Privacy: the more, the merrier?

A case study of how Amazon uses privacy protection to expand its power over IoT manufacturers

by

Thijmen van Gend

4919203

Master thesis

MSc Complex Systems Engineering and Management

Faculty of Technology, Policy, and Management

March 27, 2024

First advisor	D.J. (Donald) Bertulfo
Second advisor	Dr. F.S. (Seda) Gürses
First supervisor	Prof.dr. M.J.G. (Michel) van Eeten
Second supervisor	Prof.dr.ir. G.A. (Mark) de Reuver

TU Delft

Executive summary

Privacy-enhancing technologies (PETs) have historically been used for safeguarding individual privacy from both public and private interference. But lately, tech companies have started using PETs as one instrument for the expansion of their power over different actors. They do so by implementing PETs in their computational infrastructures (CI; i.e. the loud and mobile devices as their accessories) (Programmable Infrastructures Project, n.d.) and crafting dependencies of other actors on this infrastructure, or by excluding competitors. The same process seems to be unfolding in the case of Amazon's Sidewalk service. Sidewalk is a United States (US)-only privacy-preserving crowdsourced service that promises connectivity to Internet of Things (IoT) devices manufactured by third parties in smart-home, logistics, and utilities use-cases. Compatible IoT devices ('endpoints') are granted connectivity by 'gateways', namely smart-home devices from Amazon's Echo (smart speakers) and Ring (smart cameras and doorbells) series that donate a portion of their bandwidth to endpoints that might be owned by others. Amazon pushed a software update to these Echo and Ring devices, that turned them from smart-home devices to contributors to the Sidewalk network, unless users actively opted out, yielding a coverage of at least 90% of the US population.

With Sidewalk, Amazon leverages PETs (namely end-to-end encryption and device identifier obfuscation) to mitigate privacy concerns that the crowdsourced architecture yields. However, their governance of the service necessitates significant investments from third-party manufacturers to make their devices Sidewalk-compatible, suggesting a power emergence shaped by PETs. This case came into view in the context of the IDAIR project (funded by Fondation Botnar) and was then researched for the present Master thesis, building on ongoing research in the Programmable Infrastructures Project (funded by the TU Delft Technology Fellowship) (Programmable Infrastructures Project, n.d.).

There is little literature acknowledging the role PETs play in tech companies' power. To address this knowledge gap, I answered the research question *"How does Amazon's use of privacy-enhancing technologies in Sidewalk affect its power over IoT manufacturers?"* By comprising public and private actors with varying values, novel technologies, and a complex regulatory landscape, this Sidewalk case constitutes a complex socio-technical system that I set out to understand empirically using a single case study approach. I reviewed grey literature about Sidewalk (from tech watchers, adopters, and civil society), analysed the technology (e.g. the protocol specification and developer documentation), and engaged in elite interviewing with high-ranking employees of 8 IoT companies that have adopted Sidewalk and manufacture Sidewalk-compatible endpoints, and 1 company that provides IoT connectivity services.

My results show that Amazon leveraged PETs in Sidewalk to mitigate public security concerns raised by its crowdsourced and opt-out nature. Only in this fashion could they achieve its vast coverage and hence offer a valuable service to manufacturers and end-users. As a consequence, aspiring adopters must actively adjust their production process to make their products Sidewalk-compatible. This involves investing time, money, and skilled staff to *inter alia* arrange a complicated endpoint keying workflow to support the encryption; buying device components only from companies approved by Amazon; and complying with Amazon's governance processes, such as organisational audits, a mandatory qualification process, and obtaining their approval for the device's use-case. Meanwhile, Amazon cements AWS in the production processes of manufacturers: all Sidewalk data has to be en- or decrypted in AWS. Thus, manufacturers wishing to use servers outside AWS must resort to *"moving data around"*, incurring significant complexity, security risks, and costs. These barriers suggest that Sidewalk adoption is most feasible for large or well-funded IoT manufacturers, willing to engage with AWS.

These reconfigurations are expensive and complicated to realise, meaning that Amazon's promised benefit of Sidewalk being a cheap and ready-to-use connectivity protocol, do not hold in practice. Rather, manufacturers stressed the importance of leveraging Amazon's reputation vis-à-vis their suppliers and customers, as well as *"befriending the giant"* for they rely on Amazon for their Marketplace, cloud, and logistics. On top of that, the result of these reconfigurations is that manufacturers enter a path dependency, as both their devices' hardware constraints, and their limited organisational resources hamper adopting other protocols that are governed more openly than Sidewalk is. The fact that

manufacturers still adopt Sidewalk demonstrates the industry leverage that Amazon has. Amazon also uses this leverage to mobilise manufacturers' and silicon providers' resources to improve Sidewalk's public reception, technology, and governance. Interviewees shared that Amazon used adopters' stories to demonstrate Sidewalk's value and divert attention from privacy backlash; persuade silicon providers to teach them about hardware engineering and security; and invite companies to function as *"guinea pig"* for the development of the protocol, its security, and the qualification process.

Meanwhile, Amazon's reductionist framing of privacy and security as protecting user identity and data confidentiality, and the grey literature's focus on user privacy, means that confidentiality of manufacturers' business-sensitive information (i.e. how their endpoints work and how they manage them in AWS) is not discussed. With this vantage point, Amazon can learn which endpoint types are popular and how they work, informing their own hardware development. More saliently, they can use their vantage point to make AWS a more attractive production environment not only for Sidewalk adopters, but for any IoT company. While manufacturers' business models revolve for a large part around Sidewalk's existence, for Amazon it could be a mere (temporary) vehicle to attracting more IoT developers to AWS.

In sum, I have demonstrated that strictly pursuing user privacy (or confidentiality) in digital services may have unforeseen effects on production. PETs, in the Sidewalk case, gave rise to novel power emergences between Amazon, manufacturers, and silicon providers alike. Therefore, I call upon privacy and competition scholars, advocates, and regulators to question how privacy protection actually augments companies' power, and stepping away from their narrow *"consumer harm"* lenses. Even when arguing that gateway owners stand to lose little from being opted into Sidewalk by default, they are fundamental to Sidewalk's coverage, and hence to the value that Amazon creates for itself and other companies in the ecosystem. Still, gateway owners' autonomy is disregarded because the privacy guarantees minimise potential risks; meaning conversations about the fairness of distribution of gains are not held. Accordingly, these actors should debate a right to personal control over devices.

A mere consumer focus in studying these developments does not suffice: I established that business-to-business relations and businesses' production processes are more significantly affected than consumers. The production focus of this work lays bare the novel power dynamics between Amazon and manufacturers, shaped by PETs.

The case study could be replicated to investigate how Sidewalk grants Amazon power over silicon providers, and extended to crowdsourced finding networks by Apple and Google that seem similar in using PETs to reconfigure economic value creation. Finally, Sidewalk is part of a broader move by Amazon to expand their telecom and connectivity business intended to strengthen their position in the cloud market. Their Project Kuiper (intended to deliver satellite-based internet) and AWS Telco services could be interesting subjects for further research into Amazon's expansion of their CI.

