generated. P12, a mother using Life360 with extended family, described how family-wide sharing she had set up partly *"for, you know, safety"* took on new meaning once a cousin moved out of state: *"She'll call and be like, 'you're at HomeGoods without me'… so then she'll FaceTime me and we'll just talk and, you know, shop around the store."*

Location became an invitation—a way of recreating the peripheral awareness of cohabitation across distance. P12 named it directly: *"It's more of a connection thing."* The instrumental origin became irrelevant; what persisted was its relational meaning. This connection was not limited to distant relatives; she described sharing with a nearby sister the same way: *"we just are always together, and when we're not, we just wanna know where each other is."* P13, who had resisted location-sharing for years, described a similar revaluation after moving away from family:

> After being a hater for so many years, and now living far away from them, there is something kind of cute about being like, "Oh my sister made it home from Pittsburgh." You know what I mean?

Asked whether this made her feel closer, she was unsure: *"I don't know if it makes me feel closer to them, I just sometimes worry that…I don't know what they're doing anymore…And so in some*

ways I now have one way where I do know what they're doing." A change in relational need drove the shift. When distance created a deficit of awareness, location sharing filled it—and the arrangement that had once felt like surveillance came to feel *"kind of cute."*

4.1.3 Safety, Care, and the Production of Feeling Loved. In family and caregiving relationships, the attachment of tracking to care was most explicit. P8, a mother, framed it as enabling independence rather than restricting it: *"Mostly it was kind of to give my kids a lot more independence... it was just always helpful for me to, you know, know where they were."* The tracking is positioned here not as surveillance but as the condition that makes freedom possible, a reframing that insulates the arrangement from being experienced as control. Most revealingly, P6—an adult living alone—described her mother's habit of checking her location: *"It makes her feel better 'cause I live alone. And then also if I don't answer my phone, she'll call my phone and if I don't answer my phone, she'll look at my location and be like, where is she? If I'm at home, she's like, oh, she's just at home working. I think she gets a little anxious."* Asked how learning this made her feel, she said: *"It made me feel cared for. It made me feel like my mom has some anxiety issues."* P6 was not being tracked against her will, nor did she uncritically accept the arrangement. She experienced the tracking as an expression of her mother's concern and parental care, even as she saw the anxiety behind it. This is the dynamic at its most complete: the tracking produces the feeling of being cared for, the feeling of being cared for attaches to the tracking, and that attachment is what makes the arrangement both durable and difficult to question.

4.1.4 Platform Design and the Naturalization of Visibility. We found that the relational work of location-sharing was shaped, but not determined, by platform design. Families predominantly used Life360 and Apple's ecosystem (Find My, Apple Watch) for their persistent, always-on visibility—platforms that make location ambient rather than requested. Friend groups used Find My's passive model, where location is available without active check-in. These design choices actively reinforce care attachment by making location continuously available as background information rather than requiring an explicit act of sharing. In practice, this naturalized visibility in ways that made it feel less like disclosing sensitive information and more like simply being present for one another.

When the technology makes visibility effortless and the relationship makes it meaningful, the two reinforce each other in ways that make the arrangement increasingly difficult to examine or exit. While this infrastructure does not produce *surveillance intimacy* on its own, it creates conditions in which care can turn continuous visibility into a felt requirement of the relationship. Platforms that organize visibility around discrete events rather than continuous streams, such as activity-based sharing apps (e.g., Strava), may support different relational meanings and warrant a dedicated study; we leave them to future work.

4.2 Sharing as Relational Obligation

Surveillance intimacy also operates through relational obligation. In many relationships, sharing persists by default because turning it off demands a conversation whose social cost outweighs its practical benefit, social friction that favors keeping things as they are.

4.2.1 From Relational Default to Awkward Conversation. Among friends and romantic partners, sharing arrangements that participants were ambivalent about persisted primarily because ending them would have required naming the ambivalence—a conversation most were unwilling to have. P5 and P13 described the same pattern: what had become an established feature of the relationship carried an implicit social meaning, and disrupting it would have implied something about the relationship that nobody wanted to say out loud. Thus, it was simpler to maintain sharing than to contest it.

4.2.2 Power Asymmetry and Directional Gaze. In parent-child relationships, the costs of stopping are higher and the options more constrained. Tracking is usually framed as the parent's expression of care, with asymmetry in who is tracking. P6, an adult living alone, described this one-sidedness: her mother *"just kind of looks occasionally and it makes her feel better,"* while P6 herself does not look back: *"I have my mom, I have my brothers. I never check it."* Here, the one-sidedness reflects the direction of worry, and challenging it would mean challenging the way care is organized in the relationship. The direction is not fixed, though. P12's teenage daughters, she said, "*track me more than I track them*," and when her location went off, they called to insist she turn it back on. She put their checking down to worry: "*they are worried, you know, like, what is my mom doing?*" Reversed, the obligation works the same way: the relationship has come to expect visibility.

P13, now an adult, remembered hating the tracking as a teenager: *"I hated having this thing on my phone. I didn't wanna be tracked."* She was *"too rule following to really mess it up,"* so her objection went into workarounds instead:

> I would like turn on my airplane mode…or like realizing if I turned on my battery saving mode, it couldn't track my location, and I'd be like, oh no, I forgot. But I never forgot. It was always intentional, I wanted to be hidden.

The resistance was real but could not be voiced, because the tracking was framed as love and contesting it required contesting the love. Children's consent is structurally compromised here: the arrangement is constituted as care before the child's perspective is solicited, which means that objecting to it requires rejecting what the parent understands as an expression of concern. P12's position shows the contrast. As the parent, she could tell her daughters "*you do not need to know where I am*" before turning her location back on. Power shaped how an obligation could be contested, not whether it applied.

P7 further described the parental side of this asymmetry. She told her children she would not check their locations (*"just be where you tell me you're gonna be"*) and checked only after another parent tipped her off that they were not where they had said:

> I try and give them the benefit of the doubt, you know?…I kind of felt like in that situation I would really rather like you just be truthful…instead of me having to find out from another parent.

The location data functions as a trust-verification tool framed within care. The teen's experience of being watched is invisible to this framing because the framing is organized entirely around the parent's expectation of honesty.

4.2.3 The Social Cost of Opting Out. Platform design amplifies the relational cost of withdrawal across all relationship types. Participants understood that stopping sharing on Find My or Life360 would be visible to the other person. This turned what could be a private recalibration into a social event. P9 named the consequence:

> it can get messy…when you share with someone and decide you don't want to share, and then do you let them know you're not? Because you get a notice that they stop sharing.

P10 described the emotional register of receiving that notice: *"maybe they don't trust me."* As a result, stopping can be read as relational withdrawal, a statement about trust, regardless of what the person stopping intended. This perception gap matters analytically: withdrawal may reflect a communication failure rather than a relational change, which means that the design problem is not simply one of making exit easier but of making the meaning of exit less overdetermined. Apple's platform offers time-bounded sharing—share for one hour, until end of day, or indefinitely—but no participant in our study described using this feature as a strategy for managing ambivalence. The

social meaning attached to stopping, it seems, travels with the visibility of stopping rather than with the technical form of the exit. Most participants resolved this tension by not stopping. They maintained sharing arrangements they were ambivalent about rather than absorb the social cost of the conversation that stopping would trigger.

