The PET Paradox: How Amazon Instrumentalises PETs in Sidewalk to Entrench Its Infrastructural Power

Thijmen van Gend
Netherlands Organisation for Applied Scientific Research (TNO) &
Delft University of Technology
t.n.vangend@tudelft.nl

Donald Jay Bertulfo
Delft University of Technology
d.j.bertulfo@tudelft.nl

Seda Gürses
Delft University of Technology
f.s.gurses@tudelft.nl

Abstract

Privacy engineers originally conceptualised Privacy Enhancing Technologies (PETs) to pursue data minimisation, purpose limitation, and trust minimisation (avoiding single points of failure); thereby curbing corporate and state power over people. Through a review of Google and Apple applications, and an in-depth case study of cloud connectivity service Amazon Sidewalk, we show how companies with concentrated power over computational infrastructures implement PETs with paradoxical effects. These companies can deploy PETs on large swaths of devices – a huge benefit – while introducing new capabilities and expanding their control over devices, OSes, and applications. In doing so, these companies increase their informational, market and infrastructural power. To reveal how these paradoxes come to be, we apply a broader framework including how the design of PETs impacts (1) information flows, (2) consumer privacy, (3) infrastructural companies' control over consumer devices, and (4) business-to-business (B2B) and -government (B2G) relationships implicated by these; focussing on (3) and (4). We analyse the consequences for information, market and infrastructural power asymmetries, that affect consumers, businesses, and governments, and shape the future implementation of PETs. For the Google and Apple cases, we rely on desk research. For our case study into Amazon Sidewalk, we conduct elite interviews with 8 of the 16 adopting manufacturers. We triangulate results with Amazon's (technical) documentation and marketing as well as grey literature. We conclude by discussing how we should expand PET design and evaluation processes to avoid the paradoxical outcomes that these infrastructural players bring to being.

Keywords

privacy, privacy-enhancing technologies, PET paradox, power, production, computational infrastructure

1 Introduction

Over the last decade, there is increasing attention to the expanding power of *"Big Tech"* companies on other parties in health, law, public administration, science, education, finance, communication, (national) security, and more [e.g. 8; 174; 245; 246; 257]. Lynskey [174] argues that big tech companies possess *"data power"*: *"a multifaceted form of power ... arising from their control over data flows"* (p. 196). The volume and variety of the data that digital platforms have control over, determine how much they can surveil and profile people, and restrict or prioritise certain information flows over others, e.g. to influence how people form their opinions [174].

Increasingly, tech companies' amassing of personal and commercial data has raised surveillance [212; 282] and competition concerns [82; 147; 194; 233] in tandem. This has resonated with regulators: the European Commission has designated *inter alia* Google (ads, shopping, search, operating system, browser, app store), Apple (browser, app store) and Amazon (ads, shopping) as *"gatekeepers"* for *"core platform services"* [117]; and is currently investigating to appoint gatekeepers in cloud computing [116]. The EU's Digital Markets Act notes that these gatekeepers with considerable economic power have unique *"access to large amounts of data"*. Competition authorities have repeatedly ruled that tech companies leverage data for unfair competitive advantages [e.g. 95; 115].

If tech companies' expanding powers derive from control over vast data flows, then intuitively, Privacy Enhancing Technologies (PETs) should help to curb them. PETs are a family of technologies that engineers can utilise to provide mathematically supported privacy guarantees in systems that collect and process data, by hardwiring strict controls into the system design, in order to avoid privacy infringements and increasing information asymmetries [134; 145; 146]. Two principles have been central to PET development since the 1990s: privacy engineers strictly interpret data minimisation to the purpose of processing ('purpose limitation'), and develop distributed designs that minimise trust to avoid single points of (privacy) failure [67; 134; 145; 146]. More broadly, actors' potential to overreach using various sources of power (e.g. technical, legal), prevalently features in adversarial and threat models, underlining the importance of considering power asymmetries in designing PETs. Regulators have acknowledged this potential of PETs to minimise data and curb information power asymmetries towards states and companies alike: the EU's General Data Protection Regulation codifies privacy by design as a regulatory requirement to curb informational power asymmetries [see e.g. 60; 118; 151; 258].

Despite this promise, academics and competition authorities have raised issues with Google and Apple services that incorporate PETs to limit information flows. They argue that when these companies instrumentalise PETs to their advantage, this may constitute privacy [105; 248] or confidentiality washing [299–301], raise concerns around competition and public service delivery [283], and serve primarily to evade applicability of certain regulations regarding content moderation and data subject access requests [300; 310]. For instance, this has led to contentious use of PETs for *client-side scanning* [2]. Google and Apple also leveraged PETs to position

Proceedings on Privacy Enhancing Technologies 2026(4), 1124–1148

https://doi.org/10.56553/popets-2026-0163

themselves as arbiters of citizens' privacy vis-à-vis health authorities and researchers for Covid-19 *digital contact tracing* (DCT). Accordingly, the companies shaped how they could *"produce"* public health services Troncoso et al. [283]. With their forays into privacy preservation in *digital advertising*, authorities found, these companies entrenched their position in the business models and production processes of other companies in the digital advertising space [e.g. 64; 93; 99]. Further, with its crowdsourced *device finding* service, Apple is said to use security and privacy constraints to gatekeep and self-preference in relation to third-party tracker companies [97; 234]. By introducing PETs, Apple and Google avoid a privacy backlash even as they transform *"personal devices"* (i.e. smartphones) into an infrastructure for DCT, advertising, and device-finding services offered to users and third parties. PETs, they argue, serve to protect consumers from them (i.e. in business-to-consumer (B2C) relations), while entrenching the companies' own role in how other businesses (B2B) and governments (B2G) can deliver their services (DCT, advertising, and device finding) to these same consumers. The examples point to a curious paradox: these companies apply PETs in ways that can limit information flows they are privy to *and* accentuate their data, market and infrastructural power.

Our objective is to empirically study how this paradox comes to be, to identify its repercussion for the design and implementation of PETs. We focus specifically on the conditions of *software production* under which these PETs get deployed to study how they impact who can engineer PETs and to what purpose. 'Software' includes operating systems (OSes), protocols, web browsers, app stores and apps. Our *production view* emphasises how manufacturers' production processes change in adopting tech companies' infrastructures (hardware and software environments where they set production conditions); what role PETs play; and what power dynamics arise. Previous work has shown that by now standard industry practice of engineering software using a server-client model and agile methods are relevant for successfully designing and deploying of PETs [67; 164; 166]: in this *software production paradigm*, *"end devices"* have become vessels for delivering services, rather than being stand-alone products with a specific and fixed purpose. Consumer devices are integrated into the production of consumer software: software is continuously updated and reconfigured (downstream), while providing telemetry and feedback to its manufacturer (upstream) [135]. As a result, end devices become practically *accessories* of a company's *computational infrastructures*, and companies like Google and Apply can push PETs to billions of devices; a big win. Though, the paradoxical cases above show that they can also use it to flip devices from accessories into *extensions of their computational infrastructures* for services developed or used by third-parties (B2B), with considerable impact for PETs and beyond.

Our empirical case is Amazon's *"Sidewalk"* service. Amazon pitches Sidewalk as a crowdsourced networking service where non-Amazon IoT devices (*"endpoints"*) in the US can connect to a nearby Amazon Echo or Ring device (*"gateways"*, potentially owned by someone else). Unless gateway owners have opted out, this gateway shares part of its own wifi bandwidth with the endpoint, for the endpoint to communicate with its manufacturer's *"Application Server"* through and in Amazon's cloud (Amazon Web Services (AWS)) [39]. The network boasts coverage of about 95% of the US population [37]; public numbers for Canada and Mexico lack. The service has a double role: for consumers (B2C), it is a shared community-focused network, while for manufacturers (B2B), Sidewalk offers the possibility to remotely manage their devices through AWS.

We analyse Sidewalk from both a consumer (B2C) and manufacturer (B2B) viewpoint, emphasising the latter. For consumers, we consider how Sidewalk affects information flows and autonomy over devices. For manufacturers, we assess how Sidewalk's PET design impacts their *"production"* of IoT devices and overlaying services. Our research question is: *Whether and how does Amazon instrumentalise PETs in entrenching its computational infrastructure as a production environment for IoT manufacturers?* In other words: does Amazon's deployment of PETs in their computational infrastructure achieve its intended privacy goals? And does it raise data, market or infrastructural power imbalances over production of services in B2B contexts? We adopt an empirical qualitative mixed methods approach to do so: we triangulate interviews with IoT manufacturers, against marketing statements by them and Amazon, analysis of technical Sidewalk documentation, and news coverage. We stop short of a quantitative study of the privacy protocol in order to first conceptualise where our current evaluation frameworks for PETs fall short. The case also has legal implications that sit at the intersection of privacy and competition law, towards the analysis of which we aim to lay the empirical foundation of one such complex case.[1] We consider a full analysis beyond scope, avoid taking any position on the question of compliance with US or other laws, and limit ourselves to including any existing legal references. To ensure usefulness, we integrate feedback from two previous presentations of this work at privacy and law conferences [295; 296].

The paper proceeds as follows. After detailing our approach (§2), we study: *How does Amazon's implementation of PETs shape user privacy and Amazon's control over information flows?* (§3). This part expands from a consumer-oriented (B2C) approach to PETs use, to include greater information flows in Sidewalk, including their impact on manufacturers (B2B). Next, we adopt the production view, asking: *How does Amazon's implementation and governance of PETs in Sidewalk affect manufacturers' production of IoT devices and services?* (§4). We focus on the actors; physical and digital inputs, outputs, and processes; and (software and hardware) production environments involved in producing Sidewalk and IoT services. We then explore other cases for common patterns in infrastructural players instrumentalising PETs, explore the resulting *"PET Paradox"* (§5), and discuss the paper's limitations (§6) and implications for the future design and evaluation of PETs (§7). In sum, we contribute:

- an analysis of the novel privacy threats that Sidewalk raises despite its deployment of PETs;
- a case study to explore PETs impact on consumers as well as market and infrastructural power;
- a description of the impact of Sidewalk's privacy design on consumers and manufacturers who produce IoT devices;
- an elaboration of the consequences of these power dynamics for how the design and evaluation of PETs in the future.

[1] To the best of our knowledge, no academic legal analyses of Sidewalk have been published, nor have legal or regulatory proceedings been brought forward. Exceptions are a dismissed [268] class action *"lawsuit [that] claims the technology could lead to surprise overage charges on consumers' internet bills"* [219] and lawsuit alleging that Tile trackers' integration with Sidewalk was vital to stalking by an ex-partner [160; 250]

2 Methods and case description

2.1 The Sidewalk architecture

To explain how Sidewalk works, we walk through an example of uplink data traffic (i.e. an endpoint sending data to an application server). Figure 1 visualises a smart home Sidewalk architecture where two gateways provide connectivity to four endpoints.

Sidewalk-compatible IoT devices are called *"endpoints"* and can be produced by Amazon and third-party manufacturers. Endpoints can connect to a nearby *"gateway"* with the Sidewalk protocol, that relays communication between the endpoint and the *"application server"* of its manufacturer. Gateways are Amazon Echo (smart speakers and displays) and Ring (smart cameras, lights, doorbells, and alarms) devices in the US that use a portion of their own wifi bandwidth for this communication [39]. The endpoint owner may be someone else than the gateway owner, benefiting from Sidewalk as a *"crowdsourced"* network [32]. A gateway can also act as endpoint, i.e. tap into the connectivity of other gateways.

The Sidewalk protocol utilises Bluetooth Low Energy (BLE), Frequency-Shift Keying (FSK), and a proprietary version of LoRa [42, p. 140]. These are intended for short, medium, and long ranges, respectively; with lower data rates for longer distances [42, p. 11]. Not all endpoints, nor all gateways support all three protocols [19; 32]. Gateways check whether endpoint packets comply with the protocol format specifications and that the endpoint is not blocked from Sidewalk [32].

Between the gateway and application server sits Amazon's *"Sidewalk Network Server"*, part of its *"cloud"* [42, p. 15]. It inspects all packages sent by the gateway; routes them to the application server; maintains time synchronisation of the network; and authenticates devices and application servers, verifying that Amazon has not blocked them from Sidewalk [32].

Finally, it is the manufacturer's *"application server"* that endpoint users interact with through the endpoint's accompanying smartphone or browser interface, e.g. to consult a tracker's location. This latter interaction is outside the Sidewalk scope [42]. The server comprises *"AWS IoT Core for Sidewalk"* and may integrate other AWS services. Manufacturers that want to manage their devices from outside AWS, must interface with IoT Core through a *"Topic"* or API [42, p. 42]. Seven out of eight interviewees picked the former option, thus we only pictured one application server outside AWS.

In Sidewalk, AWS has a dual role: Amazon uses it to manage the Sidewalk network (i.e. producing connectivity as a service to manufacturers), and manufacturers use it to manage their devices and produce services for their customers. Therefore, we refer to AWS as a *software production environment.*

2.2 How Sidewalk came to be

Understanding Sidewalk's history is fundamental for understanding the role of PETs and the power dynamics at play. Amazon revealed Sidewalk during a hardware conference in September 2019, describing a pilot with 700 gateways in Los Angeles [10]. A subsequent press release detailed that certain Ring cameras and lights could share their network connectivity with each other [11], if registered to the same user account.

In September 2020, Amazon announced that Sidewalk would be launching as a crowdsourced network later that year, and named the first third-party adopters [12]. The announcement references the first version of the Privacy and Security Whitepaper [13] (further: Whitepaper), published simultaneously. This is Amazon's first mention of *"privacy"* in the context of Sidewalk – presumably in response to the privacy concerns following the 2019 announcements [e.g. 86; 211; 235; 304]. In May 2021, Amazon announced a further roll-out and more third-party adopters [15]. In June, Amazon transformed Echo and Ring devices in the US into gateways, through an opt-out OTA update [81; 294]. An email notified Echo owners a month before this launch [192], and Echo and Ring owners received an in-app notification seven days beforehand [294]; a narrow window to opt out [126; 294]. Yet, in September, Amazon published interviews with executives from two adopters, emphasising that *"Sidewalk's potential begins with privacy protection"* [14]; presumably again in response to privacy concerns [e.g. 81; 203].

In March 2023, Amazon claimed that Sidewalk had coverage of over 90% of the US population (Figure 2 in §A.3) and opened the network for developer testing [18]. Shortly after, Amazon updated the Whitepaper, making Sidewalk opt-in for new Echo and Ring devices [17; 21]; though since a March 2025 revision, the Whitepaper again declares that Sidewalk participation for new gateways is opt-out, unless disabled by the user earlier [33]. In January 2024, an executive proclaimed 95% coverage [73]. The gateway role can be performed by 43 different Echo and Ring models [19], with *"more than 80 million"* devices contributing [31].

Amazon repeated this opt-out roll-out in Canada [35] and Mexico [36] in February 2026, informing Echo users by email one month prior [217; 227]. *"Other regions, including the EU, UK, Australia, New Zealand, and Japan"* are to follow later in 2026 [229].

Amazon promotes different aspects of Sidewalk to consumers (both gateway and endpoint owners; B2C) and manufacturers (B2B) (Figure 3 in §A.3). For consumers, Amazon emphasises community benefits, additional device coverage, security, privacy, and bandwidth constraints. Only the first two advantages demonstrate Sidewalk's functional value; the latter three serve as reassurances.

On the Sidewalk homepage, Amazon positions Sidewalk as *"a shared network that ... can unlock unique benefits for your device, support other Sidewalk devices in your community, and even locate pets or lost items"* [39] (Figure 3 *d*). Sidewalk's core proposition is to make IoT devices of all kinds *"work better at home and beyond the front door"* [39] by connecting them to the cloud [12; 32]. Gateway owners' participation is central hereto. Amazon therefore frames Sidewalk as a *"community benefit"*: a B2C service that enables other B2C services (e.g. Figure 3 *b* and *d*). Gateways *"share a small portion of your internet bandwidth which is pooled together to provide these services to you and your neighbors. And when more neighbors participate, the network becomes even stronger"* [39]. Gateway owners *"contribute [their] internet bandwidth to support community extended coverage benefits such as locating pets and valuables"* [32, p. 14; 39]. Similarly, one Amazon executive said that Sidewalk *"is best described as a community network"* [73, 19:51] and another likened it to *"his native village in Southern Spain, where residents make their own soap"* and share it with their neighbours, because *"people feel good sharing"* [14]. Gateway owners allegedly need not worry about helping their neighbours: Amazon warrants Sidewalk's security (Figure 3 *a* and *d*; discussed in §3.1) and caps gateways' bandwidth

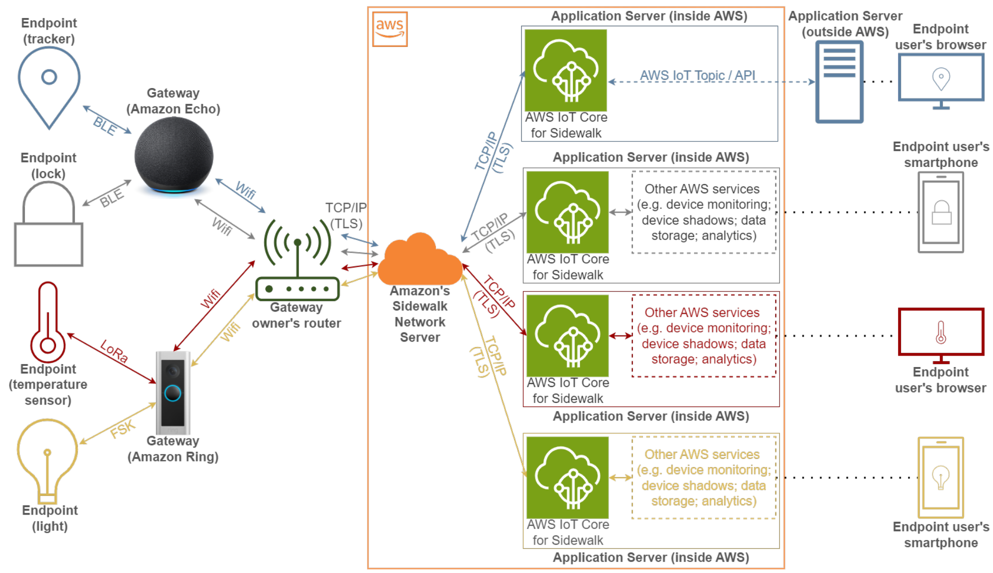

Figure 1: Example Sidewalk architecture, based on [42, pp. 14, 42; 48]. Echo and Ring images reproduced from [38; 232].

usage for Sidewalk at 500 MB per month per customer, at a bandwidth of at most 80 Kbps [32] (Figure 3 *c*).

Towards manufacturers, Amazon highlights opportunities for revenue generation and operational control over endpoints out in the world. Amazon paints Sidewalk as *"low cost"* [42, p. 11], and *"a secure, free-to-connect, long-range and low-power shared community network designed to provide connectivity for billions of devices"* [40; similarly in 18 and 42, p. 11]. More concretely, Amazon's promise is twofold. First are market opportunities: Sidewalk enables manufacturers *"to create and bring to market all types of consumer, enterprise, and public sector smart and connected devices and services"* [32, p. 2; 42, p. 45]. Endpoints may be stationary and close to homes (e.g. smart lights or motion detectors) or mobile and remote (e.g. asset trackers) [12]. Indeed, the sixteen adopters operate across various domains: logistics (five companies), in-home care (one company), utilities and industry (five companies), and building management (eight companies). Fifteen manufacturers design endpoints specifically for business or governmental users (B2B). Nine of these simultaneously sell to consumer users (B2C); although they generally focus on B2B markets. Most third-party manufacturers thus target organisations as endpoint buyers. In making this promise, Amazon depicts Sidewalk as *"a 'pipeline' that moves data back and forth between an Endpoint and its respective Application Server"* [32, p. 13; see also Figure 3 *c*], and a transport layer: *"[T]hey've been very clear [to me] that Sidewalk can do a lot of things: it's a transport layer and you can embed whatever you want into the payload. ... They said, 'remember, Sidewalk is merely a transport shell. What you put into the payload, that's totally your prerogative'"* [A6].

Second, the combination of AWS and Sidewalk connectivity promises manufacturers improved control over devices, and therefore improved development and maintenance of services. Having Sidewalk data and devices already in AWS lets manufacturers easily integrate AWS' various IoT services, that go well beyond offering flexible storage and compute. Manufacturers can utilise security-oriented cloud services [45], inspect and patch individual devices, and send firmware updates and files to multiple endpoints with *"Sidewalk Bulk Data Transfer"* [42, p. 173]. Further, AWS services enable monitoring endpoint usage; visualising metrics; detecting anomalies; managing digital *"device shadows"*; and inspecting, accessing, and updating individual devices [20; 46; 47]. Also, endpoints without GPS modules can be located with *"AWS IoT Core Device Location integration with Amazon Sidewalk"* [314]. This fulfils Sidewalk's promise of *"extending [device] lifecycle and capabilities, cost-efficiency in maintenance from remote operation, and [enabling] rapid prototyping"* [42, p. 173]. In that sense, Sidewalk and AWS may make manufacturers' production more agile [135]: an important reason for manufacturers to adopt AWS [A2; A6; A8].

