# The PET Paradox

## How Amazon Instrumentalises PETs in Sidewalk to Entrench Its Infrastructural Power

Thijmen van Gend
(t.n.vangend@tudelft.nl)
Dutch Organisation for Applied Scientific Research (TNO)
The Netherlands
Delft University of Technology (faculty of Technology, Policy and Management)
The Netherlands

Donald Jay Bertulfo
(d.j.bertulfo@tudelft.nl)
Delft University of Technology (faculty of Technology, Policy and Management)
The Netherlands

Seda Gürses
(f.s.gurses@tudelft.nl)
Delft University of Technology (faculty of Technology, Policy and Management)
The Netherlands

## Abstract

Recent applications of Privacy Enhancing Technologies (PETs) reveal a paradox. Privacy engineers originally conceptualised PETs to pursue data minimisation, purpose limitation, and avoiding single points of (privacy) failure; thereby curbing corporate and governmental power over consumers. However, recent Google and Apple services illustrate that, paradoxically, PETs can also be applied to entrench their data, market, and infrastructural power vis-à-vis other public and private organisations. In these cases, Google and Apple strategically deployed PETs to provide some privacy for applications that expand their infrastructural offerings to third parties for digital contact tracing, advertising, and device finding. Cautioned by these examples, we empirically inquire how this paradox comes to be in the case of Amazon Sidewalk. Sidewalk is a cloud connectivity service that benefits from Amazon's cloud-based control over its consumer devices. Treating them like accessories of their cloud, Amazon remotely updated Echo and Ring devices in consumers' homes, to transform them into Sidewalk *"gateways"*. These gateways share part of their wifi with compatible third-party Internet of Things (IoT) devices, called *"endpoints"*. Amazon deployed and marketed carefully engineered PETs in response to the public's privacy pushback that resulted from these opt-out over-the-air transformations. Further, while Amazon markets Sidewalk to users as a shared community-focused network, it offers Sidewalk to manufacturers as a network with which they can remotely manage their devices, through Amazon Web Services (AWS). Using the Sidewalk protocols, an endpoint can connect to their manufacturer's *"Application Server"* in AWS through a gateway. PETs in this context reveal paradoxical outcomes. First, our analysis shows that Amazon applies PETs narrowly to extend and entrench its AWS infrastructure. It suppresses some of the information flows that allow the company to give some privacy guarantees to owners of Echo and Ring devices when transforming them into gateways. Once *"flipped"*, however, these gateways constitute a crowdsourced connectivity infrastructure that covers 95% of the US population. Sidewalk connectivity thus enables novel information flows outside the scope of its PETs, that raise surveillance and competition concerns. Second, Amazon imposes broad requirements on Sidewalk-adopting IoT manufacturers, for the sake of enabling these PETs; creating the conditions for adopting PETs while funnelling manufacturers into AWS. To join Sidewalk, manufacturers must adjust their device hardware, operating system and software; cloud use; factory lines; and organisational processes. Together, these changes end up turning manufacturers' endpoints also into accessories of Amazon's computational infrastructure; further entrenching Amazon's infrastructural power. Sidewalk is thus not just a connectivity service. With it, Amazon aims to extend its cloud infrastructure as a software production environment for third-party IoT manufacturers. Accordingly, we argue that power analyses undergirding PET designs should go beyond analysing information flows. We propose future steps for policy and PET research to address this PET Paradox.

## Keywords

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

## 1 Introduction

Over the last decade, there has been widespread recognition that big tech companies have become all too powerful. Scholars and policymakers have raised concerns about the oversized influence of tech companies on other parties in health, law, public administration, science, education, finance, communication, (national) security, and more [e.g. 8; 162; 219; 220; 229]. Lynskey [162] argues that big tech companies possess *"data power"*: *"a multifaceted form of power ... arising from their control over data flows"* (p. 196). For her, the volume and variety of the data that digital platforms have control over, determine how much data power they have. With this power, they can surveil and profile participants in their digital ecosystems, and restrict or prioritise certain types of information flows over others, e.g. to influence how people form their opinions [162].

For academics, tech companies' amassing of personal and commercial data has raised contentious surveillance [192; 249] as well as competition concerns [76; 135; 178; 208]. This notion also resonates with regulators. The European Commission (EC) has designated Google (ads, shopping, search, operating system, browser, app store), Apple (browser, app store) and Amazon (ads, shopping) and other tech companies as *"gatekeepers"* for *"core platform services"* [109]; and is currently investigating whether Amazon and Google are gatekeepers for cloud computing, too [108]. The EU's

This work is currently under review for PETS 2026 Issue 3. This version was specially prepared for the Digital Competition Conference 2026. Please do not distribute it further without the authors' prior consent.

Digital Markets Act notes that these gatekeepers with considerable economic power have a unique *"access to large amounts of data"*. Similarly, competition authorities have repeatedly ruled that tech companies leverage data for unfair competitive advantages [e.g. 89; 107].

If tech companies' powers indeed derive from control over vast and varied 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. They do so by hardwiring strict controls into the design of systems that collect and process data, that may otherwise infringe individual privacy due to information asymmetries [124; 133; 134]. Two principles have been central to PET development since the 1990s: privacy engineers strictly interpret data minimisation to the purpose of processing (known as purpose limitation), and develop distributed designs that minimise trust to avoid single points of (privacy) failure [62; 124; 133; 134]. More broadly, actors and their potential to overreach using various sources of power (e.g. technical, legal), prevalently feature in adversarial and threat models, underlining the importance of considering power asymmetries in designing PETs. Privacy engineers can thus instrumentalise these two design principles and adversarial models as an evaluation framework to protect people from both companies and state bodies that process data, curbing power asymmetries in the process. Regulators have acknowledged this potential of PETs: the EU's General Data Protection Regulation codifies privacy by design as a regulatory requirement to curb informational power asymmetries [see e.g. 56; 110; 139; 230].

Despite this promise, academics and competition authorities have critiqued numerous Google and Apple services that incorporate PETs to limit information flows. They argue that these companies' instrumentalisation of PETs to their advantage constitutes privacy [99; 222] or confidentiality washing [259; 260; 262] and raises concerns around competition and public service delivery [250]. We discuss these examples in §2. In one case, Google and Apple leveraged PETs to position themselves as arbiters of citizens' privacy vis-à-vis health authorities and researchers for Covid-19 digital contact tracing (DCT). In another case, by purportedly making digital advertising more privacy-enhancing, they entrenched their position in the business models and production processes of other companies in the digital advertising space. Apple's crowdsourced device finding service Find My is also contested: antitrust authorities allege Apple of weaponising security and privacy to gatekeep and self-preference vis-à-vis third-party tracker companies. By claiming to act in privacy-preserving ways, Apple and Google are able to 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), but also entrenches 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. We discuss these examples in §2, as they point to a curious paradox: these companies apply PETs in a way that limits information flows they are privy to *and* helps accentuate their power –such as data, market or infrastructural power.

We observe that the by now standard industry practice of offering software using a server-client model and agile methods, is part and parcel to this paradox. 'Software' here includes operating systems (OSes), web browsers, app stores and apps. Continuous production processes such as Continuous Integration and Continuous Delivery that often take place in cloud infrastructures, allow to continuously update software on these devices. Taking the server-client architecture to its extreme, devices have become vessels for delivering services, rather than being stand-alone products with a specific and fixed purpose. Consumer devices are essentially integrated into the production of consumer software, being continuously reconfigured (downstream) while providing telemetry and feedback to its manufacturer (upstream). In this paradigm, we argue, end devices are practically *accessories* of these companies' *computational infrastructures*. The server-client model and agile methods are also relevant for successfully designing and deploying PETs more generally [62; 152; 154].

This control is fundamental for the way wherein Google and Apple paradoxically increased their power through PET-based services. The companies wielded their remote control over vast amounts of end devices, such that the devices together make up a larger infrastructure for a new service. Deploying particular PETs to individual devices at large scales, lets Apple and Google offer alleged privacy-preserving contact tracing, advertising, and device finding services. Thus, Google and Apple use PETs to hide some consumer information flows, protecting consumers from them (i.e. a in business-to-consumer (B2C) relations). Yet, the companies entrench their own role in how other businesses (B2B) and governments (B2G) can deliver their services (contact tracing, advertising, and device finding) to these same consumers.

Google and Apple hold unique positions in this respect. Not only can they push over-the-air updates of their own software to their millions of consumer devices, but they also limit how smartphone manufacturers and app developers can disseminate updates of their own. This is because they control device OSes, browsers, and app stores. The power to turn end devices into accessories, and repurpose them as in the provided examples, is therefore not distributed equally.

In this paper, we bring another empirical case study to examine the potentially paradoxical effect of PET implementations in computational infrastructures: the case of Amazon Sidewalk. Sidewalk is a crowdsourced networking service where non-Amazon IoT devices (*"endpoints"*) can connect to a nearby Amazon Echo or Ring device (*"gateways"*, potentially owned by someone else). 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)) [35]. In that sense, the endpoints are accessories of Amazon's infrastructure: their utility relies on reliable cloud connectivity. 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.

Amazon's decision to make Echo and Ring devices share their owners' bandwidth with strangers' endpoints sparked significant public and media backlash. The organisation remotely pushed an over-the-air opt-out update to devices already in consumers' homes that transformed them into Sidewalk gateways. According to numerous bloggers, journalists, and consumers, Sidewalk undermines users' autonomy, compromises home network security, and sets citizens up for surveillance by strangers and Amazon. Amazon answered with marketing materials and technical documentation to showcase PETs that supposedly address these concerns, and now boasts coverage of about 95% of the US population [33].

As with the earlier cases, we expect that power dynamics may manifest between Amazon and other organisations. Hence, we do not centre consumers or users, but adopt a B2B-oriented *"production view"*. This view is largely missing from the aforementioned public responses. Our main research question is: *Whether and how does Amazon instrumentalise PETs in entrenching its computational infrastructure as a production environment vis-à-vis IoT manufacturers?* In other words: does Amazon's deployment of PETs in their computational infrastructures achieve its intended privacy goals? And does it have further negative effects? We pay specific attention to how adopting Sidewalk affects the way wherein IoT manufacturers produce their devices and services; and accordingly, how power dynamics emerge between them and Amazon. This particular interplay between PETs and production has not yet been described for Sidewalk in academic or industry publications; partially because manufacturers are not always keen to detail their commercial practices. Hence, we adopt an empirical qualitative mixed methods approach. It allows us to triangulate interviews with IoT manufacturers, against marketing statements by them and Amazon, technical Sidewalk documentation, and news coverage.

The paper proceeds as follows. We first survey other instances wherein companies with infrastructural control operationalised PETs, and the power it yielded them (§2). After detailing our approach (§3), we study: *How does Amazon's implementation of PETs shape user privacy and Sidewalk's control over information flows?* (§4). This part starts from a consumer-oriented (B2C) approach to PETs use, and expands to address greater information flows in Sidewalk, including their impact on manufacturers (B2B). We skip a full-blown privacy analysis to make space for a broader power analysis. Next, we shift our inquiry to the production view, asking: *How does Amazon's implementation and governance of PETs in Sidewalk affect manufacturers' production of IoT devices and services?* (§5). 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. In the discussion (§6), we argue how these power dynamics lead to the *"PET Paradox"*. After exploring limitations (§7), we conclude with the questions that our analysis raises for academia and policy, and propose paths forward (§8). In sum, we contribute:

- an analysis of Sidewalk's technical design, scientific reports, and popular reports, to evaluate novel privacy threats that Sidewalk raises despite its PETs;
- a rich account of how tech companies instrumentalise PETs in engineered environments, and its unexpected consequences for market and infrastructural power;
- a description of the impact of Sidewalk's particular protocol design on not just users, but the manufacturers who produce IoT devices;
- an elaboration of the consequences for how we may design and deploy PETs in the future in light of these power dynamics, and of questions that the PET community should discuss going forward.