4.2.4 Employment and the Limits of Disclosure. In employment contexts, the care logic takes a structurally different form. P7—a mother who had hired in-home caregivers when her children were young—kept a Tile in each child's backpack and told the caregivers about it: *"there's always a tile in their backpack and just want you to be aware that their locations are being monitored."* The Tile tracked the children, but it also let P7 check whether a caregiver had dropped them off at school on time. She described the disclosure as part of being upfront, alongside a background check. P2 placed an AirTag on her dog's collar and did not tell the Rover sitters who walked him, reasoning that the tag was visible on the collar and that, unlike her friends, the sitters would keep him on leash. For P7's caregivers, disclosure came as part of the terms of employment, and refusing would have meant contesting those terms: employment dependency, not care, obligates agreement. For P2's sitters, the question of refusal never arose. But the structure is the same as in relational contexts; disclosure is not equivalent to choice when the alternative is losing the relationship, whether that relationship is familial or economic.

4.3 Moral Rationalization: Care as Ethical Infrastructure

The third dynamic emerges when the surveillance dimension of location-sharing becomes visible—when a tracked person expressed discomfort, when the asymmetry of the arrangement became hard to ignore, or when we asked participants directly to reflect on their practices. In these moments, the care logic does a second kind of work. It functions not just as the initial attachment that makes tracking feel intimate but as an ongoing moral resource that participants invoke to sustain *surveillance intimacy* when it might otherwise be questioned. We call this *moral rationalization*—not to suggest that participants are being dishonest, but to describe how care narratives serve as ethical infrastructure that holds the arrangement in place. We describe how participants invoked ownership and duty (Section 4.3.1) and managed how tracking was perceived (Section 4.3.2), how the care frame traveled to the tracked (Section 4.3.3), a case in which ownership displaced care (Section 4.3.4), and how rationalization varied with relationship power (Section 4.3.5).

4.3.1 Ownership, Duty, and the Extension of Care. The most direct rationalization parents invoked was ownership and obligation. P13's mother tied tracking to the responsibilities of provision: *"Under my roof, you know, my house, my rules…I pay your phone bill. Like, I wanna know where you guys are."* This framing positions the parent as the origin of the resources that make the child's mobility possible, and tracking as the natural prerogative that comes with provision. It leaves no conceptual room for the child's consent because consent is not the operative concept. Care-as-obligation is.

The ownership logic was not confined to parent-child relationships. P5 described placing AirTags on items he lent to friends so *"we can still find it again"*, framing this as protecting the object rather than monitoring the person—a rationalization that made the tracking feel categorically different from surveillance. He was emphatic that he disclosed it: "*I wouldn't like do it secretively. It's not about trying to surveil them in a covert capacity.*" Yet he also recognized what the tag made possible: "*I'm not like…seeing where they are in a secret manner…But I could, I guess theoretically. But there is that privacy issue because I bet I could.*" The surveillance dimension was not absent from his awareness; the object-ownership frame held it at a distance. P2 deployed a structurally similar rationalization: placing an AirTag on her dog after he was once lost, and also using it to check where the hired pet sitters took him. The object—the dog—provided a care justification that absorbed the surveillance

of the person caring for it. In both cases, tracking an object rather than a person provided moral cover that made the arrangement feel less like monitoring and more like reasonable stewardship.

Across these accounts, ownership provided a moral reasoning other than care—one that does not require the tracked person's consent because the thing being tracked is framed as property rather than person. It extends the reach of surveillance while insulating it from the vocabulary of consent.

4.3.2 Non-Punitive Care and the Management of Perception. A second form of moral rationalization involved participants actively managing how their tracking was perceived—working to ensure it was understood as care rather than control.

P8 described her orientation toward years of family-wide location-sharing: *"It's not a gotcha."* Asked how sharing built trust, she offered a parallel from outside the app. While cleaning her teenage son's car as a surprise, she found red Solo cups, put them back, and later mentioned them only in passing as he headed out: *"oh, you use some of those red solo cups."* She tied the two directly: *"if I weren't handling those situations the way I just described, then handling the location sharing would be very different as well."* She sustained the tracking by showing, in how she handled what she learned, that it was organized around care.

P9 used the same word about checking on her daughters (*"I'm not trying to do like a gotcha"*) but managed perception differently. Her daughters knew she had their locations (*"it wasn't a secret"*), yet *"most of the time I don't want them to know that I'm following them."* Where P8 made her restraint visible, P9 kept her checking out of view. Both kept the tracking from reading as enforcement.

P7 was comfortable being visible herself: *"the world is not a safe place really anymore…I'm happy to let people know that I get places safely."* Within her family, she grounded sharing in reciprocity: *"if you're gonna track somebody, you should be more than willing to let them track you."* Her teenage daughter, she said, was "really okay with it" because *"she uses it to track me,"* and P7 described that use with warmth: *"Mom, are you at Chipotle?"* Yet P7 had access to richer data about her daughter: Life360 also reported her daughter's driving speed, hard braking, and phone use while driving. Mutuality, even where asymmetric in practice, provides moral legitimation: if everyone can see everyone, the arrangement cannot be surveillance.

4.3.3 When the Care Logic Travels. P6's account (Section 4.1.3) suggests that the care logic can travel from tracker to tracked, colonizing both sides of the relationship. When it does, the tracked person becomes a participant in sustaining the arrangement rather than a potential challenger to it.

P15's mother illustrates the inverse: a tracked person who had not adopted the care frame because she was not fully informed of the arrangement. P15, an adult son caring for his aging mother, set up location sharing without clearly explaining what he had done: *"I don't know if I even asked her to do it…I figured she wasn't gonna completely understand it or ever use it in reverse."* He rationalized this not as deception but as stewardship: *"she is pretty trusting of me to make sound choices."* The care logic here substitutes for consent—his mother's likely acquiescence, assumed rather than solicited, is treated as sufficient because the arrangement is understood as being in her interest. P15 deployed the same moral logic that parents use to track children: the tracked person cannot fully evaluate what they are consenting to, and care authorizes the decision on their behalf.

4.3.4 Ownership, Suspicion, and the Collapse into Covert Control. In one case, ownership worked differently than in 4.3.1: not as an extension of care that forecloses the tracked person's objection, but as a property claim that replaced care as the justification—converging with relational suspicion and covert technical action. This case marks where *surveillance intimacy's* relational infrastructure ends and coercive control begins.

P1 recounted helping a friend conceal an AirTag in her husband's car without his knowledge or consent. The rationalization centered on property ownership and financial asymmetry:

> She owns everything…she works in pharma, he was a grad student…she owns their home, she owns the car…she pays for the maintenance and honestly for more of the gas than I think she should.