Contents

List of Tables

List of Figures

Acronyms

[A1], [A2], ... [A8]	Interviewee whose company has adopted Sidewalk
API	Application Programming Interface
AWS	Amazon Web Services
B2B	Business-to-Business and Business-to-Government
B2C	Business-to-Consumer
BLE	BLE
BR	Boundary Resource
CDN	Content Distribution Network
CI	Computational Infrastructure
DCT	Digital Contact Tracing
EU	European Union
FFS	Frustration Free Setup
FSK	Frequency-Shift Keying
GAEN	Google Apple Exposure Notification Framework
GDPR	General Data Protection Regulation
HSM	Hardware Security Module
IoT	Internet of Things
IP	Internet Protocol
ISP	Internet Service Provider
LPWAN	Low-Power Wide-Area Network
[N1]	Interviewee whose company has not adopted Sidewalk
OS	Operating System
PET	Privacy-Enhancing Technology
PHY	Physical layer
RF	Radio Frequency
RTOS	Real-Time Operating System
SDK	Software Development Kit
US	United States
WMN	Wireless Mesh Network

Image references

This thesis reproduces several images by other authors. For the sake of readability, the chapters only include a brief attribution, with full attribution below.

- Figure 4.1: Reproduced from Amazon Sidewalk Privacy and Security Whitepaper, by Amazon, *Amazon Sidewalk Privacy and Security Whitepaper*, by Amazon, 2023n (p. 3) (https://m.media-amazon.com/images/G/01/sidewalk/final_privacy_security_whitepaper.pdf. © Amazon.
- Figure 4.2: Ring image reproduced from *Ring Video Doorbell van Amazon*, by Ring, n.d.-e, Ring Netherlands (https://nl-nl.ring.com/products/video-doorbell-pro-2). © Ring.
- Figure 4.2: Echo image reproduced from *Amazon Devices: Echo Smart Speakers & Displays*, by Amazon, n.d.-a, Amazon India (https://www.amazon.in/amazon-echo/b?ie=UTF8&node=14156834031). © Amazon India.
- Figure 4.4: Reproduced from *Amazon Sidewalk Bridge Pro offers professional-grade connectivity*, by Amazon, 2022a, About Amazon (https://www.aboutamazon.com/news/devices/amazon-sidewalk-bridge-pro-offers-professional-grade-connectivity). © Amazon.
- Figure 4.5: Reproduced from *Thread Smart Home Fact Sheet*, by Thread Group, n.d.-b (p. 2), Thread (https://portal.threadgroup.org/DesktopModules/Inventures_Document/FileDownload.aspx?ContentID=834). © Thread Group.
- Figure 5.1, **a** and **c**: Reproduced from *Everything you need to know about Amazon Sidewalk, the secure, low-cost network that can connect devices up to half a mile away*, by O'Neill, 2023, About Amazon (https://www.aboutamazon.com/news/devices/everything-you-need-to-know-about-amazon-sidewalk). © Amazon
- Figure 5.1, **b** and **d**: Reproduced from *Amazon Sidewalk*, by Amazon, n.d.-b, Amazon (https://www.amazon.com/Amazon-Sidewalk/b?ie=UTF8&node=21328123011). © Amazon.
- Figure 6.2: Reproduced from *Amazon Sidewalk Privacy and Security Whitepaper*, by Amazon, 2023n (p. 7) (https://m.media-amazon.com/images/G/01/sidewalk/final_privacy_security_whitepaper.pdf). © Amazon.
- Figure 8.2: Separate images reproduced from *YubiHSM 2 v2.3.2*, by Yubico, n.d., Yubico (https://www.yubico.com/product/yubihsm-2/). © Yubico.
- Figure 8.1: Reproduced from *Aria*, by Deviceroy, n.d., Deviceroy (https://deviceroy.com/aria/). © Amazon.
- Figure 8.3: Reproduced from *Manage a Connected AWS IoT Device Fleet*, by Amazon Web Services, n.d.-e (https://catalog.workshops.aws/aws-iot-device-fleet-management/en-US/setup-fleet-metrics). © Amazon Web Services.
- Figure B.1: Reproduced from *What are LoRa® and LoRaWAN®?*, by Semtech, n.d.-i (https://lora-developers.semtech.com/documentation/tech-papers-and-guides/lora-and-lorawan/). ©Semtech.
- Figure B.2: Reproduced from *Amazon Sidewalk Privacy and Security Whitepaper*, by Amazon, 2023n (p. 9) (https://m.media-amazon.com/images/G/01/sidewalk/final_privacy_security_whitepaper.pdf). © Amazon.

1

Introduction

Privacy-enhancing technologies (PETs) have historically been used to protect individual privacy by contributing to the principles of data minimisation and purpose limitation (Gürses et al., 2015). For instance, PETs such as encryption and purpose-based access control limit what third parties can learn about users of a digital service, and what the collected data can be used for, thereby protecting users from public and private powers such as surveillance and profiling (Diaz & Gürses, 2012).

Ironically, despite these laudable ambitions, examples have unfolded wherein PETs played a role in large tech companies exercising power over various actors. For example, during the covid-19 pandemic, Google and Apple cemented themselves as arbiters of privacy, smartphone device performance, and public health, at the expense of public decision-makers (Troncoso et al., 2022). They achieved this by implementing the privacy-preserving Google Apple Exposure Notification (GAEN) framework at the operating system (OS) level of their smartphones, and only letting governments use a restrained API exposed by the framework in digital contact tracing applications that the governments built themselves (Google, n.d.-a). In other examples, Google and Apple significantly hamper third-party advertisers' abilities to offer personalised advertisements, while themselves retaining the ability to do so, by implementing certain PETs. Apple's *"App Tracking Transparency"* limits third-party cross-app tracking on iPhones, dealing a large blow to the business models of online advertisers including Meta (Conger & Chen, 2022; Veale, 2023a). Google's *"Privacy Sandbox"* achieves something similar by implementing PETs in their browser and smartphone OS so that Google can still serve personalised ads, while blocking conventional user tracking methods, such as cross-website tracking cookies (Google, n.d.-b; McGuigan et al., 2023; Veale, 2023a).

Common to these cases is that the large tech companies control a *"computational infrastructure"* (CI) wherein they can implement the PETs, that enables these power expansions. I borrow this term from the Programmable Infrastructures Project that this research is a part of. The group defines CI as the combination of the cloud and mobile devices (e.g. IoT devices, smartphones, and laptops) as their accessories (Programmable Infrastructures Project, n.d.). The working thesis of this project is that current-day CI are concentrated in the hands of a few large tech companies, who strive to make them the default environment for software production. Software production, then, refers to creating economic value through the engineering of software-based services. In the aforementioned cases, this manifests for Apple as control over the OS of their smartphones; and for Google as control over the OS of smartphones and over their Chrome browser.

A unique case of power emerging as result of a company's vast CI, where PETs are a fundamental enabler, is Amazon Sidewalk. Sidewalk is a United States-only privacy-preserving service that promises connectivity to Internet of Things (IoT) devices in smart-home, logistics, and utilities use-cases. Compatible IoT devices ('endpoints') are granted connectivity by 'gateways', namely smart-home devices from Amazon's Echo (smart speakers) and Ring (smart cameras and doorbells) series that donate a portion of their own bandwidth to endpoints (Amazon, n.d.-b). Amazon thus turned Echo and Ring devices already in peoples' homes into gateways, with a remote software update in 2021, only giving gateway owners a 7-day notice over email that they would have to actively opt out if they did not wish to contribute to Sidewalk (Vaas, 2021). The service now has coverage of over 90% of the United States

population (Amazon, 2023o; Bishop & Hamren, 2024). Endpoints can connect to gateways owned by others, making Sidewalk a *"crowdsourced"* network (Amazon, 2023n). The CI, here, is the combination of Amazon Web Services (AWS) and the Echo and Ring devices.