2.3 Methods

We perform a single case study [267; 312] into Sidewalk with an empirical *"no theory first"* approach. This means we stay as close as possible to the case, given the nascence of relevant literature and complexity of the instances described therein. We iteratively combine three methods: a grey literature review, technical documentation analysis, and elite interviewing. This differs from a typical PETS user study: we intend to capture power imbalances that traditional user studies may not. While user and measurement studies would strengthen our B2C and privacy arguments, we deliberately centre a novel pertinent issue: how Sidewalk's instrumentalisation of PETs raises paradoxical effects in B2B spheres and for PETs.

As elaborated below, none of the methods is in isolation sufficient to answer our research questions. Each method has its strengths, biases, and oversights. Triangulation is necessary to balance the experiences of IoT manufacturers, reporting by journalists and civil society, and marketing statements and technology documentation by Amazon. Focusing on one case is common for deep case studies [e.g. 122]. The study remains reliable [312], as it is exemplary (reveals something of broader interest about the question), complete (exhausting literature, technical documentation, and possible interviewees (half of all 16 Sidewalk-adopting manufacturers)), and contains a chain of evidence (not giving evidence separately, but triangulating, and integrating findings into narrative form). Triangulating Sidewalk's different dimensions strengthens the qualitative inquiry, by not relying on one method or source, but using multiple methods to demonstrate convergences/divergences in the data [236]. Though, *"we know there is always more to know"* [113, p. 14].

Grey literature review. With the grey literature review, we aim to (1) understand what Sidewalk promises to users and manufacturers, as well as how manufacturers use it; (2) identify what privacy and security concerns civil society, researchers and (tech) journalists raised about Sidewalk; and (3) add to our broader assessment of how Amazon governs Sidewalk. For (1), we studied Amazon's Sidewalk documentation. In lieu of an Amazon-maintained list of adopters, we thoroughly Googled and searched through all Sidewalk-related publications from Amazon, tech news outlets, and manufacturers to identify third-party manufacturers that have adopted Sidewalk, and their offerings. We found sixteen organisations; see Table 2 in Appendix A. For (2), we performed a Google search for *"Amazon Sidewalk" AND privacy*. We supplemented this with a Google Scholar search for *"Amazon Sidewalk"*, which yielded few results mostly mentioning Sidewalk in passing. For (3), we analysed Sidewalk and AWS developer documentation and policies [28], and how these changed over time [152]. For contextualisation, we also examined broader offerings for connectivity (e.g., Matter).

Technical documentation analysis. To understand Sidewalk's framing of privacy risks and safeguards, and identify the promises of Sidewalk and AWS for improving manufacturers' production of IoT devices, we analysed the technical documentation of Sidewalk and AWS IoT services. We loosely coded the documentation to understand Sidewalk's architecture; its integration with Amazon's cloud; how Sidewalk compares to other IoT connectivity protocols and network architectures; how Amazon processes and secures Sidewalk data; and the requirements that manufacturers' production processes and endpoints must fulfil. We checked our understanding with four experts in the field of networking and PETs.

Elite interviewing. Given the case context and our focus on production, we adopted an elite interviewing approach with manufacturers [157; 168; 172; 215; 254; 290]. The goal is to explore their motivation for and experience with adopting Sidewalk. We asked how integrating Sidewalk impacts the production of their devices, software and services. As such, the interviews provide empirical insights into Sidewalk's effects on production, that enrich and validate the findings from the technical documentation analysis. Of the sixteen identified Sidewalk-adopting manufacturers, we invited 94 C-level executives, department heads and high-ranking engineers through LinkedIn, of which respectively four, two, and two participated. These positions presumably bring these elites comprehensive experience with both the business and technical implications of Sidewalk adoption. We refer to them as [A1] ... [A8], with the *A* abbreviating *"adopter"*. We supplemented this sample with one non-adopter [N1]: a C-level executive who is a prominent LoRaWAN industry figure. They helped clarify what sets Sidewalk apart from the LoRaWAN protocol. We conducted all interviews remotely between November 2023 and January 2024. Moreover, we approached 13 AWS and Lab126 employees on LinkedIn, and asked participants for their contacts inside Amazon, but received no responses. As speaking to Amazon employees was not necessary to answer our research questions, we halted our attempt to include them.

For interview analysis, we iterated through two coding cycles, following the manual of Saldaña [239] and using ATLAS.ti 23 [59]. Two coders participated in coding each transcript and discussed the findings with the third. We took a predominantly inductive approach. Concretely, we devised codes during the analysis and mainly in *in vivo* fashion to capture respondents' own language and sentiment. For the first cycle, we iteratively combined initial, structure, and process coding; and evaluation coding. The second cycle involved pattern coding and axial coding. We devised 330 codes across a three-tiered coding scheme. Appendix A provides the interview questions and an excerpt of the codebook.

Ethical principles. We only refer to interviewees by pseudonym and refrain from reporting quotes or attributions when these may compromise participant anonymity. Participants' names and affiliations were not shared with other participants. Respondents signed an informed consent form, stating that they were free to skip questions or quit at any time. We also shared the transcripts with participants, allowing them to redact or edit any statement. Nobody used this opportunity. Participants were not compensated. Our institutional review board approved this approach.

3 Information flows and PETs in Sidewalk

PETs in Sidewalk serve *"to secure data flows in Sidewalk and to keep customers safe and in control"* [39] and limit *"the collection and storage of customer information"* [32, p. 3]. The design principles are that gateway owners *"do not receive any information about devices owned by others connected to Sidewalk"* [39]; that *"information [endpoint] customers would deem sensitive, like the contents of a packet sent over the Sidewalk network"* is not visible to Amazon or gateway owners [32, p. 4]; and that *"tracking of devices and associating a device to a specific user"* by Amazon, gateway owners, and eavesdroppers is prevented [32, p. 4]. To this end, Sidewalk uses two classical PETs: end-to-end encryption (with three layers, shielding both payloads and metadata) and obfuscation (of endpoint and gateway credentials, and routing information) [32; 24; 42, chapter 4]. §B.2 shortly elaborates each. Our aim with this paper is to rethink the scope of evaluating PETs, hence we cursorily reflect on privacy risks before moving on to deliberate the role of PETs in *"flipping"* consumer devices for extending Amazon's computational infrastructure.

3.1 Information flows and user privacy: the role of PETs in flipping consumer devices

Sidewalk's proposition is to allow endpoint users and manufacturers to remotely manage their devices, by casting a vast crowdsourced network with gateways. This way, Sidewalk enables new information flows; on top of the original communications between the Echos/Rings and cloud for delivering the Echo and Ring services. These new information flows raise four privacy concerns: (1) increased surveillance of consumers by other consumers and law enforcement; (2) Amazon's and manufacturers' increased ability to monitor devices and user interactions; (3) further blurring of boundaries between private and public life; and (4) undermining owners' control over their personal devices. The proprietary design and poor transparency of Sidewalk's technical workings aggravate these concerns; a red flag for privacy and security communities. Furthermore, because Sidewalk – as it is currently rolled out – is opt-out and endpoints are designed to reveal information about their environment (e.g. when doors are opened or where sensors are travelling), gateway and endpoint owners (unwittingly) violate interdependent privacy from personal (non-users being 'sensed' by endpoints), relational (intermediating and revealing relations between device owners and non-users), and spatial (the possibility that devices operate in spaces not intended for them, e.g. consumer homes) perspectives [72].

Appendix B elaborates on these four issues. Here, it suffices to conclude that Amazon takes a narrow view on privacy in Sidewalk. Measures mitigate some personal data flows (e.g. in not telling gateway owners whose endpoint connects to their Echo/Ring) while side-lining contentious novel information flows (e.g. location of endpoints) and concerns about user autonomy. Design principles fundamental to PETs, i.e., data minimisation to purpose limitation and trust minimisation, are not part of Sidewalk's privacy measures; despite the existence of (partial) solutions proposed by PETs researchers [e.g. 155; 263; 264; 303]. Nevertheless, Amazon repeatedly refers to their (narrow) privacy protections and the Whitepaper to address the public's privacy pushback. Further, Amazon obfuscates that Sidewalk mostly serves B2B applications, by repeatedly pointing to the consumer-oriented *"community benefits"* (§A.3). Indeed, Amazon called one interviewee *"a very strong opportunity for Sidewalk to show off what it can do"*, and another recounts that Amazon used them *"as a pawn basically in the game, of showing that there's value to this network"*, showcasing their company's product to distract from the backlash. [A2] confirms this reading: *"it's very obvious if you look at the timeline of when things were released and how they were released and the emphasis on things ... They were very aware of the fact that people could have an adverse reaction"*.

In sum, Amazon reduces 'privacy' to the confidentiality of certain user data, that it claims to protect with PETs. With these concerns out of the way, Sidewalk *"flips"* consumer Echo and Ring devices to become 'gateways' without further backlash. Through flipping consumer devices to gateways, Amazon *extends their AWS cloud services* with a network covering over 90% of the US population. This flipping enables plenty of information from endpoints, and control over them, to flow between endpoints, gateways, manufacturers, and AWS; exposing millions to a range of new privacy risks.

From a software production point of view, this network of consumer devices-cum-gateways, plus the AWS cloud services to manage endpoints, together constitute a production environment for IoT manufacturers to manage their devices and develop overlaying services (§A.3). Repurposing consumer devices spares Amazon the costly endeavour of building out and maintaining a dedicated connectivity infrastructure for this. Rather, Echo and Ring owners buy a device, deploy it across the country, provide it with wifi and electricity, and troubleshoot it; and ISPs move the packets between gateways and Amazon's cloud. In exchange, gateway owners are offered narrow privacy guarantees and a narrative of altruism – if they discover their participation at all.[2]

3.2 Information flows and manufacturers' confidentiality

The new information flows in Sidewalk benefit IoT manufacturers but, as our documentation review and interviews showed, also expose business-sensitive information to Amazon. Amazon has insight into a swath of telemetry (Table 1) that lets Amazon monitor the integrity and reliability of Sidewalk: *"they need metrics to see if things actually work"* [A2, A6]. This telemetry also tells Amazon the demand for endpoints of each manufacturer and their application domain. Two interviewees said they expect, and two confidently asserted that Amazon is using their vantage point for this purpose. [A1; A4] brought up that Amazon has done something similar on their Marketplace: recurrently utilising data of third-party sellers to replicate high-demand products under their own brands [115; 159; 179]. One interviewee was concerned about this, *"but in the end there's not a whole lot [they] can do about it, you know, aside from government action or lawsuits"*. Five were not concerned, thinking Amazon will not enter their line of business [A3; A5] or believing in their own company's capabilities [A2], intellectual property and patents [A3], and established brand name [A3] to outcompete them (*"Bring them on!"* [A2]). Further, multiple participants believe that Amazon's Sidewalk endeavour, even when selling similar competing endpoints, helps educate and grow their markets. [A2; A7; N1] pursue short-term revenue gain while acknowledging long-term risks for their competitiveness against Amazon, in what one interviewee called *"coopetition"*.

Beyond demand, telemetry might inform Amazon about endpoint *"power usage, connectivity usage, and data transfer"* patterns [A8], and *"help them if they were gonna do things like [design] their battery model for their [device] and figure out how many times someone [triggers the device] or something like that"* [A1]. Three interviewees supposed that the encryption of payload data inhibits such learning or that this knowledge is not so valuable that it would warrant *"stealing information"*. Table 1 disproves the former.

Finally, with its insight into endpoint behaviours and how manufacturers manage them in AWS, Amazon can improve AWS for IoT manufacturers at large. As [A4] put it: *"To credit Amazon, with AWS in particular, ... they also did a great job of seeing what customers were doing with their products and introducing new services that better met those needs. So they're very good at that. To what extent are they doing that with Sidewalk? I honestly don't know. But I'm sure they are."* Optimising AWS as a software production environment aligns with [A5]'s conception of the AWS business model: *"the business model is 'data has gravity'. So they want the data coming to AWS. ... That's where they make their money"*.

In short, while Amazon may not look into actual payloads, these metadata provide Amazon plenty of operational advantages, sometimes even towards manufacturers that have adopted Sidewalk.[3] Interviewees responded to this with resignation, nonchalance, or a

[2] A survey of users' perceptions of Sidewalk and satisfaction with its proclaimed benefits would be interesting but goes beyond the research question of this paper.

[3] In January 2026, Ring unveiled new Sidewalk sensors with functionalities similar to existing third-party endpoints [230], though we cannot speak on causality or potential partnerships with manufacturers.

bet on coopetition; with very few voicing concerns. Combined with the findings from §3.1, we conclude that Amazon instrumentalises PETs in Sidewalk to transform personal devices to gateways and pit themselves in a powerful vantage position vis-à-vis manufacturers. This is similar to Veale's [299] conclusion that tech companies use PETs not only to encrypt communication, but also to enable novel cross-party functionality, in our case through new information flows that they consider irrelevant for privacy protection.

4 PETs transforming production

Moving beyond information flows, we investigate the actual engineering and governance of PETs in Sidewalk. Amazon not only specifies privacy and associated security requirements, but takes an active role in defining their implementation. We focus on how implementation arrangements change production of IoT manufacturers as their devices become accessories of AWS.

4.1 Implementation of encryption in endpoints

Amazon's implementation of PETs in Sidewalk requires manufacturers to embed encryption keys and certificates in endpoints (*"keying"*). Factories must use a *"YubiHSM"* hardware security module (HSM) [313] programmed to sign the device certificate with the private key of the manufacturer, so that only the endpoint and manufacturer's application server can decrypt each other's packets. The manufacturer must purchase the HSM and send it to Amazon for *"factory support"* [20], i.e. to program a *"device attestation key"* and the *"Sidewalk certificate chain"* onto the HSM [20; 24]. Thereafter, the manufacturer sends the HSM to their factory, that connects it to a computer on the factory line [26]. The factory must also share logs of manufactured devices (including unique persistent identifiers) with Amazon, for routing and authentication by the Sidewalk Network Server. Implementing the keying workflow surfaced as *"affect[ing] the actual physical production, quite severely. Because Amazon has stringent requirements on security for production. They have very high standards on how they actually get keys into devices"* [A2]. It is not standard for factories to use computers on their factory lines [A1]. For smaller and inexperienced manufacturers, this is *"a big change. It's a big step up in security. ... it will take some while to get the production of this up"* [A2]. Especially manufacturers of less sophisticated devices might struggle: *"it's definitely a hurdle to get over, ... especially if it's something simple like a light or something, like 'I just want to make a light and ... why do I have to figure out how to provision all this stuff in order to make it work?'"* [A1]. The keying requirement showcases Amazon's ability to go beyond specifications, to stipulate workflows that change how IoT manufacturers organise their physical production process.

4.2 Transmission and hardware requirements

Amazon does not merely specify capabilities that hardware must meet to implement their PETs. According to an interviewee, endpoints must use the real-time operating system FreeRTOS (stewarded by AWS). Furthermore, *"only certain processors [are] allowed to operate on Sidewalk because they have to have that encryption zone built into it. You have to have a certain amount of memory. You have to handle data in certain ways"*. Manufacturers must pick from five approved partner development kits [30; 34]. Additionally, endpoints must comply with data rate, volume, synchronism, and frequency requirements in radio transmissions [42].

These requirements impact manufacturers' production processes and product offerings. The Sidewalk stack is hard to implement: *"especially in the very beginning, the efforts to make it work were pretty complex"*. Four interviewees noted that the stack requires relatively powerful and therefore costly hardware, e.g. in terms of memory. The cost is especially felt in the B2C domain, where price-sensitive consumers lead manufacturers to minimise device costs [A1; A6; A7; N1]. The large firmware footprint means that some manufacturers could not fit additional connectivity protocols in the same device. For one manufacturer the FreeRTOS requirement came after their admission to the Sidewalk program. It forced them to move from coding for bare metal, to coding for different such OSes, and ultimately for FreeRTOS; demanding fundamental changes in development that Amazon provided little transparency around.

4.3 Organisational governance and certification

Amazon effectuates their program requirements through an *ex-ante* qualification process and its encryption key infrastructure. To qualify, manufacturers must inform Amazon about their organisation and product, obtain *"development keys"* to connect their prototype to Sidewalk during testing, have a test facility run test cases for the prototypes, and pay a qualification fee (currently zero) [23; 30; 43]. Only after approval may manufacturers advertise Sidewalk compatibility and can their devices access the network.

Complying with the Sidewalk policies is a continuous process and prone to change [29]. Endpoints must be reliable and contribute to *"an overall good customer experience"*, e.g. not suffer from repeated disruptions or latency [29]. Furthermore, manufacturers must keep providing security updates to endpoints (*"no less than 4 years from the last shipping date of the device"* [23]); address security vulnerabilities that the manufacturer encounters within a time period that Amazon defines [29], immediately notify Amazon, and *"take all appropriate steps to remedy such vulnerability, including cooperating with [Amazon]"* [22]; and propagate Sidewalk updates – that can be for *"firmware update, reporting, or debugging purposes"* – to all endpoints, again within a certain period, and share the collected metrics with Amazon [22]. Ironically, the terms forbid manufacturers to monitor *"the availability, performance, or functionality of any of [Amazon's] products or services"* themselves [22]. As another example, a top-down policy change adjusted the uplink traffic rates and introduced a daily limit in early 2024 [25; 42, p. 18]. Also, Amazon reserves the right to re-audit or recertify adopters at later stages, and arranges periodic check-in meetings with adopters to elicit their feedback [A6]. Amazon may retroactively revoke authentication keys from infringing manufacturers and *"if a third party fails to act in good faith"* [32, p. 14].

Interviewees' experiences show that the qualification process is less standardised and runs deeper than the documentation describes. One participant incurred a delay in their prototypes testing: Amazon kept on retesting because they were not finding anything wrong with it. Furthermore, Amazon performed in-person security inspections of the factory that a participant worked with, although this is not mentioned in the qualification documentation.

Table 1: Endpoint data and telemetry that is visible for Amazon and manufacturers (✓) or not (×); all hidden from gateway owners. Based on Amazon documentation [32; 24; 42, pp. 33-40, 42, 49-55, 60, 175; 44] and interviews. Unknowns marked with ?.

Endpoint data	Visible to Amazon	Visible to manufacturer
Persistent device characteristics		
Manufacturer	✓	✓
Serial number (generated by manufacturer)	✓	✓
Advertised Product ID (APID; generated by AWS for manufacturer)	✓	✓
Sidewalk Manufacturing Serial Number (hash of APID and device serial number or (if absent) a universally unique identifier)	✓	✓
Sidewalk ID (might be the device's serial number)	✓	✓
Device profile (DeviceTypeId; created by manufacturer in AWS IoT Wireless to specify the device capabilities)	✓	✓
Qualification process identifier	✓	✓
Associated application server identifier	✓	✓
Supported connectivity protocols (BLE, FSK, LoRa) and parameters (e.g. preferred protocol, (a)synchronous)	✓	✓
Power source (battery- or line-powered)	✓	✓
Maximum transmit power per protocol	✓	✓
Variable metadata		
Payload (e.g endpoint sensor data)	×	✓
Transmission identifier (rotating hash of Sidewalk ID)	✓	✓
Unspecified *"auxiliary data (device and user-related)"* that the *"AWS IoT asset services"* provide to the application server [42, p. 42]	?	✓
Identifier of connected gateway	✓	×
Location of connected gateway	✓	×
Location of endpoint (Amazon through gateway location; manufacturer through AWS integration [e.g. 249; 314])	✓	✓
Battery level	✓	✓
Whether the endpoint is throttling down its traffic rate (can be adjusted by Amazon remotely)	✓	✓
Sidewalk SDK version and supported features	✓	✓
Signal strength in endpoint-gateway transmission	✓	✓
Variable telemetry that Amazon can make the endpoint (not) report to them at a periodicity it can change		
Periodicity of sending the below metrics to Amazon (by default once a day)	✓	?
Number and frequency of uplink and downlink messages, per connectivity type	✓	✓
Average size of uplink and downlink messages	✓	?
Number of (un)successful connections	✓	✓
Minimum and maximum time taken for a successful connection	✓	✓
Number and type of communication failures	✓	✓
Round trip time for messages	✓	✓
Number of duplicated and retried messages	✓	✓
Number of decryption and authentication errors	✓	?
Minimum and maximum time for a successful connection	✓	?
Timeout configured for connecting using a certain protocol	✓	?
Number of (un)successful registrations	✓	?
Number of (un)successful key refreshes	✓	?
Number of frustration-free networking retry attempts	✓	?
Number of time sync requests performed and received	✓	?
Periodicity of time sync requests	✓	?
Difference between time as perceived by endpoint and Sidewalk Network Server	✓	?
Number of (un)successful Sidewalk Bulk Data Transfer file transfers	✓	✓
Whether endpoint has sufficient memory, storage, and battery to install a Sidewalk Bulk Data Transfered update	✓	✓

Amazon was said to leverage its inspections for commercial reasons: i.e. polishing Sidewalk's image. An early adopter shared Amazon's interest in their finances: *"they audited the company, they audited the objectives of the company ... They had to understand how we were being financed, to determine if we're going to be around for a while, or if we were just a start-up that was going to disappear in 6 months"*. Amazon also verified adopters' *"market potential"* so that their endpoint could contribute to Sidewalk's marketability (§3.1).