The friend's reasoning extended this ownership claim directly to location access: *"this is my property and I'm suspect that you're coming home late and you're using the car to do so…therefore, you are with the car and wherever the car is."* The conclusion followed: *"If he wants privacy, he needs to get his own car."*

P1 believed that asking directly would have backfired: had her friend asked, "*that would've been confrontational and that would've been like, 'why you don't trust me.'*" To raise the question of surveillance would itself have been read as a relational accusation. The AirTag was instead concealed physically: *"underneath the back mats…we cut a little hole and we really got it in there."*

This case matters for three reasons. First, it shows ownership rationalization operating without even the pretense of care: the framing is not *I track because I love you* but *I track because I own the thing you are in*. The moral logic has shifted from care ethics to property rights, but the outcome—covert, non-consensual, continuous location monitoring—is structurally identical. Second, it shows that the tools of *surveillance intimacy* transfer to people outside the relationship: P1 helped implement surveillance of someone else's partner, applying the same technical and moral infrastructure the prior cases document. Third, it shows the upstream-of-abuse condition that *surveillance intimacy* names: the relational arrangement in which asking directly is already foreclosed, the technology is already normalized, and the only remaining question is how covertly to deploy it.

4.3.5 The Direction of Care and the Structure of Rationalization. The care logic appeared across the full range of relationship types in our study, but its moral work varied with the power structure of the relationship. The pattern is most visible in contrast. In parent-child and elder-care relationships, the moral rationalization was directional: the person doing the tracking held structural authority and invoked care to foreclose the less powerful party's objection. P15's mother was not in a position to contest an arrangement she did not fully know existed. P13's teenage resistance could not be voiced because contesting the tracking meant contesting the love it expressed.

In more formally equal relationships, the care logic operated differently. P10 tracked her partner on 3 a.m. rides to the airport for early flights, not from a position of authority but from worry: *"that idea of him like being at night and like they get into a car crash…there's nothing I can do about it."* Her partner knew she checked, tolerated it, and told her to go back to sleep. The care logic was shared rather than imposed; the rationalization was mutual rather than foreclosing. P10 also noted that they had never had an explicit conversation about how they would use each other's locations—the arrangement had simply grown from practical need without negotiation. The mutuality of the care frame meant that neither party had occasion to contest what neither party framed as surveillance.

P11 described a structurally distinct configuration. Location-sharing during dates with strangers was organized not around relational care but around safety from structural vulnerability: *"I don't want you to murder me."* The moral logic—someone should know where I am—was self-directed rather than relational, produced by gendered risk rather than intimacy. P11 was explicit about the distinction, noting that with a trusted long-term partner the same logic did not apply: *"I don't even think they look…it's more something I share with them."*

The hidden AirTag case, finally, shows ownership rationalization operating outside the care frame and yet deploying the same technical infrastructure and relational silence that care-motivated tracking produces. Across these variations, moral narratives performed the same function: they resolved the tension that would otherwise make surveillance visible as surveillance. The resolution takes different forms—care, stewardship, ownership, self-protection—but the outcome is the same: the surveillance dimension of the arrangement does not require explicit acknowledgment or consent

because the moral logic speaks for it. And as the hidden AirTag case shows, once that infrastructure is in place, it is available for uses that the care frame no longer governs.

4.4 Everyday Tuning: Managing Visibility Without Contesting Care

The three dynamics documented above might suggest that *surveillance intimacy*, once established, simply persists—a stable background condition of relationships in which continuous location-sharing has become constitutive of care. However, across our data, participants who could not openly contest their sharing arrangements did not accept them unchanged: they made small, often covert adjustments to visibility that recovered partial autonomy without disrupting the relationship or making the contest explicit. We call this practice *everyday tuning*. Its triggers were varied—a care frame thin enough to feel more like monitoring than love, an obvious asymmetry, a destination that needed to remain undisclosed—but they all shared that opting out openly carried a social cost the participant was unwilling to pay.

4.4.1 The Structure of the Problem: Renegotiation Is Unavailable. P6, an adult living alone, shared her location continuously with her mother via Apple's Find My. The sharing had begun incidentally—her brother introduced it so the family could track ferry arrival times—and its surveillance dimension only became visible when her location stopped appearing on her mother's screen, a glitch she attributed to her phone not having updated. Her mother's distress at the outage revealed that she checked P6's location regularly, using it to manage her anxiety about her daughter living alone: if P6 did not answer her phone, her mother would check the app and, seeing her at home, conclude she was simply occupied. This revelation posed a problem P6 had not previously needed to solve. In the same answer in which she described feeling cared for, she added: *"there's some places that I go that I don't want her to know that I'm going there."* This included a BDSM club she sometimes attended. P6's difficulty was not the destination specifically but the structural position she occupied. She was unsure whether adjusting her sharing settings would notify her mother (*"I don't know if that sends her like a notification"*), and a notification would prompt questions. Explaining her reasons would require disclosures she was unwilling to make. At the time of the interview, P6 had not yet resolved the problem: her working assumption was that her mother would not connect her location to its implications—*"I don't even think she'd put it together."* This is obscurity reasoning in Hartzog's sense: not seeking invisibility but relying on the gap between data availability and interpretability as a de facto privacy resource [25]. When the interviewer raised airplane mode as a possible workaround, P6 had not considered it: *"I hadn't thought about [airplane mode]…I was just like, I don't even think she'd put it together."* Her situation illustrates the problem everyday tuning addresses. If explicitly stopping location sharing sends a notification to the other party, it makes the act of opting out visible and socially consequential. Airplane mode produces a dropped signal rather than an explicit opt-out, preserving the appearance of a technical artifact rather than a relational choice. However, airplane mode carries its own limitations: it disables communication on the device entirely. P7's account suggests that associated accessories such as AirPods may remain visible to family members, as we describe in the next subsection. P6 had not worked through these trade-offs; she was still navigating the gap between her need for privacy and her unwillingness to contest the care relationship the sharing expressed.

4.4.2 Covert Recalibration: Workarounds That Preserve the Relationship Surface. Where participants had developed solutions, these took the form of technical workarounds that adjusted visibility without triggering social consequences. These workarounds were performed from both sides of the tracking relationship: by those being tracked seeking partial autonomy, and by trackers seeking to maintain visibility after an attempted opt-out.

Gaps and leaving the phone behind. P13's teenage airplane-mode and battery-saver workarounds (Section 4.2.2) made each gap look like an accident rather than a choice. P9, still sharing location with an ex-partner after their breakup, wanted to run an errand without him knowing where she went: *"rather than just turn it off, I left my phone at home."* Where P13's workarounds dropped the information, P9's kept it running but wrong, showing her at home while she was elsewhere. Both, like the airplane mode raised with P6, avoided the visible withdrawal that turning sharing off would have meant.

Exploiting incomplete opt-outs. Trackers also tuned, exploiting gaps that allowed them to maintain visibility without acknowledging it. Unlike the hidden AirTag (Section 4.3.4), which was premeditated, this case involved opportunistic use of a gap the tracked person had inadvertently left open. P7's adult son, back from military training, turned off his location sharing on Find My but left his AirPods connected to the family Apple account. P7 discovered this oversight and began using it. When she wanted him to pick up groceries near his gym, she would check his AirPod location first and then text him as if the errand had occurred to her independently: *"is he at the gym?… if he's over there, I'm gonna ask him to pick up some fish."* She did not tell him she could see his location. His attempt at privacy was absorbed into the care relationship's normal functioning, his location remaining available while the relationship continued as before.