## 2 PETs as a source of power

Over the last decade, more and more tech companies have included PETs in their repertoires. Their rise to prominence is also evident in the PET Symposium programme of the last decade. While we can consider these positive developments, tech companies may leverage PETs strategically, e.g. to claim that certain regulations no longer apply when they use PETs [260; 270]. Some of this is due to the underlying protection mechanisms: moderating content or providing data access to data subjects, researchers, and public bodies may be hard when said data is encrypted. This has also led to contentious use of PETs for client side scanning [2].

We focus on recent large-scale implementations that have raised further concerns with respect to PETs being used not only to protect privacy, but also to entrench the market and infrastructural position of these already powerful players in the production of services by other actors. We discuss three instances that demonstrate how, in doing so, they increase their influence in public service delivery (i.e. digital contact tracing), bolster their market position (i.e. device finding networks), and remain central to digital advertising.

**Instance 1: Digital Contact Tracing.** During the Covid-19 pandemic, Google and Apple leveraged PETs to position themselves as arbiters of citizens' privacy vis-à-vis health authorities and researchers for DCT. Accordingly, the companies shaped how they could *"produce"* public health services, as Troncoso et al. [250] elaborate.

As the pandemic unfolded at great speed and scale, governments called for taking advantage of high penetration numbers of *"smart phones"* for a key public health service: contact tracing. Various coalitions from industry and academia responded to the call. One such coalition proposed the Decentralised Privacy-Preserving Proximity Tracking (DP3T) protocol, that aimed to maximise privacy preservation and purpose limitation [250]. DP3T relied on persistent background functioning, that OSes prohibit for privacy and performance reasons. This required Google and Apple, that control 99% of the smartphone OSes in the concerned regions [231], to adjust their OSes.

Amidst a greater controversy around decentralised solutions prioritising privacy over information flowing to public health authorities [1], the companies came forth with an implementation of DP3T in their OSes. This they called the *"Google and Apple Exposure Notification"* (GAEN) framework. GAEN exposed APIs that contact tracing apps developed by health authorities could invoke. However, these APIs presented health authorities with a *"heavily constrained set of parameters"*, which *"strongly limited the design choices of app developers in making tradeoffs among privacy, security, and epidemiological utility of the applications"* (p. 53). To illustrate: in the name of user privacy, the API would initially only expose highly summarised information, hampering calculation of daily viral exposure accumulation by epidemiologists. By pushing the protocol into their OSes, Google and Apple positioned themselves as public health infrastructure providers; resolved a public controversy around DCT architectures on their own terms; and secured seats in the public health decision-making arena [250].

**Instance 2: Device finding networks.** With an opt-out update [113], Apple turned *"hundreds of millions"* [50] Apple products into a crowdsourced privacy-preserving infrastructure for finding devices, called Find My. This feat cannot be pulled off by other tracking companies that do not control a smartphone OS, yet was found to compromise their competitive position.

*"Finding devices"* report the location of nearby Find My-compatible devices to their owners [47; 48]. Compatible devices include Apple's own devices and asset trackers (AirTags), but also third-party trackers and products (e.g. earphones) [68; 172]). Third-party tracker manufacturers typically have smaller networks and rely on customers downloading a smartphone app, to both manage their own tracker and report the location of others' [85; 201; 246]. For instance, Chipolo's network counts five million contributing devices [85].

Apple allows other businesses to make Find My-compatible products, under potentially unfair constraints. Adopting companies must join Apple's developer programs and pass a certification process [50]. Their devices may not support Apple's and their own network simultaneously [97; 200]; according to an unofficial publication of the Find My specification, this *"may interfere with the security and privacy requirements"* [46, p. 14]. Granted Apple's ability to remotely turn consumer-owned Apple devices into *"finders"*, adopting Find My and subjecting themselves to its policies may feel inevitable for other tracker manufacturers [71]. These conditions for adoption were investigated by antitrust authorities worldwide [91; 97; 106; 203; 209; 245; 254], alleging Apple of gatekeeping and self-preferencing while weaponising security and privacy.

**Instance 3: Digital advertising.** In this case, efforts by Apple and Google to purportedly make digital advertising more privacy-enhancing, entrenched their position in the business models and production processes of companies in the digital advertising space.

In 2021, Apple implemented the *"App Tracking Transparency"* (ATT) framework in their mobile OS. Consequently, app developers must ask user consent to use device identifiers for cross-app tracking [49]. Estimates of opt-in rates vary widely between 11% and 50% [51; 96; 164; 267]. As privacy-enhancing alternative for ad attribution, Apple offers the SKAdNetwork framework. SKAdNetwork uses on-device processing and delays and anonymises attribution reporting with advertisers [170].

ATT seriously hurt the revenue of Meta [94] and had a small effect of steering app developers from advertising revenue models to paid apps and in-app payments [150]. Meanwhile, Apple's advertising market share tripled [169]. The UK competition Authority [91, pp. 233-244] and McGuigan et al. [171] claim this could be because (1) Apple exempts their own tracking of users across Apple apps from ATT, claiming it constitutes first-party data; (2) their *"Personalised Ads"* nudge users to opt in, whereas ATT pop-ups nudge users to opt out; and (3) Apple uses the Ads Attribution API for Apple ads, while other app developers and ad networks must make do with the SKAdNetwork APIs, that yield advertisers delayed and less granular information. Accordingly, Apple can track user behaviour more accurately and provide advertisers with richer ad performance insights than competing ad networks. Competition and consumer authorities in multiple countries are investigating or have fined Apple for increasing barriers of entry and self-preferencing with ATT [57–59; 73; 91; 255; 256].

In early 2020, Google announced *"Privacy Sandbox"* (PS) for Chrome and Android. For Chrome, PS would deprecate third-party cookies, but still allow first-party cookies [216]. PS includes APIs to substitute third-party cookies' functionalities in an allegedly more privacy-preserving way, with decentralised PETs that run inside users' browsers [117]. In fact, Google's instrumentalisation of PETs entrenches their role in online advertising, aggravating dependencies of advertisers, publishers, and adtech providers on them. While deprecating third-party cookies could be a win for user privacy [67], governmental authorities have started antitrust investigations [87; 88, pp. G123-124; 89, p. 296; 90; 92, pp. 17-18, 31-32; 93; 202]. Google announced in July 2024 a pivot to a user consent model, mentioning the UK competition authority's investigation [83], before ultimately killing most PS APIs in late 2025 [64; 84].

The authorities argued that Google disproportionally disadvantages publishers and adtech companies, and 'self-preferences', 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 [87], while costing publishers ad revenue, and necessitating a technologically complex and expensive implementation [138; 197]. Alternatives to PS for publishers suffer similar complexity, effectiveness, and cost issues. Further, Google may benefit from publishers flocking to its advertising services (e.g. Google Ad Manager [197]); and from advertisers moving to closed ecosystems with better tracking capabilities (e.g. mobile, search, and social media) [247; 248], where Google allegedly has higher margins [105; 218]. When shifting to the user consent model in 2024, Google further upset publishers by lacking communications about a timeline and details about the opt-out design. The company created uncertainty on what level of third-party cookie adoption publishers could expect and by when [63; 146]. This especially affected smaller publishers with less resources to invest in testing alternatives [146; 221].

Arguably, it is not surprising that businesses that bank on surveillance would suffer when PETs work well. However, authorities and academics have also cast doubt on Apple and Google's privacy enhancement promises. ATT has not significantly reduced tracking libraries in iOS apps, and developers circumvent ATT with other tracking mechanisms [151]. PS increases first-party tracking and tracking collaborations between website providers [65; 87; 161], and its governance structure does not assure that it actually fulfils its privacy promises [92, pp. 17-18, 31-32]. Using on-device PETs could also realise a *"perverse outcome where companies try to use more sensitive data than before as part of their business models"* [259, 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 [259; 262], data anonymisation, limiting access to personal information, and preventing third-party tracking

[170]. By framing privacy narrowly to advance their competitive positions, these companies *"sanitiz[e] surveillance"* [171, p. 9] and distract from power asymmetries [171] and *"power dynamics congealed within adtech infrastructures"* [170, p. 18].

**Different views on and types of power.** In all three instances, PETs rely on complex computing and on-device processing. This puts Google and Apple in unique positions to deploy them, granted their control over users' devices, operating systems and browsers [259]. The analyses provide different perspectives on how PETs enable power. The DP3T analysis exemplifies a *sovereignty view*, showing how Google and Apple asserted themselves as arbiters of privacy and key decision-makers in public health vis-à-vis researchers and governments [250]. The Find My and advertising instances raise *competition* concerns: they underline how these companies gain market persistence or advantage, by using PETs to turn personal devices or browsers into infrastructures for delivering services to third parties. All of this happens while these companies reframe privacy narrowly.

The *production view* in this paper empirically studies how such moves impact third parties' production. Beyond scrutinising dependencies and interfaces between manufacturers and tech companies, or even how well the PETs work, we emphasize how manufacturers' production processes change in adopting their infrastructures; what role PETs play; and what power dynamics arise.

## 3 Methods and case description

### 3.1 Methods

We perform a case study [239; 272] 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 the complexity of the instances described therein. We iteratively combine three methods: a grey literature review, technical documentation analysis, and elite interviewing. As the elaboration below will show, 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. Hence, we present the findings of each method in one coherent narrative.

**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 1 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 [140]. For contextualisation, we also briefly studied broader offerings for connectivity (e.g., Matter).

**Technical documentation analysis.** To understand Sidewalk's framing of privacy risks and safeguards, and to identify what Sidewalk and AWS promise to manufacturers in terms of improving the production of IoT devices, we analysed the technical documentation of Sidewalk and associated 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 our focus on production and the context of the case, we adopted an elite interviewing approach to interview manufacturers [145; 156; 160; 195; 227; 253]. The goal is to explore their motivation for and experience with adopting Sidewalk. We asked them 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. These positions presumably bring these elites comprehensive experience with both the business and technical implications of Sidewalk adoption. Eight ultimately participated: four hold a C-level position, two are department heads, and two are high-ranking engineers. 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.

For interview analysis, we iterated through two coding cycles, following the manual of Saldaña [213] and using ATLAS.ti 23 [55]. 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. We refrained from reporting quotes or attributing them when these may compromise participant anonymity. Participants' names and affiliations were not shared with other participants. Additionally, respondents signed an informed consent form, stating that they were free to skip questions or withdraw from participation at any time. We also shared the transcripts with participants, to allow them to redact or edit any statement. Nobody used this opportunity. Our institutional review board approved this approach.

### 3.2 The Sidewalk architecture

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

Sidewalk-compatible IoT devices are called *"endpoints"* and can be produced by Amazon and third parties (*"adopters"* or *"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 (also known as *"bridges"*) are Amazon Echo (smart speakers and displays) and Ring (smart cameras, lighting, doorbells, and alarms) devices in the US that use a portion of their own wifi bandwidth for this communication [35]. The endpoint owner may be someone else than the gateway owner, benefiting from Sidewalk as a *"crowdsourced"* network [20]. A gateway can also act as endpoint, i.e. benefit from the connectivity of other gateways.