Amazon took the liberty to give some manufacturers a favourable treatment, depending on their relations. One respondent's organisation skipped part of the qualification process; though this was *"not typically how you do it"* and a privilege they ascribed to *"the world [being] a small place"*, as they were acquainted with someone leading Sidewalk. An early-adopter interviewee had a *"little bit different but ... similar process"*, *"because we've been working kind of hand-in-hand with them for a while"*. One participant said they would not even undergo qualification, despite Amazon and themselves advertising their Sidewalk adoption. When another B2C-focused participant nearly abandoned Sidewalk because they did not see sufficient value for the necessary endpoint hardware upgrades, Amazon created special software for them: *"the Sidewalk implementation with [our devices] on both sides is quite custom"*; *"We have custom APIs, they have built custom firmware for [some gateways] around this. Yeah, it's a very [our company]-specific implementation"*. Consequently, their endpoints do not use the full Sidewalk security scheme. Amazon apparently permitted this security lapse for the sake of onboarding this particular organisation.

Contrary to similar protocols (e.g. Bluetooth, Matter, and LoRaWAN), Sidewalk is not governed by a standards body but solely by Amazon. Their strong position enables these unilaterally imposed obligations, arbitrary policy deviations, and liberal interpretations of broadly-formulated obligations (e.g. the *"good customer experience"*); exposing manufacturers to power asymmetries. With their governance process, Amazon obtains long-lasting agency over how endpoints work and how manufacturers produce and manage them. On top of this, Amazon is the only party operating the network's backbone, i.e. the Network Server and gateways. If Amazon were to pull the plug on either, all endpoints would lose Sidewalk connectivity, hurting users and manufacturers alike.[4] Granted repeated lay-offs [214] and Amazon's devices division losing billions between 2017 and 2021 [180], this poses a realistic risk.

4.4 Application server in AWS

AWS ties all the ends together in the implementation of Sidewalk's PETs. All Sidewalk traffic must originate from or be sent to an application server within AWS [42]: *"there's no option for the data not going to AWS"* [A5], because *"Sidewalk is decoded and decrypted in Amazon's cloud"* [A6]. This process entails both en- and decrypting packets, and authenticating devices and application servers [32]. Once manufacturers land on AWS, they can utilise the myriad of cloud services part of AWS' production offerings (see §A.3) that make their production more agile [135]. While seemingly convenient, Amazon's tight coupling of Sidewalk and AWS hinders manufacturers in managing endpoints from a non-AWS server. It would require moving data around or exposing APIs from within AWS to these other servers. [A5; A6; A7] have such APIs that their organisational customers can interact with. One said that *"if a [customer] wanted to use Azure, then we could just get the data to Azure, that's fine, that takes ... a fraction of a millisecond. ... You gotta pull it out, it'll go into your AWS S3 bucket and go into a place, and then you can get that to wherever that needs to go. ... Moving data around is a pretty solved problem these days."*. Another finds it *"doable"*, but *"not as easy as is said"* because *"there's still a copy and paste effort"*. Passing through AWS incurs duplication; increasing complexity, data integrity challenges, and security risks. Accordingly, Amazon effectively *"funnel[s] people"* into using AWS [A7].

The funnelling is consequential. First, Sidewalk cannot be called a wireless mesh network (WMN) [as e.g. 81; 167; 255, do] because endpoints and gateways cannot communicate bidirectionally and locally over Sidewalk [7]. Instead, the protocol requires all IoT communications to pass over an application server. Second, it demonstrates that Sidewalk is not *"just a pipe"*, contrary to Amazon's framing (see §A.3). Amazon's appeal to being a pipe implies that they barely intermediate in Sidewalk[5], granting manufacturers and endpoint users autonomy over data flows. On the contrary: Amazon embeds Sidewalk closely in AWS and its IoT-related services. Sidewalk thus does not provide internet connectivity, but *cloud* connectivity [27; 42, p. 9].[6] This setup incentivises manufacturers to utilise AWS services for managing their endpoints, allowing Amazon to monetise Sidewalk without charging manufacturers or users for the connectivity itself. Meanwhile, Amazon obtains the power to shape what endpoints can(not) do, by virtue of both designing the Sidewalk protocol and the IoT services in AWS that manufacturers must use; going far beyond what a *"pipe"* could do.

4.5 How PETs give Amazon an upper hand in production

Amazon's marketing of Sidewalk as a crowdsourced network that benefits consumers obscures the greater movements at play. Sidewalk does not only allow Amazon to extend their computational infrastructure with a crowdsourced network, but also turns third-party IoT devices into accessories of their cloud. As our interviewees highlighted, AWS' cloud services provide them great operational control. They can continuously update service functionality to reflect changes in business objectives and outcomes, and improve security. In return, manufacturers need to accept the incursions Amazon makes into their production. Amazon's control over the implementation of PETs allows it to intervene in endpoint hardware (e.g. qualified chips), software (e.g. complex software that must be kept up-to-date), operating systems (e.g. the requirement to implement FreeRTOS) and the environments producing and managing them (e.g. the mandatory use of AWS, keying of devices, and organisational governance). Further, by adopting Sidewalk, manufacturers enter a path dependency that aggravates these power asymmetries. Sidewalk demands significant and perpetual technical (hardware, software, cloud) and organisational (staff time, knowledge, and production lines) resources that cannot be spent otherwise. Multiple interviewees, especially from smaller companies, indicated this made it hard for them to adopt and retain knowledge about and compatibility with other connectivity protocols. As [A3] aptly summarises: *"it's hard trying to figure out where you put your eggs, where you focus, is a really important question for viability of a business"*. Finally, Sidewalk's funnelling of manufacturers into AWS raises the bar for employing non-AWS cloud services. Thus, once in, shifting away from Sidewalk and AWS becomes challenging as manufacturers are distanced further from alternatives, while Amazon's infrastructure and governance mechanisms become so deeply engrained in their production process, that they perpetually reshape and complicate them. This exemplifies Amazon's power to reorganise business relations between Amazon, Sidewalk adopters, and the companies they source their hardware components from.

These power asymmetries raise the question: do Sidewalk's functional propositions for manufacturers, outweigh the myriad of dependencies on Amazon and their infrastructure? For multiple participants, their other engagements with Amazon (e.g. *"a major retail relationship"* or using AWS) influenced their decision to adopt Sidewalk; even if its requirements or bandwidth limitations made Sidewalk *"not a perfect fit for [them]"*, as one interviewee said. One participant stated that *"there's an aspect of an ongoing partnership with Amazon, which is a huge company"*. Another relies on and envisions future integrations with Amazon's logistics services, seeing Sidewalk as *"a stepping stone towards future development ... It can create a more intimate relationship with Amazon to wanna do future developments for [our company]. I would say that's probably the point."* Indeed, *"it's like befriending the giant, right? ... If we create*

[4]One respondent said Amazon is *"in the works of creating a development kit"* so that third-party endpoints can double as a gateway, which their company is anticipating and developing towards. Though, they *"can't say that [Amazon has] ever given us a true answer ... there's a lot of vagueness. ... I'm wondering if it's because they still wanna hold that control ... I see it happening eventually, I just can't give you a timeline, because they don't give us a timeline"*. To date, we have not found any information about this kit. Manufacturers internalise the risks of such uncertainty: *"if they shared a little bit more, then we could develop a gateway with them. But you know, we're not there"*.

[5]In net neutrality discussions [271], connectivity and hosting providers would argue that as a *"dumb pipe"* or *"mere conduit"* (i.e. linking end users to content providers over the internet, without moderating content) [106; 156], they have reduced liability over content [149; 228; 297].

[6]This difference also distinguishes Sidewalk from wifi hotspot services, wherein ISPs utilise routers in consumers' homes as wifi hotspots for other consumers or people with a dedicated subscription to said service [e.g. 75; 108; 123; 311].

a rocky relationship with them and shut them out, well, that's going to eliminate a huge portion that we could have for business with them. And we really aren't trying to create that kind of rough rockiness". But to do this, the interviewee adjusts to Amazon's moves: *"There's always about, you know, who's holding the more power? ... We just kind of play ball the way they play ball, and hopefully develop an innovation that can drive the growth. That's all"*. In sum, Amazon's infrastructural and market power (i.e. being a big player in the cloud, logistics, retail, and home IoT domains) begets more power (i.e. the power over Sidewalk-adopting manufacturers' production).

5 Discussion

5.1 PETs as a source of power in other cases

We explored whether and how Amazon instrumentalised PETs in Sidewalk to entrench their computational infrastructure, in order to identify its implications for the design and evaluation of PETs. Contrary to PETs' promise to tackle data power by inserting strict controls over information flows, Amazon's implementation of PETs is designed to constrain them only to a limited extent, while entrenching their computational infrastructures. Notably, Sidewalk is not an isolated instance.

Digital Contact Tracing (DCT). In response to governmental calls for smartphone-based DCT during the Covid-19 pandemic, an industry and academia coalition proposed the Decentralised Privacy-Preserving Proximity Tracking (DP3T) protocol, that aimed to maximise privacy preservation and purpose limitation [283]. DP3T relied on persistent background functioning, that Google's and Apple's OSes – with a 99% market share in these regions [259] – prohibit for privacy and performance reasons. Amidst a greater controversy around decentralised solutions prioritising privacy over information flowing to public health authorities [1], the companies implemented a DP3T-like protocol in their OSes. This *"Google and Apple Exposure Notification"* framework exposed APIs that DCT apps developed by health authorities could invoke. By pushing the protocol into their OSes, Google and Apple positioned themselves as infrastructure providers for public health services; resolved a public controversy around DCT architectures on their own terms; settled *"tradeoffs among privacy, security, and epidemiological utility"* (p. 53) through its API designs; and secured seats in the public health decision-making arena [283].

Device finding networks. With an opt-out update [121], Apple turned *"hundreds of millions"* [53] of products into a crowd-sourced privacy-preserving infrastructure for finding devices, called Find My. *"Finding devices"* report the location of nearby Find My-compatible devices to their owners [50; 51]; spanning Apple's own devices and trackers (AirTags), and third-party trackers and products (e.g. earphones) [74; 184]). Conversely, third-party tracker manufacturers typically rely on customers downloading a smartphone app to manage their own tracker and report the location of others', meaning they have fewer finding devices (e.g. Chipolo has five million [91]) [91; 223; 279]. Third-party (tracker) manufacturers wishing to make Find My-compatible products must join Apple's developer programs and pass a certification process [53]. Their devices may not support Apple's and their own network simultaneously [103; 222]; according to an unofficial publication of the Find My specification, this *"may interfere with the security and privacy requirements"* [49, p. 14]. Granted Apple's ability to remotely turn consumer-owned Apple devices into *"finders"*, adopting Find My may impact manufacturers' choice over using other protocols [77]. Antitrust authorities worldwide investigated these adoption conditions [97; 103; 114; 225; 234; 278; 291], alleging Apple of gatekeeping and self-preferencing while weaponising security and privacy.

Digital advertising. In 2021, Apple implemented the *"App Tracking Transparency"* (ATT) framework in iOS. Promoted mainly as a privacy feature, app developers are required to ask user consent to use device identifiers for cross-app tracking [52], with consequent opt-in rates varying between 11% and 50% [54; 102; 176; 307]. Its PET-based alternative for ad attribution, the SKAdNetwork framework, uses on-device processing, and delays and anonymises attribution reporting to advertisers [182]. Apple still tracks users across Apple apps and uses the more timely and granular Ads Attribution API for Apple Ads, claiming these practices constitute first-party data. Accordingly, Apple can track users more accurately and provide advertisers with richer ad performance insights than competing ad networks [97; 183]. After introducing ATT, Apple's advertising market share tripled [181], some app developers moved from advertising to other revenue models [162] and Meta's ad revenue took a significant hit [100]. Multiple competition and consumer authorities are investigating or have already fined Apple for increasing barriers of entry and self-preferencing with ATT [61–64; 79; 97; 292; 293].

Relatedly, Google's *"Privacy Sandbox"* (PS) for Chrome and Android, announced in early 2020, would deprecate third-party cookies in Chrome, introducing APIs as alternatives, with decentralised PETs running inside users' browsers [127; 242]. Faced with regulatory antitrust investigations [93; 94, pp. G123-124; 95, p. 296; 96; 98, pp. 17-18, 31-32; 99; 224], Google pivoted to a user consent model for third-party cookies in 2024 [89], and killed most PS APIs in late 2025 [69; 90]. The authorities argued that PS disproportionally disadvantages publishers and adtech companies, and 'self-preferences' Google, i.e. leverages its browser-developing position to treat its own adtech services favourably over others'. The PS APIs are less effective than third-party cookies [93], cost publishers ad revenue, and require technologically complex and expensive implementations [150; 218]. Consequently, Google may benefit from publishers and advertisers flocking to its advertising services (e.g. Google Ad Manager [218]) and higher-margin ad networks (e.g. mobile and search) [111; 244; 280; 281]. The consent model pivot added uncertainty for publishers about third-party cookie adoption to this mix [68; 158], particularly affecting smaller publishers with less resources for testing alternatives [158; 247].

Arguably, it is not surprising that surveillance-based businesses suffer when PETs work well. However, authorities and academics have also cast doubt on Apple and Google's privacy promises. ATT has not significantly reduced tracking libraries in iOS apps, and developers circumvent ATT with other tracking mechanisms [163]. PS increases first-party tracking and tracking collaborations between websites [71; 93; 173], and its governance structure does not guarantee its privacy promises are held [98, pp. 17-18, 31-32]. Using on-device PETs may also realise a *"perverse outcome where companies can access more sensitive data than before"* [299, p. 46] since data remains decentralised and confidential – albeit in the presence of a single party with great control over the underlying infrastructure. In sum, these companies narrow privacy down to confidentiality of 'personal information' [299; 301], data anonymisation, and preventing third-party tracking [182] while becoming a single point of failure. By framing privacy narrowly to advance their competitive positions, these companies *"sanitiz[e] surveillance"* [183, p. 9] and distract from power asymmetries [183] and *"power dynamics congealed within adtech infrastructures"* [182, p. 18].

5.2 The PET Paradox

We refer to the pattern that emerges across these cases as a two-faceted *PET Paradox*, that reveals infrastructural power as distinct from informational power. First, tech companies can adopt PETs to *"flip"* consumer devices, with surveillance and exploitative effects. When the Sidewalk roll-out generated privacy backlash, Amazon applied PETs to suppress select sensitive information flows between Amazon, manufacturers, and gateway and endpoint users. These PETs helped calm backlash and raised IoT security standards, but addressed privacy only narrowly. Sidewalk, even with PETs, casts a countrywide network that enables new information flows between endpoints and IoT manufacturers, extending their surveillance infrastructure (B2C) and market asymmetries (B2B). Furthermore, Sidewalk's appropriation of consumer connectivity is akin to Google and Apple appropriating compute, sensing capabilities, browsing and app habits. The companies weave consumer devices together, creating an *extension of their computational infrastructure* with substantial population coverage. This extension lets them offer novel services to consumers, businesses, and governments; such as *"privacy-preserving"* contact tracing, device finding, advertising, and cloud connectivity. When companies frame flipping consumer devices purely as a privacy issue, PETs can be depicted as necessary and sufficient solutions – sidelining economic concerns. These cases underline how these companies design PETs to arbitrate what privacy is and what information flows count as relevant, while unfolding surveillance infrastructures for economic interests.

Second, our work confirms that end devices becoming accessories of clouds is a mixed blessing for deploying PETs. This pits infrastructural companies as powerful players to deploy, but also to compromise (decentralised) PETs [284]. Moreover, control over gateways and endpoints allows infrastructural companies to wield PETs to entrench their power as a centralised authority towards consumers, businesses, and governments alike.

Remotely reprogramming devices through OTA update infrastructures may benefit privacy and security – e.g. by enabling (silent) patching [112; 193; 256], though compromising the conditions for applying PETs. Amazon's very control over remote programmability, by managing gateway firmware and a connected cloud infrastructure, is what enables the company to *"flip"* Echo and Ring devices. That same control can be used to deploy privacy technologies en masse, or to compromise their privacy guarantees.

Mundane aspects of these infrastructures, like OTA, combined with privacy governance and implementation requirements, allow Amazon (and Google and Apple) to deepen its capacity to furnish end devices as extensions of their software production environments to third parties. By dictating how manufacturers must implement Sidewalk's PETs, Amazon increases weak privacy standards in the IoT domain. However, it also gains influence over manufacturers' device hardware and software, cloud environment, factory lines, and organisational processes, with update obligations (e.g., on firmware) ensuring its persistence over time.

Consequently, Amazon's implementation of PETs entrenches its computational infrastructure in and agency over manufacturers' production. The entrenchment puts into place potentially long-lasting power asymmetries in how IoT manufacturers may produce their devices, granted the encountered path dependencies. It further centralises a single entity's control over devices' hardware, OS, connectivity, and remote management. Amazon becomes a centralised authority that instrumentalises PETs to introduce a web of control around devices that, paradoxically, erode assumptions PETs researchers can make about devices being a trusted base for decentralised PETs [284].

5.3 Alternative designs

The private initiative **FON** which pursued *"ubiquitous and universal Wi-Fi"* (p. 168) [190], and the community initiative Freifunk that aims to reduce reliance on centralised ISPs locally [124] can resemble Sidewalk. Mesh networks differentiate themselves through varying compensation models and degrees of centralisation in network topology, all based on volitional participation. In contrast, the production-oriented connectivity model of Sidewalk is an offshoot of computational infrastructures that have come to play a central role in privacy and (software) production with what has been coined as the *"agile turn"* [135; 164]. In the agile production model, companies leverage control over 'edge' or 'end devices' from remote servers, to continuously push new functionalities to, and garner information from devices; enabling continuous optimisation of production [135]. For example, TVs historically only received linear broadcasts; while contemporary 'smart' TVs and streaming devices enable upstream traffic, reconfigurability, and remote addressability, hereby exposing personal (viewership) information to TV manufacturers and ad platforms [177; 191; 298]. Sidewalk hence exists because the digitalisation of everyday objects happens increasingly through their transformation into 'accessories of clouds'. Amazon introducing Sidewalk to consumer devices reinforces this dynamic. Compared to mesh protocols, Sidewalk is a-production oriented connectivity protocol that centralises traffic to AWS, expands on an opt-out basis, and lacks compensation.

Commercial contenders of Sidewalk utilise open standards, and assert less control over information flows, consumers and manufacturers. **Thread** is an IPv6-based low-resource mesh networking protocol that can power multiple application layers, including Apple HomeKit and Matter [274]. Matter, in turn, is a standard to make devices in one household interoperate locally over protocols including WiFi, Bluetooth, and Thread [285–287]. Thread Border Router functionality is supported by many affordable and common chipsets [210; 273] and is already supported by a myriad of devices (e.g. TVs, speakers, routers [286; 288]). Endpoint manufacturers that wish to adopt Thread can pick from "certified stacks, silicon platforms or modules" [274] that offer significantly more choice [275] than Sidewalk. Choice of cloud infrastructure use and device provisioning is not strictly regulated [276].

Alternatively, **Helium** offers a crowdsourced low-resource IoT network (based on LoRaWAN) and a network for cellphone/wifi connectivity. The networks cater to residential and industrial use-cases, and reward gateway owners with the native cryptocurrency HNT [143; 205; 206]. Abuse mitigation and routing is performed by hotspots in decentralised fashion [136; 204; 253]. IoT manufacturers can tap into the Helium network through a LoRaWAN Network Server [143]. **Nebula** [305] is a crowdsourced, privacy-first protocol for uplink traffic, with smartphones as gateways paid per data transfer. The central platform provider coordinates the network, payments and hosting, and signs the cryptographic certificate that the application server provisions its corresponding sensors with to authenticate traffic. Routing and abuse mitigation are decentralised to application servers and gateways. The protocol adopts Tor and secure messaging/mixnets to hide metadata and gateway identities towards central entities. Ashur et al. [58] propose a fully decentralized **BLE-based asset tracking system**, where 'beacons' installed at fixed locations throughout covered areas sense nearby tags. Work on downlink architectures shows they face greater authentication, abuse mitigation, participant privacy protection, and reliability challenges [70].