4.4.3 The Labor of Tuning. Everyday tuning shows that *surveillance intimacy* requires ongoing work to maintain—not only from those who track, but from those who are tracked. P6's effort to assess whether her mother would connect a location to its meaning; P7's son's incomplete opt-out that became P7's surveillance resource; P13's staged forgetting; P9's phone left at home—these are all expressions of labor performed to sustain the surface of a care relationship while managing its surveillance dimension underneath.

This labor is asymmetrically distributed. In our data, it fell more heavily on those with less relational power: on adult children navigating parental expectations, on younger adults managing family visibility, on those whose care relationships are organized around their being seen. Those with more power benefit from the arrangement without performing equivalent maintenance. The care layer within the relationship naturalizes this asymmetry: calibrating your own visibility appears as ordinary relationship navigation rather than as uncompensated labor imposed by the relationship's structure. Everyday tuning is the behavioral signature of *surveillance intimacy*: it is what people do when care has made renegotiation unspeakable, obligation has made exit costly, and moral rationalization has made the arrangement feel stable to everyone except the person performing the invisible work of living inside it.

5 Discussion

Our findings document four dynamics through which *surveillance intimacy* takes hold and persists in close relationships: location visibility constituted as care, tracking hardened into relational obligation, moral rationalization as ongoing ethical infrastructure, and everyday tuning as the covert labor of living inside an arrangement that cannot be openly contested. In this section, we examine what this framework contributes theoretically and what it demands from designers.

5.1 Theoretical Contributions

5.1.1 Reversing the Surveillance–Intimacy Relation. The dominant vocabulary for location-based tracking in close relationships treats care and surveillance as structurally opposed—either in tension or one exploiting the other as cover. Foucault's disciplinary model and Lyon's surveillance theory position monitoring as an exercise of institutional power [21, 33]. Applied to families, Boesen et al.'s *domestic panopticon* describes asymmetric visibility sustained by care norms [11]; Widmer and

Albrechtslund describe parents' informal tracking etiquettes [64]. These accounts capture a real tension between care and surveillance. What they do not capture is how that tension resolves over time and what the relationship looks like once continuous visibility has become routine. Our data suggest that care and surveillance do not merely coexist; they co-produce each other, gradually, until the sharing arrangement becomes part of what the relationship constitutes. Participants described sharing that started for convenience and accumulated relational weight until, as P1 put it, "*we just never turned it off. And it just kind of naturally, it just became ubiquitous.*" The technical arrangement stayed the same. What changed was its meaning. P13's trajectory runs the opposite direction but lands in the same place. As a teenager she resisted tracking for years (Section 4.2.2), but her objections could not be voiced and went into workarounds instead, because the tracking was framed as love, and contesting it meant contesting the care. After she moved away, the app came to feel "*kind of cute*" once it told her when family arrived home (Section 4.1.2). Distance created a gap in awareness, and the notifications helped fill it. P6 and P12 (Section 4.1) show where these arcs end: arrangements that began instrumentally came to be experienced as love and co-presence. Where prior literature [11, 23, 37] treats care as the frame surveillance borrows, we find care is the mechanism through which surveillance reproduces itself, and that this operates on both sides of the arrangement: trackers framed monitoring as an expression of care—protecting, coordinating, keeping an eye on loved ones—and some of the tracked, like P6, came to experience being watched as being cared for.

Foundational intimacy theory supports this dynamic by arguing that closeness is produced by disclosure [24] and depends on the possibility of withholding [2]. Continuous location-sharing collapses this: when visibility becomes a background condition, removing it is not a privacy choice but a relational one [7]. Our findings extend this—once a single disclosure activates the sharing arrangement, closeness accumulates automatically, in the background, independent of intention. If continuous visibility produces intimacy rather than expressing it, privacy controls alone are insufficient. They address access, not attachment [8]. The design challenge is how tracking systems can support exit from arrangements that users experience not as a feature they enabled, but as part of the relationship itself.

5.1.2 Specifying What Privacy Theory Leaves Underspecified. HCI's privacy frameworks have progressively better explained why privacy in close relationships is hard to exercise. Palen and Dourish frame privacy as ongoing boundary negotiation [43]; Nissenbaum evaluates flows against relational context norms [41]; McDonald and Forte show that power asymmetries determine whose practices constitute those norms [38]. Each makes an advance. Each nonetheless assumes that some form of negotiation remains available—that the design task is to characterize or protect it. Our findings show where that assumption breaks down in close relationships. P13's resistance could not be voiced (Section 4.2.2): contesting the tracking meant contesting the love it expressed, leaving resistance no open outlet. P6 accepted a one-sided arrangement on those terms because challenging it meant challenging the care structure the relationship was built on. The problem is not an information flow violation. Continuous tracking *is* the norm in which the relationship operates. Amirkhani et al. [3, 4] describe a similar silence in romantic partnerships: people avoid explicit privacy negotiation because speaking up risks being read as mistrust or accusation. In location sharing, and across the relationship types we studied, silence is sustained not only by that risk but by location-sharing itself having become a source of care and closeness. Visibility mediates care, sustains intimacy, and hardens prior consent into relational obligation. The issue, then, is not only that preferences remain unspoken, but that continuous tracking becomes infrastructural to the relationship, making renegotiation difficult both relationally and practically.

Researchers studying bystanders and non-primary users of networked sensing typically define these roles by who adopted, configured, or owns a device [9, 44, 68]. In *surveillance intimacy*, these roles are more fluid. Many of our participants had opted in on their own devices and had the technical ability to stop sharing at any time, positioning them as primary users. Yet within the same arrangement, they were also continuously visible to others, occupying a position closer to that of a bystander or incidental user [28] whenever they were the ones being watched. As everyday tuning shows, some participants were also unsure what the technologies would communicate if they paused or stopped sharing. In surveillance intimacy, who holds the controls matters less than who can use them without concern that the change will read as a withdrawal of care.

5.1.3 Naming the Condition Upstream of Coercive Control. The tech-abuse literature reviewed in Section 2.4.3 documents the far end of the continuum on which *surveillance intimacy* sits. Our findings add an account of the upstream condition: the care framing that perpetrators use may not originate in abuse but be borrowed from the ordinary relational logic of close relationships. Parents granting teens independence through tracking (P8), siblings checking safe arrival (P13)—these are the relationships that establish visibility as an expression of love, long before coercion enters the picture. That prior relational ground is what makes the care narrative so readily available and so difficult to contest. The relational infrastructure that makes P6's mother's routine checks feel like care is the same infrastructure that lets P15 set up tracking his mother never fully understood and frame it as stewardship. P1's account shows the far end of this continuity: her friend's hidden AirTag rested on property rather than care ("*it's my car,*" as P1 recounted her friend's reasoning), yet relied on the same normalized infrastructure and the same foreclosure of directly asking. The way these justifications were layered suggests that when care alone no longer felt sufficient, ownership became an additional resource for rationalizing ongoing surveillance. The distance between these cases is a matter of degree and acknowledgment. By theorizing the upstream condition—how care and visibility become fused in ordinary relationships—the four dynamics extend the abuse literature's account of why the care frame is so durable and why exit from it is so hard to secure. The design challenge is to address surveillance tensions while maintaining relational meaning—something existing privacy paradigms were not built to do. We close by examining what designing for this requires, and where design's reach ends.