Public backlash followed the Sidewalk roll-out. Much grey literature expressed concerns about privacy and security for endpoint and gateway owners, taking issue with the opt-out scheme, crowdsourced architecture, and that all data is routed through Amazon's infrastructure (e.g. Callas, 2021; Chase, 2021; Crist, 2021; Despres et al., 2022; Goodin, 2021; Vaas, 2021). After all, the IoT revolves around providing people with information about and control over their surroundings with sensors and actuators (Sethi & Sarangi, 2017), necessitating data protection measures (Kumar et al., 2019; Sahmim & Gharsellaoui, 2017). Indeed, Amazon seeks to alleviate these concerns using PETs – primarily encryption and identifier obfuscation techniques – and publishing about these measures in their Sidewalk Privacy and Security Whitepaper (Amazon, 2023n). As it turns out, though, most Sidewalk-adopting companies cater predominantly to businesses and public service organisations (further referred to as 'business-to-business' or B2B), in addition to or instead of targeting consumers ('business-to-consumer' or B2C). The use cases, including the privacy concerns, differ between these contexts, whereas most literature is concerned with B2C applications of Sidewalk.

Third-party IoT manufacturers that want to make their IoT devices Sidewalk-compatible, must comply with a multitude of technical and contractual requirements that Amazon imposes to accommodate these PETs. As the thesis demonstrates, examples include that manufacturers must buy chips from certain silicon providers, work with Amazon to be able to embed encryption keys in endpoints during manufacturing, and route all data to and from Sidewalk endpoints through AWS. As such, Amazon's use of PETs enables them to latch these third-party devices onto their CI, in the meantime impacting the production processes of these third-party IoT manufacturers. In addition, with all Sidewalk data and operating logic (i.e. the processes that manufacturers configure to manage and control their Sidewalk devices within AWS) passing through Amazon's infrastructure, manufacturers might inform Amazon how they can improve their own IoT hardware and make AWS an as attractive environment for IoT services as possible. Thus, in the Sidewalk case, intricate power dynamics emerge.

However, academic literature to understand the contribution of PETs to the expansion of Amazon's CI and their power over IoT manufacturers' production processes lacks. Current literature about Sidewalk is predominantly concerned with user privacy and security. Further, while there is other academic literature about tech companies expanding their power over other actors in reconfigurations of their CI that included implementing PETs (documenting the aforementioned GAEN and online advertising cases), the Sidewalk case goes further by constituting both a reconfiguration and expansion of CI. The power dynamics are therefore different.

More broadly, scholars have written about how control over technologies can be a source of power for large tech companies, including in the context of platform ecosystems. For instance, authors have argued that Google and Apple use their technical control to *"gatekeep"* how citizens use their smartphones and interact with app developers and advertisers, by designing application programming interfaces (APIs) and software development kits (SDKs), and enacting rules that they must adhere to (van Hoboken & Fathaigh, 2021; Veale, 2022). This rule-setting makes Google and Apple *de facto* privacy regulators (van Hoboken & Fathaigh, 2021) and lets them reshape app developers' revenue models (Fahy et al., 2018). Much of this literature considers how boundary resources should be aligned to spur innovation, whereas I am interested more in societal consequences of power. Literature that takes this angle exists, but usually do not consider privacy, or interpret it merely as a matter of who has access to which user data. Moreover, this literature tends to flatten power dynamics between platform providers and third-party businesses by designating the latter as *"complementors"*; a black-boxing that I attempt to undo in this work. Finally, this body of work does not scrutinise the effect that technologies have on the (software) production processes of organisations that adopt the services at hand parties (i.e. governments performing digital contact tracing, and advertising companies serving digital advertisements), usually taking the existing boundary resources for granted or only assessing their expansion, rather than studying how they have come to be. As such, the dynamics of knowledge, hardware, software, and strategic partnerships are not wholly in view.

Hence, in this thesis, I answer the research question *"How does Amazon's use of privacy-enhancing technologies in Sidewalk affect its power over IoT manufacturers?"* To do so, I ask three subquestions, argued for in Chapter 2:

1. What is Amazon Sidewalk?
2. What role do privacy-enhancing technologies play in Sidewalk?
3. How does Amazon's technical design and governance of Sidewalk affect the production of IoT devices?

In the research, I take a qualitative case study approach that synthesises business, social, and technical perspectives, and combines various methods. I review academic literature to explore the notion of privacy and PETs, and examine what others have written about PETs being used for power expansion. Moreover, I study grey literature to assess the public reception of Sidewalk and understand how IoT manufacturers that have adopted Sidewalk are using it. Further, I research actual technology of Sidewalk by scrutinising developer documentation and the protocol specification. Moreover, I prepared a network analysis of a Sidewalk endpoint and gateway in collaboration with a colleague in the IMDEA Networks Institute. This analysis is not completed yet, but nonetheless granted insight into how Sidewalk works. These studies make clear what requirements Amazon imposes on Sidewalk adopters, by means of technology and contracts. Finally, I interview 8 employees of IoT companies that have adopted Sidewalk, as well as 1 employee of an IoT connectivity service provider. These interviews give a grasp of manufacturers' path to adopting Sidewalk, how the adoption influences their production and business, and how they think Amazon can use their vantage point to further expand AWS as production environment for IoT. The thesis contributes a detailed account of one case wherein a large tech company uses PETs to expand its power, explaining to policy makers, scholars, and privacy activists that a rigid focus on 'protecting privacy' in digital products and services has intricate adverse implications.

I structured the thesis in a way that tells a narrative, devoting two chapters to each subquestion. To situate the case and argue for the scientific contribution, I start by presenting related literature and the research question that the thesis addresses (Chapter 2). Next, I argue for the case study research approach and methods used to answer the subquestions (Chapter 3). The case study results follow. Starting with questions about what Sidewalk is (Chapter 4) and how it is used (Chapter 5), I detail how privacy and PETs come into the picture (Chapter 6). Next, I elaborate the myriad effects that Sidewalk's PETs and governance have on the production of aspiring adopters (Chapter 8), and how these generate long-lasting and self-reinforcing dependencies between manufacturers and Amazon (Chapter 9). Finally, I conclude the thesis by describing the scientific and practical contributions, as well as limitations and suggestions for further research (Chapter 10).

2

Related literature

The introduction suggested ways in which Amazon exercises power over IoT manufacturers that adopt Sidewalk, and instrumentalises PETs to both enable and justify these moves. In this chapter, I look at what existing literature says about how the way businesses deploy digital technologies can grant them greater power. First, in §2.1 I explore literature about how technologies can grant their providers power. Next, in §2.2 I examine literature on power specifically in the context of privacy and privacy by design, and power. This section highlights ways wherein PETs are expected to curtail the power of companies over end-users, as alluded to in Chapter 1. After, §2.3 gives an overview of recent literature arguing that large tech companies can also use PETs to achieve the opposite, namely an expansion of their power. The final part of that section argues why Sidewalk is unique compared to other cases in the literature that demonstrate the use of privacy to increase the power of providers. §2.4 then provides the main research question to address this knowledge gap and contribute to the referenced literature.

Note that I provide examples of different types of power in technology contexts, but refrain from adopting a particular definition of *"power"*. For instance, I discuss instances of dependencies, control, and infrastructural power. My approach does not start with defining concepts from a single theoretical framework to investigate how a predefined notion of power appears within Sidewalk. Rather, I depart from an empirical case that allows me to study a new phenomenon (i.e. Sidewalk) and use that specific phenomenon to understand how new forms of power emerge from the entanglement of privacy and production, in the specific Sidewalk context. Therefore, I adopt a *"no theory first"* case study approach (Ridder, 2017, p. 286), that Chapter 3 expounds on. This allows me to stay close to the empirical results and acknowledge the myriad manifestations of power in the case, without losing out of view forms of power that might otherwise fall outside the scope of an*ex ante* adopted interpretation. This is especially valuable given the nascence of literature about PETs entrenching providers' power (§2.3).