The Sidewalk protocol utilises Bluetooth Low Energy (BLE), Frequency-Shift Keying (FSK), and a proprietary version of LoRa [40, p. 140]. These are intended for short, medium, and long ranges, respectively; with lower data rates for longer distances [40, p. 11]. Not all endpoints, nor all gateways support all three protocols [20; 36]. Similarly, endpoints must contain specified chips from Amazon-approved silicon providers. Gateways check whether endpoint packets comply with the protocol format specifications and that the endpoint is not blocked from Sidewalk [20].

Between the gateway and application server sits Amazon's *"Sidewalk Network Server"*, part of its *"cloud"* [40, p. 15]. It routes traffic from the gateway to the application server. It inspects all packages; routes them; maintains time synchronisation of the network; and authenticates devices and application servers, verifying that Amazon has not blocked them from Sidewalk [20].

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 [40]. The server comprises at least *"AWS IoT Core for Sidewalk"* and potentially other AWS services. Manufacturers that want to manage their devices from outside AWS, must interface with IoT Core through a *"Topic"* or API [40, p. 42]. Seven out of eight interviewees picked the former option, thus we only pictured an application server outside AWS for one manufacturer.

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*.

### 3.3 How Sidewalk came to be

Understanding Sidewalk's history is fundamental for understanding the role of PETs and power dynamics at play, as will become clear later in the article. Amazon revealed Sidewalk during a hardware conference in September 2019, describing a pilot with 700 gateways in Los Angeles [10]. A press release followed soon after, detailing that certain Ring cameras and lights could share their network connectivity with each other [11]. During the pilot, connectivity was restricted to devices registered under 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]. Simultaneously, they published the first version of the Privacy and Security Whitepaper [13] (further: Whitepaper), that the announcement also references. This is Amazon's first mention of *"privacy"* in the context of Sidewalk – presumably as a response to publications voicing privacy concerns following the 2019 announcements [e.g. 80; 191; 210; 265].

In May 2021, Amazon announced a further roll-out and more third-party adopters [15]. In June, Amazon transformed Echo and Ring devices of US-based consumers into gateways, through an opt-out OTA update [75; 257]. An email notified Echo owners a month before this launch [177], and Echo and Ring owners received an in-app notification seven days beforehand [257]; a narrow window to opt out [116; 257]. 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. 75; 187].

In March 2023, Amazon claimed to have coverage of over 90% of the US population (Figure 2) and opened the network for developer testing [18]. Shortly after, Amazon updated the Whitepaper to say that Sidewalk was now opt-in for new Echo and Ring devices [17; 20]. About 10 months later, an executive proclaimed 95% coverage [66]. As of now, the gateway role can be performed by 33 different Echo and Ring models [36], with *"more than 80 million"* devices contributing [31].

### 3.4 Amazon's marketing of Sidewalk to consumers and manufacturers

Amazon promotes different aspects of Sidewalk to consumers (both gateway and endpoint owners; B2C) and manufacturers (B2B) (see Figure 3 in Appendix B). 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"* [35] (Figure 3 *d*). Sidewalk's core proposition is to make IoT devices of all kinds *"work better at home and beyond the front door"* [35] by connecting them to the cloud [12; 20].

Gateway owners' participation is central to Sidewalk's coverage. Accordingly, Amazon frames Sidewalk as a *"community benefit"*-generating service: a B2C service enabling 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"* [35]. Gateway owners *"contribute [their] internet bandwidth to support community extended coverage benefits such as locating pets and valuables"* [20, p. 15; 35]. Similarly, one Amazon executive said that Sidewalk *"is best described as a community network"* [66, 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"*

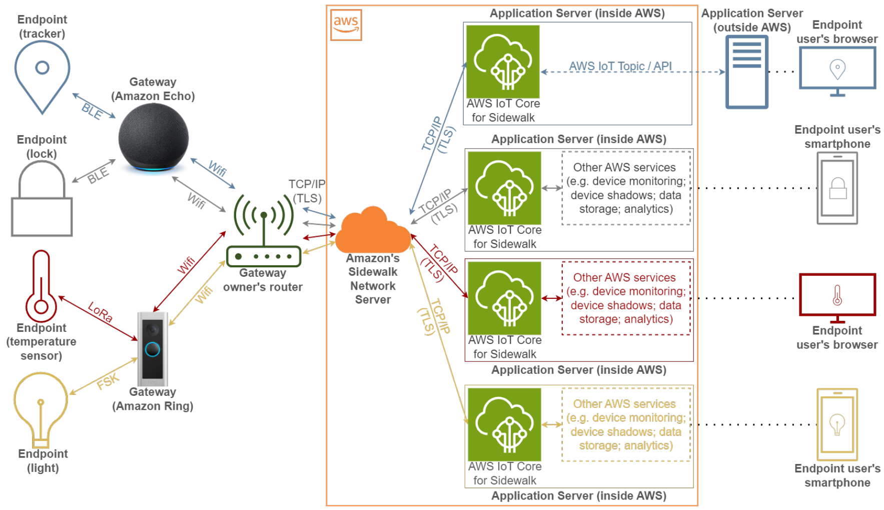


**Figure 1: Example Sidewalk architecture, based on [40, pp. 14, 42; 45]. Echo and Ring images reproduced from [34; 207].**

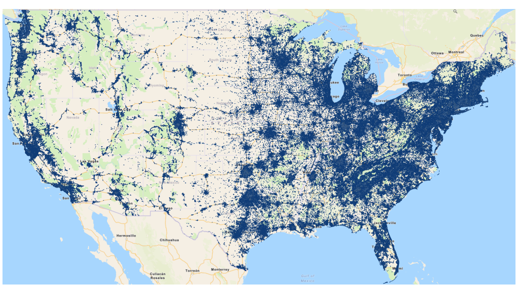

**Figure 2: Sidewalk coverage in the contiguous US on November 29th 2024 [32]. Blue dots indicate coverage.**

[14]. Gateway owners allegedly need not worry about helping their neighbours: Amazon warrants Sidewalk's security (Figure 3 *a* and *d*; discussed in §4.1) and caps gateways' bandwidth usage for Sidewalk at 500 MB per month per customer, at a bandwidth of at most 80 Kbps [20] (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"* [40, p. 11], and *"a secure, free-to-connect, long-range and low-power shared community network designed to provide connectivity for billions of devices"* [37; similarly in 18 and 40, 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"* [20, p. 2; 40, p. 45] Indeed, the sixteen adopters operate across various (not mutually exclusive) 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 (further referred to as B2B). Nine of these simultaneously sell to consumer users (B2C); although they generally focus on B2B markets. The overwhelming majority of third-party manufacturers thus targets organisations as endpoint buyers. Also, endpoints may be close to homes (e.g. smart lights or motion detectors) or more remote (e.g. asset trackers) [12].

In making this promise, Amazon depicts Sidewalk as *"a 'pipeline' that moves data back and forth between an Endpoint and its respective Application Server"* [20, 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 connect them to AWS' variety of IoT services, that go well beyond offering flexible storage and compute. For one, manufacturers can utilise security-oriented cloud services [42], inspect and patch individual devices, and send firmware updates and files to multiple endpoints with *"Sidewalk Bulk Data Transfer"* [40, p. 173]. A second promise is *"extending [device] lifecycle and capabilities, cost-efficiency in maintenance from remote operation, and [enabling] rapid prototyping"* [40, p. 173]. Relevant functionalities include monitoring how users use their endpoints; visualising metrics; detecting anomalies; managing digital *"device shadows"*; and inspecting, accessing, and updating individual devices [19; 43; 44]. In that sense, Sidewalk and AWS can make manufacturers' production more agile [125].

## 4 Information flows and PETs in Sidewalk

PETs in Sidewalk serve *"to secure data traveling on Sidewalk and to keep customers safe and in control"* [35] and limit *"the collection and storage of customer information"* [20, p. 3]. The design principles are that gateway owners *"do not receive any information about devices owned by others connected to Sidewalk"* [35]; that *"[i]nformation [endpoint] customers would deem sensitive, like the contents of a* *packet sent over the Sidewalk network"*, is not visible to Amazon or gateway owners [20, p. 4]; and that *"tracking of devices and associating a device to a specific user"* by Amazon, gateway owners, and eavesdroppers is prevented [20, 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) [20; 23; 40, chapter 4]. A short elaboration of each is given in §C.2. A traditional privacy analysis would look to see whether the implementation of these PETs leaves privacy risks unaddressed. We briefly do so (§4.1), but then take a step back to deliberate the role of PETs in *"flipping"* consumer devices for extending Amazon's computational infrastructure.

## 4.1 Information flows and user privacy

Sidewalk limits some information flows with PETs while, simultaneously, casting a vast crowdsourced network that enables *additional* information flows. After all, the proposition o Sidewalk's connectivity and the range of AWS services is allowing endpoint users to remotely manage their devices; and manufacturers to collect telemetry and deploy OTA updates. A concrete example: Amazon does not inform gateway owners when their gateway provides connectivity to an asset tracker; but this connectivity enables information to flow from the tracker to its owner, its manufacturer, and Amazon. These new information flows are irrespective of the original communications between the Echos/Rings and cloud necessary for delivering services to the customers that bought them.

Considering these new information flows, we identify four types of unresolved 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 of owners' control over their personal devices. We explain these concerns in Appendix C. Herein, we note that the proprietary design and a lack of transparency of Sidewalk's technical workings further aggravate these concerns; a red flag for privacy and security communities. PETs researchers have repeatedly proposed (partial) solutions to such problems [e.g. 143; 235; 236; 264], but these are not part of Sidewalk's PETs. We conclude that Amazon takes a narrow view on the privacy concerns that arise from Sidewalk.

## 4.2 The role of PETs in flipping consumer devices

Amazon came up with multiple responses to the privacy pushback that Sidewalk generated over the years. Most obvious is publishing and repeatedly referencing the Whitepaper that outlines Sidewalk's privacy, security, and bandwidth restriction measures (§3.3). Further, Amazon obfuscates the predominant B2B nature of third party devices by repeatedly pointing to B2C applications (§3.4). Additionally, an interviewee recounts that Amazon strategically released stories of adopters' products, to demonstrate Sidewalk's value and distract from the backlash. Amazon used them *"as a pawn basically in the game, of showing that there's value to this network"*. Amazon also called another participant *"a very strong opportunity for Sidewalk to show off what it can do"*. Together, Amazon uses these angles to craft a narrative that their transformation of personal devices benefits gateway owners: they can help their community without having to worry about bandwidth and privacy.

This strategy suggests that Amazon had to address privacy concerns to justify *"flipping"* consumers' Echo and Ring devices to include gateway functionality; leading Amazon to widely advertise the PETs they put in place. [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"*.

## 4.3 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 (see Table 3 in §C.4). This data lets Amazon monitor the integrity and reliability of Sidewalk [A2; A6]: *"they need metrics to see if things actually work"* [A2].

But with this telemetry, Amazon can also learn the demand for endpoints of each manufacturer and thus 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 [107; 147; 166]. Two other respondents think this benefit is negligible.

Only one interviewee was concerned about this premise, *"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, and them potentially 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 this knowledge is not so valuable for endpoint development that it would warrant *"stealing information"* or that the encryption of payload data inhibits such learning. Table 3 disproves the latter.

Finally, Amazon can improve AWS for IoT manufacturers at large, with its insight into endpoint behaviours and how manufacturers manage them in AWS. 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"*. This notion posits that collecting large amounts of data in one environment increases the odds of attracting other data and services therein [168].