These examples demonstrate that making IoT devices *"work better at home and beyond the front door"* [39] can be done with actual mesh networking. The distributed routing and abuse mitigation designs provide resilience and greater privacy through distribution of trust. Beyond privacy, Nebula, Helium, and Thread leave manufacturers greater choice of cloud provider, network provider, authentication schemes, transmission sizes and rates, and hardware components. Manufacturers face less strict governance and certification processes. The alternatives suggest that the PET Paradox that infrastructural companies raise are not inevitable, but require addressing infrastructural power in the design of PETs.

5.4 Ways forward for the PETs community

The alternatives demonstrate that existing approaches to PETs can be used to improve the first PET Paradox facet (i.e. selective application of PETs to information flows, raising concerns about 'privacy-washing'). However, the second facet requires expanding how we do privacy analysis, and design and evaluate PETs; especially when PETs are deployed by infrastructural companies to expand their power in clouds and on end devices. Accordingly, we recommend the following to PETs researchers and practitioners:

Mitigate privacy-washing through data minimisation to purpose: selective confidentiality of *"personal data"* flows (facet 1) should raise red flags for researchers and practitioners. This sort of privacy- or confidentiality-washing can be mitigated by recentring *data minimisation towards a purpose, across all data flows* in designing and evaluating PETs [134; 146]. Selective confidentiality of data flows is not a sufficient condition for privacy claims; rather, PETs are those technologies that constrain all data flows to those absolutely necessary for a purpose, even if this data is not personal or business sensitive.

Extend privacy analysis for PETs to identify when constrained information flows mask exploitation of end devices by infrastructural companies: We showed concretely how companies instrumentalise PETs to appropriate resources from end devices, repurposing them as extensions of their own infrastructure for economic gain. Researchers and practitioners should raise red flags when PETs are used to extend control over end devices for economic extraction and broader surveillance [e.g. 99; 183; 238; 299]. Concretely, information flow analysis should be broadened to limit new control points, to ensure companies do not reduce increased control over end devices (i.e., through centralising control over hardware, software, and remote management infrastructure) to a matter of confidentiality of information flows.

Incorporate market and infrastructural power in adversarial analysis: Adversarial analysis is fundamental to PETs design. It identifies whether privacy guarantees hold up against the capabilities of an attacker with particular goals. We show that existing infrastructural control and the ability to redefine what end devices can do – even if in a privacy-preserving way – are places where power beyond information flows can impact the privacy guarantees of PETs and subvert their original aims. Such power is currently concentrated in the hands of a few companies that can also deploy PETs to billions of devices. In this context, "who" designs and deploys PETs [67], with what impact on end devices, for what economic and political outcomes, and based on whose resources, are relevant questions to surface adversarial capacities when deploying PETs. Further, when B2B relations are implied in PET implementations, considering how information flows enabled or disabled by a privacy-preserving protocol may impact these relationships, should be part of the power analysis. The objective of such analysis is not to compromise privacy to ensure benefit for third parties (e.g. advertisers, governments); but to scrutinise the centralised authorities that may instrumentalise PETs to (selectively) suppress information flows for economic, political and technical advantage.

Challenge the centralising force of computational infrastructures on engineering PETs: As Troncoso et al. [284] argue, many decentralised systems designed to enhance privacy, (sometimes tacitly) assume centralisation of network information, computations, and trust establishment. In Sidewalk, centralisation manifests in networking (e.g. managing network topology, routing, onboarding, authentication, abuse mitigation, and key exchange), the cloud environment (e.g. funnelling manufacturers into AWS, and defining how AWS services work), and in manufacturers' production processes (e.g. certification, hardware, and software update requirements). Sidewalk is not an anomaly: dependency on cloud infrastructures is already prevalent in the production of services on smart end devices. One study found 65% of IoT device companion apps to use Bluetooth, implying that 35% have network- or cloud-based communication [241]. The impact of cloud-centricity in smartphones has also been problematised, e.g. for push notifications in secure messaging [240]. These centralising forces – and the power dynamics they create between users, manufacturers, and tech companies – would benefit from *more empirical studies like this one, to guide the PETs community in identifying and addressing concrete challenges* due to computational infrastructures acting as centralised software production environments. We urge the PETs community to resist accepting these as inevitable [178; 308]; incorporate dependencies of users and manufacturers on these computational infrastructures that are abstracted away when designing PETs [67]; and address centralisation of network information, computations and trust establishment [284].

Develop technical architectures to keep end devices a viable infrastructure for PETs: User control over end devices is fundamental to PET deployment [83; 134; 284] and privacy as autonomy [120; 128]. Groschupp et al. [129] pitch a trusted execution-based smartphone architecture that curbs Apple and Google's ability to constrain device functionality through their OSes. This design reduces the need for user trust in OSes regarding privacy, while making *"users sovereign over their phones"* (p. 1); empowering them, phone manufacturers, and app developers. Our work underlines that similar efforts for OTA infrastructures, OSes, cloud environments, and hardware implementations of public key infrastructures are needed. This research should not merely assess privacy and security, but study how to avoid entrenching existing computational infrastructures technically, economically, politically and socially.

Engage conversations across affected players: Outside the PETs community, scholars and regulators are analysing the advertising and finding network instances as potentially anticompetitive applications. The DCT instance raised governmental sovereignty and public decision-making questions. From a policy perspective, privacy, competition, and sovereignty lenses aim to address power asymmetries. However, we need greater discussion on how well they do so, given that they leave tech companies' infrastructural hold over software production mostly out of view. We show that governance and implementation of PETs, and their impact on production of hardware and services, are fruitful areas for future research. Overall, assessing privacy claims made by companies or governments using PETs should include a broader (technical, economic, and political; B2B and B2G) power analysis beyond confidentiality (e.g. data minimisation; B2C). Similarly, we call for greater legal protection of consumer control over devices, such that manufacturers cannot co-opt them to deliver services to others to their economic and infrastructural benefit. These discussions should include policymakers, researchers, and (to be) affected companies alike; with privacy, competition, and sovereignty as areas of concern.

6 Limitations

Our work knows multiple methodological limitations. First, interviewing is time-consuming, necessitating a limit on the number of interviews and reducing the generalisability of the findings [9]. Additionally, the population of Sidewalk-adopting manufacturers is limited to sixteen companies. While our eight Sidewalk-adopting interviewees cover half of this group, others might have different stories about Sidewalk's effect on their production. Further, with eight out of nine interviewees having adopted Sidewalk, the interviewee sample is likely positively biased towards Sidewalk. Interviewing more non-adopters could enrich our story.

Similarly, the consulted grey literature was frequently biased, inaccessible, and incomplete; complicating analysis. Three interviewees alleged that some tech journalists do not comprehend the Sidewalk technology or are excessively negative about Amazon for the sake of *"clickbait"*. Consulted industry press releases generally serve marketing purposes. Next to that, Amazon restricts access to certain documents and development portals to Sidewalk-authorised developers [e.g. 41], and often does not disclose all details of technical implementations. As illustration, it does not become clear precisely what (meta)data Amazon processes, and how, for service optimisation [32; 42]. The protocol specification also considers a *"Detailed specification of Gateways and the Amazon Sidewalk Cloud"*, and interactions between them, outside its scope [42, p. 10].

To mitigate and increase the robustness of the case studies and interviews, we triangulated multiple data sources [237; 254; 312].

7 Conclusion

On the surface, deploying PETs to millions of devices seems a win for privacy and for curbing corporate and state power. Our empirical case study of Amazon Sidewalk demonstrates that expanding the analysis of PET implementations to include impact on manufacturers, reveals a more complex story: tech companies' implementation of PETs constrains only some information flows, while entrenching their computational infrastructures.

The case study helps articulate a two-faceted *PET Paradox* specific to companies with infrastructural power. Firstly, Sidewalk's deployment of PETs to large swaths of consumer devices provides narrow privacy protections to users while flipping devices into an infrastructure for services that generate new information flows and power asymmetries. These new flows compromise privacy of nearby (non-)users by going beyond the original Echo and Ring functionalities, and compromise the confidentiality and competitive position of manufacturers with respect to Amazon. Seen this way, PETs in Sidewalk reduce and exacerbate information asymmetry-based power imbalances with broad political and economic impacts (facet 1).

Secondly, implementation requirements of PETs defined by Amazon improve security standards as well as increase their influence on the hardware and software production environments of manufacturers. Amazon single-handedly defines the governance and implementation requirements of PETs. This move raises the bar for privacy (and security) in the IoT domain – a sector with a weak track record. However, Sidewalk also introduces system requirements and architectures that incentivise third-party manufacturers to adopt more AWS services. With this influence, Amazon turns 'endpoints' into accessories of Amazon's cloud, increasing AWS evolving capacity to manage IoT devices remotely. Meanwhile, its governance eats into companies' technical and organisational bandwidth, incurring a path dependency. Increased remote and material control expands Amazon's market and infrastructural power over IoT manufacturers. Most concerning, this undermines the reliability of accessorised devices to serve as a trusted base for PETs that avoid single points of failure (facet 2). Amazon's existing market and infrastructural power is thus central to, and also benefits from this paradox.

Existing approaches in PETs can be used to improve the first facet (i.e. avoid selective application of PETs to information flows as a form of 'privacy-washing'). However, the second facet requires expanding how we design and evaluate PETs; especially when PETs are deployed by companies to expand their infrastructural power over hardware and (software) production. Our recommendations to the PETs community (§5.4) express concretely how such power asymmetries can be addressed.

Acknowledgments

This work is part of the Programmable Infrastructures Project[7] and was partially funded by Fondation Botnar and NWO project Public Values in the Algorithmic Society (AlgoSoc, file number 024.005.017)[8]. For fruitful discussions on earlier drafts, we thank Agathe Balayn, Aniketh Girish, Bernd Kasparek, Carmela Troncoso, Corinne Cath, Joris van Hoboken, Mark de Reuver, Martina Lindorfer, Michael Veale, Michel van Eeten, Narseo Vallina-Rodriguez, Petros Terzis, Tobias Fiebig; and the participants of the Privacy Law Scholars Conference Europe 2024, Dagstuhl Seminar 25112 *"PETs and AI: Privacy Washing and the Need for a PETs Evaluation Framework"*, and Knight-Georgetown Institute's Digital Competition Conference 2026. The primary author conducted the majority of this work in his position at Delft University of Technology.

References

[1] 2020. *Joint Statement on Contact Tracing.* Technical Report. https://teamusec.de/JointStatement.pdf
[2] Harold Abelson, Ross Anderson, Steven M Bellovin, Josh Benaloh, Matt Blaze, Jon Callas, Whitfield Diffie, Susan Landau, Peter G Neumann, Ronald L Rivest, Jeffrey I Schiller, Bruce Schneier, Vanessa Teague, and Carmela Troncoso. 2024. Bugs in Our Pockets: The Risks of Client-Side Scanning. *Journal of Cybersecurity* 10, 1 (2024), tyad020. https://doi.org/10.1093/cybsec/tyad020
[3] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and Human Behavior in the Age of Information. *Science* 347, 6221 (Jan. 2015), 509–514. https://doi.org/10.1126/science.aaa1465
[4] Alessandro Acquisti, Curtis Taylor, and Liad Wagman. 2016. The Economics of Privacy. *Journal of Economic Literature* 54, 2 (June 2016), 442–492. https://doi.org/10.1257/jel.54.2.442
[5] Airthings. 2023. *Annual Report 2022.* Technical Report. Airthings, Oslo, Norway. https://www.airthings.com/hubfs/Website/investors/reports/Airthings-Annual-Report-2022.pdf
[6] Airthings. n.d.. Airthings. https://www.airthings.com/en/
[7] Ian F. Akyildiz and Xudong Wang. 2009. *Wireless Mesh Networks* (1 ed.). Advanced Texts in Communications and Networking Series, Vol. 3. Wiley, Newark, United Kingdom. https://doi.org/10.1002/9780470059616
[8] Roger P Alford. 2022. The Bipartisan Consensus on Big Tech. *Emory Law Journal* 71, 5 (Jan. 2022), 893–932. https://scholarlycommons.law.emory.edu/elj/vol71/iss5/1/
[9] Hamza Alshenqeeti. 2014. Interviewing as a Data Collection Method: A Critical Review. *English Linguistics Research* 3, 1 (March 2014), 39–45. https://doi.org/10.5430/elr.v3n1p39
[10] Amazon. 2019. Amazon Devices Event – September 2019. https://www.aboutamazon.com/news/devices/amazon-devices-event-september-2019
[11] Amazon. 2019. Introducing Amazon Sidewalk. https://www.aboutamazon.com/news/devices/introducing-amazon-sidewalk
[12] Amazon. 2020. Amazon Sidewalk: A New Way to Stay Connected. https://www.aboutamazon.com/news/devices/amazon-sidewalk-a-new-way-to-stay-connected
[13] Amazon. 2020. *Amazon Sidewalk Privacy and Security Whitepaper.* Technical Report. https://web.archive.org/web/20210116191954/https://m.media-amazon.com/images/G/01/sidewalk/final_privacy_security_whitepaper.pdf
[14] Amazon. 2021. CareBand and Life360 Tap Amazon Technology to Help People Stay Connected. https://www.aboutamazon.com/news/devices/careband-and-life360-tap-amazon-technology-to-help-people-stay-connected
[15] Amazon. 2021. Echo, Tile, and Level Devices Join Amazon Sidewalk. https://www.aboutamazon.com/news/devices/echo-tile-and-level-devices-join-amazon-sidewalk
[16] Amazon. 2022. Amazon Response to Senator Markey. https://www.markey.senate.gov/imo/media/doc/amazon_response_to_senator_markey-july_13_2022.pdf
[17] Amazon. 2022. *Amazon Sidewalk Privacy and Security Whitepaper.* Technical Report. https://web.archive.org/web/20230328145953/https://m.media-amazon.com/images/G/01/sidewalk/final_privacy_security_whitepaper.pdf
[18] Amazon. 2023. Amazon Invites Developers to Test Sidewalk and Build the Next Billion Connected Devices. https://press.aboutamazon.com/2023/3/amazon-invites-developers-to-test-sidewalk-and-build-the-next-billion-connected-devices
[19] Amazon. 2023. Amazon Sidewalk Gateways. http://web.archive.org/web/20231211071017/https://docs.sidewalk.amazon/introduction/sidewalk-gateways.html
[20] Amazon. 2023. Amazon Sidewalk Manufacturing Setup and Workflow. https://docs.sidewalk.amazon/manufacturing/sidewalk-manufacturing-setup-works.html
[21] Amazon. 2023. *Amazon Sidewalk Privacy and Security Whitepaper.* Technical Report. https://m.media-amazon.com/images/G/01/sidewalk/final_privacy_security_whitepaper.pdf
[22] Amazon. 2023. Amazon Sidewalk Program Security Requirements. https://docs.sidewalk.amazon/sidewalk-terms-and-agreements/security-program-requirements.html
[23] Amazon. 2023. Amazon Sidewalk Qualification Concepts. https://docs.sidewalk.amazon/qualification/works-with-sidewalk/sidewalk-qualification-concepts.html
[24] Amazon. 2023. Components of Amazon Sidewalk Manufacturing. https://docs.sidewalk.amazon/manufacturing/sidewalk-manufacturing-components.html
[25] Amazon. 2023. How Amazon Sidewalk Works. https://docs.sidewalk.amazon/introduction/sidewalk-how-works.html
[26] Amazon. 2023. How To Manufacture & Produce Devices: Step 1: Setting up the Host. https://docs.sidewalk.amazon/manufacturing/manufacture-provision/sidewalk-host-installation.html
[27] Amazon. 2023. Introduction to Amazon Sidewalk. https://docs.sidewalk.amazon/introduction/
[28] Amazon. 2023. Terms and Agreements. https://docs.sidewalk.amazon/sidewalk-terms-and-agreements/
[29] Amazon. 2023. Works with Amazon Sidewalk Qualification Guidelines. https://docs.sidewalk.amazon/sidewalk-terms-and-agreements/wwas-sidewalk-qualification-guidelines.html
[30] Amazon. 2023. Works With Amazon Sidewalk Qualification Process. https://docs.sidewalk.amazon/qualification/works-with-sidewalk/qualification-works-path.html
[31] Amazon. 2024. Embedded Software Engineer - Amazon Sidewalk, Amazon Sidewalk. https://web.archive.org/web/20240213093646/https://www.amazon.jobs/en/jobs/2553181/embedded-software-engineer-amazon-sidewalk-amazon-sidewalk
[32] Amazon. 2025. *Amazon Sidewalk Privacy and Security Whitepaper.* Technical Report. https://web.archive.org/web/20250414233224/https://m.media-amazon.com/images/G/01/sidewalk/final_privacy_security_whitepaper.pdf
[33] Amazon. 2025. *Amazon Sidewalk Privacy and Security Whitepaper.* Technical Report. https://web.archive.org/web/20250923180804/https://m.media-amazon.com/images/G/01/sidewalk/final_privacy_security_whitepaper.pdf
[34] Amazon. 2025. Qualified Development Kits. https://docs.sidewalk.amazon/getting-started/Qualified-Development-Kits.html
[35] Amazon. 2026. Introducing Amazon Sidewalk and Ring Sensors: Smart Home Protection That Stays Connected. https://www.aboutamazon.ca/news/devices/introducing-amazon-sidewalk-and-ring-sensors-smart-home-protection-that-stays-connected
[36] Amazon. 2026. Presentamos Amazon Sidewalk y Ring Sensors: Protección Inteligente para tu Hogar, Siempre Conectada. https://www.aboutamazon.mx/noticias/dispositivos-y-servicios/presentamos-amazon-sidewalk-y-ring-sensors-proteccion-inteligente-para-tu-hogar-siempre-conectada
[37] Amazon. 2026. Sidewalk Coverage Maps. https://coverage.sidewalk.amazon/
[38] Amazon. n.d.. Amazon Devices: Echo Smart Speakers & Displays. https://www.amazon.in/amazon-echo/b?ie=UTF8&node=14156834031
[39] Amazon. n.d.. Amazon Sidewalk. https://www.amazon.com/Amazon-Sidewalk/b?ie=UTF8&node=21328123011
[40] Amazon. n.d.. Amazon Sidewalk Test Kit. https://sidewalk.amazon/testkit
[41] Amazon. n.d.. Sidewalk360. https://360.sidewalk.amazon/
[42] Amazon Technologies. 2024. *Amazon Sidewalk Specification.* Technical Report Protocol Stack 1.0, Document Revision A.2. https://docs.sidewalk.amazon/assets/pdf/Amazon_Sidewalk_Specification-1.0-rev-A.2-090924.pdf
[43] Amazon Technologies. 2024. *Amazon Sidewalk Test Specification.* Technical Report Protocol Stack 1.0, Document Revision A.4. https://docs.sidewalk.amazon/assets/pdf/Amazon_Sidewalk_Test_Specification-1.0-rev-A.4.pdf
[44] Amazon Web Services. n.d.. Add Your Device to AWS IoT Core for Amazon Sidewalk - AWS IoT Wireless. https://docs.aws.amazon.com/iot-wireless/latest/developerguide/iot-sidewalk-create-device.html
[45] Amazon Web Services. n.d.. AWS IoT Device Defender. https://aws.amazon.com/iot-device-defender/
[46] Amazon Web Services. n.d.. Manage a Connected AWS IoT Device Fleet. https://catalog.workshops.aws/aws-iot-device-fleet-management/en-US
[47] Amazon Web Services. n.d.. What Is AWS IoT Core for Amazon Sidewalk? https://docs.aws.amazon.com/iot/latest/developerguide/amazon-sidewalk-intro.html

[7] www.tudelft.nl/en/tpm/our-faculty/departments/multi-actor-systems/research/projects/programmable-infrastructures-project
[8] www.algosoc.org