2.1. Technologies as a source of power

In the Sidewalk case, a specific kind of technologies, namely PETs, seemingly play a role in the emergence of power over manufacturers of IoT devices. I begin by examining literature that studies the design and organisation of technologies as a source of power. For this, I describe what boundary resources are and how they can yield power (§2.1.1). While making a sharp cut between fields is hard and not my ambition, information systems literature (§2.1.2) and legal, media, and tech policy studies (§2.1.3) relate these concepts to power in different ways. Finally, I elicit takeaways from this literature and differences with Sidewalk case remain (§2.1.4).

2.1.1. Power through boundary resources

A number of works tie power of large tech companies to their control over *"boundary resources"* (BRs), which include APIs, SDKs, and app stores (Eaton et al., 2015; Ghazawneh & Henfridsson, 2013); see for an exhaustive list with more examples page 5 of Petrik and Herzwurm (2020). These tools enable third parties to develop apps and services complementary to a platform, by exposing certain functions and data of the platform in a piece of software that this third-party software can leverage, under certain conditions (Eaton et al., 2015; Tiwana, 2014; van der Vlist et al., 2022). Platform providers enjoy a great

amount of power by being able to set technical standards (e.g. what an SDK, API, or app can(not) do), define contractual standards (e.g. terms of service governing an API or rules relating to commissions that Apple charges mobile app developers), and enforce their rules (e.g. removing apps from app stores or revoking developer accounts) (van Hoboken & Fathaigh, 2021).

An evolution of this literature looks at power and dependencies in platform *ecosystems*. Van Dijck et al. (2019) posit that power should not be considered at the level of individual services (e.g. Amazon's Marketplace and AWS), but across the entire *"platform ecosystem"* of all services that the large tech company at hand operates, as they jointly contribute to and are a space to wield power. Likewise, Hein et al. (2019) argue for an ecosystem perspective that adds *"inter-organizational economic, business, and social perspectives on ecosystems"* (p. 89) to the social and technical paradigms of BR literature.

In short, this literature provides pointers as to how power manifests in technical systems: control over technical resources manifests in both the enforcement of rules, standards, and contracts, and in the ability to gatekeep access to data and services. These forms of power emerge across entire ecosystems.

2.1.2. Information Systems literature

Information systems literature generally assesses how BRs stifle or spur innovation and economic value for ecosystem providers, complementors, and end-users. For one, Eaton et al. (2015) study a diverse group of 30 BRs of Apple's *"iOS service system"* (p. 217), ranging from its App Store, to rules governing code execution and the use of specific iPhone hardware components. They notice Apple exercising power over a variety of actors (including third-party app developers and other large tech companies) through technical, financial, and policy measures affecting their BRs. In some cases, this was a competitive move, e.g. so that Apple would remain the single party offering some service. The focus and findings of Ghazawneh and Henfridsson (2013) are similar. Over time, third-parties' asset-specific investment into and accumulated ecosystem understanding of these BRs create a path dependency and hence lock-in (Cutolo & Kenney, 2021). Additionally, Rodon Modol and Eaton (2021) discuss a case of how a digital healthcare infrastructure provider collapsed formerly stand-alone services into their own architecture because other parts of this architecture had started to rely on it. As a result, third parties that could once integrate these services as stand-alone components into their own environment, are now funnelled to adopt the provider's entire architecture. They call such a component *"generatively entrenched"* (p. 346), defining it after Wimsatt (2007, p. 133-134) as *"one that has many other things depending on it because it has played a role in generating them"* (p. 346). However, the authors do not explicate what power this control grants the provider, nor over whom.

Hein et al. (2019) tie power only to the ownership of the platform, distinguishing between single-owner, consortia, and peer-to-peer community ownership models. Further, Cutolo and Kenney (2021) use the term *"platform-dependent entrepreneurs"* for businesses providing services through a platform ecosystem (p. 584). Borrowing from power-dependence theory, they trace power back to the platform owner's control over resources that the entrepreneur needs, and a potential lack of alternative sources thereof. Because entrepreneurs wish to retain access to the platform user base, they subject themselves to the platform owner unilaterally changing platform conditions, using their view into complementors' use of the platform to offer competing services, and self-preferencing. As such, control over the infrastructure lets tech companies grow into other existing markets and outcompete third-party sellers there, for instance when Amazon develops a new product line after seeing which products are in high demand (Cutolo & Kenney, 2021).

This ecosystem perspective also acknowledges that platform owners cannot unilaterally construct power. Hurni et al. (2021) point out the *"power paradox"* (p. 311), where the platform owner holds great power over users and complementary service providers, but simultaneously depends on the complementors to develop services for others to use within the ecosystem and hence spur its value, as the aforementioned BRs enable them to do. They furthermore devise a process model of how power is exercised and generated in platform ecosystems, identifying a the central power cycle (where complementors willingly subjugate themselves to the platform owner's power, because they expect the benefits to outweigh the drawbacks), the partnership accommodation cycle (where the platform owner grants more advantages or makes concessions to a complementor to keep them on-board when tensions arise), and the ecosystem redefinition cycle (where the competitive landscape of the ecosystem undergoes an unforeseen change, for instance due to new technologies, leading the platform owner to unilaterally reshape their *"ecosystem framework"* and the complementor to reconsider their partnership).

An assumption in this body of work is that the relations between platforms and software development are already in place. For instance, Ghazawneh and Henfridsson (2015) extend the definition of digital platforms by Tiwana et al. (2010) as *"software-based external platforms consisting of the extensible codebase of a software-based system that provides core functionality shared by the modules that interoperate with it and the interfaces through which they interoperate"* (p. 199). Similarly, de Reuver et al. (2018) speak of third parties recombining *"existing layered-modular resources"* that BRs such as OSes, hardware elements, SDKs, and APIs in add-on services that the provider of these BRs had not envisioned (p. 126).

This literature contributes further details about how businesses become dependent on platform providers and how they expose the BRs as entry points to an ecosystem. This view helps surface complex and seemingly paradoxical relationships among actors that all benefit from growing the ecosystem: in order to share in the created value, complementors need to subject themselves to governance mechanisms set by the owner of the technical system. Consequently, they become locked into the ecosystem on the long term, while running the risk that the platform provider enters their business to outcompete them.

2.1.3. Legal, media, and tech policy studies

Literature with a legal, media, and technology regulation angle on platform providers' power is primarily concerned with societal outcomes, public values, and how they should be regulated. Power imbalances are then not necessarily problematic for stifling economic value and innovation, but for contradicting the fact that we deem competition and a level playing field for businesses important as a society.

For instance, by studying the APIs of Facebook, Van der Vlist et al. (2022) conclude that *"the technicity of Facebook's API governance represents a major source of the platform's 'infrastructural power'"* (p. 1). Their argument is that because Facebook has the sole control over how their service technically works, they decide what functionalities and data third-party developers can access, and under which conditions (e.g. how often per hour and at what costs). Thus, while Facebook invites others to build on the BRs to create services that expand the platform ecosystem and its value to Facebook, its users, and these developers, there is a power asymmetry to the advantage of Facebook giving them disproportional power over *"the social and economic processes they sustain"* (p. 1). They also point out previous literature with similar findings in the context of digital platforms (Blanke & Pybus, 2020; Busch, 2021; Iyer & Getchell, 2018; Munn, 2020).

Further, Van der Vlist and Helmond (2021) examine how third parties shape the platform owner's power. They strengthen it by participating in the platform ecosystem and subjecting themselves to their governance mechanisms, but can also curb it by rallying in trade associations, developing open standards, or boycotting services of companies deemed too powerful.