### 4.4 Instrumentalisation of PETs to extend Amazon's computational infrastructure

From this section, we conclude that while Sidewalk implements PETs to provide some privacy, the story is more complex. Amazon reduces privacy to the confidentiality of certain user data, that it can address with PETs. With these concerns out of the way, Sidewalk *"flips"* consumer Echo and Ring devices to enable new information flows. Once *"flipped"*, information and control flow between other endpoints and their users, manufacturers, and Amazon. With consumer devices flipped to gateways, Amazon *extends their AWS production environment* with a network covering over 90% of the US population, while sparing the company the costly endeavour of building out and maintaining a new physical connectivity infrastructure. 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.[1] The consumer devices-cum-gateways extend Amazon's computational infrastructure; that now offers cloud services and connectivity as a production environment to IoT manufacturers. Meanwhile, Sidewalk exposes an area that covers 90% of the US population to novel privacy concerns. The PETs also do not shield manufacturers' business-sensitive information from Amazon. Interviewees responded to this with resignation, nonchalance, or a bet on coopetition; with very few voicing concerns.

Amazon, we conclude, 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 [259] 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.

## 5 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 Amazon's AWS.

### 5.1 Implementation of encryption in endpoints

Amazon's implementation of PETs in Sidewalk requires manufacturers to embed encryption keys and certificates in endpoints; a process that interviewees called *"keying"*. Factories must use a *"YubiHSM"* hardware security module (HSM) [273] 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"* [19]. This entails Amazon programming a *"device attestation key"* and the *"Sidewalk certificate chain"* onto the HSM [19]. Thereafter, the manufacturer sends the HSM to the factory, that connects it to a computer on the factory line [25]. The factory must also share logs of manufactured devices (including unique persistent identifiers) with Amazon, for routing and authentication by the Sidewalk Network Server.

In the interviews, 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]. For instance, it is not standard for factories to use computers on their factory lines [A1]. For manufacturers that are relatively small or have less experience, this is *"a big change. It's a big step up in security. ... if you don't have these kind of systems from before when you do production, then it's a significant change. ... 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 organize their physical production process.

### 5.2 Transmission and hardware requirements

Amazon does not merely specify capabilities that hardware must meet to implement their PETs. According to [A7], *"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"*. Therefore, manufacturers must pick from one of four approved partner development kits [27; 30]. Additionally, endpoints must use the real-time operating system FreeRTOS (stewarded by AWS) and comply with data rate, volume, synchronism, and frequency requirements in radio transmissions.

That Amazon goes beyond specifying hardware requirements to prescribing four *qualified* silicon providers has varied affects on IoT manufacturers. 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 problematic in the B2C domain, where price-sensitive consumers lead manufacturers to minimise device costs [A1; A6; A7; N1]. The high firmware footprint means that some manufacturers could not fit additional connectivity protocols in the same device. Furthermore, one manufacturer said that 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 FreeRTOS; demanding fundamental changes in development that Amazon provided little transparency around.

[1] 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.

### 5.3 Organisational governance and certification

Contrary to similar protocols such as Bluetooth, Matter, and LoRaWAN, Sidewalk is not governed by a standards body but solely by Amazon. Amazon is also the only party operating the network's backbone, i.e. the Network Server and gateways.

Amazon effectuates their implementation requirements through an *ex-ante* qualification process and its encryption key infrastructure. To qualify, manufacturers must inform Amazon about their organisation and product, and obtain *"development keys"* to connect their prototype to Sidewalk during testing; have a test facility prove that prototypes pass the Sidewalk test cases; and pay a qualification fee (currently zero) [22; 30; 39]. Only after approval may manufacturers advertise Sidewalk compatibility and may 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"* [22]); 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]"* [21]; 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 [21]. Ironically, the terms forbid manufacturers to monitor *"the availability, performance, or functionality of any of [Amazon's] products or services"* [21].

In another example, Amazon adjusted the uplink traffic rates and introduced a daily limit in early 2024, a top-down change in policy [24; 40, p. 18]. 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"* [20, 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 them 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.

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 (§4.2).

Amazon took the liberty to give some manufacturers a favourable treatment, depending on their relations. One respondent's organisation only partially completed the qualification process in order to bring Sidewalk functionality to endpoints later with an OTA update. This is *"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. Another B2C-focused participant indicated that their current endpoints could not accommodate the firmware and saw insufficient value in Sidewalk to use more powerful hardware. In response, 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. They did not extend the privilege to other partners as the pool of adopters grew, underlining Amazon's sole decision-making power over *qualified* implementations.

Amazon has firmly established themselves as Sidewalk's sole governing party, enabling them to unilaterally impose obligations, arbitrarily deviate from their policies, and liberally interpret their 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. Meanwhile, the lack of checks and balances means Amazon can hardly be held accountable for favouritism and arbitrariness in enforcement.

Amazon's sole reign also implies that manufacturers and users rely on their dedication to maintain the Network Server and gateways. If Amazon were to pull the plug on either, all endpoints would lose Sidewalk connectivity. Granted repeated lay-offs [194] and Amazon losing billions of dollars on their devices division between 2017 and 2021 [167], this poses a realistic risk.

One respondent says Amazon is *"in the works of creating a development kit"* to enable manufacturers to have their endpoint double as a gateway, which their company is anticipating and developing towards. We had (and have) not found any other information about this kit, to which the interviewee replied: *"I can't say that they've 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"*. 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"*.

### 5.4 Application server in AWS

AWS ties all the ends together in the implementation of Sidewalk's PETs. Sidewalk requires that all traffic originates from or is sent to an application server within AWS [40]: *"there's no option for the data not going to AWS"* [A5], because *"Sidewalk is decoded and decrypted in Amazon's cloud"* [A6]. This decoding and decrypting entails both en- and decrypting packets, and authenticating of devices and application servers [20]. Once manufacturers land on AWS, they can utilise the myriad of cloud services part of AWS' production offerings (see §3.4) that make their production more agile [125]. The operational control that these services yield is an important reason for manufacturers to adopt AWS [A2; A6; A8].

While seemingly convenient, Amazon's tight integration of Sidewalk with AWS severely hinders manufacturers to manage endpoints from a non-AWS (cloud) server. If manufacturers (or their business customers) wish to use other non-AWS infrastructure, they must move data around or expose APIs from within AWS to these other servers. [A5; A6; A7] have such APIs that their business customers can interact with. [A5] 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."*. [A7] thinks it is *"doable"*, but *"not as easy as is said"* because *"there's still a copy and paste effort"*.

Regardless of whether it is easy, we underline that the data has to be moved around in the first place, as AWS cannot be avoided. This duplication effort entails increased complexity, data integrity challenges, and security risks. Accordingly, Amazon effectively *"funnel[s] people"* into using AWS [A7].

This funnelling has two discursive consequences. First, we cannot refer to Sidewalk as a wireless mesh network (WMN) [as e.g. 75; 155; 228, do]. Contrary to a WMN [7], endpoints and gateways cannot communicate bidirectionally and locally over Sidewalk. This promotes the model of production where all IoT communications pass over an application server. For instance, one study found that about 65% of IoT device companion apps use Bluetooth, implying that 35% has network- or cloud-based communication [215].

Second, the funnelling demonstrates that Sidewalk is not *"just a pipe"*, contrary to Amazon's framing (§3.4). Amazon's appeal to being a pipe implies that they barely intermediate in Sidewalk;[2] granting manufacturers and endpoint users autonomy in deciding what data they send where. On the contrary, Amazon embeds Sidewalk closely in AWS and its IoT-related services. Sidewalk thus does not provide internet connectivity, but *cloud* connectivity [26; 40, p. 9].[3] 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"* would do.

### 5.5 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. This yields benefits for security, but also for continuously updating service functionality to reflect changes in business objectives and outcomes of the service provider.

To receive these advantages, however, manufacturers need to accept the interventions 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. the large and 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 indicated this made it hard for them to adopt and retain knowledge about 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"*. Indeed, one interviewee did not yet turn Sidewalk on despite already making their device hardware compatible: *"we would need to prioritize the R&D bandwidth to actually do the work, versus all other products or projects. So then it becomes a 'portfolio management' kind of thing"* [A2]. Finally, Sidewalk's funnelling of manufacturers into AWS raises the bar for them to use non-AWS cloud services. Thus, once in, shifting away from Sidewalk and AWS becomes challenging; both because manufacturers are distanced further from alternatives and because Amazon's infrastructure and governance mechanisms become so deeply engrained in their production process, that they perpetually reshape and complicate them. This entrenching exemplifies Amazon's power to reorganise business relations between Amazon, Sidewalk adopters, and the companies they source their hardware components from.

## 6 Discussion

### 6.1 The PET Paradox

We explored whether and how Amazon instrumentalised PETs in Sidewalk to entrench their computational infrastructure, to identify its implications for PET design and different types of power. With Amazon's narrow definition of privacy and rudimentary use of PETs, Sidewalk suppresses some sensitive information flows between Amazon, manufacturers, and gateway and endpoint users. This leveraging of PETs was key to apprehend consumer and media pushback against flipping consumer devices into Sidewalk gateways. With these concerns addressed, Amazon repurposes gateways to cast a network that enables new information flows between endpoints and IoT manufacturers. We showed that by exerting sole control over the requirements, design and PETs implementation in Sidewalk, Amazon entrenches its extended infrastructure in and gains agency over manufacturers' production. This entrenchment puts into place potentially long-lasting power asymmetries in how manufacturers produce their devices and services. Amazon's use of PETs in Sidewalk therefore not only has implications for users of

[2] In net neutrality discussions [242], 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) [100; 144], they have reduced liability over content [137; 205; 258].

[3] 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. 69; 102; 114; 271].

gateways and endpoints, but also, if not more, for endpoint manufacturers.

Contrary to PETs' purported contribution to tackling data power by inserting strict controls over information flows, Amazon's implementation of PETs gives rise to a two-faceted *PET Paradox*. First, tech companies can adopt PETs with a narrow interpretation of privacy to *"flip"* consumer devices, enable novel flows of information, and generate economic value. With this, they may expand their infrastructural power, creating new forms of surveillance (B2C) and market asymmetries towards companies adopting their infrastructures (B2B). Hence, rather then constraining their power, PETs in the hands of these companies allow them to arbitrate what privacy is and what information flows count as relevant.

Second, devices becoming accessories of clouds has advantages for implementing privacy (and security), but also grave disadvantages for PET design. In modern-day service architectures, devices are increasingly managed and programmable accessories. This is a win for privacy, as manufacturers can patch vulnerabilities of devices already in use, or deploy and update decentralised PETs – in the case of Sidewalk even without user intervention. However, the very control over the mechanisms for remote programmability, enabled through mobile device management with push notifications, OTA infrastructure, and identity and access management through clouds, is also what enables Amazon to *"flip"* Echo and Ring devices. In other words, Amazon is a centralised authority, making it powerful in deploying but also in compromising PETs, even if these are designed to be decentralised [251].

Moreover, the case study confirms that powerful companies can wield PETs to entrench their power as a central authority. As detailed in Section §5, by dictating how manufacturers must implement Sidewalk's PETs, Amazon gains influence in manufacturers' device hardware and software, cloud environment, factory lines, and organisational processes. The combination of Amazon's control over consumer devices to make them gateways, and ability to set requirements towards manufacturers, extends Amazon's control beyond its own devices to those produced by third parties; entrenching their computational infrastructure in the process. This entrenchment further centralises the single entity's control over the hardware, OS, and network connectivity of these devices. Amazon is hence not only a centralised authority that deploys a decentralised solution, but introduces a web of control around devices that erode assumptions PETs researchers can make about devices being a trusted or personal base for decentralised PETs [251]. These interventions entrench Amazon's computational infrastructure – now extended to include consumers' gateways – in the process.