5.2 Designing for Sociotechnical Systems of Care

Care ethics scholarship establishes care not as sentiment but as relational practice—ongoing, asymmetric, and structurally distributed [19, 58]. HCI has begun to take this seriously, examining care as a design resource [57, 63], a site of labor [30], and a lens for rethinking security [62]. *Surveillance intimacy* extends this line of work by showing that care is not only a context in which technology operates—it is the mechanism through which certain sociotechnical arrangements become difficult to contest. Four design principles follow from this, addressed in turn to the relational meaning of exit, the distribution of its cost, the opacity of platform mechanics, and the granularity of what sharing exposes. These principles identify design directions that address the relational conditions our findings surface—conditions in which expressing a preference is costly—while acknowledging that empirical evaluation and safety-specific design for abuse contexts remain critical future work.

5.2.1 Make renegotiation legible as care, not its withdrawal. The problem is not that participants lack a way to stop sharing; it is that every available option communicates something about the relationship. P9 observed that stopping sharing on Find My can get "*messy*" because, as she understood it, the other person receives a notification; P10 read such a notice as "maybe they don't trust me." A system in which visibility can lapse softly—indistinguishably from a dead battery, not

announced as a deliberate choice—severs the connection between technical recalibration and social signal. At the same time, such soft lapses carry real risk in contexts of intimate partner violence or coercive control, where disappearing from a safety network without warning can increase danger and where abusers may exploit ambiguity to intensify monitoring or retaliation [14, 22]. Any implementation of soft lapses would therefore need to be accompanied by safety-centered safeguards and explicit guidance for high-risk users. Time-bounded sharing with logistically framed renewal prompts—"your sharing from last week is still active; continue?"—might make the end of sharing feel like completion rather than rejection, creating occasions in which renegotiation is part of the relational grammar rather than a challenge to it.

5.2.2 Mutualize the occasion of renegotiation to redistribute its relational cost. In our data, the labor of managing visibility fell mostly on those with the least power to renegotiate openly. P13, as a teenager, hid behind airplane mode and battery saver; P7's son managed his visibility through an incomplete opt-out that P7 exploited—not maliciously, but because the care relationship already licensed her access. Design cannot resolve the underlying power asymmetry, but it can refuse to amplify it. Surfacing, for both parties simultaneously, how often location is accessed versus shared makes legible what *surveillance intimacy* renders invisible—creating conditions for conversation that do not begin from grievance. Asked whether she would want to be notified each time her mother looked, P6 said: *"I would like that actually… I think that might make me feel a little bit better."* For example, a system could provide periodic, joint summaries such as "You have shared location continuously for three months; your friend has checked it 10 times," accompanied by a neutral prompt inviting both parties to review or adjust the arrangement together. We offer this as a hypothetical illustration to show how renegotiation might be framed as shared maintenance rather than unilateral withdrawal.

5.2.3 Surface the mechanics of visibility to those who are trying to tune it. Everyday tuning depends on platform literacy that platforms do little to support. P6 had not considered airplane mode as a privacy tool until the interviewer raised it; P7's son appears not to have known that disabling Find My left his AirPods visible to her. In both cases, the platform's opacity undermined an attempted opt-out—and that opacity is not neutral. When platform mechanics are legible primarily to those with greater technical familiarity, and when technical familiarity aligns with relational power, the platform amplifies an asymmetry it did not create.

We acknowledge that this is a legibility suggestion, and we have argued that the legibility model's central limitation is its assumption that dissatisfaction will surface as an adjustable preference. That critique stands: knowing what airplane mode does does not resolve the relational cost of using it. But legibility is a necessary condition even where it is not sufficient. The design implication is therefore modest: to make mechanics legible to users already trying to tune their own visibility, surfacing what any opt-out action does and does not change across associated devices, and communicating the difference between a deliberate withdrawal and a signal dropout: distinctions that currently exist only in the platform's implementation, often invisible to the user who needs them. Prior work on privacy notice design establishes that effective notices must be timely, contextually relevant, and actionable [47], criteria current platforms fail to meet at the moments users attempt to recalibrate their visibility.

5.2.4 Separate the care function of visibility from its surveillance function. Current platforms bundle welfare confirmation and location audit into a single indistinguishable act. When P6's mother checks her location to manage anxiety, she receives both reassurance and a continuous record of her daughter's movements. P6 valued her mother having the first; the platform offered no way to provide one without the other. Some tools now separate the two for a single occasion: Apple's

Check In and Google's Safety Check confirm arrival or welfare for a single session and share location only if the user fails to respond. Arrival alerts within continuous-sharing platforms, such as Life360's No-Show Alerts and Snap Map's Arrival Notifications, instead build on existing location sharing, and Life360's are set by the tracker, extending continuous visibility rather than replacing it. Neither approach matches the standing arrangements our participants described, in which they wanted reassurance daily rather than for one trip or time window. A standing, low-granularity welfare signal (arrived, home, okay), with detailed location reserved for explicit, time-bounded consent, would let the care relationship continue without full surveillance exposure. Coarse signals still convey information ("not home" at 2 a.m. is a disclosure), so granularity becomes part of the arrangement to be renegotiated rather than a fixed setting: for adults, something the person being seen can adjust; for children, something that can loosen as they gain independence.

5.2.5 Acknowledge design's limits. These principles address the surface at which design can intervene. They cannot resolve the relational conditions that make *surveillance intimacy* durable in the first place—the power asymmetries, the care obligations, the absence of a livable position from which to contest an arrangement that has come to mean the relationship itself. P13's resistance could not be voiced because the relationship had already foreclosed the question; it instead went into airplane mode and battery-saver workarounds. Design can create conditions for renegotiation; it cannot make renegotiation safe when the relational stakes are high enough. Some of these principles also carry risks that design cannot fully resolve. As noted in Section 5.2.1, soft lapses could serve someone managing unwanted surveillance or let someone in danger disappear from a safety network unnoticed. We do not think this tension defeats the principle, but it does mean that features designed to redistribute visibility labor cannot be evaluated in isolation from the relational contexts they enter—and that the populations the tech-abuse literature documents require separate, safety-centered design consideration that these principles do not provide. What lies beyond design's reach—how relationships enter and exit *surveillance intimacy* arrangements over time, and whether the dynamics we document are reversible—is the empirical and theoretical work this concept opens rather than closes.

5.3 Limitations and Future Directions

Here we consider how the limitations outlined in Section 3.4 shape the claims we make about *surveillance intimacy*. Our claims are grounded in 15 interviews from a specific regional and demographic context, conducted at a single moment in arrangements that evolve over years. The care-as-mechanism argument is strongest for the parent-child and intergenerational relationships that dominate our data; its operation in romantic partnerships and friend groups—where power asymmetry is less structural—was present but requires further elaboration. Future work should examine whether the mechanism operates differently in relationships of greater formal equality and whether cultural contexts beyond those represented in our data produce different configurations of care, visibility, and the social cost of renegotiation.

The single-sided interview design constrains the theoretical claims most directly: our account of how the care frame travels from tracker to tracked rests on one party's reconstruction of an arrangement with one exception (the married couple). We cannot determine from our data whether the care frame operated symmetrically, or only appeared to from the position of the person who described it. A dyadic and longitudinal design could show whether, and how, *surveillance intimacy* is co-produced from both parties.