Munn (2022) is not centred on BRs, but considers power specifically for combined cloud and edge architectures. He notes that the cloud resembles traditional power interpretations by virtue of being *"a centralized site, underpinned by formidable resources, where information is collected and processed, with the results being distributed throughout the cloud empire to individual subjects"* (p. 987). Referencing academic and industry reports, he predicts the cloud to be augmented by decentralised devices with fewer computational resources that sit closer to people and objects, and can hence sense or actuate them (i.e. the edge). Indeed, Sidewalk is also a cloud (AWS) and edge (endpoints) architecture. This augmentation, in his words, suggests that a power combining these two philosophies will take shape. He compares this model of a sophisticated, compute-rich 'cloud' combined with the less sophisticated but dispersed and low-level sensing 'edge' infrastructure, to Foucault's model of police power. In that model, a state agency connected to the heart of political sovereignty (i.e. the police; cf. the cloud) is supplemented by a pervasive decentralised network of officers monitoring and steering everyday activities and behaviour, however mundane those may be (cf. the edge). As such, the result of synthesising cloud and edge is *"a power formation that combines lightness and heaviness, drawing together the fortress and the frontier, the situated and the mobile, the resource-rich with the resource-poor"* (p. 988). This work captures exactly what is at stake if Amazon successfully pit themselves at the heart of this cloud-edge architecture. He does not consider the role of privacy, though.

Other works in this community do examine how tech companies submit privacy as reason to wield their control over BRs and constrain third party's access to data and services. For instance, Van der Vlist et al. (2022) write that while privacy justifies limiting third-party access to data or functionalities, Facebook can misappropriate this argument to hamper competition. Further, the control of Apple and Google over APIs and how software can be run on smartphones makes them *de facto*

privacy regulators (van Hoboken & Fathaigh, 2021) and lets them reshape app developers' revenue models (Fahy et al., 2018). As illustration, app developers and a US governmental antitrust committee accused Apple of blocking apps from their App Store that competed with their own functionalities, with Apple claiming to have done so in the name of privacy and security (van Hoboken & Fathaigh, 2021).

The scholarship referenced here clarifies that tech companies' power does not only affect economic value creation, but has other societal consequences, too. They become interpreters of privacy regulation, and at the same time use privacy as anticompetitive measure reducing consumer choice and undermining a level playing field. In addition, the cloud-edge architecture that Sidewalk constitutes, could vest Amazon with great disciplinary power.

2.1.4. Differences with Sidewalk

While validly describing how power can emerge through technologies, a number of factors set the Sidewalk case apart from the discussed literature. This means both that the concepts are insufficient to grasp the power dynamics at play, and that the case of Sidewalk can contribute to the literature. I make three contributions to this literature: namely with a unique consideration of where power emerges, taking a production perspective, and minding the specific role of privacy in enabling power.

Emergence of power

The information systems literature about platforms and BRs (§2.1.2) assumes the construct of a platform as pertinent to digital markets (de Reuver et al., 2018) and studies how to nurture such platforms to spur innovation and improve market conditions for platform providers and complementors (e.g. Cutolo & Kenney, 2021; Eaton et al., 2015; Hein et al., 2019). In other words, similar to this thesis, this literature engages platforms' influence on software development and its impact on certain types of economic activity. However, with the exception of a few (Eaton et al., 2015), the authors are not primarily concerned with the power imbalances that have come to accrue in them as a result of these practices, which has given rise to grave concerns about market, infrastructural and legal power concentrated in the hands of a few players.

While control of platform owners over complementors is a concern in this literature, it is seen as something that is pertinent to the generativity of a platform business and that can be optimized by redesigning BRs such as APIs and SDKs towards better economic outcomes (Eaton et al., 2015; Ghazawneh & Henfridsson, 2013; Petrik & Herzwurm, 2020). In contrast, I am interested in the power imbalances this control may bring about and how these impact parties beyond *"third-party developers"* or their development practices. For example, while most literature about BRs considers how they facilitate communication between software environments, I ask how manufacturing is reorganised to depend on Amazon as a cloud provider. As I will show, this hardware component yields Amazon a source of power, *inter alia* by requiring that endpoints use chips from selected silicon providers and have their devices qualified by Amazon. Further, as the authors I discuss in §2.2 do, I explore under what infrastructural conditions tech companies can deploy PETs and whether this benefits some players over others. These questions go beyond focusing on BRs, how they are used, or how they come to be (Eaton et al., 2015).

The focus of legal, media, and tech policy studies on BRs constituting power is closer aligned to my focus in this research, namely considering the regulatory and societal consequences thereof. However, both research communities discussing how business users of platforms are subjected to platform owners' power, classify these businesses as *"complementors"*. Accordingly, platform owners only attract them to the ecosystem if they offer services complementary to the platform that enhance its value proposition (Cutolo & Kenney, 2021; Hein et al., 2019). The main advantage for these complementors to offering services on the platform, is getting access to a vast established user base (Cutolo & Kenney, 2021). However, this assumption flattens differences between different types of third-party developers.

Applying this logic to Sidewalk would mean manufacturers launch Sidewalk-compatible endpoints so they can cater to the user base of Sidewalk users. But who, then, are these Sidewalk users? Sidewalk cannot be *"used"* as stand-alone service: it is always a part of using a compatible IoT device. Sidewalk's end-users (i.e. endpoint users) are not primarily interested in using Sidewalk itself and looking around for endpoints that enable them to do so, but rather in the functionalities of IoT devices that can be enhanced if they support Sidewalk. Third parties developing Sidewalk-compatible endpoints therefore do not add value to users of Sidewalk as these authors assume complementors to do. Therefore, the

power dynamics that authors point out between complementors and platform owners should not be expected to map precisely to Sidewalk; although the concerns about lock-in and platform owners' view into third-party use of the platform (e.g. Cutolo & Kenney, 2021; van Dijck et al., 2019) do hold.

Production view
In addition, platform literature lacks a comprehensive understanding of how tech companies influence the production processes of manufacturers. Simultaneously, platform literature mostly concerns how BRs facilitate communication between software environments. Conversely, being an IoT service, both hardware and software are integral to Sidewalk. Sidewalk revolves around connecting physical devices and the software running on them to a server of the manufacturer, through Amazon's own cloud (see §4.2.2 for more information). As the thesis will show, Amazon also obtains sources of power from the hardware component, *inter alia* by requiring prototypes to be 'qualified' by Amazon, and by mandating the use of chips by selected silicon providers. While the broader 'BRs' term does capture exclusive control of a platform owner over hardware, it still focuses on third parties wishing to create services for or utilise parts of hardware developed by another company (e.g. an iPhone). On the contrary, for Sidewalk, IoT manufacturers produce their IoT devices themselves, albeit having to adapt this process to accommodate Amazon's demands. In sum, how platforms affect the production by third parties and are themselves the product of production processes is not seen, meaning that the dynamics of people, software, hardware, partnerships, component purchasing, and technical infrastructure is remains unscrutinised for both actors.

The role of privacy in enabling power
Finally, when the BR literature addresses privacy, it is to consider how it can be best applied appropriate to modes of production in platforms with access to users and user data as angle (de Reuver et al., 2020), but not necessarily to study the unexpected consequences of them yielding more power to tech companies within their closed infrastructures. Chapter 1 highlighted the curious properties of PETs that could grant their providers power in a novel and different fashion than other technologies, necessitating consideration thereof. Sidewalk's promise to manufacturers is not providing access to users or data that Amazon has gathered about them in their infrastructure. Rather, it is about Amazon enabling a flow of data and control between endpoints and their manufacturers, with this flow passing through their infrastructure. Herein, privacy concerns include gateway owners' lack of control over their own devices, and that data passes through someone else's gateway, Amazon's Sidewalk Network Server, and AWS. This also has consequences for confidentiality of manufacturers' business-sensitive data, e.g. how their devices work and how they manage them in the cloud, as Cutolo and Kenney (2021) similarly warn for.