## 6.2 PETs in the "clipping economy"

Expanding and entrenching the infrastructure of these companies using PETs also has an economic dimension. Service providers have long been *"clipping"* a portion of revenue from parties using their services. For instance, Apple and Stripe charge a commission for sales in their App Store and payment platform, respectively. We refer to this phenomenon as the *"clipping economy"*. But Sidewalk, and the other instances in §2, constitute a new chapter therein.

Instead of taking a cut from revenue, Amazon, Apple, and Google utilise their control over critical masses of spatially dispersed and capable consumer-owned devices to *"clip"* portions of their compute, sensing capabilities, browsing and app habits, and bandwidth (in fact realised by telecommunication providers). The companies weave the consumer devices together, creating an *extension of their computational infrastructure* with substantial population or spatial coverage. This extension lets them offer novel services to consumers, businesses, and governments: *"privacy-preserving contact tracing, device finding, advertising, and connectivity"*.

PETs, regardless of their sophistication, serve two central functions that enable tech companies to treat consumer devices as extensions of their infrastructure for generating economic value. First, when companies frame flipping purely as a privacy issue, PETs can be depicted as necessary and sufficient solutions. By deploying PETs, these firms persuade device owners, advocates and regulators that repurposing personal devices for third-party services does not compromise privacy. Even when (rightfully) attacking these claims, as the media and public have done, economic concerns are rendered secondary. Second, these companies' self-claimed authority over implementation of PETs and control over associated information flows, serves to deepen their capacity to furnish end-devices as extensions of their software production environments to third parties. Our case study confirms this trend for Amazon and the way it instrumentalizes PETs to extract value from consumer-owned devices, now rendered extensions of their infrastructures for production of third-party services.

## 6.3 Betting on rising with giants

The power asymmetries between Amazon and manufacturers raise the question: does Sidewalk provide manufacturers sufficient functional benefits to risk these dependencies on Amazon and their infrastructure? Multiple participants mentioned that 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 mean Sidewalk is *"not a perfect fit for [them]"*, as one interviewee said. One participant expressed that *"there's an aspect of an ongoing partnership with Amazon, which is a huge company"*. Another respondent relies on and envisions future integrations with Amazon's logistics and parcel delivery 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 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"*.

These argumentations clearly show how manufacturers rely on Amazon for a myriad of services vital to their current or future business proposition. These parallel dependencies lead them to accept the new or aggravated dependencies that adopting Sidewalk brings with it. 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).

## 7 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. 38], 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 [20; 40]. The protocol specification also considers a *"Detailed specification of Gateways and the Amazon Sidewalk Cloud"*, and interactions between them, outside its scope [40, p. 10].

To mitigate and increase the robustness of the case studies and interviews, we triangulated multiple data sources to [211; 227; 272].

## 8 Conclusion

On the surface, deploying PETs to millions of devices seems a win for citizen privacy and curbing corporate and state power. Our empirical study of Amazon Sidewalk reveals a more complex story. We started with the hypothesis that tech companies may implement PETs in their computational infrastructure such that they entrench it in the production of other organisations. We showed how this comes to be through various sources and first-hand experiences of Sidewalk-adopting IoT manufacturers.

Our study made concrete how Amazon's implementation of PETs in Sidewalk manifests a two-faceted *PET Paradox*. Leveraging PETs and control over consumer devices, Amazon clips a part of an infrastructure of internet-connected devices (gateways; managed by consumers and ISPs) for a closed network that hooks IoT devices (endpoints of manufacturers) onto their cloud. While PETs conceal some information flows, they open up possibilities for novel ones, expanding the AWS production environment to include IoT telemetry of third-party manufacturers. For users and non-users alike, the new flows compromise privacy; for manufacturers, they compromise their confidentiality and competitive position with respect to Amazon. Seen this way, PETs in Sidewalk exacerbate rather than reduce information asymmetry-based power imbalances (facet 1).

Additionally, Amazon influences the production of Sidewalk-adopting manufacturers; spanning across hardware, software, and the environments for producing and managing their devices and services. With this influence, Amazon turns third-party IoT devices into accessories of Amazon's cloud, while its governance of Sidewalk eats into companies' technical and organisational bandwidth, incurring a path dependency. Thus, Amazon tailors privacy in a fashion that entrenches their computational infrastructure, and thereby infrastructural power, in the production activities of other companies. Aside from incentivising third-party manufacturers to adopt more AWS services, this PET-leveraging *"flipping"* increases Amazon's capacity to remotely manage devices through AWS. At the same time, it undermines the assumption that user devices can be a trusted base for decentralised PETs (facet 2).

Both outcomes are orthogonal to the original aim of privacy engineers and researchers, to curb corporate and governmental power through PETs that pursue data minimisation, purpose limitation, and preventing single points of privacy failure.

Going forward, we imagine the following steps to better articulate infrastructural power and its impact on the adoption of PETs as well as competition, and to mitigate some of these effects.

**Identify when privacy masks an extractive intervention:** In all our examples, powerful companies render their attempts to increase control over end devices (i.e., through centralisation of control over hardware, software, and remote management infrastructure) to a matter of confidentiality of information flows. We showed concretely how companies instrumentalise PETs to *"clip"* resources from end devices: they repurpose them as extensions of their own infrastructure; claiming their compute, personal data, and connectivity for economic gain. Researchers and practitioners should continue to raise red flags when PETs are used to distract from the underlying economic extraction [e.g. 93; 171; 212; 259].

**Mitigate privacy-washing through 'data minimisation to purpose':** The first facet of the PET Paradox suggests that selective confidentiality of *"personal data"* flows should raise red flags. Focusing on what (non-)personal data is visible to whom in PET applications distracts from more fundamental power issues, as shown for Sidewalk in this paper, as well as for digital advertising in earlier work. For the latter, McGuigan et al. [171] speak of *"cynical resignation"* and Veale [259] of *"confidentiality washing"*. This privacy- or confidentiality-washing can be mitigated by re-centering a criterium that has been fundamental for designing and evaluating PETs [124; 134], namely *data minimisation across all data flows towards a purpose*. Data flows can harm (non-)user privacy and autonomy, and confidentiality of business-sensitive information, even if this data is not personal or kept confidential. Therefore, data flows should not (only) be assessed based on whether they reveal personal information, also on but whether they are necessary and proportionate.

**Extend PET evaluation to include market and infrastructural power:** Our work shows 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 comes to play. Such power is concentrated in the hands of a few companies. Thus, when assessing PET applications as per the previous paragraph, it is imperative to consider *"who"* designs and deploys PETs [62], with what impact on end devices, for what economic outcomes, and based on whose resources. Further, when B2B relations are implied in PET applications, considering how information flows enabled by a purportedly 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 competition benefits for parties that have a bad privacy track record (e.g. punishing Apple for the anticompetitive effects of its allegedly privacy-improving ATT on advertisers and adtech companies); but to include in adversarial analysis the centralised authorities that instrumentalise PETs to selectively suppress information flows to their (economic) advantage.

**Challenge the centralising force of computational infrastructures on engineering PETs:** Many PETs rely on decentralisation to achieve their privacy benefits. Though Troncoso et al. [251] argue that when doing so, many decentralised systems designed to enhance privacy, (sometimes tacitly) assume centralisation of network information, computations, and trust establishment. These centralisations may be technical (e.g. key exchange, network information) and social (e.g. identity management). In Sidewalk, centralisation manifests in networking (e.g. managing network topology, gateways, routing, 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 already seems 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 [215]. The impact of cloud-centricity in smartphones has also been problematised, e.g. for push notifications in secure messaging [214]. User control over end devices is fundamental to PET deployment [77; 124; 251] and to privacy as autonomy [112; 118]. Yet, part and parcel to Amazon, Apple and Google *"clipping"* compute, sensing capabilities, browsing and app habits, and bandwidth of consumer devices, is their ability to remotely transform them; what Veale [261] calls their *"orchestration power"*. The centralising forces enabling this – and the power dynamics they create between users, manufacturers, and tech companies – would benefit from *more empirical studies like this one, to guide privacy, competition, and engineering communities in identifying and addressing concrete challenges* due to computational infrastructures as centralised software production environments.

Specifically, we urge PET designers to *look more critically at dependencies of users and manufacturers on these computational infrastructures that are abstracted away when designing PETs* [62], and resist accepting them as inevitable [165; 268]. An example alternative technical architectures is the trusted execution-based smartphone architecture pitched by Groschupp et al. [119], 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) and empowering them, phone manufacturers, and app developers. Our work underlines that similar efforts for OTA infrastructures, OSes, cloud environments, patches and updates, and hardware implementations of public key infrastructures are needed. This research should not merely assess privacy and security, but study how they may avoid entrenching existing computational infrastructures.

Meanwhile, competition and privacy scholars and authorities should question the centralising forces exerted by these computational infrastructures of large tech companies, when any company wishes to deploy PETs. Our work demonstrates that these forces have consequences for both privacy (i.e. feasibility of deploying truly privacy-enhancing technologies) and antitrust (i.e. the control of third parties over how they produce and deploy software, hardware, and services). This means going beyond focusing on app stores, cloud infrastructures, APIs, platforms, or control over and insight into (personal data); instead taking as point of departure tech companies' control over software production in their computational infrastructures. It would be worthwhile to explore extending legal regimes to allow sideloading and otherwise improve user control over devices; and curb tech companies' control over them.

**Engage conversations across affected players:** To pursue these recommendations, it is vital that policymakers, researchers, and (to be) affected companies come together; with technology (e.g. cloud, OS, cryptography), privacy, competition, sovereignty, and public policy as areas of concern. Multidisciplinarity is necessary. Already, scholars and regulators are actively analysing the advertising and finding network instances as potentially anticompetitive application of PETs (see §2). The contact tracing instance raised governmental sovereignty and public decision-making questions: Google and Apple became arbiters of privacy and obtained an important role in public healthcare. 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' 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 privacy (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 without further ado.

## Acknowledgments

This work is part of the Programmable Infrastructures Project[4] and was partially funded by Fondation Botnar and NWO project Public Values in the Algorithmic Society (AlgoSoc, file number 024.005.017)[5]. For fruitful discussions on earlier drafts, we thank Agathe Balayn, Aniketh Girish, Bernd Kasparek, Carmela Troncoso, Corinne Cath, 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 and Dagstuhl Seminar 25112 *"PETs and AI: Privacy Washing and the Need for a PETs Evaluation Framework"*.

## 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

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

[5] www.algosoc.org

[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/ Accessed 2024-01-21.

[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 Accessed 2024-07-23.

[11] Amazon. 2019. Introducing Amazon Sidewalk. https://www.aboutamazon.com/news/devices/introducing-amazon-sidewalk Accessed 2024-07-23.

[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 Accessed 2024-07-23.

[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 Accessed 2024-01-21.

[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 Accessed 2024-01-21.

[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 Accessed 2024-01-13.

[19] Amazon. 2023. Amazon Sidewalk Manufacturing Setup and Workflow. https://docs.sidewalk.amazon/manufacturing/sidewalk-manufacturing-setup-works.html Accessed 2024-01-09.

[20] Amazon. 2023. *Amazon Sidewalk Privacy and Security Whitepaper.* Technical Report. https://m.media-amazon.com/images/G/01/sidewalk/final_privacy_security_whitepaper.pdf

[21] Amazon. 2023. Amazon Sidewalk Program Security Requirements. https://docs.sidewalk.amazon/sidewalk-terms-and-agreements/security-program-requirements.html Accessed 2024-03-16.

[22] Amazon. 2023. Amazon Sidewalk Qualification Concepts. https://docs.sidewalk.amazon/qualification/works-with-sidewalk/sidewalk-qualification-concepts.html Accessed 2024-03-16.