[48] Amazon Web Services. n.d.. What Is AWS IoT Wireless? https://docs.aws.amazon.com/iot-wireless/latest/developerguide/what-is-iot-wireless.html
[49] Apple. 2020. *Find My Network Accessory Specification*. Technical Report Version 1.0 Developer Preview Release R1. Apple. https://images.frandroid.com/wp-content/uploads/2020/06/Find_My_network_accessory_protocol_specification.pdf
[50] Apple. 2021. Apple Introduces AirTag. https://www.apple.com/newsroom/2021/04/apple-introduces-airtag/
[51] Apple. 2021. Apple's Find My Network Now Offers New Third-Party Finding Experiences. https://www.apple.com/newsroom/2021/04/apples-find-my-network-now-offers-new-third-party-finding-experiences/
[52] Apple. 2024. If an App Asks to Track Your Activity. https://support.apple.com/en-us/102420
[53] Apple. n.d.. Find My Network. https://developer.apple.com/find-my
[54] AppsFlyer. 2024. AppsFlyer Data Reveals Increase in User Opt-In Rates and Ad Spend on iOS Three Years After Apple's App Tracking Transparency. https://www.appsflyer.com/company/newsroom/pr/att-data-findings/
[55] Arrive. 2023. Arrive Announces Successful Integration with Amazon Sidewalk. https://www.prnewswire.com/news-releases/arrive-announces-successful-integration-with-amazon-sidewalk-301888521.html
[56] Arrive. 2024. Arrive. https://web.archive.org/web/20240602143635/https://www.arrive.tech/
[57] Arrive. n.d.. Arrive Campaign on PicMii Crowdfunding. https://www.picmiicrowdfunding.com/deal/arrive/
[58] Tomer Ashur, Jeroen Delvaux, Sanghan Lee, Pieter Maene, Eduard Marin, Svetla Nikova, Oscar Reparaz, Vladimir Rožić, Dave Singelée, Bohan Yang, and Bart Preneel. 2018. A Privacy-Preserving Device Tracking System Using a Low-Power Wide-Area Network. In *Cryptology and Network Security (Lecture Notes in Computer Science, Vol. 11261)*, Srdjan Capkun and Sherman S. M. Chow (Eds.). Springer, Cham, 347–369. https://doi.org/10.1007/978-3-030-02641-7_16
[59] ATLAS.ti. 2023. ATLAS.Ti Desktop. https://atlasti.com/atlas-ti-desktop
[60] Jef Ausloos. 2020. Foundations of Data Protection Law. In *The Right to Erasure in EU Data Protection Law*, Jef Ausloos (Ed.). Oxford University Press, 37–116. https://doi.org/10.1093/oso/9780198847977.003.0002
[61] Autorità Garante della Concorrenza e del Mercato. 2025. A561 - The Italian Competition Authority fines Apple over 98 million euro for abuse of a dominant position. https://en.agcm.it/en/media/press-releases/2025/12/A561
[62] Autorité de la concurrence. 2021. Targeted Advertising / Apple's Implementation of the ATT Framework. The Autorité Does Not Issue Urgent Interim Measures against Apple but Continues to Investigate into the Merits of the Case. https://www.autoritedelaconcurrence.fr/en/communiques-de-presse/targeted-advertising-apples-implementation-att-framework-autorite-does-not
[63] Autorité de la concurrence. 2023. Advertising on iOS Mobile Applications: The General Rapporteur Confirms Having Notified the Apple Group of an Objection. https://www.autoritedelaconcurrence.fr/en/press-release/advertising-ios-mobile-applications-general-rapporteur-confirms-having-notified-apple
[64] Autorité de la concurrence. 2025. Targeted Advertising: The Autorité de La Concurrence Imposes a Fine of €150,000,000 on Apple for the Implementation of the App Tracking Transparency ("ATT") Framework. https://www.autoritedelaconcurrence.fr/en/press-release/targeted-advertising-autorite-de-la-concurrence-imposes-fine-eu150000000-apple
[65] Laoise Ballance. 2024. Wave: Understanding the Connectivity and Compatibility of Your Wave. https://help.airthings.com/en/articles/6009826-wave-understanding-the-connectivity-and-compatibility-of-your-wave
[66] Laoise Ballance. 2024. What's the Difference between Airthings Smart Products? https://help.airthings.com/en/articles/5161848-what-s-the-difference-between-airthings-smart-products
[67] Ero Balsa, Helen Nissenbaum, and Sunoo Park. 2022. Cryptography, Trust and Privacy: It's Complicated. In *Proceedings of the 2022 Symposium on Computer Science and Law (Cslaw '22)*. Association for Computing Machinery, New York, NY, USA, 167–179. https://doi.org/10.1145/3511265.3550443
[68] Kayleigh Barber. 2024. Why Google's Cookie Deprecation Reversal Isn't Actually a Reprieve for Publishers. https://digiday.com/media/why-googles-cookie-deprecation-reversal-isnt-actually-a-reprieve-for-publishers/
[69] Kendra Barnett. 2025. Google's Privacy Sandbox Is Officially Dead. https://www.adweek.com/media/googles-privacy-sandbox-is-officially-dead/
[70] Alex Bellon, Tess Despres, Prabal Dutta, Pat Pannuto, and Sylvia Ratnasamy. 2025. The Case for Crowd-Sourcing Communication to BLE-Only Devices. In *Proceedings of the 24th ACM Workshop on Hot Topics in Networks (HotNets '25)*. ACM, UMD Campus College Park MD USA, 377–383. https://doi.org/10.1145/3772356.3772394
[71] Yohan Beugin and Patrick McDaniel. 2024. Interest-Disclosing Mechanisms for Advertising Are Privacy-Exposing (Not Preserving). *Proceedings on Privacy Enhancing Technologies* 2024, 1 (2024), 41–57. https://doi.org/10.56553/popets-2024-0004
[72] Gergely Biczók and Pern Hui Chia. 2013. Interdependent Privacy: Let Me Share Your Data. In *Financial Cryptography and Data Security*, Ahmad-Reza Sadeghi (Ed.), Vol. 7859. Springer, Berlin, Heidelberg, 338–353. https://doi.org/10.1007/978-3-642-39884-1_29
[73] Todd Joel Bishop. 2024. 'Unfinished Business': Ring CEO Liz Hamren Leads Amazon's Home Monitoring Products into the AI Era. https://www.geekwire.com/2024/unfinished-business-ring-ceo-liz-hamren-leads-amazons-home-monitoring-products-into-the-ai-era/
[74] Tucker Bowe. 2022. All the Non-Apple Gadgets the "Find My" App Can Find. https://www.gearpatrol.com/tech/g36063168/apple-find-my-compatible-gadgets/
[75] British Telecommunications. n.d.. BT Wi-Fi. https://info.btwifi.com
[76] Jon Brodkin. 2023. FTC: Amazon/Ring Workers Illegally Spied on Users of Home Security Cameras. https://arstechnica.com/tech-policy/2023/06/ftc-amazon-ring-workers-illegally-spied-on-users-of-home-security-cameras/
[77] Marques Brownlee. 2021. Apple vs The Paradox of Choice! https://www.youtube.com/watch?v=qNAo0UdYF6g
[78] Christopher Budd. 2020. Amazon Sidewalk Rollout Shows the Future of 'Forced Opt-in,' Taking Lessons from Xfinity Wifi. https://www.geekwire.com/2020/amazon-sidewalk-rollout-shows-future-forced-opt-taking-lessons-xfinity-wifi/
[79] Bundeskartellamt. 2022. Bundeskartellamt Reviews Apple's Tracking Rules for Third-Party Apps. https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2022/14_06_2022_Apple.html
[80] Dan Calacci, Jeffrey J. Shen, and Alex Pentland. 2022. The Cop In Your Neighbor's Doorbell: Amazon Ring and the Spread of Participatory Mass Surveillance. In *Proceedings of the ACM on Human-Computer Interaction*, Vol. 6(CSCW2). Article 400. https://doi.org/10.1145/3555125
[81] Jon Callas. 2021. Understanding Amazon Sidewalk. https://www.eff.org/deeplinks/2021/06/understanding-amazon-sidewalk
[82] Alessandra Calvi, Gianclaudio Malgieri, and Dimitris Kotzinos. 2024. The Unfair Side of Privacy Enhancing Technologies: Addressing the Trade-Offs between PETs and Fairness. In *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency (FAccT '24) (FAccT '24)*. ACM, New York, United States, 2047–2059. https://doi.org/10.1145/3630106.3659024
[83] Srdjan Capkun, Shweta Shinde, Ivan Puddu, Morits Schneider, Mark Kuhne, and Friederike Groschupp. n.d.. Secure and Sovereign Smartphone Platform. https://zisc.ethz.ch/research/projects/secure-and-sovereign-smartphone-platform/
[84] CareBand. n.d.. Products. https://carebandremembers.com/products/
[85] CareBand. n.d.. Technology. https://carebandremembers.com/technology/
[86] Sophie Charara. 2019. Amazon and Apple Are Quietly Building Networks That Know the Location of Everything. https://www.wired.co.uk/article/amazon-sidewalk-apple-u1-networks
[87] Jon Chase. 2021. Amazon Sidewalk Will Share Your Internet With Strangers. It's Not As Scary As It Sounds. https://www.nytimes.com/wirecutter/blog/amazon-sidewalk-review/
[88] David Chatting, Nick Taylor, and Jon Rogers. 2021. Design for Reappearance in Smart Technologies. In *CSCW 2021 Workshop on Designing for Data Awareness*. www.nick-taylor.co.uk/wp-content/uploads/chatting_cscw21_workshop.pdf
[89] Anthony Chavez. 2024. A New Path for Privacy Sandbox on the Web. https://privacysandbox.com/news/privacy-sandbox-update
[90] Anthony Chavez. 2025. Update on Plans for Privacy Sandbox Technologies. https://privacysandbox.com/news/update-on-plans-for-privacy-sandbox-technologies/
[91] Chipolo. n.d.. Chipolo. https://chipolo.net/en/
[92] Peter Cleave. 2021. Two Suns? Data Doppelgangers and the Construction of the Digital Self. *Te Kaharoa* 14, 1 (May 2021). https://doi.org/10.24135/tekaharoa.v17i1.352
[93] Commission Nationale de l'Informatique et des Libertés. 2024. Publicité en ligne : la CNIL se prépare aux évolutions des modèles d'affaires. https://www.cnil.fr/fr/publicite-en-ligne-la-cnil-se-prepare-aux-evolutions-des-modeles-daffaires
[94] Competition and Markets Authority. 2020. *Appendix G: The Role of Tracking in Digital Advertising*. Technical Report. Competition and Markets Authority. https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study#final-report
[95] Competition and Markets Authority. 2020. *Online Platforms and Digital Advertising: Market Study Final Report*. Technical Report. Competition and Markets Authority. https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study#final-report
[96] Competition and Markets Authority. 2022. *Case 50972 - Privacy Sandbox: Google Commitments Offer*. Technical Report. Competition and Markets Authority. https://assets.publishing.service.gov.uk/media/62052c6a8fa8f510a204374a/100222_Appendix_1A_Google_s_final_commitments.pdf
[97] Competition and Markets Authority. 2022. *Mobile Ecosystems: Market Study Final Report*. Technical Report. Competition and Markets Authority. https://www.gov.uk/cma-cases/mobile-ecosystems-market-study#final-report
[98] Competition and Markets Authority. 2024. *CMA Q1 2024 Update Report on Implementation of the Privacy Sandbox Commitment*. Technical Report. Competition and Markets Authority. https://assets.publishing.service.gov.uk/media/662baa3efee48e2ee6b81eb1/1._CMA_Q1_2024_update_report_on_

Google_Privacy_Sandbox_commitments.pdf
[99] Competition and Markets Authority. 2024. Investigation into Google's 'Privacy Sandbox' Browser Changes. https://www.gov.uk/cma-cases/investigation-into-googles-privacy-sandbox-browser-changes
[100] Kate Conger and Brian X. Chen. 2022. A Change by Apple Is Tormenting Internet Companies, Especially Meta. https://www.nytimes.com/2022/02/03/technology/apple-privacy-changes-meta.html
[101] Ry Crist. 2021. Amazon Sidewalk Will Create Entire Smart Neighborhoods. Here's What You Should Know. https://www.cnet.com/home/smart-home/amazon-sidewalk-will-create-entire-smart-neighborhoods-faq-ble-900-mhz/
[102] David Curry. 2024. App Tracking Transparency Opt-In Rates (2024). https://www.businessofapps.com/data/att-opt-in-rates/
[103] Kirsten Daru. 2021. *Testimony of Kirsten Daru before the Senate Committee on the Judiciary Subcommittee on Competition Policy, Antitrust, and Consumer Rights.* Technical Report. Washington, D.C. https://www.judiciary.senate.gov/imo/media/doc/04.21.21%20Kirsten%20Daru%20Senate%20Judiciary%20Testimony%20Final.pdf
[104] Matt Day. 2024. Amazon's Ring to Stop Letting Police Request Doorbell Video From Users. https://www.bloomberg.com/news/articles/2024-01-24/amazon-s-ring-to-stop-letting-police-request-video-from-users
[105] Emiliano De Cristofaro, Kris Shrishak, Thorsten Strufe, Carmela Troncoso, and Felix Morsbach. 2025. *PETs and AI: Privacy Washing and the Need for a Pets Evaluation Framework.* Technical Report 25112. Dagstuhl Report.
[106] Miguel Ángel de Diego Martín. 2016. *Net Neutrality: Smart Cables or Dumb Pipes? An Overview on the Regulatory Debate about How to Govern the Network.* Technical Report. College of Europe, Brugge, Belgium. https://aei.pitt.edu/85831/1/researchpaper_3_2016_miguel_angel_de_diego_martin.pdf
[107] Tess Despres, Shishir Patil, Alvin Tan, Jean-Luc Watson, and Prabal Dutta. 2022. Where the Sidewalk Ends: Privacy of Opportunistic Backhaul. In *Proceedings of the 15th European Workshop on Systems Security (EuroSec '22).* ACM, New York, United States, 1–7. https://doi.org/10.1145/3517208.3523757
[108] Deutsche Telekom. 2013. Mobility: Online Any Time, Anywhere. https://www.telekom.com/en/company/details/mobility-online-any-time-anywhere-358830
[109] Deviceroy. 2023. Aria Spec Sheet. https://web.archive.org/web/20240705150847/https://deviceroy.com/wp-content/uploads/2023/04/Aria-Spec-Sheet-1.pdf
[110] Deviceroy. 2023. Connectivity Revolution: Deviceroy's Aria Integrates with Amazon Sidewalk at CES. https://web.archive.org/web/20240906221434/https://deviceroy.com/connectivity-revolution-deviceroys-aria-integrates-with-amazon-sidewalk-at-ces/
[111] Tom Dotan. 2022. Here's the Ranking of Google's Most to Least Profitable Businesses as Investors Press It to Cut Costs. https://www.businessinsider.com/google-alphabet-businesses-most-profitable-2022-12
[112] Thomas Duebendorfer and Stefan Frei. 2007. *Why Silent Updates Boost Security.* Technical Report TIK 302. ETH Zurich. https://tik-old.ee.ethz.ch/file/ef72343372ca8659a9ae8a98873167c0/TIKReport302.pdf
[113] Laura L Ellingson. 2009. Introduction to Crystallization. In *Engaging Crystallization in Qualitative Research.* SAGE Publications, Inc., 1–28. https://doi.org/10.4135/9781412991476.d3
[114] Javier Espinoza. 2020. Apple Accused of Competition Abuse over Tracking Apps. https://www.ft.com/content/a08627c5-61d6-4513-9e7e-acac6b1ba862
[115] European Commission. 2022. Antitrust: Commission Accepts Commitments by Amazon barring It from Using Marketplace Seller Data, and Ensuring Equal Access to Buy Box and Prime. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7777
[116] European Commission. 2025. Commission Launches Market Investigations on Cloud Computing Services under the Digital Markets Act. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2717
[117] European Commission. n.d.. DMA Designated Gatekeepers. https://digital-markets-act.ec.europa.eu/gatekeepers_en
[118] European Union Agency for Cybersecurity. 2022. *Data Protection Engineering: From Theory to Practice.* Technical Report. European Union Agency for Cybersecurity (ENISA). https://doi.org/10.2824/09079
[119] Cyrus Farivar. 2020. Cute Videos, but Little Evidence: Police Say Amazon Ring Isn't Much of a Crime Fighter. https://www.nbcnews.com/news/all/cute-videos-little-evidence-police-say-amazon-ring-isn-t-n1136026
[120] Ed Felten. 2002. Freedom to Tinker. In *11th USENIX Security Symposium (USENIX Security 02).* USENIX Association, San Francisco, CA. https://www.usenix.org/conference/11th-usenix-security-symposium/freedom-tinker
[121] Glenn Fleishman. 2021. How to Opt out of the Find My Network. https://www.macworld.com/article/347243/how-to-opt-out-of-the-find-my-network.html
[122] Bent Flyvbjerg. 2006. Five Misunderstandings About Case-Study Research. *Qualitative Inquiry* 12, 2 (April 2006), 219–245. https://doi.org/10.1177/1077800405284363
[123] Fon. 2014. Fon and OTE Announce WiFi Partnership In Greece. https://fon.com/fon-and-ote-announce-wifi-partnership-in-greece/
[124] freifunk. n.d.. What Is Freifunk About? https://freifunk.net/en/what-is-it-about/
[125] Antone Gonsalves. 2023. OnAsset Logistics Service Taps Amazon Sidewalk. https://www.techtarget.com/searchnetworking/news/365534914/OnAsset-logistics-service-taps-Amazon-Sidewalk
[126] Dan Goodin. 2021. Amazon Devices Will Soon Automatically Share Your Internet with Neighbors. https://arstechnica.com/gadgets/2021/05/amazon-devices-will-soon-automatically-share-your-internet-with-neighbors/
[127] Google. 2024. What Is the Privacy Sandbox? https://web.archive.org/web/20240822053016/https://developers.google.com/privacy-sandbox/overview
[128] Friederike Groschupp, Mark Kuhne, Moritz Schneider, Ivan Puddu, Shweta Shinde, and Srdjan Capkun. 2023. It's Teetime: A New Architecture Bringing Sovereignty to Smartphones. ArXiv. https://arxiv.org/abs/2211.05206
[129] Friederike Groschupp, Mark Kuhne, Moritz Schneider, Ivan Puddu, Shweta Shinde, and Srdjan Capkun. 2023. It's TEEtime: A New Architecture Bringing Sovereignty to Smartphones. https://doi.org/10.48550/arXiv.2211.05206 arXiv:2211.05206
[130] Matthew Guariglia. 2020. What to Know Before You Buy or Install Your Amazon Ring Camera. https://www.eff.org/deeplinks/2020/02/what-know-you-buy-or-install-your-amazon-ring-camera
[131] Matthew Guariglia. 2024. Victory! Ring Announces It Will No Longer Facilitate Police Requests for Footage from Users. https://www.eff.org/deeplinks/2024/01/ring-announces-it-will-no-longer-facilitate-police-requests-footage-users
[132] Matthew Guariglia and Dave Maass. 2021. LAPD Requested Ring Footage of Black Lives Matter Protests. https://www.eff.org/deeplinks/2021/02/lapd-requested-ring-footage-black-lives-matter-protests
[133] Matthew Guariglia, Erica Portnoy, and Bill Budington. 2021. Amazon Ring's End-to-End Encryption: What It Means. https://www.eff.org/deeplinks/2021/02/amazon-rings-end-end-encryption-what-it-means
[134] Seda Gürses, Carmela Troncoso, and Claudia Diaz. 2015. Engineering Privacy by Design Reloaded. In *Amsterdam Privacy Conference 2015.* Amsterdam, The Netherlands. https://www.esat.kuleuven.be/cosic/publications/article-2589.pdf
[135] Seda Gürses and Joris van Hoboken. 2018. Privacy after the Agile Turn. In *The Cambridge Handbook of Consumer Privacy*, Evan Selinger, Jules Polonetsky, and Omer Tene (Eds.). Cambridge University Press, Cambridge, 579–601. https://doi.org/10.1017/9781316831960.032
[136] Amir Haleem, Andrew Allen, Andrew Thompson, Marc Nijdam, and Rahul Garg. 2018. *Helium: A Decentralized Wireless Network.* Technical Report. Helium Systems.
[137] Daniel A Hanley. 2021. *Eyes Everywhere: Amazon's Surveillance Infrastructure and Revitalizing a Fair Marketplace.* Technical Report. Open Markets. https://papers.ssrn.com/abstract=4089858
[138] Mark Harris. 2018. Video Doorbell Firm Ring Says Its Devices Slash Crime—but the Evidence Looks Flimsy. https://www.technologyreview.com/2018/10/19/103922/video-doorbell-firm-ring-says-its-devices-slash-crimebut-the-evidence-looks-flimsy/
[139] Caroline Haskins. 2019. Amazon Requires Police to Shill Surveillance Cameras in Secret Agreement. https://www.vice.com/en/article/mb88za/amazon-requires-police-to-shill-surveillance-cameras-in-secret-agreement
[140] Caroline Haskins. 2019. Ring Told People to Snitch on Their Neighbors in Exchange for Free Stuff. https://www.vice.com/en/article/ne8wqx/ring-told-people-to-snitch-on-their-neighbors-in-exchange-for-free-stuff
[141] Caroline Haskins. 2019. US Cities Are Helping People Buy Amazon Surveillance Cameras Using Taxpayer Money. https://www.vice.com/en/article/d3ag37/us-cities-are-helping-people-buy-amazon-surveillance-cameras-using-taxpayer-money
[142] Alexander Heinrich, Leon Würsching, and Matthias Hollick. 2024. Please Unstalk Me: Understanding Stalking with Bluetooth Trackers and Democratizing Anti-Stalking Protection. *Proceedings on Privacy Enhancing Technologies* 2024, 3 (July 2024), 353–371. https://doi.org/10.56553/popets-2024-0082
[143] Helium. n.d.. LoRaWAN Network Servers. https://docs.helium.com/iot/lorawan-network-servers/
[144] Stacey Higginbotham. 2023. CareBand Bet on Amazon Sidewalk. How Will It Turn Out? https://staceyoniot.com/careband-bet-on-amazon-sidewalk-how-will-it-turn-out/
[145] Jaap-Henk Hoepman. 2014. Privacy Design Strategies. In *ICT Systems Security and Privacy Protection*, Nora Cuppens-Boulahia, Frédéric Cuppens, Sushil Jajodia, Anas Abou El Kalam, and Thierry Sans (Eds.). Springer, Berlin, Heidelberg, 446–459. https://doi.org/10.1007/978-3-642-55415-5_38
[146] Jaap-Henk Hoepman. 2018. *Privacy Design Strategies (The Little Blue Book).* Radboud University, Nijmegen, The Netherlands. hdl:2066/195397 https://hdl.handle.net/2066/195397
[147] Erik Hovenkamp. 2022. The Antitrust Duty to Deal in the Age of Big Tech. *Yale Law Journal* 131 (2022), 1483–1558. https://heinonline.org/HOL/Page?handle=hein.journals/ylr131&id=1537&div=&collection=
[148] Justine Humphry and Chris Chesher. 2021. Visibility and Security in the Smart Home. *Convergence: The International Journal of Research into New Media Technologies* 27, 5 (Oct. 2021), 1170–1188. https://doi.org/10.1177/13548565211030073