2.2. Privacy-Enhancing Technologies: The What and Why

Having seen how technologies may grant power to their provider, and the discrepancies between this literature and the present case, I explore specific research about power emergences in PETs in §2.3. Before I go there, we must understand what PETs are and do. Therefore, §2.2.1 explores multiple definitions of privacy. §2.2.2 then explains what PETs are and how they contribute to privacy. Next, §2.2.3 elaborates how developers can implement them in their services, and how PETs protect end-users both from surveillance and from an extractivist logic that repurposes users as co-developer. Finally, §2.2.4 examines why companies would want to implement PETs in their services.

2.2.1. Privacy: a broad notion

Many understandings of privacy exist. The wide notion spans at least *"freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations"* (Solove, 2008, p. 1). By shielding citizens from interference by both public and private actors, and hence enabling independent development of ideas, privacy is a fundamental underpinning of innovation and liberal democratic societies (Cohen, 2013). Simultaneously, disclosing personal information can create value, for instance to accelerate research or to offer personalised services (Acquisti et al., 2016). Consequently, how people perceive privacy differs between contexts, depending on e.g. the place, time, and actors involved (Nissenbaum, 2004).

Besides the strong cultural nature of privacy, numerous regulations codify some form of a right to privacy. For instance, the right to respect for the private and family life is codified in the European Convention on Human Rights by the Council of Europe (article 8), the EU Charter of Fundamental Rights

(article 7), and the Dutch constitution (article 10). The EU ePrivacy Directive protects the confidentiality of private communication. The right to protection of personal data is laid down in article 8 of this Directive, and also in article 16 of the Treaty on the Functioning of the EU, and more broadly in the General Data Protection Regulation (GDPR).

Because of this variety of codifications, and the broadness of the notion of privacy, it is important to acknowledge that privacy and data protection cannot be equalled. Whereas the GDPR is often referred to as a 'privacy regulation', the word 'privacy' does not appear anywhere in the GDPR. According to (Mahieu, 2021), privacy is generally not concerned with sharing information more widely, opposed to data protection rights such as the right to access to personal data, that also help society scrutinise decision-making processes and countervail the power of the information processor.

2.2.2. PETs and their contribution to privacy

Knowing what the concept of privacy entails, enables us to study how privacy can be enhanced with technologies. Gürses et al. (2015) describe what PETs are and how they are implemented in products or services. PETs are understood as technologies (e.g. encryption) that fulfil a certain functionality (e.g. exchanging messages) while maintaining a certain form of privacy protection (e.g. confidentiality of communication for others than the people exchanging messages). The rationale is that PETs reduce risk (i.e. the impact and probability of a privacy breach) and need for trust (i.e. *"the need to rely on other entities to behave as expected with respect to sensitive data"*, p. 5). Strategies to achieve these goals are minimising how much data the system captures, discloses, and replicates; minimising data centralisation (to avoid single points of failure); minimising linkability of data; and limiting data retention.

But how do PETs embody the conceptualisations of privacy elicited in §2.2.1? Diaz and Gürses (2012) helpfully map the three privacy research paradigms that Gürses (2010) distinguishes to common PETs. First, *privacy as confidentiality* refers to concealing personal information from others, such as the general public, governments, or – as was the context for Warren and Brandeis (1890) when they defined privacy as *"the right to be let alone"* (p. 193) – journalists. These PETs may encrypt or hide communication (meta)data, or have a trusted authority share only certain verified attributes of a user to an inquirer. An example of the latter is that when a person buys alcohol, the trusted authority only needs to prove to an inquirer that the person is of legal age, without them needing to show their identity card.

Privacy as control goes further by including both the hiding of information and the ability to control what happens to it. Some well-known notions such as the concept of informational self-determination (Bundesverfassungsgericht, 1983) and Westin's definition of privacy as *"the right [...] to decide what information about himself should be communicated to others and under what circumstance"* (Westin, 1970) fall under this umbrella. Privacy settings, access control mechanisms, and auditing are types of privacy as control. It follows that the 'control' may be exercised both by the affected person, and an organisation processing their data.

Finally, *privacy as practice* covers the social dimension of privacy, rather than the more security-oriented privacy as confidentiality and privacy as control. In this paradigm, privacy is considered part of one's identity that is constantly renegotiated. The renegotiation happens by sharing select information and receiving feedback when interacting with other individuals. Technologies of this category help the person understand how information is processed and disclosed, so that they can make an informed decision. Examples are the *"Platform for Privacy Preferences protocol"* that allows website operators to inform users of data processing practices by supplying said information in a machine-readable format, and *"Privacy Mirrors"* informing people how a system and the organisation(s) using it processes their information (p. 4).

2.2.3. Implementing PETs in systems

How, then, do developers implement PETs in a concrete system? The first step in this process, Gürses et al. (2015) elaborate, is defining a *"reference system"*, i.e. a specification of what the system should do, what its goals are, and which privacy concerns exists for its stakeholders. Departing from this specification, engineers can incorporate technologies to alleviate the privacy concerns while attaining the system's functionalities and goals. The authors mention the following methods to achieve this, in descending order of the strength of their privacy guarantees: not sending data (e.g. processing data on a user's device and not sharing it with a central server); encrypting data that is shared; using privacy-preserving cryptography (e.g. zero-knowledge proofs); and obfuscating or anonymising data. A key principle that the authors emphasise for this exercise is identifying which data is absolutely

necessary for which purpose by which actor. Following this argument, I reason that PETs contribute not only to data minimisation, but also to purpose limitation and therefore function creep, as the data that is processed is tailored to their envisioned use. This happens, for instance, in purpose-based access control systems (Gürses et al., 2015)

However, as Kostova et al. (2020) note, this practice assumes that the service is developed in a monolith and waterfall way, i.e. in a linear process wherein developers first assess the requirements that the system must fulfil, and then build the entire system with little iteration once the final version is completed. According to these authors, this is no longer accurate for most of today's digital services, given the rise of agile and modularity principles.

Gürses and van Hoboken (2018) refer to this change as the *"agile turn"* caused by three simultaneous developments. One is a change from waterfall to lean and agile development methods. The latter have short development and deployment timelines, and are centred around users, therefore also including refinement of services based on user feedback. Two is a move from *"shrink wrapped software"* (p. 582; i.e. software sold as monolith in sealed boxes), to service-oriented architectures (with software being composed of multiple loosely coupled services that can be tweaked through over-the-air updates post-installation). Three is a shift from personal computing to cloud computing, where powerful cloud servers compensate for users' devices becoming more mobile and therefore resource-limited.

As the authors reason, this agile turn has as consequence that traditional information privacy understandings and privacy engineering practices might not hold anymore. To illustrate this, they resort to the conceptualisation of privacy as capture, after Agre (1994). In short, this paradigm *"implies the development and imposition of 'grammars of action' – specifications of possible activities that are enabled by systems and can be mixed and matched by users – that, when put into use, can come to reconfigure everyday activities while subjecting them to commodification and economic incentives"* (p. 594). The authors point out that this model departs from automation and industrial management, rather than from surveillance. With this philosophy, service providers obtain power over users by being able to *"reorganize and optimize user activities"* (p. 595) for their own economic benefit.