[23] Amazon. 2023. Components of Amazon Sidewalk Manufacturing. https://docs.sidewalk.amazon/manufacturing/sidewalk-manufacturing-components.html Accessed 2024-01-09.

[24] Amazon. 2023. How Amazon Sidewalk Works. https://docs.sidewalk.amazon/introduction/sidewalk-how-works.html Accessed 2024-03-15.

[25] Amazon. 2023. How To Manufacture & Produce Devices: Step 1: Setting up the Host. https://docs.sidewalk.amazon/manufacturing/manufacture-provision/sidewalk-host-installation.html Accessed 2024-09-13.

[26] Amazon. 2023. Introduction to Amazon Sidewalk. https://docs.sidewalk.amazon/introduction/ Accessed 2024-02-10.

[27] Amazon. 2023. Qualified Development Kits. https://docs.sidewalk.amazon/getting-started/Qualified-Development-Kits.html Accessed 2024-04-02.

[28] Amazon. 2023. Terms and Agreements. https://docs.sidewalk.amazon/sidewalk-terms-and-agreements/ Accessed 2024-02-23.

[29] Amazon. 2023. Works with Amazon Sidewalk Qualification Guidelines. https://docs.sidewalk.amazon/sidewalk-terms-and-agreements/wwas-sidewalk-qualification-guidelines.html Accessed 2024-03-16.

[30] Amazon. 2023. Works With Amazon Sidewalk Qualification Process. https://docs.sidewalk.amazon/qualification/works-with-sidewalk/qualification-works-path.html Accessed 2024-02-06.

[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 Accessed 2024-02-13.

[32] Amazon. 2024. Sidewalk Coverage Maps. https://coverage.sidewalk.amazon/ Accessed 2024-09-30.

[33] Amazon. 2025. Sidewalk Coverage Maps. https://coverage.sidewalk.amazon/ Accessed 2025-11-14.

[34] Amazon. n.d.. Amazon Devices: Echo Smart Speakers & Displays. https://www.amazon.in/amazon-echo/b?ie=UTF8&node=14156834031 Accessed 2024-03-02.

[35] Amazon. n.d.. Amazon Sidewalk. https://www.amazon.com/Amazon-Sidewalk/b?ie=UTF8&node=21328123011 Accessed 2024-04-02.

[36] Amazon. n.d.. Amazon Sidewalk Gateways. web.archive.org/web/20240302142350/https://docs.sidewalk.amazon/introduction/sidewalk-gateways.html Accessed 2024-11-29.

[37] Amazon. n.d.. Amazon Sidewalk Test Kit. https://sidewalk.amazon/testkit Accessed 2024-02-12.

[38] Amazon. n.d.. Sidewalk360. https://360.sidewalk.amazon/ Accessed 2024-02-23.

[39] Amazon Technologies. 2023. *Amazon Sidewalk Test Specification.* Technical Report Protocol Stack 1.0, Document Revision A.1. https://docs.sidewalk.amazon/assets/pdf/Amazon_Sidewalk_Test_Specification-1.0-rev-A.1.pdf

[40] 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

[41] 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 Accessed 2024-10-30.

[42] Amazon Web Services. n.d.. AWS IoT Device Defender. https://aws.amazon.com/iot-device-defender/ Accessed 2024-03-20.

[43] Amazon Web Services. n.d.. Manage a Connected AWS IoT Device Fleet. https://catalog.workshops.aws/aws-iot-device-fleet-management/en-US Accessed 2024-04-02.

[44] 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 Accessed 2024-09-27.

[45] Amazon Web Services. n.d.. What Is AWS IoT Wireless? https://docs.aws.amazon.com/iot-wireless/latest/developerguide/what-is-iot-wireless.html Accessed 2024-09-27.

[46] 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

[47] Apple. 2021. Apple Introduces AirTag. https://www.apple.com/newsroom/2021/04/apple-introduces-airtag/ Accessed 2024-08-28.

[48] 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/ Accessed 2024-08-28.

[49] Apple. 2024. If an App Asks to Track Your Activity. https://support.apple.com/en-us/102420 Accessed 2023-10-16.

[50] Apple. n.d.. Find My Network. https://developer.apple.com/find-my Accessed 2024-08-28.

[51] 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/ Accessed 2024-07-29.

[52] Arrive. 2023. Arrive Announces Successful Integration with Amazon Sidewalk. https://www.arrive.tech/news/arrive-announces-successful-integration-with-amazon-sidewalk Accessed 2024-01-21.

[53] Arrive. 2024. Arrive. https://www.arrive.tech Accessed 2024-01-21.

[54] Arrive. n.d.. Arrive Campaign on PicMii Crowdfunding. https://www.picmiicrowdfunding.com/deal/arrive/ Accessed 2024-01-21.

[55] ATLAS.ti. 2023. ATLAS.Ti Desktop. https://atlasti.com/atlas-ti-desktop

[56] 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

[57] Autorità Garante della Concorrenza e del Mercato. 2023. A561-A561B - Italian Competition Authority: Investigation Opened against Apple for Alleged Abuse of Dominant Position in the App Market. https://en.agcm.it/en/media/press-releases/2023/5/A561-A561B Accessed 2024-08-20.

[58] 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 Accessed 2024-08-20.

[59] 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 Accessed 2024-08-20.
[60] 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 Accessed 2024-01-21.
[61] 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 Accessed 2024-01-21.
[62] 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* (Washington DC, USA) *(CSLAW '22)*. Association for Computing Machinery, New York, NY, USA, 167–179. https://doi.org/10.1145/3511265.3550443
[63] 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/ Accessed 2024-08-01.
[64] Kendra Barnett. 2025. Google's Privacy Sandbox Is Officially Dead. https://www.adweek.com/media/googles-privacy-sandbox-is-officially-dead/ Accessed 2025-11-26.
[65] 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
[66] 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/
[67] Stephen Bonner. 2024. ICO Statement in Response to Google Announcing It Will No Longer Block Third Party Cookies in Chrome. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/07/ico-statement-in-response-to-google-announcing-it-will-no-longer-block-third-party-cookies/ Accessed 2024-07-30.
[68] 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/ Accessed 2024-02-25.
[69] British Telecommunications. n.d.. BT Wi-Fi. https://info.btwifi.com Accessed 2024-09-29.
[70] 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/ Accessed 2024-02-24.
[71] Marques Brownlee. 2021. Apple vs The Paradox of Choice! https://www.youtube.com/watch?v=qNAo0UdYF6g
[72] 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/ Accessed 2024-03-14.
[73] 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 Accessed 2024-08-20.
[74] 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
[75] Jon Callas. 2021. Understanding Amazon Sidewalk. https://www.eff.org/deeplinks/2021/06/understanding-amazon-sidewalk Accessed 2024-02-28.
[76] 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
[77] 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/ Accessed 2025-11-26.
[78] CareBand. n.d.. Products. https://carebandremembers.com/products/ Accessed 2024-01-21.
[79] CareBand. n.d.. Technology. https://carebandremembers.com/powered-by-third-wave/ Accessed 2024-01-21.
[80] 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 Accessed 2022-08-22.
[81] 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/ Accessed 2024-02-28.
[82] 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
[83] Anthony Chavez. 2024. A New Path for Privacy Sandbox on the Web. https://privacysandbox.com/news/privacy-sandbox-update Accessed 2024-07-29.
[84] Anthony Chavez. 2025. Update on Plans for Privacy Sandbox Technologies. https://privacysandbox.com/news/update-on-plans-for-privacy-sandbox-technologies/ Accessed 2025-11-26.
[85] Chipolo. n.d.. Chipolo. https://chipolo.net/en/ Accessed 2024-08-27.
[86] 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
[87] 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 Accessed 2024-08-22.
[88] 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
[89] 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
[90] 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
[91] 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
[92] 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
[93] 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 Accessed 2024-07-30.
[94] 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 Accessed 2024-02-28.
[95] 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/ Accessed 2024-02-22.
[96] David Curry. 2024. App Tracking Transparency Opt-In Rates (2024). https://www.businessofapps.com/data/att-opt-in-rates/ Accessed 2024-08-01.
[97] 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
[98] 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 Accessed 2024-02-24.
[99] 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.
[100] 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
[101] 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
[102] Deutsche Telekom. 2013. Mobility: Online Any Time, Anywhere. https://www.telekom.com/en/company/details/mobility-online-any-time-anywhere-358830 Accessed 2024-09-29.
[103] Deviceroy. 2023. Aria Spec Sheet. https://deviceroy.com/wp-content/uploads/2023/04/Aria-Spec-Sheet-1.pdf Accessed 2024-01-21.
[104] Deviceroy. 2023. Connectivity Revolution: Deviceroy's Aria Integrates with Amazon Sidewalk at CES. https://deviceroy.com/connectivity-revolution-