[149] Martin Husovec and Irene Roche Laguna. 2023. Digital Services Act: A Short Primer. In *Principles of the Digital Services Act*, Martin Husovec and Irene Roche Laguna (Eds.). Oxford University Press, advance online publication. http://dx.doi.org/10.2139/ssrn.4153796
[150] Index Exchange. 2024. Insights from Our Privacy Sandbox Testing. https://www.indexexchange.com/2024/07/02/insights-privacy-sandbox-testing/
[151] Information Commissioner's Office. 2023. *Privacy-Enhancing Technologies (PETs)*. Technical Report. Information Commissioner's Office. https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies-1-0.pdf
[152] Internet Archive. n.d.. Wayback Machine. https://web.archive.org/
[153] Umar Iqbal, Pouneh Nikkhah Bahrami, Rahmadi Trimananda, Hao Cui, Alexander Gamero-Garrido, Daniel J. Dubois, David Choffnes, Athina Markopoulou, Franziska Roesner, and Zubair Shafiq. 2023. Tracking, Profiling, and Ad Targeting in the Alexa Echo Smart Speaker Ecosystem. In *Proceedings of the 2023 ACM on Internet Measurement Conference (IMC '23)*. ACM, Montreal, Canada, 569–583. https://doi.org/10.1145/3618257.3624803
[154] Catherine Jackson and Angela Orebaugh. 2018. A Study of Security and Privacy Issues Associated with the Amazon Echo. *International Journal of Internet of Things and Cyber-Assurance* 1, 1 (March 2018), 91–100. https://doi.org/10.1504/IJITCA.2018.090172
[155] Md Jakaria, Danny Yuxing Huang, and Anupam Das. 2024. Connecting the Dots: Tracing Data Endpoints in IoT Devices. *Proceedings on Privacy Enhancing Technologies* 2024, 3 (2024), 495–522. https://doi.org/10.56553/popets-2024-0090
[156] Mark A. Jamison. 2018. Net Neutrality Policies and Regulation in the United States. *Review of Network Economics* 17, 3 (Sept. 2018), 151–173. https://doi.org/10.1515/rne-2018-0041
[157] Danny L. Jorgensen. 1989. *Participant Observation: A Methodology for Human Studies*. Applied Social Research Methods Series, Vol. 15. Sage, California, United States. https://search.worldcat.org/title/781976430
[158] Seb Joseph and Ronan Shields. 2024. Google Assures Ad Execs of Revised Third-Party Cookie Controls but Timeline Is Uncertain. https://digiday.com/marketing/google-assures-ad-execs-of-revised-third-party-cookie-controls-but-timeline-is-uncertain/
[159] Aditya Kalra and Steve Stecklow. 2021. Amazon Copied Products and Rigged Search Results, Documents Show. https://www.reuters.com/investigates/special-report/amazon-india-rigging/
[160] Jude Karabus. 2023. Stalking Victims Sue Tile and Amazon for Negligence over Tracking Tech. https://www.theregister.com/2023/08/17/tile_and_amazon_lawsuit/
[161] K. A. Kelly. 2022. The Ring Video Doorbell and the Entry of Amazon into the Smart Home: Implications for Consumer-Initiated Surveillance. *Journal of Consumer Policy* 46 (Dec. 2022), 95–104. https://doi.org/10.1007/s10603-022-09534-3
[162] Reinhold Kesler. 2023. The Impact of Apple's App Tracking Transparency on App Monetization. https://doi.org/10.2139/ssrn.4090786
[163] Konrad Kollnig, Anastasia Shuba, Max van Kleek, Reuben Binns, and Nigel Shadbolt. 2022. Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy Labels. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency (FAccT '22) (FAccT '22)*. ACM, New York, United States, 508–520. https://doi.org/10.1145/3531146.3533116
[164] Blagovesta Kostova, Seda Gürses, and Carmela Troncoso. 2020. Privacy Engineering Meets Software Engineering. On the Challenges of Engineering Privacy By Design. https://doi.org/10.48550/arXiv.2007.08613 arXiv:SSRN
[165] Fiona Kuan. 2023. Extend Your IoT Devices Range with Amazon Sidewalk Devices from MOKOSmart. https://www.mokosmart.com/amazon-sidewalk-devices-from-mokosmart/
[166] Immanuel Kunz, Konrad Weiss, Angelika Schneider, and Christian Banse. 2023. Privacy Property Graph: Towards Automated Privacy Threat Modeling via Static Graph-Based Analysis. *Proceedings on privacy enhancing technologies* 2 (2023), 171–187. https://petsymposium.org/2023/files/papers/issue2/popets-2023-0046.pdf
[167] Frederic Lardinois. 2023. Amazon Sidewalk Adds New Partners, Plans to Open to Developers Soon. https://techcrunch.com/2023/01/05/amazon-sidewalk-adds-new-partners-plans-to-open-to-developers-soon/
[168] Bruno Latour. 1987. *Science in Action: How to Follow Scientists and Engineers through Society*. Harvard University Press, Massachusetts, United States. http://archive.org/details/scienceinaction0000unse
[169] Level. n.d.. Multifamily. https://web.archive.org/web/20240224191314/https://level.co/multifamily/
[170] Level. n.d.. Smart Lock Catalog. https://level.co/smart-lock/
[171] Level. n.d.. Support: Home Integrations: Sidewalk. https://level.co/support/sections/Sidewalk03
[172] John Lofland and Lyn H. Lofland. 1984. *Analyzing Social Settings: A Guide to Qualitative Observation and Analysis* (2 ed.). Wadsworth, California, United States. http://archive.org/details/analyzingsocial00lofl
[173] Minjun Long and David Evans. 2024. Evaluating Google's Protected Audience Protocol. *Proceedings on Privacy Enhancing Technologies* 2024, 4 (2024), 892–906. https://doi.org/10.56553/popets-2024-0147
[174] Orla Lynskey. 2019. Grappling with "Data Power": Normative Nudges from Data Protection and Privacy. *Theoretical Inquiries in Law* 20, 1 (March 2019), 189–220. https://doi.org/10.1515/til-2019-0007
[175] Kim Lyons. 2021. Amazon's Ring Now Reportedly Partners with More than 2,000 US Police and Fire Departments. https://www.theverge.com/2021/1/31/22258856/amazon-ring-partners-police-fire-security-privacy-cameras
[176] Donald MacKenzie. 2024. Hey Big Spender. *London Review of Books* 46, 16 (Aug. 2024). https://www.lrb.co.uk/the-paper/v46/n16/donald-mackenzie/hey-big-spender
[177] Sapna Maheshwari. 2018. How Smart TVs in Millions of U.S. Homes Track More Than What's On Tonight. https://www.nytimes.com/2018/07/05/business/media/tv-viewer-tracking.html
[178] Moxie Marlinspike. 2026. Reflections: The Ecosystem Is Moving. https://signal.org/blog/the-ecosystem-is-moving/
[179] Dana Mattioli. 2020. Amazon Scooped Up Data From Its Own Sellers to Launch Competing Products. https://www.wsj.com/articles/amazon-scooped-up-data-from-its-own-sellers-to-launch-competing-products-11587650015
[180] Dana Mattioli. 2024. Alexa Is in Millions of Households—and Amazon Is Losing Billions. https://www.wsj.com/tech/amazon-alexa-devices-echo-losses-strategy-25f2581a
[181] Patrick McGee. 2021. Apple's Privacy Changes Create Windfall for Its Own Advertising Business. https://www.ft.com/content/074b881f-a931-4986-888e-2ac53e286b9d
[182] Lee McGuigan, Ido Sivan-Sevilla, Patrick Parham, and Yan Shvartzshnaider. 2023. Private Attributes: The Meanings and Mechanisms of "Privacy-Preserving" Adtech. *New Media & Society* (Nov. 2023). https://doi.org/10.1177/14614448231213267
[183] Lee McGuigan, Sarah Myers West, Ido Sivan-Sevilla, and Patrick Parham. 2023. The after Party: Cynical Resignation in Adtech's Pivot to Privacy. *Big Data & Society* 10, 2 (July 2023). https://doi.org/10.1177/20539517231203665
[184] Pradeep Menon. 2023. Best Find My Devices for iPhone in 2023. https://www.xda-developers.com/best-find-my-devices-iphone/
[185] MerryIoT. 2023. MerryIoT Sensors & MerryIoT for Amazon Sidewalk: Quick Installation Guide. https://m.media-amazon.com/images/I/B1UOdj9x16L.pdf
[186] MerryIoT. n.d.. Product. https://web.archive.org/web/20230921152153/merryiot.com/product
[187] Meshify. 2023. Defender S Leak Sensor Product Data Sheet. https://meshify.wpenginepowered.com/wp-content/uploads/2023/10/User-Manual-LDLT003.pdf
[188] Meshify. 2025. Defender Slim Sensor Product Data Sheet. https://meshify.com/wp-content/uploads/2025/05/Meshify-Defender-Slim-Spec-Sheet.pdf
[189] Meshify. n.d.. About. https://meshify.com/about/
[190] Catherine A. Middleton and Amelia Bryne. 2011. An Exploration of User-Generated Wireless Broadband Infrastructures in Digital Cities. *Telematics and Informatics* 28, 3 (Aug. 2011), 163–175. https://doi.org/10.1016/j.tele.2010.08.003
[191] Hooman Mohajeri Moghaddam, Gunes Acar, Ben Burgess, Arunesh Mathur, Danny Yuxing Huang, Nick Feamster, Edward W. Felten, Prateek Mittal, and Arvind Narayanan. 2019. Watching You Watch. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (ACM Conferences)*. 131–147. https://doi.org/10.1145/3319535.3354198
[192] Patrick Moorhead. 2021. Amazon Sidewalk Focuses On Security And Privacy For All IoT Users. https://www.forbes.com/sites/patrickmoorhead/2021/06/07/amazon-sidewalk-focuses-on-security-and-privacy-for-all-iot-users/
[193] Imanol Mugarza, Jose Luis Flores, and Jose Luis Montero. 2020. Security Issues and Software Updates Management in the Industrial Internet of Things (IIoT) Era. *Sensors* 20, 24 (Dec. 2020), 7160. https://doi.org/10.3390/s20247160
[194] Shaoor Munir, Konrad Kollnig, Anastasia Shuba, and Zubair Shafiq. 2024. Google's Chrome Antitrust Paradox. *Vanderbilt Journal of Entertainment & Technology Law* 27 (Feb. 2024). https://papers.ssrn.com/abstract=4780718
[195] Netvox. 2023. New Netvox S315 Series Devices Integrate with Amazon Sidewalk Technology. http://www.netvox.com.tw/news2.asp?pro=107
[196] Netvox. n.d.. Products: Amazon Sidewalk: S315 Series. http://www.netvox.com.tw/protest.asp?pro=a1
[197] New Cosmos USA. 2023. DeNova Detect 807NAS Spec Sheet. https://cdn.shopify.com/s/files/1/0679/6270/0053/files/DeNova_Detect_807NAS_Spec_Sheet--NC0013D.pdf?v=1684865150
[198] New Cosmos USA. n.d.. Amazon Sidewalk Smart Natural Gas Detector. https://web.archive.org/web/20240224120639/https://denovadetect.com/pages/amazon-sidewalk
[199] New Cosmos USA. n.d.. DeNova Detect. https://denovadetect.com/
[200] Lily Hay Newman. 2021. How to Turn Off Amazon Sidewalk. https://www.wired.com/story/turn-off-amazon-sidewalk/
[201] Alfred Ng. 2019. Ring Doorbells Had Vulnerability Leaking Wi-Fi Login Info, Researchers Find. https://www.cnet.com/home/smart-home/ring-doorbells-had-vulnerability-leaking-wi-fi-login-info-researchers-found/
[202] Aiha Nguyen and Eve Zelickson. 2022. *At the Digital Doorstep: How Customers Use Doorbell Cameras to Manage Delivery Workers*. Technical Report. Data &

Society. http://dx.doi.org/10.2139/ssrn.4225083
[203] David Nield. 11-5-21. How Amazon Sidewalk Works—and Why You May Want to Turn It Off. https://www.wired.com/story/how-amazon-sidewalk-works/
[204] Nova Labs. 2026. Helium/Denylist. Helium. https://github.com/helium/denylist
[205] Nova Labs. n.d.. Helium IoT Network. https://www.helium.com/iot
[206] Nova Labs. n.d.. Helium Mobile Network. https://www.helium.com/mobile
[207] OnAsset Intelligence. 2023. OnAsset Intelligence Launches Dedicated Supply Chain Monitoring Device on Amazon Sidewalk. https://onasset.com/2023/03/28/onasset-intelligence-launches-dedicated-supply-chain-monitoring-device-on-amazon-sidewalk/
[208] OnAsset Intelligence. n.d.. Products. https://www.onasset.com/products/#sentinel100
[209] Sean O'Neill. 2023. Everything You Need to Know about Amazon Sidewalk, the Secure, Low-Cost Network That Can Connect Devices up to Half a Mile Away. https://www.aboutamazon.com/news/devices/everything-you-need-to-know-about-amazon-sidewalk
[210] OpenThread. 2025. OpenThread Border Router. https://openthread.io/guides/border-router
[211] Will Oremus. 2019. Amazon Just Became the Everywhere Store. https://onezero.medium.com/amazon-just-became-the-everywhere-store-dce9353decd3
[212] Peter Ormerod. 2024. Privacy Law's Incumbency Problem. *UC Davis Law Review* 58, 1 (2024). https://papers.ssrn.com/abstract=4819613
[213] Douglas A. Orr and Laura Sanchez. 2018. Alexa, Did You Get That? Determining the Evidentiary Value of Data Stored by the Amazon® Echo. *Digital Investigation* 24 (March 2018), 72–78. https://doi.org/10.1016/j.diin.2017.12.002
[214] Jennifer Ortakales and Eugene Kim. 2024. Amazon Layoffs: A Timeline of the Company's Hiring Freezes, Restructuring Efforts, and Staff Reductions into 2024. https://www.businessinsider.com/amazon-layoffs
[215] Susan A Ostrander. 1993. "Surely You're Not in This Just to Be Helpful": Access, Rapport, and Interviews in Three Studies of Elites. *Journal of Contemporary Ethnography* 22, 1 (April 1993), 7–27. https://doi.org/10.1177/089124193022001002
[216] Lauren R. Pace, LaSean A. Salmon, Christopher J. Bowen, Ibrahim Baggili, and Golden G. Richard. 2023. Every Step You Take, I'll Be Tracking You: Forensic Analysis of the Tile Tracker Application. *Forensic Science International: Digital Investigation* 45, Supplement (July 2023), Article 301559. https://doi.org/10.1016/j.fsidi.2023.301559
[217] Vincent Paquette. 2026. Amazon Sidewalk débarque au Canada, c'est quoi ça? https://francoischarron.com/gadgets-techno/web-applications/amazon-sidewalk-debarque-au-canada-cest-quoi-ca/DDny9Sfkog/
[218] Todd Parsons. 2024. Privacy Sandbox Testing Results Show Shortfalls to Meet CMA Requirements. https://www.criteo.com/blog/privacy-sandbox-testing-results-show-shortfalls-to-meet-cma-requirements/
[219] Jon Parton. 2021. Amazon's Sidewalk Technology Faces Federal Class Action. https://www.courthousenews.com/amazons-sidewalk-technology-faces-federal-class-action
[220] Ben Patterson. 2021. Welcome to Amazon Sidewalk! Now Here's How to Turn It off. https://www.techhive.com/article/579021/how-to-turn-off-amazon-sidewalk.html
[221] Ben Patterson and Michael Simon. 2019. How to Keep Amazon, Apple, and Google from Listening to Your Alexa, Siri, and Assistant Recordings. https://www.techhive.com/article/583911/how-to-keep-amazon-and-google-from-listening-to-your-alexa-and-assistant-voice-recordings.html
[222] Pebblebee. n.d.. Clip, Card and Tag - Apple Find My™ vs Google's Find My Device. https://web.archive.org/web/20240914083235/https://help.pebblebee.com/article/lurhtifwcm-card-and-clip-on-an-android-and-ios
[223] Pebblebee. n.d.. Pebblebee. https://pebblebee.com/
[224] Pôle d'expertise de la régulation numérique. 2022. *Privacy Sandbox : une collection d'outils pour une publicité en ligne exempte de cookies tiers.* Technical Report 3. Pôle d'expertise de la régulation numérique, Paris, France. https://www.peren.gouv.fr/rapports/2022-04-07%20-%20Eclairage-sur-privacy-sandbox_FR.pdf
[225] Michael Potuck. 2021. Apple Antitrust Hearing: Tile Likens Find My Network to a 'hostage' Program, App Store Scam Apps, More. https://9to5mac.com/2021/04/21/apple-antitrust-hearing-tile-spotify-more/
[226] Primax Electronics. n.d.. Primax Electronics Ltd. Launches a New Smart Door Lock That Works With Amazon Sidewalk. https://www.primax.com.tw/en/press-center/company-news?view=article&id=251:primax-electronics-ltd-launches-a-new-smart-door-lock-that-works-with-amazon-sidewalk&catid=15
[227] John Quintet. 2026. Amazon Sidewalk Arrives in Canada Feb. 26: How to Opt Out of the Shared Network. https://www.iphoneincanada.ca/2026/01/27/amazon-sidewalk-arrives-in-canada-feb-26-how-to-opt-out-of-the-shared-network/
[228] Andrea Renda and Christopher Yoo. 2015. Telecommunications and the Internet: TTIP's Digital Dimension. In *Rule-Malers or Rule Takers? Exploring the Transatlantic Trade and Investment Partnership*, Daniel S Hamilton and Jacques Pelkmans (Eds.). Rowman & Littlefield International, London, England, 371–422. https://scholarship.law.upenn.edu/faculty_scholarship/2621/
[229] Ring. 2026. Ring Unveils a New Generation of Smarter, More Connected Security at CES 2026. https://blog.ring.com/about-ring/ring-unveils-a-new-generation-of-smarter-more-connected-security-at-ces-2026/
[230] Ring. 2026. Ring Unveils a New Generation of Smarter, More Connected Security at CES 2026. https://blog.ring.com/about-ring/ring-unveils-a-new-generation-of-smarter-more-connected-security-at-ces-2026/
[231] Ring. n.d.. Products. https://ring.com/collections/all-products
[232] Ring. n.d.. Video Doorbell Pro 2. https://nl-nl.ring.com/products/video-doorbell-pro-2
[233] Viktoria H. S. E. Robertson. 2022. Antitrust, Big Tech, and Democracy: A Research Agenda. *The Antitrust Bulletin* 67, 2 (June 2022), 259–279. https://doi.org/10.1177/0003603X221082749
[234] Nick Robins-Early. 2024. US Accuses Apple of 'Broad, Sustained, and Illegal' Smartphone Monopoly. https://www.theguardian.com/technology/2024/mar/21/us-antitrust-lawsuit-apple
[235] Benjamin Romano. 2019. Amazon Rolls out New Devices amid Swirl of Privacy Questions. https://www.seattletimes.com/business/amazon/amazon-rolls-out-new-devices-amid-swirl-of-privacy-questions/
[236] Paulette M. Rothbauer, J. Moran-Ellis, V. D. Alexander, A. Cronin, M. Dickinson, J. Fielding, and J. Sleney. 2008. Triangulation. In *The SAGE Encyclopedia of Qualitative Research Methods*. SAGE Publications, Inc. https://doi.org/10.4135/9781412963909.n468
[237] Jennifer Rowley. 2002. Using Case Studies in Research. *Management Research News* 25, 1 (Jan. 2002), 16–27. https://doi.org/10.1108/01409170210782990
[238] Shivan Kaul Sahib. 2023. Trust Issues. In *Eaten by the Internet*, Corinne Cath (Ed.). Meatspace Press, Amsterdam, The Netherlands, 35–42. https://archive.org/details/eaten-by-the-internet
[239] Johnny Saldaña. 2021. *The Coding Manual for Qualitative Researchers* (4 ed.). SAGE, London, England. https://search.worldcat.org/title/1233312600
[240] Nikita Samarin, Alex Sanchez, Trinity Chung, Akshay Dan Bhavish Juleemun, Conor Gilsenan, Nick Merrill, Joel Reardon, and Serge Egelman. 2024. The Medium Is the Message: How Secure Messaging Apps Leak Sensitive Data to Push Notification Services. *Proceedings on Privacy Enhancing Technologies* 2024, 4 (2024), 967–982. https://doi.org/10.56553/popets-2024-0151
[241] David Schmidt, Carlotta Tagliaro, Kevin Borgolte, and Martina Lindorfer. 2023. IoTFlow: Inferring IoT Device Behavior at Scale through Static Mobile Companion App Analysis. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS '23) (CCS '23)*. ACM, New York, United States, 681–695. https://doi.org/10.1145/3576915.3623211
[242] Justin Schuh. 2020. Building a More Private Web: A Path towards Making Third Party Cookies Obsolete. https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html
[243] Evan Selinger and Darrin Durant. 2022. Amazon's Ring: Surveillance as a Slippery Slope Service. *Science as Culture* 31, 1 (Jan. 2022), 92–106. https://doi.org/10.1080/09505431.2021.1983797
[244] Eric Benjamin Seufert. 2024. Why Is Google Killing Cookies? https://mobiledevmemo.com/why-is-google-killing-cookies/
[245] Tamar Sharon and Raphaël Gellert. 2024. Regulating Big Tech Expansionism? Sphere Transgressions and the Limits of Europe's Digital Regulatory Strategy. *Information, Communication & Society* 27, 15 (Nov. 2024), 2651–2668. https://doi.org/10.1080/1369118X.2023.2246526
[246] Tamar Sharon, Marthe Stevens, Andrew Hoffman, Steven Kraaijeveld, and Lotje Siffels. n.d.. Sphere Transgression Watch. https://www.sphere-transgression-watch.org/
[247] Ronan Shields and Seb Joseph. 2024. Ad Tech Bosses Balance Frustration and Focus after Google's Latest Shift on Third-Party Cookies. https://digiday.com/marketing/ad-tech-bosses-balance-frustration-and-focus-after-googles-latest-shift-on-third-party-cookies/
[248] Kris Shrishak. 2025. Privacy Washing through PETs: The Case of Worldcoin. https://cacm.acm.org/blogcacm/privacy-washing-through-pets-the-case-of-worldcoin/
[249] Manny Sidhu and Ben Cooke. 2024. Building Track and Trace Applications Using AWS IoT Core for Amazon Sidewalk. https://aws.amazon.com/blogs/iot/building-track-and-trace-applications-using-aws-iot-core-for-amazon-sidewalk/
[250] Suzanne Smalley. 2024. Plaintiffs in Tile Suit File More Examples of Company Allegedly Blocking Law Enforcement. https://therecord.media/lawsuit-alleges-tile-tracker-blocked-law-enforcement
[251] Smart Water Watch. 2023. Subeca Aims to Bring Amazon Experience to Water Sector. https://www.globalwaterintel.com/global-water-intelligence-magazine/24/7/smart-water-watch/subeca-aims-to-bring-amazon-experience-to-water-sector
[252] Adrienne So. 2023. Why We Don't Recommend Ring Cameras. https://www.wired.com/story/why-we-do-not-recommend-ring/
[253] Solana Foundation. 2025. Case Study: A Technical Deep Dive on Helium. https://solana.com/news/case-study-helium-technical-guide