Part and parcel of this agile turn, these authors continue, is that developers of modern services increasingly monitor user behaviour to inform development choices with. The underlying assumption is that user behaviour reflects user intent – a reasoning that the privacy paradox (i.e. user behaviour not aligning with their goals or desires around data privacy) demonstrates is flawed. One example the authors provide is A/B-testing, where users are put into different testing groups that receive a different service interface, so that the provider knows which interface is 'best received' or generates the most profit.

In this section, I thus established that the traditional methods of engineering and implementing PETs aim to achieve data minimisation (Gürses et al., 2015), and therefore purpose limitation constraining purpose creep. Thereafter, I demonstrated that digital service providers possess the power to continuously adapt their user activities (Gürses & van Hoboken, 2018), because the traditional conceptualisation of PET engineering does not hold for agile software development (Kostova et al., 2020). Kostova et al. (2020) mention that purpose limitation can curb the power of digital service providers that becomes visible under the privacy as capture paradigm. Gürses extends that argument in Gürses et al. (2024), to state that PETs protect end-users not only from surveillance by keeping their data confidential, but also from an extractive logic that instrumentalises them as a sort of implicit co-developers for the pursuit of revenue.

2.2.4. Why do companies adopt PETs?

If PETs curb the power and revenue generation model of companies, then why would they want to implement them in their services, besides perhaps considering protecting their users the 'right thing to do'? One popular stream of academic literature (and consequently, public and policy discourse) states that the business models of large tech companies, Amazon included, have for an important part relied on processing users' personal data. This personal data can be sold to other companies, and used to personalise services and advertisements (see e.g. Casadesus-Masanell & Hervas-Drane, 2015; G. Day & Stemler, 2019; Zuboff, 2023). According to this narrative, monopolistic access to user data has enabled the huge growth of these companies, with worldwide consequences for privacy, democracy, and economies (e.g. Fukuyama et al., 2021; Klinge et al., 2023; McIntosh, 2019). Against this backdrop, Amazon's adoption of PETs might seem counter-intuitive. After all, Amazon could configure Sidewalk

such that they could look into all data that endpoints and gateways generate to then personalise their services to their users and show personalised advertisements for products on their Marketplace. But apparently Amazon decided against this for the Sidewalk case. To explore why, this section discusses why tech companies would want to adopt PETs that prevent them from peeking into all sorts of data of their users, and how these reasons may apply to Sidewalk.

A first reason is a company's *public image*. The organisation might craft a reputation of protector of user rights to appeal to their users. As such, it can respond to past public backlash in trying to continue its current business activities but now in a more privacy-friendly way (e.g. Meta using PETs to continue their business model of delivering personalised ads), or enter into new markets with privacy-aware services and branding (e.g. the DuckDuckGo web browser that profiles itself as privacy-enhancing) (Steed & Acquisti, 2024). This is similar to how companies may move servers abroad to evade a certain state's jurisdiction (Woods, 2018). Cloud companies providing their European customers with data centres that are on paper owned by subsidiaries to cater to European data sovereignty concerns (e.g. Microsoft (Mukherjee, 2024) and Amazon (Sawers, 2023)) are a concrete example: these initiatives cater to European data sovereignty concerns and claim to reduce the US governments' control over and insight into data processed in clouds, and hence improve privacy (Baur, 2023); although they are in reality still subject to the US CLOUD Act, prescribing that US companies must provide data to US law enforcement in certain circumstances, regardless of whether that data physically resides (Baur, 2023; Blancato, 2023).

Sidewalk endpoint and gateway owners might be reassured to send their data over someone else's gateway, or lend their own device and bandwidth to unknown people, respectively, because of Sidewalk's security measures. The converse is also true: as §6.1 elaborates, significant public backlash resulted because gateway owners felt infringed upon their autonomy and privacy, regardless of whether their perception of how secure Sidewalk is (not) aligns with reality (as also noted by an interviewee; see §6.4.1).

Second, PETs can contribute to *regulatory compliance*, such as regarding data protection. PETS can offer data minimisation, anonymisation, pseudonymisation, and security of data processing, hence contributing to the data protection by design and by default obligations in various data protection regulations (e.g. GDPR article 25 (1)) (Srouji & Mechler, 2020). For instance, if a company refers to devices or users only with temporary identifiers that are rotated periodically, then the consequences of an adversary tracing this identifier back to a device or user is reduced because of its ephemeral nature. Again, this rationale enables both new privacy-friendly services, and improvement of current practices, for the same reasons listed above. Consequently, many data protection and cybersecurity authorities call for their adoption (e.g. European Union Agency for Cybersecurity, 2022; Information Commissioner's Office, 2023)

Sidewalk's PETs also contribute to these principles. As §6.3 elaborates, Amazon obfuscates Sidewalk device identifiers and encrypts device payloads so that Amazon cannot see what information comes to and from endpoints (Amazon, 2023o). This curbs the impact of traffic sniffing or of adversaries gaining access to Amazon's Sidewalk Network Server.

Third, PETs might help *evade certain regulations* (Veale, 2023b; Woods, 2018). For instance, if using a PET means that data cannot be traced back to a data subject, the data protection regulation may not apply thanks to the data no longer qualifying as personal (see the definition of 'personal data' in article 4 (1) of the GDPR). Likewise, PETs help service providers escape the liability to moderate content and grant data access to data subjects, law enforcement, intelligence agencies, researchers, and competitors, as prescribed by various regulations (Veale, 2023b), such as the EU's Data Act, Digital Markets Act, Digital Services Act, and GDPR; and the US Patriot Act).

In the Sidewalk context, Amazon might be trying to evade data protection regulation questions through the aforementioned PETs. If Amazon encrypts device payloads so that they cannot see what information comes to and from endpoints, and also cannot map rotated device identifiers to devices or users, the data may not be considered personal (Amazon, 2023o). This is a hypothetical analysis, though; a study of how Amazon does or does not comply with data protection frameworks in the US and elsewhere is not within the scope of this thesis.

A fourth very practical motivation is that adopting PETs could *enhance data management*, subsequently

increasing organisational efficiency or improving product quality. This advantage is described by Steed and Acquisti (2024), who performed interviews with technology companies, NGOs, and government organisations that use PETs for their analytics. One example is that adopting PETs puts data minimisation practices in the company back on the agenda and can thus free up organisational resources previously spent on processing unnecessary data. This narrative would then mitigate the argument that PET adoption requires much time and many resources. However, according to the researchers, this latter factor was never the single reason for companies in their sample to adopt PETs; it was merely an additional benefit.

This advantage is not likely to be of significant value to Sidewalk, because it has integrated PETs since its inception. Conversely, the description of Steed and Acquisti (2024) pertains to existing practices transformed by PET adoption.

Finally, *businesses might want to offer a service to others, or realise a service together with others, while the data of each involved party is hidden to the others*. One example is using *"operable technology"*, enabling two parties to perform a joint computation on their two separate datasets, despite using datasets that are themselves unintelligible because they are encrypted (European Union Agency for Cybersecurity, 2022, p. 9). An example hereof is multi-party computation; a PET that has proven to enhance joint computations on confidential data between businesses in the telecom (Ofe et al., 2022) and automotive (Agahari et al., 2022) sector.