deviceroys-aria-integrates-with-amazon-sidewalk-at-ces/ Accessed 2024-01-21.
[105] 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 Accessed 2024-07-30.
[106] Javier Espinoza. 2020. Apple Accused of Competition Abuse over Tracking Apps. https://www.ft.com/content/a08627c5-61d6-4513-9e7e-acac6b1ba862 Accessed 2024-08-27.
[107] 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 Accessed 2024-02-18.
[108] 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 Accessed 2025-11-26.
[109] European Commission. n.d.. DMA Designated Gatekeepers. https://digital-markets-act.ec.europa.eu/gatekeepers_en Accessed 2025-07-25.
[110] 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
[111] 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 Accessed 2024-02-22.
[112] 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
[113] 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 Accessed 2024-02-26.
[114] Fon. 2014. Fon and OTE Announce WiFi Partnership In Greece. https://fon.com/fon-and-ote-announce-wifi-partnership-in-greece/ Accessed 2024-09-29.
[115] Antone Gonsalves. 2023. OnAsset Logistics Service Taps Amazon Sidewalk. https://www.techtarget.com/searchnetworking/news/365534914/OnAsset-logistics-service-taps-Amazon-Sidewalk Accessed 2024-01-21.
[116] 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/ Accessed 2024-02-28.
[117] Google. 2024. What Is the Privacy Sandbox? https://developers.google.com/privacy-sandbox/overview Accessed 2024-08-22.
[118] 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
[119] 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
[120] 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 Accessed 2024-02-22.
[121] 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 Accessed 2024-02-24.
[122] 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 Accessed 2024-02-22.
[123] 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 Accessed 2024-02-24.
[124] 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
[125] 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
[126] 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
[127] 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/ Accessed 2024-02-22.
[128] 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 Accessed 2024-02-22.
[129] 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 Accessed 2024-02-22.
[130] 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 Accessed 2024-02-22.
[131] 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
[132] 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/ Accessed 2024-01-21.
[133] 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
[134] 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
[135] 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=
[136] 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
[137] 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
[138] Index Exchange. 2024. Insights from Our Privacy Sandbox Testing. https://www.indexexchange.com/2024/07/02/insights-privacy-sandbox-testing/ Accessed 2024-07-30.
[139] 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
[140] Internet Archive. n.d.. Wayback Machine. https://web.archive.org/ Accessed 2024-03-02.
[141] 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
[142] 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
[143] 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
[144] 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
[145] 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
[146] 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/ Accessed 2024-08-01.
[147] 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/ Accessed 2024-02-18.
[148] 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/ Accessed 2024-02-24.
[149] 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
[150] Reinhold Kesler. 2023. The Impact of Apple's App Tracking Transparency on App Monetization. https://doi.org/10.2139/ssrn.4090786
[151] 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
[152] 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
[153] Fiona Kuan. 2023. Extend Your IoT Devices Range with Amazon Sidewalk Devices from MOKOSmart. https://www.mokosmart.com/amazon-sidewalk-devices-from-mokosmart/ Accessed 2024-01-21.
[154] Immanuel Kunz, Konrad Weiss, Angelika Schneider, and Christian Banse. 2023. Privacy Property Graph: Towards Automated Privacy Threat Modeling via Static Graph-based Analysis. In *Proceedings on Privacy Enhancing Technologies*, Vol. 2. The Association for Privacy Enhancing Technologies, 171–187. https://petsymposium.org/2023/files/papers/issue2/popets-2023-0046.pdf
[155] 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/ Accessed 2024-02-08.
[156] 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
[157] Level. n.d.. Multifamily. https://level.co/multifamily/ Accessed 2024-01-21.
[158] Level. n.d.. Smart Lock Catalog. https://level.co/smart-lock/ Accessed 2024-01-21.
[159] Level. n.d.. Support: Home Integrations: Sidewalk. https://level.co/support/sections/Sidewalk03 Accessed 2024-01-21.
[160] 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
[161] 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
[162] 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
[163] 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 Accessed 2024-02-22.
[164] 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
[165] Moxie Marlinspike. 2026. Reflections: The Ecosystem Is Moving. https://signal.org/blog/the-ecosystem-is-moving/ Accessed 2025-12-01.
[166] 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 Accessed 2024-02-18.
[167] 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 Accessed 2024-09-13.
[168] Dave McCrory. 2010. Data Gravity – in the Clouds. https://datagravitas.com/2010/12/07/data-gravity-in-the-clouds/ Accessed 2024-09-12.
[169] Patrick McGee. 2021. Apple's Privacy Changes Create Windfall for Its Own Advertising Business. https://www.ft.com/content/074b881f-a931-4986-888e-2ac53e286b9d Accessed 2024-02-22.
[170] 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
[171] 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
[172] Pradeep Menon. 2023. Best Find My Devices for iPhone in 2023. https://www.xda-developers.com/best-find-my-devices-iphone/ Accessed 2024-02-25.
[173] MerryIoT. 2023. MerryIoT Sensors & MerryIoT for Amazon Sidewalk: Quick Installation Guide. https://www.merryiot.com/Product/P_12/C_Install/V_1.0/MerryIoT%20Sensor%20Home%20Kit%20QIG%20Sidewalk%2020230724(BQW_02_0045.001).pdf
[174] MerryIoT. n.d.. Product. https://www.merryiot.com/Product Accessed 2024-01-21.
[175] Meshify. n.d.. About. https://meshify.com/about/ Accessed 2024-01-21.
[176] Meshify. n.d.. Meshify Defender S. https://meshify.com/products/defender-s/ Accessed 2024-04-02.
[177] 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/ Accessed 2023-11-08.
[178] 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
[179] Netvox. 2023. New Netvox S315 Series Devices Integrate with Amazon Sidewalk Technology. http://www.netvox.com.tw/news2.asp?pro=107 Accessed 2024-01-21.
[180] Netvox. n.d.. Products: Amazon Sidewalk: S315 Series. http://www.netvox.com.tw/protest.asp?pro=a1 Accessed 2024-01-21.
[181] 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 Accessed 2024-01-21.
[182] New Cosmos USA. n.d.. Amazon Sidewalk Smart Natural Gas Detector. https://denovadetect.com/pages/amazon-sidewalk Accessed 2024-04-02.
[183] New Cosmos USA. n.d.. DeNova Detect. https://denovadetect.com/ Accessed 2024-01-21.
[184] Lily Hay Newman. 2021. How to Turn Off Amazon Sidewalk. https://www.wired.com/story/turn-off-amazon-sidewalk/ Accessed 2024-02-24.
[185] 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/ Accessed 2024-02-22.
[186] 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
[187] 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/ Accessed 2023-11-08.
[188] OnAsset Intelligence. 2023. OnAsset Intelligence Launches Dedicated Supply Chain Monitoring Device on Amazon Sidewalk. https://onasset.com/sentinel200-amazon-sidewalk/ Accessed 2024-01-21.
[189] OnAsset Intelligence. n.d.. Products. https://www.onasset.com/products/#sentinel100 Accessed 2024-04-02.
[190] 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 Accessed 2023-05-27.
[191] Will Oremus. 2019. Amazon Just Became the Everywhere Store. https://onezero.medium.com/amazon-just-became-the-everywhere-store-dce9353decd3 Accessed 2024-09-23.
[192] Peter Ormerod. 2024. Privacy Law's Incumbency Problem. *UC Davis Law Review* 58, 1 (2024). https://papers.ssrn.com/abstract=4819613
[193] 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
[194] 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 Accessed 2024-09-13.
[195] 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
[196] 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
[197] 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/ Accessed 2024-07-30.
[198] 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 Accessed 2023-11-08.
[199] 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 Accessed 2024-02-24.
[200] Pebblebee. n.d.. Clip, Card and Tag - Apple Find My™ vs Google's Find My Device. https://help.pebblebee.com/article/lurhtifwcm-card-and-clip-on-an-android-and-ios Accessed 2024-08-28.
[201] Pebblebee. n.d.. Pebblebee. https://pebblebee.com/ Accessed 2024-08-28.

[202] 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
[203] 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/ Accessed 2024-08-29.
[204] 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 Accessed 2024-04-02.
[205] 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/
[206] Ring. n.d.. Products. https://ring.com/collections/all-products Accessed 2024-02-24.
[207] Ring. n.d.. Video Doorbell Pro 2. https://nl-nl.ring.com/products/video-doorbell-pro-2 Accessed 2024-03-03.
[208] 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
[209] 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 Accessed 2024-08-27.
[210] 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/ Accessed 2023-11-08.
[211] Jennifer Rowley. 2002. Using Case Studies in Research. *Management Research News* 25, 1 (Jan. 2002), 16–27. https://doi.org/10.1108/01409170210782990
[212] 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
[213] Johnny Saldaña. 2021. *The Coding Manual for Qualitative Researchers* (4 ed.). SAGE, London, England. https://search.worldcat.org/title/1233312600
[214] 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
[215] 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
[216] 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 Accessed 2024-07-29.
[217] 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
[218] Eric Benjamin Seufert. 2024. Why Is Google Killing Cookies? https://mobiledevmemo.com/why-is-google-killing-cookies/ Accessed 2024-07-30.
[219] 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
[220] Tamar Sharon, Marthe Stevens, Andrew Hoffman, Steven Kraaijeveld, and Lotje Siffels. n.d.. Sphere Transgression Watch. https://www.sphere-transgression-watch.org/ Accessed 2025-06-26.
[221] 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/ Accessed 2024-08-01.
[222] Kris Shrishak. 2025. Privacy Washing through PETs: The Case of Worldcoin. https://cacm.acm.org/blogcacm/privacy-washing-through-pets-the-case-of-worldcoin/
[223] 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/ Accessed 2024-10-29.
[224] 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 Accessed 2024-11-29.
[225] 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 Accessed 2024-04-02.
[226] Adrienne So. 2023. Why We Don't Recommend Ring Cameras. https://www.wired.com/story/why-we-do-not-recommend-ring/ Accessed 2024-10-10.
[227] 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
[228] 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 Accessed 2023-11-08.
[229] Nick Srnicek. 2022. *Data, Compute, Labor*. The MIT Press. https://direct.mit.edu/books/oa-edited-volume/5319/chapter/3800166/Data-Compute-Labor
[230] 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
[231] StatCounter. 2024. Mobile Operating System Market Share Worldwide Dec 2019 - June 2024. https://gs.statcounter.com/os-market-share/mobile/worldwide Accessed 2024-06-10.
[232] 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
[233] Subeca. 2023. Enhancing Water Utility Surveillance and Response (SRS) with Subeca - Subeca. https://www.subeca.com/blogs/enhancing-water-utility-surveillance-and-response-srs-with-subeca Accessed 2024-01-21.
[234] Subeca. 2023. Subeca, Inc. Joins Forces with Amazon Sidewalk to Innovate and Simplify Water Metering. https://www.subeca.com/blogs/subeca-inc-joins-forces-with-amazon-sidewalk-to-innovate-and-simplify-water-metering Accessed 2024-01-21.
[235] 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
[236] 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
[237] Surfshark. 2024. The Insights of Our Smart Home Privacy Checker. https://surfshark.com/research/smart-homes/insights Accessed 2024-09-09.
[238] Surfshark. 2024. Methodology. https://surfshark.com/research/smart-homes/methodology Accessed 2024-09-09.
[239] 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
[240] Tag-N-Trac. n.d.. Smart Sensing. https://www.tagntrac.com/smart-sensing/ Accessed 2024-01-21.
[241] Texas Instruments. 2020. Connect: Amazon Sidewalk Chat with Airthings and Tag-n-Trac. https://www.youtube.com/watch?v=qIXSgGq2iKw Accessed 2024-01-21.
[242] 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
[243] Thingy-IoT. n.d.. Home. https://thingy-iot.au/ Accessed 2024-01-21.
[244] 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 Accessed 2024-01-21.
[245] 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
[246] Tile. n.d.. How Tile Works. https://www.tile.com/en-eu/how-it-works Accessed 2024-08-29.
[247] Trey Titone. 2024. Assessing the Impact of Google's Privacy Sandbox. https://adtechexplained.com/assessing-the-impact-of-googles-privacy-sandbox/ Accessed 2024-07-30.
[248] Trey Titone. 2024. Why Is Google No Longer Deprecating Cookies? https://adtechexplained.com/why-is-google-no-longer-deprecating-cookies/ Accessed 2024-07-30.
[249] 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

[250] 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

[251] 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

[252] 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

[253] 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

[254] 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 Accessed 2024-08-29.

[255] Urząd Ochrony Konkurencji i Konsumentów. 2021. Apple - the President of UOKiK initiates an investigation. https://archiwum.uokik.gov.pl/aktualnosci.php?news_id=18092 Accessed 2024-08-20.

[256] 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 Accessed 2025-11-29.

[257] Lisa Vaas. 2021. Amazon Sidewalk Poised to Sweep You Into Its Mesh. https://threatpost.com/amazon-sidewalk-to-sweep-you-into-its-mesh/166581/ Accessed 2023-11-08.

[258] 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/ Accessed 2024-11-08.

[259] 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

[260] 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

[261] Michael Veale. 2023. Some Commonly-Held but Shaky Assumptions about Data, Privacy and Power. https://doi.org/10.31235/osf.io/z8tw6

[262] 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

[263] 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/ Accessed 2024-01-21.

[264] 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

[265] Charlie Warzel. 2019. Opinion: Amazon Wants to Surveil Your Dog. https://www.nytimes.com/2019/10/01/opinion/amazon-privacy.html Accessed 2024-09-23.

[266] 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

[267] Tiahn Wetzler. 2023. ATT Two Years on: Opt-in Rates Keep Climbing. https://www.adjust.com/blog/app-tracking-transparency-opt-in-rates/ Accessed 2024-07-29.

[268] 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/

[269] Lewis Wight. 2023. The Promised Growth of IoT. https://meshify.com/the-promised-growth-of-iot/ Accessed 2024-01-21.

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

[271] Xfinity. n.d.. Xfinity WiFi Home Hotspot FAQs. https://www.xfinity.com/support/articles/xfinity-wifi-hotspots Accessed 2024-09-29.

[272] 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

[273] Yubico. n.d.. YubiHSM 2 v2.3.2. https://www.yubico.com/product/yubihsm-2/ Accessed 2024-04-02.

# A Elaboration of methods

This appendix further details our methods (§3.1). We present the identified adopters (§A.1), the codebook (§A.2), and interview questions (§A.3).