[254] Angelo M. Solarino and Herman Aguinis. 2021. Challenges and Best-practice Recommendations for Designing and Conducting Interviews with Elite Informants. *Journal of Management Studies* 58, 3 (2021), 649–672. https://doi.org/10.1111/joms.12620

[255] Victoria Song. 2023. Are Amazon Sidewalk's Privacy Protocols Ready for the Real World? https://www.theverge.com/2023/4/8/23671594/amazon-sidewalk-privacy-echo-ring-smart-home

[256] I. Dwaraka Srihith, A. David Donald, T. Aditya Sai Srinivas, D. Anjali, and A. Chandana. 2023. Firmware Attacks: The Silent Threat to Your IoT Connected Devices. *International Journal of Advanced Research in Science, Communication and Technology* 3, 2 (April 2023), 145–154. https://doi.org/10.48175/IJARSCT-9104

[257] Nick Srnicek. 2022. *Data, Compute, Labor*. The MIT Press. https://direct.mit.edu/books/oa-edited-volume/5319/chapter/3800166/Data-Compute-Labor

[258] Joseph Srouji and Thibault Mechler. 2020. How Privacy-Enhancing Technologies Are Transforming Privacy by Design and Default: Perspectives for Today and Tomorrow. *Journal of Data Protection & Privacy* 3, 3 (June 2020), 268–280. https://ideas.repec.org/a/aza/jdpp00/y2020v3i3p268-280.html

[259] StatCounter. 2024. Mobile Operating System Market Share Worldwide Dec 2019 - June 2024. https://gs.statcounter.com/os-market-share/mobile/worldwide

[260] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, Danny Yuxing Huang, and Rahul Chatterjee. 2023. Abuse Vectors: A Framework for Conceptualizing {IoT-Enabled} Interpersonal Abuse. In *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, United States, 69–86. https://www.usenix.org/conference/usenixsecurity23/presentation/stephenson-vectors

[261] Subeca. 2023. Enhancing Water Utility Surveillance and Response (SRS) with Subeca - Subeca. https://web.archive.org/web/20240424082609/https://www.subeca.com/blogs/enhancing-water-utility-surveillance-and-response-srs-with-subeca

[262] Subeca. 2023. Subeca, Inc. Joins Forces with Amazon Sidewalk to Innovate and Simplify Water Metering. https://www.subeca.com/resources/subeca-inc-joins-forces-with-amazon-sidewalk-to-innovate-and-simplify-water-metering

[263] Wei Sun, Tingjun Chen, and Neil Gong. 2024. SoK: Secure Human-centered Wireless Sensing. *Proceedings on Privacy Enhancing Technologies* 2024, 2 (2024), 313–329. https://doi.org/10.56553/popets-2024-0052

[264] Wei Sun, Hadi Givehchian, and Dinesh Bharadia. 2025. Revealing Hidden IoT Devices through Passive Detection, Fingerprinting, and Localization. *Proceedings on Privacy Enhancing Technologies* 2025, 1 (2025), 184–197. https://doi.org/10.56553/popets-2025-0011

[265] Surfshark. 2024. The Insights of Our Smart Home Privacy Checker. https://surfshark.com/research/smart-homes/insights

[266] Surfshark. 2024. Methodology. https://surfshark.com/research/smart-homes/methodology

[267] Richard Swedberg. 2020. Exploratory Research. In *The Production of Knowledge: Enhancing Progress in Social Science*, Colin Elman, John Gerring, and James Mahoney (Eds.). Cambridge University Press, Cambridge, England, 17–41. https://doi.org/10.1017/9781108762519.002

[268] Christina Tabacco. 2022. The Road Ends for Consumers Pursuing Amazon 'Sidewalk' Mesh Network Class Action. https://lawstreetmedia.com/news/tech/the-road-ends-for-consumers-pursuing-amazon-sidewalk-mesh-network-class-action/

[269] Tag-N-Trac. n.d.. Smart Sensing. https://web.archive.org/web/20231205120611/https://tagntrac.com/smart-sensing/

[270] Texas Instruments. 2020. Connect: Amazon Sidewalk Chat with Airthings and Tag-n-Trac. https://www.youtube.com/watch?v=qIXSgGq2iKw

[271] Adam Thierer. 2005. Are "Dumb Pipe" Mandates Smart Public Policy? Vertical Integration, Net Neutrality, and the Network Layers Model. *Journal on Telecommunications & High-Technology Law* 3 (2005), 275–308. https://heinonline.org/HOL/LandingPage?handle=hein.journals/jtelhtel3&div=16

[272] Thingy-IoT. n.d.. Home. https://thingy-iot.au/

[273] Thread Group. 2020. Thread Border Router: The Simple Component to Get Your Thread Network Started. https://threadgroup.org/Newsroom/Blog/thread-border-router-the-simple-component-to-get-your-thread-network-started

[274] Thread Group. 2022. *Thread Smart Home Fact Sheet*. Technical Report. California, United States. https://portal.threadgroup.org/DesktopModules/Inventures_Document/FileDownload.aspx?ContentID=834

[275] Thread Group. n.d.. Certified Products. https://threadgroup.org/What-is-Thread/Certified-Products

[276] Thread Group. n.d.. Developers. https://threadgroup.org/What-is-Thread/Developers

[277] Tile. 2021. Amazon Sidewalk Is About to Strengthen the Finding Power of Your Tiles. https://www.tile.com/en-us/blog/sidewalk-strengthening-the-power-of-your-tiles

[278] Tile. 2021. *Observations of Tile on the Statement of Scope of the CMA's Mobile Ecosystems Market Study*. Technical Report. https://www.gov.uk/cma-cases/mobile-ecosystems-market-study#responses-to-statement-of-scope

[279] Tile. n.d.. How Tile Works. https://www.tile.com/en-eu/how-it-works

[280] Trey Titone. 2024. Assessing the Impact of Google's Privacy Sandbox. https://adtechexplained.com/assessing-the-impact-of-googles-privacy-sandbox/

[281] Trey Titone. 2024. Why Is Google No Longer Deprecating Cookies? https://adtechexplained.com/why-is-google-no-longer-deprecating-cookies/

[282] Félix Tréguer. 2019. Seeing like Big Tech: Security Assemblages, Technology, and the Future of State Bureaucracy. In *Data Politics*. Routledge. https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9781315167305-8/seeing-like-big-tech-f%C3%A9lix-tr%C3%A9guer

[283] Carmela Troncoso, Dan Bogdanov, Edouard Bugnion, Sylvain Chatel, Cas Cremers, Seda Gürses, Jean-Pierre Hubaux, Dennis Jackson, James R. Larus, Wouter Lueks, Rui Oliveira, Mathias Payer, Bart Preneel, Apostolos Pyrgelis, Marcel Salathé, Theresa Stadler, and Michael Veale. 2022. Deploying Decentralized, Privacy-Preserving Proximity Tracing. *Commun. ACM* 65, 9 (Aug. 2022), 48–57. https://doi.org/10.1145/3524107

[284] Carmela Troncoso, Marios Isaakidis, George Danezis, and Harry Halpin. 2017. Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments. *Proceedings on Privacy Enhancing Technologies* 2017, 4 (June 2017), 404–426. https://doi.org/10.1515/popets-2017-0056

[285] Jennifer Pattison Tuohy. 2022. Amazon Announces a Phased Rollout of Matter to Its Alexa Smart Home Platform. https://www.theverge.com/2022/11/3/23438286/amazon-matter-support-alexa-echo-smart-home-platform

[286] Jennifer Pattison Tuohy. 2023. What Matters about Matter, the New Smart Home Standard. https://www.theverge.com/22832127/matter-smart-home-products-thread-wifi-explainer

[287] Jennifer Pattison Tuohy. 2024. There's a Secret Smart Home Radio in Your New Mac. https://www.theverge.com/2024/6/5/24170446/apple-macbook-ipad-imac-thread-radio

[288] Jennifer Pattison Tuohy. 2026. Ikea Tried to Build a Smart Home for Everyone — Here's Why It's Not Working yet. https://www.theverge.com/tech/896006/ikea-matter-thread-smart-home-problems

[289] Kieron Ivy Turk, Alice Hutchings, and Alastair R. Beresford. 2023. Can't Keep Them Away: The Failures of Anti-stalking Protocols in Personal Item Tracking Devices. In *Security Protocols XXVIII (Lecture Notes in Computer Science)*, Frank Stajano, Vashek Matyáš, Bruce Christianson, and Jonathan Anderson (Eds.). Springer Nature Switzerland, Cham, 78–88. https://doi.org/10.1007/978-3-031-43033-6_9

[290] Trond Arne Undheim. 2003. Getting Connected: How Sociologists Can Access The High Tech Élite. *The Qualitative Report* 8, 1 (June 2003), 104–128. https://doi.org/10.46743/2160-3715/2003.1902

[291] United States Senate Committee on the Judiciary. 2021. Antitrust Applied: Examining Competition in App Stores. https://www.judiciary.senate.gov/committee-activity/hearings/antitrust-applied-examining-competition-in-app-stores

[292] Urząd Ochrony Konkurencji i Konsumentów. 2021. Apple - the President of UOKiK initiates an investigation. https://archiwum.uokik.gov.pl/aktualnosci.php?news_id=18092

[293] Urząd Ochrony Konkurencji i Konsumentów. 2025. Is Apple Restricting Competition? President of UOKiK Brings Charges. https://uokik.gov.pl/en/is-apple-restricting-competition-president-of-uokik-brings-charges

[294] Lisa Vaas. 2021. Amazon Sidewalk Poised to Sweep You Into Its Mesh. https://threatpost.com/amazon-sidewalk-to-sweep-you-into-its-mesh/166581/

[295] Thijmen van Gend, Donald Jay Bertulfo, and Seda Gürses. 2024. Privacy: The More, the Merrier?. In *Privacy Law Scholars Conference Europe*. Amsterdam, The Netherlands. https://www.ivir.nl/plsce2024/accepted-abstracts/

[296] Thijmen van Gend, Donald Jay Bertulfo, and Seda Gürses. 2026. The PET Paradox: How Amazon Instrumentalises PETs in Sidewalk to Entrench Its Infrastructural Power. In *Digital Competition Conference 2026*. Knight-Georgetown Institute, Washington DC, USA. https://kgi.georgetown.edu/events/digital-competition-conference-2026/

[297] Suzanne van Geuns and Corinne Cath. 2020. How Hate Speech Reveals the Invisible Politics of Internet Infrastructure. https://www.brookings.edu/articles/how-hate-speech-reveals-the-invisible-politics-of-internet-infrastructure/

[298] Janus Varmarken, Hieu Le, Anastasia Shuba, Athina Markopoulou, and Zubair Shafiq. 2020. The TV Is Smart and Full of Trackers: Measuring Smart TV Advertising and Tracking. *Proceedings on Privacy Enhancing Technologies* 2020, 2 (April 2020), 129–154. https://doi.org/10.2478/popets-2020-0021

[299] Michael Veale. 2023. Confidentiality Washing in Online Advertising. In *Eaten by the Internet*, Corinne Cath (Ed.). Meatspace Press, Amsterdam, The Netherlands, 43–48. https://archive.org/details/eaten-by-the-internet

[300] Michael Veale. 2023. Denied by Design? Data Access Rights in Encrypted Infrastructures. In *Research Access to Digital Infrastructures*, Jef Ausloos and Siddharth P de Souza (Eds.). Advance online publication. https://doi.org/10.31235/osf.io/94y6r

[301] Michael Veale. n.d.. Rights for Those Who Unwillingly, Unknowingly and Unidentifiably Compute! In *The Person and the Future of Private Law*, Hans-Wolfgang Micklitz and Giuseppe Vettori (Eds.). Hart. doi.org/10.31235/osf.io/4ugxd

[302] Scott Waller. 2022. Thingy and Sidewalk for Wildfire Smoke and Air Quality. https://web.archive.org/web/20220705152429/https:/thingy.us/thingy-and-sidewalk-for-wildfires/

[303] Zhaohui Wang, Bo Luo, and Fengjun Li. 2025. PrivacyGuard: Exploring Hidden Cross-App Privacy Leakage Threats In IoT Apps. *Proceedings on Privacy Enhancing Technologies* 2025, 1 (2025), 776–791. https://doi.org/10.56553/popets-2025-0040

[304] Charlie Warzel. 2019. Opinion: Amazon Wants to Surveil Your Dog. https://www.nytimes.com/2019/10/01/opinion/amazon-privacy.html

[305] Jean-Luc Watson, Tess Despres, Alvin Tan, Shishir G. Patil, Prabal Dutta, and Raluca Ada Popa. 2024. Nebula: A Privacy-First Platform for Data Backhaul. In *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, Los Alamitos, CA, USA, 3184–3202. https://doi.org/10.1109/SP54263.2024.00092

[306] Emily West. 2019. Amazon: Surveillance as a Service. *Surveillance & Society* 17, 1/2 (March 2019), 27–33. https://doi.org/10.24908/ss.v17i1/2.13008

[307] Tiahn Wetzler. 2023. ATT Two Years on: Opt-in Rates Keep Climbing. https://www.adjust.com/blog/app-tracking-transparency-opt-in-rates/

[308] Meredith Whittaker. 2025. Signal's President on Using AWS: The Real Problem Is Infrastructure Monopoly. https://aboutsignal.com/news/signals-president-on-using-aws-the-real-problem-is-infrastructure-monopoly/

[309] Lewis Wight. 2023. The Promised Growth of IoT. https://meshify.com/the-promised-growth-of-iot/

[310] A.K. Woods. 2018. Litigating Data Sovereignty. *Yale Law Journal* 128, 2 (2018), 328–406. https://www.yalelawjournal.org/article/litigating-data-sovereignty

[311] Xfinity. n.d.. Xfinity WiFi Home Hotspot FAQs. https://www.xfinity.com/support/articles/xfinity-wifi-hotspots

[312] Robert K. Yin. 2017. *Case Study Research and Applications: Design and Methods* (6 ed.). SAGE Publications, Inc, Washington, D.C. https://us.sagepub.com/en-us/nam/case-study-research-and-applications/book250150

[313] Yubico. n.d.. YubiHSM 2 v2.3.2. https://www.yubico.com/product/yubihsm-2/

[314] Channy Yun. 2025. Introducing AWS IoT Core Device Location Integration with Amazon Sidewalk. https://aws.amazon.com/blogs/aws/introducing-aws-iot-core-device-location-integration-with-amazon-sidewalk/

A Elaboration of case description and methods

This appendix further details our case description and methods (§2.3). We present the identified adopters (§A.1), some Sidewalk marketing materials (§A.2), the codebook (§A.4), and interview questions (§A.5).

A.1 Overview of identified adopters

Table 2 displays the Sidewalk adopters identified in the grey literature review and interviews. To protect participants' anonymity, we make no reference to specific interviewees here. For most companies, catering to businesses or consumers is not a binary choice: consumer devices can also be bought by businesses for office use. Where marketing strategies, public materials, or interviews signalled a focus on one target group over the other, we list this targeted audience.

A.2 Sidewalk marketing visuals

Figure 2 shows the current coverage of Sidewalk [37]. Figure 3 shows examples of how Amazon visualises Sidewalk to consumers (both gateway and endpoint owners).

A.3 Sidewalk's value proposition

Figure 3 shows multiple visuals that Amazon uses to convey Sidewalk's value proposition, targeted at gateway and endpoint owners. The graphics emphasise different aspects of the service.

A.4 Codebook

Table 3 shows the eleven top-level categories and the corresponding second-tier codes. We do not include the lowest-tier codes for maintaining anonymity of participants as well as readability.

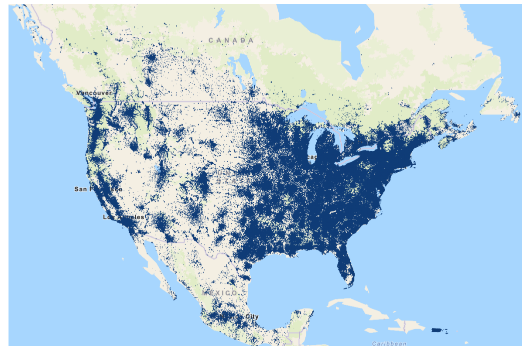

Figure 2: Sidewalk coverage in May 2026 [37]. Blue dots indicate coverage.

Figure 3: Visuals that stress Sidewalk's multi-layered encryption *(a, d)*, crowdsourced nature benefiting communities *(b, d)*, bandwidth constraints *(c)*, and use cases *(d)*. *a* and *c* reproduced from [209]; *b* and *d* reproduced from [39].