Additionally, our participant group skews toward women (12 of 15), which limits the transferability of our findings across gender. This may partly reflect differential uptake of location-sharing practices, but it may also reflect something analytically relevant: feminist care ethics scholarship

has long argued that care reasoning is unevenly distributed along gender lines, with women more likely to frame relational obligations in the expression of care [19, 59]. If care is both the mechanism we theorize and a framework women are more likely to inhabit, our findings may be more descriptive of how *surveillance intimacy* operates for women than across the fuller range of people who use location-sharing technologies. Whether men experience and rationalize continuous visibility through different moral frameworks—ownership, responsibility, or protection rather than care per se—is an open question future work should pursue.

6 Conclusion

Location-sharing technologies did not create the conditions this paper documents. They inherited them. The practices of care that make continuous visibility feel like love—attending to someone's whereabouts, worrying about their safety, wanting to know they arrived—are older than any app. Platforms like Find My and Life360 render those dynamics technical, persistent, and difficult to exit without social consequence. In doing so, they become infrastructure not just for coordination but for the relational obligations that coordination encodes.

CSCW and HCI have long understood that systems do not merely support social practices; they shape them, sediment them into background conditions, and make some arrangements easier to sustain than others. *Surveillance intimacy* extends this insight to a domain the field has tended to analyze at its extremes: the caring uses of location-sharing on one end, the coercive on the other. What our findings reveal is that the mechanism connecting those ends is neither intent nor platform design alone, but the ordinary relational work of care—and that this work is already underway, in arrangements no one would call harmful, long before coercion becomes legible as such.

This has consequences for how the community designs, studies, and evaluates location-sharing systems. Consent flows, privacy dashboards, and granular sharing controls—the legibility model that has organized our field's design imagination—address a problem of preference expression. *Surveillance intimacy* identifies a different problem: one in which preferences are not hidden but structurally unspeakable, and in which the relational cost of exercising a technical option can exceed the cost of forgoing it. Systems designed without accounting for that asymmetry do not leave it unaddressed—they resolve it by default in favor of whoever holds more relational power.

The questions *surveillance intimacy* opens are ones our community is well-positioned to pursue: how do sociotechnical systems participate in the normalization of visibility over time? What would longitudinal or dyadic methods reveal about how care framings shift as relationships change? And what does it mean to design for renegotiation in arrangements where the relationship itself is what is at stake?

This study demonstrates how location-sharing technologies are not simply tools for convenience or safety, but instead embed new forms of *surveillance intimacy* into everyday life. *Surveillance intimacy* names a condition that accounts for the relational arrangement in which intimacy, care, and continuous visibility become mutually constitutive, each sustaining and intensifying the other. Through fifteen interviews across diverse close relationships, we have documented four dynamics through which this condition takes hold—relational visibility constituted as care, sharing as a relational obligation, moral rationalization as ongoing ethical infrastructure, and quiet, everyday tuning as the covert labor of living inside an arrangement that is difficult to openly contest. This work offers pathways to move HCI towards sociotechnical systems of care—systems that make renegotiation legible as care rather than its withdrawal, that mutualize the relational cost of adjusting visibility, and that separate the care function of location-sharing from its surveillance function. These are not incremental improvements to existing paradigms. They are a different design target, addressed to a different problem: not the individual's capacity to express a preference, but the relational conditions under which any expression of preference becomes possible at all.

Acknowledgments

We thank all the individuals who participated in this study for their time and contribution. Further we thank Emily Tseng for her thoughtful input, which helped ground this work in feminist care ethics. This work has been supported by the US National Science Foundation under grants 2236822 and 2142795.

Author Contributions

CW led the framing, study design, data analysis, and writing, and developed the core theoretical argument. SM contributed to framing, study design, data analysis, theory development, writing, and revisions. AD contributed to data analysis, theory development, and writing, and provided substantive feedback on manuscript revisions. JP assisted with framing, study design, and manuscript revisions. All authors approved the final submitted version.

References

[1] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. 2020. Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (Oct. 2020), 1–28. doi:10.1145/3415187

[2] Irwin Altman, Anne Vinsel, and Barbara B. Brown. 1981. Dialectic Conceptions in Social Psychology: An Application to Social Penetration and Privacy Regulation. In *Advances in Experimental Social Psychology*, Leonard Berkowitz (Ed.). Vol. 14. Academic Press, 107–160. doi:10.1016/S0065-2601(08)60371-8

[3] Sima Amirkhani, Mahla Alizadeh, Farzaneh Gerami, Dave Randall, and Gunnar Stevens. 2026. "Talking about privacy always feels like opening a can of worms.": How Intimate Partners Navigate Boundary-Setting in Mobile Phone Without Words. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems* (Barcelona, Spain) *(CHI '26)*. Association for Computing Machinery, New York, NY, USA, Article 1208, 15 pages. doi:10.1145/3772318.3791972

[4] Sima Amirkhani, Farzaneh Gerami, Mahla Alizadeh, Dave Randall, and Gunnar Stevens. 2025. Privacy Silence: Trust and Boundary-Setting in Mobile Phone Use Within Intimate Relationships. In *Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (CHI EA '25)*. Association for Computing Machinery, New York, NY, USA, Article 449, 7 pages. doi:10.1145/3706599.3719752

[5] Rosanna Bellini, Emily Tseng, Nora McDonald, Rachel Greenstadt, Damon McCoy, Thomas Ristenpart, and Nicola Dell. 2021. "So-called privacy breeds evil": Narrative Justifications for Intimate Partner Surveillance in Online Forums. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (Jan. 2021), 1–27. doi:10.1145/3432909

[6] Cynthia L. Bennett, Daniela K. Rosner, and Alex S. Taylor. 2020. The Care Work of Access. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, 1–15. doi:10.1145/3313831.3376568

[7] Lauren Berlant. 1998. Intimacy: A Special Issue. *Critical Inquiry* 24, 2 (Jan. 1998), 281–288. doi:10.1086/448875

[8] Lauren Berlant. 2011. *Cruel Optimism*. Duke University Press, Durham, NC.

[9] Julia Bernd, Ruba Abu-Salma, Junghyun Choy, and Alisa Frik. 2022. Balancing power dynamics in smart homes: nannies' perspectives on how cameras reflect and affect relationships. In *Proceedings of the Eighteenth USENIX Conference on Usable Privacy and Security* (Boston, MA, USA) *(SOUPS'22)*. USENIX Association, USA, Article 37, 20 pages.