## A.1 Overview of identified adopters

Table 1 displays the Sidewalk adopters identified with the grey literature review. These results were at points supplemented with information obtained during the 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 Elite interviews: codebook

Table 2 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.

## A.3 Interview questions

Below is a compilation of the prepared interview questions. 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 in one case where the participant requested us to. We only provided the 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.

### *A.3.1 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.3.2 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)*

**Table 1: Overview of identified Sidewalk adopters, products, and business orientations**

| Company name | Product name (if available): functionality | Sells to businesses (B2B) and/or consumers (B2C) | References |
|---|---|---|---|
| Airthings | Sensing CO2, radon, temperature, humidity, and air quality | B2B, B2C | [5; 6; 60; 61; 241] |
| Arrive | Point, Bank, Convey, Package Tower: smart mailbox(es), Mailbox as a Service | B2B | [52–54] |
| CareBand | CareBand: panic button, location and activity detection; for elderly people, contact tracing, and outdoors worker safety | B2B, B2C | [78; 79; 132] |
| DeNova Detect (by New Cosmos) | 807NAS: natural gas alarm | B2B, B2C | [181–183] |
| Deviceroy | Aria: relaying an industrial device's readings to the internet | B2B | [103; 104] |
| Level | Level: smart door lock | B2B, B2C | [15; 157–159] |
| MerryIoT (by Browan Communications) | Four devices for sensing CO2, motion, door/window open/close, water leak, temperature, and humidity | B2C | [173; 174] |
| Meshify (by HSB) | Defender S: water leak and water pipe freeze/break sensing | B2B | [175; 176; 269] |
| MOKO-Smart | Motion detection, asset and person tracking, smart plug | B2B (OEM) | [153] |
| Netvox | S315 series: integrates modular sensors; supports sensing temperature, humidity, motion, water leaks, vibration, light, and door contact | B2B (OEM) | [18; 179; 180] |
| OnAsset | Sentinel 200: asset tracking and condition monitoring) | B2B | [18; 115; 188; 189] |
| Primax | Woody: smart door lock | B2B (OEM) | [18; 204] |
| Subeca | Pin: Advanced Meter Infrastructure sensor for water utilities | B2B | [225; 233; 234] |
| Tag-n-Trac | Smart Sense: asset tracking and condition monitoring | B2B | [240; 241] |
| Thingy | Thingy: air quality sensing, specifically for early wildfire detection | B2B | [243; 263] |
| Tile | Tile: asset tracking | B2B, B2C | [15; 244] |

(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; 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

**Table 2: 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 | | |

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.3.3 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 Sidewalk marketing visuals

Figure 3 shows examples of how Amazon visualises Sidewalk to consumers (both gateway and endpoint owners).

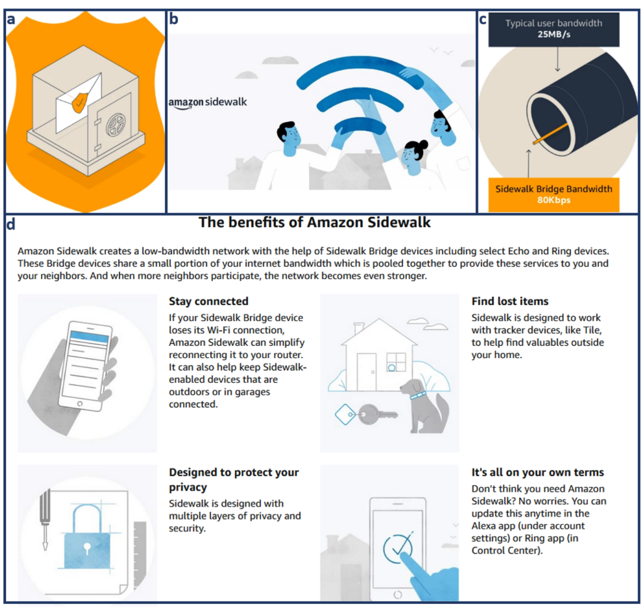


**Figure 3: A compilation of visuals that Amazon uses to stress Sidewalk's multi-layered encryption *(a, d)*, crowdsourced nature benefiting communities *(b, d)*, bandwidth constraints *(c)*, and use cases *(d)*. *a* and *c* reproduced from [190]; *b* and *d* reproduced from [35].**

# C Elaboration of information flows and PETs in Sidewalk

This appendix supplements the analysis of information flows and PETs in Sidewalk (§4). We first discuss privacy concerns of Echo and Ring devices irrespective of Sidewalk (§C.1). Next, we elaborate on Sidewalk's PETs (§C.2). This allows us to outline which privacy concerns they leave unaddressed (§C.3), and which telemetry information flows they do not prevent (§C.4).

## C.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 [206]. Ring and Echo users can monitor their environments, including family, neighbours, passers-by, and workers, that are generally unable to avoid this monitoring [149; 217; 232]. In fact, Amazon has rewarded citizens with discounts or free products when grouping up in Ring *"Digital Neighborhood Watches"* and reporting crime [129]. Nguyen and Zelickson [186] 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 [74].

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. 141; 149; 266]. 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 [237; 238]. Further, Amazon has a history of giving employees too liberate access to Ring users' videos and Echo voice recordings, without informing users thereof [70; 199]. In this context, we also point out Ring's history of cybersecurity issues [e.g. 120; 123; 185].

Third, Echo and Ring devices stimulate *law enforcement surveillance*, that Amazon actively pursues through extensive partnerships with police departments [e.g. 226]. Echo devices could aid police investigations [193] and US law enforcement set out to insert voice recordings of an Echo in a criminal court case in 2017 [142]. 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 [163]; for instance to have law enforcement hand out devices to citizens for free and to train officers in PR and handling press questions [128]. Amazon also persuaded municipalities to subsidise residents' purchases of Ring products [130]. 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 [163]. 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 [98]. 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. 121]. The sensitivity of these requests is illustrated by the Los Angeles police requesting Ring feeds capturing Black Lives Matters protests [122]. Meanwhile, numerous reports refute Ring's alleged contribution to combating crime [111; 120; 127].

## C.2 Elaboration of Sidewalk's PETs

This section briefly outlines how Sidewalk's two PETs work [20; 23; 40, 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"* [20, pp. 11-12], 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 used for routing packets cleared every 24 hours.

## C.3 Privacy concerns that Sidewalk raises or exacerbates

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

*C.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 [126]. 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 [75; 257]. 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 [148; 224]. Asset trackers more generally have been used for stalking and domestic abuse, that technical solutions proposed by their manufacturers fail to robustly tackle [131; 252]. In theory, *law enforcement* could also use Sidewalk trackers to track suspects; or, as Pace et al. [196] detail, recover a tracker's previous locations.

Relatedly, the information flows from endpoints to Amazon and manufacturers, and vice versa (Table 3) enable *customer surveillance.* For instance, Amazon can determine endpoints' and thus their users' locations [e.g. 95], as Amazon can see which gateways endpoints connect to [101]. According to Despres et al. [101], 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) [40, 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"* [20, 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"* [20, p. 6].

*C.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 [75; 257]. Amazon has not published details about how precisely it implements its security measures in Sidewalk, nor enabled independent reviews [75]. This pits Amazon as a single point of failure and increases the need for users to trust them, contrary to the rationale of PETs.

*C.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 [82]. 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 [136], scaling smart homes up to smart neighbourhoods [95] that Amazon mediates. Thus, Sidewalk is not a digital service confined to cyberspace, but invades public and private physical spaces [86].

*C.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. 75; 81; 116; 184; 198]. 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"* [72], 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 [75; 116; 184; 198].

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.

## C.4 Endpoint data and telemetry visibility for Amazon and manufacturers

Table 3 lists what endpoint data and telemetry is visible for Amazon and to manufacturers. None of this data is visible to gateway owners. Where applicable, Amazon specifies the metadata per connectivity type (e.g. specifying the number of connection attempts individually for BLE, FSK, and LoRa). Metadata about radio frequency broadcasting or signal strength pertains to endpoint-gateway connections. The table is based on Amazon documentation [20; 23; 40, pp. 33-40, 42, 49-55, 60, 175; 41] and interviews. Where the references were not specific or complete, we made assumptions (*"Presumably yes"*) or provide no judgment (*"Unknown"*).

**Table 3: Visibility of endpoint data and telemetry for Amazon and manufacturers.**

| Endpoint data | Visible to Amazon | Visible to manufacturer |
|---|---|---|
| ***Persistent device characteristics*** | | |
| Manufacturer | Yes | Yes |
| Serial number (generated by manufacturer) | Yes | Yes |
| Advertised Product ID (APID; generated by AWS for manufacturer) | Yes | Yes |
| Sidewalk Manufacturing Serial Number (hash of serial number, APID, and device serial number or (if absent) a universally unique identifier) | Yes | Yes |
| Sidewalk ID (might be the device's serial number) | Yes | Yes |
| Device profile (DeviceTypeId; created by manufacturer in AWS IoT Wireless to specify the device capabilities) | Yes | Yes |
| Qualification process identifier | Yes | Yes |
| Associated application server identifier | Yes | Yes |
| Supported connectivity protocols (BLE, FSK, LoRa) and parameters (e.g. preferred protocol, (a)synchronous) | Yes | Yes |
| Power source (battery- or line-powered) | Yes | Yes |
| Maximum transmit power per protocol | Yes | Yes |
| ***Variable metadata*** | | |
| Payload (e.g endpoint sensor data) | No | Yes |
| Transmission identifier (rotating hash of Sidewalk ID) | Yes | Yes |
| Unspecified *"auxiliary data (device and user-related)"* that the *"AWS IoT asset services"* provide to the application server [40, p. 42] | Presumably yes | Yes |
| Identifier of connected gateway | Yes | No |
| Location of connected gateway | Yes | No |
| Location of endpoint | Yes (through gateway location) | Yes (if manufacturer adds location tracking capability [e.g. 223]) |
| Battery level | Yes | Yes |
| Whether the endpoint is throttling down its traffic rate (can be adjusted by Amazon remotely) | Yes | Yes |
| Sidewalk SDK version and supported features | Yes | Yes |
| Signal strength | Yes | Yes |
| ***Variable telemetry that Amazon can make the endpoint (not) report to them*** | | |
| Periodicity of sending the below metrics to Amazon (by default once a day) | Yes (and can change this periodicity) | Unknown |
| Number and frequency of uplink and downlink messages | Yes | Yes |
| Average size of uplink and downlink messages | Yes | Presumably yes |
| Number of (un)successful connections | Yes | Unknown |
| Minimum and maximum time taken for a successful connection | Yes | Unknown |
| Number and type of communication failures | Yes | Unknown |
| Round trip time for messages | Yes | Yes |
| Number of duplicated and retried messages | Yes | Yes |
| Number of decryption and authentication errors | Yes | Unknown |
| Minimum and maximum time for a successful connection | Yes | Unknown |
| Timeout configured for connecting using a certain protocol | Yes | Presumably yes |
| Number of (un)successful registrations | Yes | Unknown |
| Number of (un)successful key refreshes | Yes | Unknown |
| Number of frustration-free networking retry attempts | Yes | Unknown |
| Number of time sync requests performed and received | Yes | Unknown |
| Periodicity of time sync requests | Yes | Unknown |
| Difference between time as perceived by endpoint and Sidewalk Network Server | Yes | Unknown |
| Number of (un)successful Sidewalk Bulk Data Transfer file transfers | Yes | Yes |
| Whether the endpoint has sufficient memory, storage, and battery to install a Sidewalk Bulk Data Transfer-issued update | Yes | Yes |
| Which of these Amazon-sanctioned metrics the endpoint is currently reporting to Amazon | Yes (and can change which) | Unknown |