A.5 Interview questions

The prepared interview questions are given below. Because of the semi-structured nature, and because some questions were not applicable for all respondents, we may have skipped certain questions or formulated them differently. Likewise, and in order to ensure spontaneous answers, we did not share interview questions beforehand – except upon one participant's request. We only provided interviewees with the clarifications appended to the question between parentheses if they did not understand the question, to prevent inducing bias in their answer. Further personal questions used for rapport building are not included to protect anonymity of the participants.

Table 2: Overview of identified Sidewalk adopters, products, and business orientations

Company name	Product name (if available): functionality	Main business model	References
Airthings	Sensing CO2, radon, temperature, humidity, and air quality	B2B, B2C	[5; 6; 65; 66; 270]
Arrive	Point, Bank, Convey, Package Tower: smart mailbox(es), Mailbox as a Service	B2B	[55–57]
CareBand	CareBand: panic button, location and activity detection; for elderly people, contact tracing, and outdoors worker safety	B2B, B2C	[84; 85; 144]
DeNova Detect (by New Cosmos)	807NAS: natural gas alarm	B2B, B2C	[197–199]
Deviceroy	Aria: relaying an industrial device's readings to the internet	B2B	[109; 110]
Level	Level: smart door lock	B2B, B2C	[15; 169–171]
MerryIoT (by Browan Communications)	Four devices for sensing CO2, motion, door/window open/close, water leak, temperature, and humidity	B2C	[185; 186]
Meshify (by HSB)	Defender S, Defender Slim: water leak and water pipe freeze/break sensing	B2B	[187–189; 309]
MOKO-Smart	Motion detection, asset and person tracking, smart plug	B2B (OEM)	[165]
Netvox	S315 series: integrates modular sensors; supports sensing temperature, humidity, motion, water leaks, vibration, light, and door contact	B2B (OEM)	[18; 195; 196]
OnAsset	Sentinel 200: asset tracking and condition monitoring)	B2B	[18; 125; 207; 208]
Primax	Woody: smart door lock	B2B (OEM)	[18; 226]
Subeca	Pin: Advanced Meter Infrastructure sensor for water utilities	B2B	[251; 261; 262]
Tag-n-Trac	Smart Sense: asset tracking and condition monitoring	B2B	[269; 270]
Thingy	Thingy: air quality sensing, specifically for early wildfire detection	B2B	[272; 302]
Tile	Tile: asset tracking	B2B, B2C	[15; 277]

A.5.1 Rapport building.

Background and expertise of interviewee

(1) Can you tell me about your company and your role therein?

Company profile

(2) What kind of customers do you cater to, and which has your primary focus? *(E.g. business or consumer users; geographical area of focus; market domain (building management, logistics, utilities))*
(3) What share of your customers is business or consumer?
(4) What drew you to catering to these types of customers?
(5) What are the differences in the requirements from and use cases of the different customer types that you cater to?
(6) What type of customer do you think Sidewalk has a stronger case for? *(E.g. B2C or B2B)*

A.5.2 Grand tour and mini-tour questions.

Adoption and motivation

(7) How did you discover Sidewalk?
(8) What novel opportunities does Sidewalk provide? *(E.g. compared to other connectivity protocols)*
(9) How important is Sidewalk to your product, service, or company? *(E.g. compared to the other connectivity modes you use)*
(10) Is your service really based on the availability of Sidewalk, or were you already developing your service before Sidewalk was published?
(11) Which of the three connectivity protocols of Sidewalk do you use (i.e. LoRa, FSK, BLE)?
(12) What connectivity methods other than Sidewalk have you considered? *(E.g. LoRaWAN, Bluetooth, Matter)*
(13) How does Sidewalk compare to these other methods?
(14) I found references mentioning your company's (prospective) adoption of Sidewalk, but your product page does not mention Sidewalk and lacks the 'Works with Amazon Sidewalk'-badge. What is your adoption status?
(15) Your organisation sells both Sidewalk-compatible devices, and non-compatible counterparts using other connectivity methods. Why the separation?
(16) Did you have doubts around adopting Sidewalk? How were they addressed, or what pulled you over the line?

Privacy and security

(17) Has your use of Sidewalk changed the privacy architecture or governance of your IoT offerings?
(18) Does Sidewalk help address privacy and/or cybersecurity concerns better than other communication methods?

Production and cloud usage

(19) Does your company use the cloud for offering or producing your products and services? If so, which provider do you use?
(20) Were you already using cloud services before adopting Sidewalk?
(21) Has adopting Sidewalk led to a change in how you use the cloud? If yes, how?
(22) Did your earlier use of AWS ease your adoption of Sidewalk?
(23) How do you process data sent over Sidewalk?
(24) How do you use AWS IoT Core for Sidewalk?
(25) How do you process data sent over other connectivity protocols? *(E.g. LoRaWAN)*
(26) Is the data sent over Sidewalk processed differently than data sent over other connectivity protocols, such as LoRaWAN?
(27) Has adopting Sidewalk changed the way in which you produce your devices? If yes, how? *(E.g. with relation to key management or enabling device authentication with Sidewalk;*

Table 3: Excerpt of codebook, showing the first-tier (in bold) and second-tier codes

Code	Grounded	Code (cont.)	Grounded (cont.)
Advantages of Sidewalk	**48**	**IoT industry dynamics, competition, and partnerships**	**138**
A connectivity service without the manufacturer nor end-user needing to put out gateways	11	Amazon competing with telecom providers and tech companies	5
Cheap	10	Competition by Amazon: countermeasures taken	8
Developing the LoRa/IoT/smarthome ecosystems and markets	13	Competition by Amazon: perceived impact / level of concern	24
Improves / eases user experience	8	Competition by Amazon: perceived probability	22
Improves adopter’s reputation / leverages Amazon’s reputation	4	Competition by Apple and Google	4
Perception of (the significance of) Sidewalk’s value for company	10	Manufacturer’s other partnerships	6
Alternative connectivity protocols	**88**	Manufacturer’s perception of Sidewalk longevity/sustainability	3
Bluetooth	3	Relation of Amazon with silicon providers	11
Cellular	1	Relation of manufacturer with Amazon not regarding Sidewalk (e.g. Marketplace)	15
Comcast MachineQ	3	Relation of manufacturer with Amazon regarding Sidewalk	26
Complicated to support multiple protocols	3	Relation of manufacturer with silicon provider	15
Experience with supporting multiple protocols simultaneously	30	Risk of commoditisation when adopting another company’s network/protocol	3
Helium	2	Vision of competitive ecosystem: comparison with Amazon: "choices ... based on what we knew, is the same as someone who probably knows more"	2
LoRa	16	Vision of future Sidewalk/LoRaWAN ecosystem ("I think at the end of the day, LoRaWAN Alliance would prevail")	10
LoRa satellite	2	**Privacy**	**55**
Matter	12	(Merits of) public privacy concerns of Sidewalk’s privacy, and PETs to address them	18
Rationale for supporting multiple protocols simultaneously	21	Advantage of opt-out roll-out: coverage without user intervention	6
Sigfox	3	Company’s privacy governance: no change after adopting Sidewalk	7
UWB	1	PETs and data visibility	15
Wi-SUN	1	Privacy as a (more or less important) customer requirement / precondition for delivering IoT services	7
Wifi	3	Public reception of other crowdsourced services/infrastructures	4
Xfinity Connect (Comcast)	1	**Production before and after adopting Sidewalk**	**57**
Amazon’s culture and motivation to develop and marketing of Sidewalk	**46**	(Changes in) rationales for cloud usage	15
"everybody wanted to own the smart home"	2	Changes in (producing with) chips / endpoint hardware	3
Amazon culture and the position of Sidewalk vis-à-vis other services/products/departments	8	Cloud usage (AWS)	23
Creating an ecosystem / infrastructure / layer for IoT networking	9	Cloud usage (non-AWS)	15
Expectation of Sidewalk roll-out outside USA	4	Experienced difficulty in adopting Sidewalk	5
Increase manufacturers’ use of AWS	2	Factory line, device provisioning, and implementing encryption	10
Marketing towards consumers (gateway/endpoint users/owners)	7	**Security**	**46**
Marketing towards manufacturers	3	Company’s security measures and principles (in addition to Sidewalk’s / before adopting)	14
Obtaining "data"	2	Competing on security with other IoT companies	5
Potentially useful for logistics department	1	Customer’s perception / assessment of security for interviewee’s services and/or Sidewalk	5
Reduction of Amazon’s hardware business	9	Perception of Sidewalk’s level of security	18
Disadvantages of Sidewalk	**42**	Specific security requirements for own product/service	6
Gateway owners did not consent	2	Using cloud services for cybersecurity regulation compliance	3
Insufficient coverage	1	**Sidewalk governance**	**47**
Lacking functionality/utility	4	Certification process	9
Need other protocols as backup/mitigation for reliance	6	Closed, proprietary network	20
Negative public reception of Sidewalk	8	Invite-only early stages of Sidewalk development	2
Reliances on and conflicts of interest with Amazon	11	Organisational and factory auditing	7
Technical and organisational resource constraints (e.g. processing capability, bandwidth)	11	Policies/usage requirements	7
Interviewee company profiles	**63**	Watchdog role	3
B2B and B2C interplay	8	**Technical architectures of endpoints**	**25**
Endpoint use cases and company’s domains of activity	12	Endpoint architectures, functionalities, and integrations	22
Interviewee’s path to adopting Sidewalk	23	Utilisation of Sidewalk architecture (e.g. mostly up- or downlink traffic)	3
Rationales for B2B orientation	20		
Rationales for B2C orientation	18		

or by enabling remote updating of endpoints or having them send more telemetry)

(28) Who is your silicon provider? What is your collaboration with them like, also with regards to adopting Sidewalk?

Governance

(29) Have you encountered any policies and/or requirements that your product or organisation is subject to because of using Sidewalk?

(30) I saw that there is a quite elaborate process on how to get your devices Sidewalk-certified. How did this process go for you?

(31) Can you elaborate on the relation between the LoRa Alliance and Amazon?

Information flows to and competition with Amazon

(32) I imagine there might be usage data that gives away how your device functions. For example, how big are the payloads; how quick does the battery deplete; how often does the device communicate with the cloud. What information do you think Amazon is able to see about your devices and cloud use?

(33) Do you think Amazon could use this information to improve their own offerings? *(E.g. their own IoT devices, or their AWS services)*

(34) Do you have insights into whether Amazon is developing new endpoints themselves?

Reliance

(35) How would your organisation or service be affected if Amazon were to pull the plug on Amazon, or if your partnership falls through?

A.5.3 Closing questions.

(36) Is there anything that you expected me to ask that I have not, or anything else that you would like to share?

(37) Now that you understand what kind of questions and subjects interest me, and given your expertise in the field, are there other people that you think I should talk to, in your organisation or broader network?

B Elaboration of information flows and PETs in Sidewalk

This appendix supplements the analysis of information flows and PETs in Sidewalk (§3). We first discuss privacy concerns of Echo and Ring devices irrespective of Sidewalk (§B.1). Next, we elaborate on Sidewalk's PETs (§B.2). This allows us to outline which privacy concerns they leave unaddressed (§B.3).

B.1 Echo and Ring privacy concerns regardless of Sidewalk

We distinguish three types of surveillance that Echo and Ring devices enable, that infringe individual privacy. First is *peer surveillance*, here defined as consumers using Echo and Ring devices to surveil their peers, e.g. neighbours, partners, or family members. Amazon's Ring brand offers an extensive suite of surveillance products and services, including video doorbells, cameras, and security systems [231]. Ring and Echo users can monitor their environments, including family, neighbours, passers-by, and workers, that are generally unable to avoid this monitoring [161; 243; 260]. In fact, Amazon has rewarded citizens with discounts or free products when grouping up in Ring *"Digital Neighborhood Watches"* and reporting crime [140]. Nguyen and Zelickson [202] argue that Ring lets Amazon convert a labour cost of monitoring their delivery drivers and parcels themselves, into a source of income: Ring users can monitor deliverers with cameras and sanction them through reviews or sharing recordings on social media. Other scholarship outlines how Ring surveillance grows racial injustices, and that Ring users tend to over-exaggerate how suspicious or criminal a passer-by is [80].

Second is *customer surveillance*, i.e. Amazon monitoring customers' devices, as well as how people interact with them. Numerous articles outline how Amazon logs interactions with their devices to improve their own services or offer personalised services and advertisements [e.g. 153; 161; 306]. A report from a cybersecurity company found Amazon's IoT device companion apps to be the most *"data-hungry"* of the 290 apps they studied [265; 266]. Further, Amazon has a history of giving employees too liberate access to Ring users' videos and Echo voice recordings, without informing users thereof [76; 221]. In this context, we also point out Ring's history of cybersecurity issues [e.g. 130; 133; 201].

Third, Echo and Ring devices stimulate *law enforcement surveillance*, that Amazon actively pursues through extensive partnerships with police departments [e.g. 252]. Echo devices could aid police investigations [213] and US law enforcement set out to insert voice recordings of an Echo in a criminal court case in 2017 [154]. On top of that, Amazon has clear ambitions to offer access to its country-wide surveillance network to law enforcement. Reportedly, Amazon counts over 2,000 US police and fire departments as their partners [175]; for instance to have law enforcement hand out devices to citizens for free and to train officers in PR and handling press questions [139]. Amazon also persuaded municipalities to subsidise residents' purchases of Ring products [141]. Resultingly, Ring cameras are widespread throughout the US. Amazon provided authorities a map of Ring devices and, until February 2024, an easy way to request footage from a camera's owner that Ring owners could approve in a smartphone app, without requiring a warrant [175]. Even though Amazon has now removed this button, authorities can still obtain footage with a warrant or by demonstrating to Amazon that they need it for an ongoing emergency [104]. Indeed, Amazon has disclosed video feeds without warrants to authorities based on their own *"good-faith determination"* [16, p. 4], a practice that some authors rightfully take issue with [e.g. 131]. The sensitivity of these requests is illustrated by the Los Angeles police requesting Ring feeds capturing Black Lives Matters protests [132]. Meanwhile, numerous reports refute Ring's alleged contribution to combating crime [119; 130; 138].

B.2 Elaboration of Sidewalk's PETs

This section briefly outlines how Sidewalk's two PETs work [32; 24; 42, chapter 4]. Sidewalk features a three-layer end-to-end *encryption scheme*. This scheme encrypts both payload data and certain metadata from being visible to and tampered with by others. To illustrate: this works as follows for an endpoint sending information to an application server. The *endpoint* encrypts the payload data with an Application Server Key (only known to the endpoint and application server), and encrypts the result and the network layer frame with a Sidewalk Network Server Key (only known to the endpoint and Sidewalk Network Server). The endpoint then sends the packet to the *gateway*, that adds a third layer using the Gateway Network Server Key (only known to the gateway and Sidewalk Network Server). The *network server* then decrypts the second and third layer and forwards the packet to the appropriate *application server*, that decrypts the final layer and processes the payload. Accordingly, manufacturers must embed appropriate certificates and key pairs into endpoints during their production. Downlink traffic is secured similarly.

Second is *device identifier obfuscation*. For the encryption and authentication, all endpoints and gateways must carry unique credentials. To *"minimize data tied to customers"* [32, pp. 11], Amazon uses temporary identifiers derived from the unique credentials for some functionalities. For instance, transmission and gateway identifiers (which are different than the device's persistent identifier, usually its serial number) are renewed every fifteen minutes and information about which gateway routed an endpoint's packets is cleared every 24 hours.

B.3 Privacy concerns that Sidewalk raises or exacerbates

Despite its PETs, Sidewalk compromises user privacy by facilitating surveillance (§B.3.1), not providing insight into the security mechanisms (§B.3.2), blurring privacy boundaries (§B.3.3), and undermining owner control over their devices (§B.3.4).

B.3.1 Surveillance. While Echo and Ring devices already enabled three types of surveillance, Sidewalk expands the area wherein Echo and Ring devices can work, because they are both a gateway and endpoint simultaneously. They can thus be placed outside the range of the owner's wifi router, that previously constituted a technical boundary circumscribing where these devices could be used. Sidewalk functions as a thread connecting smaller patches of surveillance products into one great surveillance network across entire neighbourhoods and cities [137]. Consequently, Sidewalk amplifies these already existing privacy issues; but also adds to them.

Regarding *peer surveillance*, among Sidewalk-enabled devices are asset trackers that stalkers can misappropriate [81; 294]. In fact, two stalking victims filed a lawsuit against Tile and Amazon over Tile's integration with Sidewalk, arguing that Sidewalk's coverage was vital to the stalking by an ex-partner [160; 250]. Asset trackers more generally have been used for stalking and domestic abuse, that technical solutions proposed by their manufacturers fail to robustly tackle [142; 289]. In theory, *law enforcement* could also use Sidewalk trackers to track suspects; or, as Pace et al. [216] detail, recover a tracker's previous locations.

Relatedly, the information flows from endpoints to Amazon and manufacturers, and vice versa (Table 1) enable *customer surveillance*. For instance, Amazon can determine endpoints' and thus their users' locations [e.g. 101], as Amazon can see which gateways endpoints connect to [107]. According to Despres et al. [107], the Whitepaper *"claims to forget the device ID associated with a transmission after replacing it with a temporary rotating identifier. In reality, ... device IDs are kept to enable bidirectional communication, as the most likely gateway to still be in communication with the device is the one that handled its last transmission"* (p. 3). To be more precise, Sidewalk identifies endpoints with one of three identifiers, namely the Sidewalk Manufacturing Serial Number (before an endpoint's registration to Sidewalk), Sidewalk ID (loaded into the device during registration), and the Transmission Identifier (after registration) [42, pp. 49-50]. Amazon also uses these persistent identifiers to block endpoints from accessing the network if these are reported as lost, suffer from security issues, or *"if a third party [manufacturer] fails to act in good faith"* [32, p. 14]. Manufacturers can similarly track their users, as Amazon acknowledges in its Whitepaper: *"Third-party Sidewalk device manufacturers may maintain their own logs that are subject to their respective retention periods and privacy notices"* [32, p. 6].

B.3.2 Security and lack of transparency. Some authors remark that novel technologies are rarely bug-free; Sidewalk's quick opt-out rollout and resulting large coverage could mean that security flaws are only uncovered when it is already widely used [81; 294]. Amazon has not published details about how precisely it implements its security measures in Sidewalk, nor enabled independent reviews [81]. This pits Amazon as a single point of failure and increases the need for users to trust them, contrary to the rationale of PETs.

B.3.3 Blurring privacy boundaries. Sidewalk tightens Amazon's grip over citizens' personal households and physical livelihoods. Sidewalk differs from conventional mental images of the internet, granted that Sidewalk endpoints are not connected by virtue of their owner's router, but by other people's gateways (and their routers) and the Sidewalk Network Server [88]. With connectivity enabling digital services that reach beyond the range of one's home router(s), i.e. into the yard or streets, Sidewalk gateways further blur the borders between private and public spaces around people's homes [148], scaling smart homes up to smart neighbourhoods [101] that Amazon mediates. Thus, Sidewalk is not a digital service confined to cyberspace, but invades public and private physical spaces [92].

B.3.4 Undermining owner control over devices. A prominent objection to Sidewalk by journalists and advocates is to Amazon's opt-out and relatively silent transformation of Echo and Ring devices into Sidewalk gateways. This undermines owners' control over their devices, and puts them at risk of violating the terms of service agreements with their ISPs [e.g. 81; 87; 126; 200; 220]. We question how many users will have seen the notification in their Echo and Ring apps that announced Sidewalk, and how often they open these apps in the first place. Similarly, not all Echo owners might be inclined to open an email titled *"Echo Update: Amazon Sidewalk is coming soon"* [78], which does not mention that a crowd-sourced networking service is approaching in opt-out nature. In line with research demonstrating that people tend not to deviate from default settings and that tech companies actively hide privacy settings [e.g. 3; 4], authors speculate that Amazon deployed Sidewalk in opt-out fashion to increase gateway participation and thus coverage [81; 126; 200; 220].

On top of that, the Sidewalk rollout changes the relationship between gateway owners and their device to launch the Sidewalk service. Firstly, Sidewalk gateways will by default share connectivity with endpoints owned by other consumers: something that the gateway owner likely did not envision when bringing the device into their home. Secondly, third-party IoT manufacturers adopting Sidewalk predominantly target business customers. Accordingly, the Echo and Ring devices that consumers have bought, may be used for business or – in the case of the utilities domain – public purposes. By stitching together small bandwidth contributions from gateway owners across the US, Amazon constitutes an additional connectivity infrastructure that it allocates to manufacturers. Manufacturers may, in turn, deliver wholly novel services to their customers that gateway owners may not foresee.