[10] Clara Berridge, Jodi Halpern, and Karen Levy. 2019. Cameras on Beds: The Ethics of Surveillance in Nursing Home Rooms. *AJOB Empirical Bioethics* 10, 1 (2019), 55–62. doi:10.1080/23294515.2019.1568320

[11] Julie Boesen, Jennifer A. Rode, and Clara Mancini. 2010. The domestic panopticon: location tracking in families. In *Proceedings of the 12th ACM international conference on Ubiquitous computing*. ACM, Copenhagen Denmark, 65–74. doi:10.1145/1864349.1864382

[12] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (Jan. 2006), 77–101. doi:10.1191/1478088706qp063oa

[13] Virginia Braun and Victoria Clarke. 2019. Reflecting on reflexive thematic analysis. *Qualitative research in Sport, Exercise and Health* 11, 4 (2019), 589–597. doi:10.1080/2159676X.2019.1628806

[14] Jimmy Briggs and Christine Geeng. 2022. BLE-Doubt: Smartphone-Based Detection of Malicious Bluetooth Trackers. In *2022 IEEE Security and Privacy Workshops (SPW)*. IEEE, San Francisco, CA, USA, 208–214. doi:10.1109/SPW54247.2022.9833870

[15] Barry Brown, Alex S. Taylor, Shahram Izadi, Abigail Sellen, Joseph Kaye, and Rachel Eardley. 2007. Locating Family Values: A Field Trial of the Whereabouts Clock. In *Proceedings of the 9th International Conference on Ubiquitous Computing (UbiComp 2007) (Lecture Notes in Computer Science, Vol. 4717)*. Springer, 354–371. doi:10.1007/978-3-540-74853-3_21

[16] Kevin Childs, Cassidy Gibson, Anna Crowder, Kevin Warren, Carson Stillman, Elissa M. Redmiles, Eakta Jain, Patrick Traynor, and Kevin R. B. Butler. 2024. "I Had Sort of a Sense that I Was Always Being Watched...Since I Was": Examining Interpersonal Discomfort From Continuous Location-Sharing Applications. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security* (Salt Lake City, UT, USA) *(CCS '24)*. Association for Computing Machinery, New York, NY, USA, 4197–4211. doi:10.1145/3658644.3690342

[17] Sunny Consolvo, Ian E. Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. 2005. Location disclosure to social relations: why, when, & what people want to share. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, Portland Oregon USA, 81–90. doi:10.1145/1054972.1054985

[18] Jessica Nihlén Fahlquist. 2015. Responsibility and Privacy — Ethical Aspects of Using GPS to Track Children. *Children & Society* 29, 4 (2015), 371–380. doi:10.1111/chso.12016

[19] Berenice Fisher and Joan C. Tronto. 1990. Toward a Feminist Theory of Caring. In *Circles of Care: Work and Identity in Women's Lives*, Emily K. Abel and Margaret K. Nelson (Eds.). SUNY Press, Albany, NY, 35–62.

[20] Colin Fitzpatrick and Jeremy Birnholtz. 2018. "I Shut the Door": Interactions, tensions, and negotiations from a location-based social app. *New Media & Society* 20, 7 (July 2018), 2469–2488. doi:10.1177/1461444817725064

[21] Michel Foucault. 1977. *Discipline and punish: the birth of the prison*. Pantheon, New York.

[22] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–13. doi:10.1145/3173574.3174241

[23] Katleen Gabriels. 2016. 'I keep a close watch on this child of mine': a moral critique of other-tracking apps. *Ethics and Information Technology* 18, 3 (Sept. 2016), 175–184. doi:10.1007/s10676-016-9405-1

[24] Anthony Giddens. 1992. *The Transformation of Intimacy: Sexuality, Love and Eroticism in Modern Societies*. Polity Press, Cambridge.

[25] Woodrow Hartzog. 2018. *Privacy's Blueprint: The Battle to Control the Design of New Technologies*. Harvard University Press.

[26] Karey Helms and Ylva Fernaeus. 2021. Troubling Care: Four Orientations for Wickedness in Design. In *Proceedings of the 2021 ACM Designing Interactive Systems Conference*. ACM, 789–801. doi:10.1145/3461778.3462025

[27] Zoë Hitzig. 2024. On the Grid: How Surveillance Became a Love Language. *The Drift* (Dec. 2024). https://www.thedriftmag.com/on-the-grid/

[28] Ohad Inbar and Noam Tractinsky. 2009. The incidental user. *Interactions* 16, 4 (July 2009), 56–59. doi:10.1145/1551986.1551998

[29] Maya A Kaneko, Caitlin Lustig, Daniela Rosner, and Audrey Desjardins. 2024. Care Layering: Complicating Design Patterns. In *Proceedings of the 2024 ACM Designing Interactive Systems Conference* (Copenhagen, Denmark) *(DIS '24)*. Association for Computing Machinery, New York, NY, USA, 1533–1546. doi:10.1145/3643834.3660740

[30] Cayla Key, Fiona Browne, Nick Taylor, and Jon Rogers. 2021. Proceed with Care: Reimagining Home IoT through a Care Perspective. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, Article 166. doi:10.1145/3411764.3445602

[31] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (Nov. 2018), 1–31. doi:10.1145/3274371

[32] Karen Levy. 2015. Intimate surveillance. *Idaho Law Review* 51, 3 (2015), 679–693.

[33] David Lyon (Ed.). 2006. *Theorizing Surveillance*. Willan. doi:10.4324/9781843926818

[34] Clara Mancini, Yvonne Rogers, Keerthi Thomas, Adam N. Joinson, Blaine A. Price, Arosha K. Bandara, Lukasz Jedrzejczyk, and Bashar Nuseibeh. 2011. In the best families: tracking and relationships. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, Vancouver BC Canada, 2419–2428. doi:10.1145/1978942.1979296

[35] Paolo Massa, Chiara Leonardi, Bruno Lepri, Fabio Pianesi, and Massimo Zancanaro. 2015. If You Are Happy and You Know It, Say "I'm Here": Investigating Parents' Location-Sharing Preferences. In *Human-Computer Interaction – INTERACT 2015*, Julio Abascal, Simone Barbosa, Mirko Fetter, Tom Gross, Philippe Palanque, and Marco Winckler (Eds.). Springer International Publishing, Cham, 315–332.

[36] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F. Churchill, and Sunny Consolvo. 2017. Stories from Survivors: Privacy & Security Practices when Coping with Intimate Partner Abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 2189–2201. doi:10.1145/3025453.3025875

[37] Jane Mavoa, Simon Coghlan, and Bjørn Nansen. 2023. "It's About Safety Not Snooping": Parental Attitudes to Child Tracking Technologies and Geolocation Data. *Surveillance & Society* 21, 1 (March 2023), 45–60. doi:10.24908/ss.v21i1.

15719

[38] Nora McDonald and Andrea Forte. 2020. The Politics of Privacy Theories: Moving from Norms to Vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Honolulu HI USA, 1–14. doi:10.1145/3313831.3376167

[39] Carman Neustaedter and Saul Greenberg. 2012. Intimacy in Long-Distance Relationships over Video Chat. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2012)*. ACM, 753–762. doi:10.1145/2207676.2207785

[40] Helen Nissenbaum. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford Law Books.

[41] Helen Nissenbaum. 2011. A Contextual Approach to Privacy Online. *Daedalus* 140, 4 (Oct. 2011), 32–48. doi:10.1162/DAED_a_00113

[42] Ihudiya Finda Ogbonnaya-Ogburu, Angela D.R. Smith, Alexandra To, and Kentaro Toyama. 2020. Critical Race Theory for HCI. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–16. doi:10.1145/3313831.3376392

[43] Leysia Palen and Paul Dourish. 2003. Unpacking "privacy" for a networked world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, Ft. Lauderdale Florida USA, 129–136. doi:10.1145/642611.642635

[44] James Pierce, Claire Weizenegger, Parag Nandi, Isha Agarwal, Gwenna Gram, Jade Hurrle, Hannah Liao, Betty Lo, Aaron Park, Aivy Phan, Mark Shumskiy, and Grace Sturlaugson. 2022. Addressing Adjacent Actor Privacy: Designing for Bystanders, Co-Users, and Surveilled Subjects of Smart Home Cameras. In *Designing Interactive Systems Conference*. ACM, Virtual Event Australia, 26–40. doi:10.1145/3532106.3535195

[45] Eimaan Saqib, Shijing He, Junghyun Choy, Ruba Abu-Salma, Jose Such, Julia Bernd, and Mobin Javed. 2025. Bystander Privacy in Smart Homes: A Systematic Review of Concerns and Solutions. *ACM Transactions on Computer-Human Interaction* 32, 5 (Oct. 2025), 1–43. doi:10.1145/3731755

[46] Peter Schaar. 2010. Privacy by Design. *Identity in the Information Society* 3, 2 (2010), 267–274. doi:10.1007/s12394-010-0055-x

[47] Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. 2015. A design space for effective privacy notices. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security* (Ottawa, Canada) *(SOUPS '15)*. USENIX Association, USA, 1–17.

[48] Emily Schildt, Martin Leinfors, and Louise Barkhuus. 2016. Communication, Coordination and Awareness around Continuous Location Sharing. In *Proceedings of the 19th International Conference on Supporting Group Work*. ACM, Sanibel Island Florida USA, 257–265. doi:10.1145/2957276.2957289

[49] Christina Schneegass, Diana Irmscher, Florian Bemmann, and Daniel Buschek. 2021. LYLO – Exploring Disclosed Configurations for Inter-Personal Location Sharing. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI EA '21)*. Association for Computing Machinery, New York, NY, USA, Article 320, 6 pages. doi:10.1145/3411763.3451652

[50] Irina Shklovski, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and creepiness in app space: perceptions of privacy and mobile app use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14)*. Association for Computing Machinery, New York, NY, USA, 2347–2356. doi:10.1145/2556288.2557421

[51] Brian Simpson. 2014. Tracking children, constructing fear: GPS and the manufacture of family safety. *Information & Communications Technology Law* 23, 3 (Sept. 2014), 273–285. doi:10.1080/13600834.2014.970377

[52] Valerie Steeves and Olaf Blaschke Jones. 2010. Editorial: Surveillance, Children and Childhood. *Surveillance & Society* 7, 3/4 (2010).

[53] Neilly H. Tan, Richmond Y. Wong, Audrey Desjardins, Sean A. Munson, and James Pierce. 2022. Monitoring Pets, Deterring Intruders, and Casually Spying on Neighbors: Everyday Uses of Smart Home Cameras. In *CHI Conference on Human Factors in Computing Systems*. ACM, New Orleans LA USA, 1–25. doi:10.1145/3491102.3517617

[54] Karen P. Tang, Jialiu Lin, Jason I. Hong, Daniel P. Siewiorek, and Norman Sadeh. 2010. Rethinking location sharing: exploring the implications of social-driven vs. purpose-driven location sharing. In *Proceedings of the 12th ACM international conference on Ubiquitous computing*. ACM, Copenhagen Denmark, 85–94. doi:10.1145/1864349.1864363

[55] Xinru Tang, Gabriel Lima, Li Jiang, Lucy Simko, and Yixin Zou. 2025. Beyond "Vulnerable Populations": A Unified Understanding of Vulnerability From A Socio-Ecological Perspective. *Proceedings of the ACM on Human-Computer Interaction* 9, 2 (May 2025), 1–30. doi:10.1145/3710935

[56] Lisa Thomas, Pam Briggs, and Linda Little. 2013. Location tracking via social networking sites. In *Proceedings of the 5th Annual ACM Web Science Conference*. ACM, Paris France, 405–412. doi:10.1145/2464464.2501852

[57] Austin Toombs, Laura Devendorf, Patrick Shih, Elizabeth Kaziunas, David Nemer, Helena Mentis, and Laura Forlano. 2018. Sociotechnical Systems of Care. In *Companion of the 2018 ACM Conference on Computer Supported Cooperative Work and Social Computing*. ACM, 479–485.

[58] Joan C. Tronto. 1993. *Moral Boundaries: A Political Argument for an Ethic of Care.* Routledge, New York.
[59] Joan C. Tronto. 1998. An Ethic of Care. *Generations: Journal of the American Society on Aging* 22, 3 (1998), 15–20.
[60] Janice Y Tsai, Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. 2010. Location-Sharing Technologies: Privacy Risks and Controls. *I/S: A Journal of Law and Policy for the Information Society* 6, 2 (2010), 119–152.
[61] Emily Tseng, Rosanna Bellini, Nora McDonald, Matan Danos, Rachel Greenstadt, Damon McCoy, Nicola Dell, and Thomas Ristenpart. 2020. The tools and tactics used in intimate partner surveillance: an analysis of online infidelity forums. In *Proceedings of the 29th USENIX Conference on Security Symposium (SEC'20).* USENIX Association, USA, Article 107, 17 pages.
[62] Emily Tseng, Mehrnaz Sabet, Rosanna Bellini, Harkiran Kaur Sodhi, Thomas Ristenpart, and Nicola Dell. 2022. Care Infrastructures for Digital Security in Intimate Partner Violence. In *CHI Conference on Human Factors in Computing Systems.* ACM, New Orleans LA USA, 1–20. doi:10.1145/3491102.3502038
[63] Zixuan Wang, Yuanrong Guo, Eilidh Bowman, Yuxiang Zhai, Xinhuan Shu, Shengchen Zhang, Karey Helms, Tara Capel, and John Vines. 2026. Caring about Care: A Meta-Narrative Review of HCI Research on Care. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems.* ACM. doi:10.1145/3772318.3790811
[64] Sarah Widmer and Anders Albrechtslund. 2021. The ambiguities of surveillance as care and control: Struggles in the domestication of location-tracking applications by Danish parents. *Nordicom Review* 42, s4 (Sept. 2021), 79–93. doi:10.2478/nor-2021-0042
[65] Jason Wiese, Patrick Gage Kelley, Lorrie Faith Cranor, Laura Dabbish, Jason I. Hong, and John Zimmerman. 2011. Are you close with me? Are you nearby?: Investigating social groups, closeness, and willingness to share. In *Proceedings of the 13th International Conference on Ubiquitous Computing.* ACM, Beijing China, 197–206. doi:10.1145/2030112.2030140
[66] Maximiliane Windl and Sven Mayer. 2022. The Skewed Privacy Concerns of Bystanders in Smart Environments. *Proceedings of the ACM on Human-Computer Interaction* 6, MHCI (Sept. 2022), 1–21. doi:10.1145/3546719
[67] Richmond Y. Wong, Jason Caleb Valdez, Ashten Alexander, Ariel Chiang, Olivia Quesada, and James Pierce. 2023. Broadening Privacy and Surveillance: Eliciting Interconnected Values with a Scenarios Workbook on Smart Home Cameras. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference.* ACM, Pittsburgh PA USA, 1093–1113. doi:10.1145/3563657.3596012
[68] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 1–24. doi:10.1145/3359161

Received 31 March 2026; revised 17 July 2026; accepted 17 September 2026