The rationale of hiding business-sensitive data from competitors also extends to third parties doing business with Amazon. Amazon has abused business-sensitive data about third-party sellers and their products that is not available to other third-party sellers, to then replicate parts of their products under their own brands, and to decide at what price to sell them. Reports sprung up of this practice in the US (Mattioli, 2020), India (Kalra & Stecklow, 2021), and EU (European Commission, 2022). After an investigation by the European Commission, Amazon has been legally bound to not use this data to *"calibrate its retail decisions"* since December 2022 for 5 years (European Commission, 2022). This practice is now also prohibited under the EU's Digital Market Act (art. 6 (2)), following Amazon's designation as gatekeeper (European Commission, 2023). Similarly, Sidewalk manufacturers would benefit from Amazon not seeing how their devices work, because Amazon also sells IoT devices and could use this knowledge to better compete with the IoT companies. Note, though, that this is strictly seen a case of 'confidentiality' and not of privacy. Privacy per definition relates to natural persons, while this hypothesis concerns businesses.

2.3. Privacy-Enhancing Technologies as a source of power

We have now seen how PETs can constrain the power (§2.2) that tech companies have over users by virtue of controlling technologies (§2.1). However, Chapter 1 raised examples wherein large tech companies actually repurposed PETs to expand their control or power over other actors. Literature about how technologies in general grant power, do not map well to the present case of Sidewalk (§2.1.4), but literature specific about such repurposing of PETs might. This section explores these examples, namely in the case of the Google and Apple Exposure Notification Framework used for digital contact tracing during the Covid-19 pandemic (§2.3.1), PETs used by content delivery networks (§2.3.2), and PETs that allegedly make online advertising more privacy-enhancing (§2.3.3). The section concludes by elucidating the differences between these cases and Sidewalk (§2.3.4).

2.3.1. Digital Contact Tracing

A group of researchers that developed a protocol for digital contact tracing (DCT) during the Covid-19 pandemic experienced first-hand how Google and Apple crafted a powerful role for themselves in the domain of public health. A major subset of this group details their story in Troncoso et al. (2022).

Amidst the pandemic, momentum for deploying smartphone-based DCT systems arose. Automated contact tracing, using devices that many citizens of western European countries carry with them virtually all the time, was envisioned to augment manual contact tracing; the latter was known for being time-intensive and not being able to track down anonymous contacts, such as people encountered in public transport. A team of researchers united to design the Decentralized Privacy-Preserving Proximity Tracing (DP3T) protocol. The DP3T team picked up the challenge of building a DCT infrastructure, as privacy-preserving and purpose-limiting as possible; both for ethical reasons, and for buy-in and

legal compliance. This meant, for instance, preventing use of the infrastructure for surveillance and stigmatisation, as other forms of contact tracing already had led to.

In the DP3T protocol, smartphones devise random identifiers that change periodically and repeatedly broadcast one identifier at a time. The devices also log identifiers of other phones that are within range, as well as how strong the received signal is, as proxy for the distance to the other devices. Finally, each phone regularly contacts a central server to fetch identifiers that are marked as belonging to infectious people. The smartphone then compares these reported identifiers to the log of encountered identifiers, to determine if the user has been exposed to an infectious contact and should receive a warning notification.

Google and Apple took this design and implemented a slightly adjusted version of it in what they coined the *"Google and Apple Exposure Notification"* (GAEN) framework. They implemented this framework in their OSes; health authorities could then develop apps to do the actual contact tracing, invoking the GAEN API that would return a *"heavily constrained set of parameters"* (p. 53). Because the protocol relies on periodic broadcasting and sensing of Bluetooth identifiers, necessitating background functioning, this could not be achieved with conventional smartphone apps: the OSes prevent this for privacy and performance (e.g. battery consumption) reasons.

These tightly-held reigns over how the smartphones work, caused the researchers to experience a great reliance on Google and Apple. In their words, the fact that the companies constrained the parameters that the actual contact tracing apps could obtain *"strongly limited the design choices of app developers in making tradeoffs among privacy, security, and epidemiological utility of the applications"* (p. 53). One example is that the API would initially only expose highly summarised information, therefore hampering calculation of daily viral exposure accumulation and thereby the work of epidemiologists. This comes from the fact that Bluetooth signal strength is an approximation for distance to another device, that can become more reliable if there are more measurements. Thus, how often the device can measure the distance, affects the accuracy of estimating whether a nearby device counts as an actual contact. Another illustration the authors provide is that Apple and Google would decide when different OS versions (and thus device models) would support the framework, excluding users of older devices from using DCT until that time. The researchers conclude that they encountered *"many practical obstacles to privacy that have their roots in today's service-oriented software engineering practices"* (p. 56).

This example shows how Google and Apple claimed a spot at the decision-making table in the public health domain, leveraging the technical control they have over their smartphones. Privacy is relevant here not only for legal and ethical reasons, but also because the companies leveraged this as an argument to hide certain information from contact tracing apps. They leveraged their technical control to obtain power over governments and health authorities, making them as commercial company the arbiter between public health and other values, rather than delegating that decision-making power to scientific researchers or democratically elected bodies.

2.3.2. Content Delivery Networks

A second example of PETs constituting power comes from Sahib (2023), who studies the implementation of PETs by Content Delivery Networks (CDNs). Most importantly, he argues that *"the reliance on expensive infrastructure has the effect of making them deployable only by large tech companies. This has ramifications for the politics of access to privacy on the internet and a danger that smaller organisations acting in the public interest will not be able to afford to provide privacy for their users"* (p. 36). He builds the argument by describing that CDNs *"store"* content close to end-users (e.g. Netflix viewers) to reduce loading times. End-users' privacy can then be improved if users querying the CDN for content are not identified personally, but batched up and seen as just one of many visitors (granted that no other information of them is collected). The underlying assumption is that there is *"protection in the crowd"* (p. 39), meaning that the larger the crowd, the better the privacy of everyone involved. PETs with this assumption as fundament therefore only make sense for companies with sufficient users. Because greater user numbers require a greater infrastructure, using these PETs is only feasible for companies with big infrastructures that have large user numbers and can accommodate them with their infrastructure, such as CDNs and Google. In this case, it is not the design of PETs that is prohibitive for smaller companies, but the complexity and cost of running them, as well as the large user numbers required to render them effective. And to make good on this investment, services based on these PETs come with a hefty price tag, hindering their adoption by smaller clients with lower budgets.

While the concern of PET and privacy affordability for end-users and business customers is a legitimate one, this work does not recognise business customers of the PET-deploying company becoming more entangled in the ecosystem of the latter. In the context of his work, this could be Netflix becoming folded into the CDN company's infrastructure. Thus, this thesis is unique in studying how Amazon entrenches the use of AWS by manufacturers of Sidewalk-enabled endpoints. Another difference is that the CDN example is not crowdsourced, making the involvement of device owners different than in the Sidewalk case.

2.3.3. Digital advertising

A third example concerns making the digital advertising market more privacy-enhancing (allegedly), and comprises a range of initiatives from both Apple and Google. Google proposes multiple technologies in their 'Privacy Sandbox' project for both on the web (in their Chrome browser) and on smartphones (in their Android OS), that still enable personalised advertising but without conventional tracking technologies (Google, n.d.-b). McGuigan et al. (2023) refer to this process of obfuscating data flows while still being able to target individuals *"sanitizing surveillance"* (p. 9). In fact, part of this project is Google ending support for these conventional technologies (e.g. cross-website tracking cookies) in their web browser. In Google's words, Privacy Sandbox *"reduces cross-site and cross-app tracking while helping to keep online content and services free for all"* by blocking third-party cookies and replacing them with decentralised technologies that run on users' devices (Google, n.d.-b).

Apple has pulled off something similar. They implemented an *"App Tracking Transparency"* framework in their mobile OS that makes cross-app tracking on iPhones opt-in, which seriously hurt the revenue of Facebook-parent Meta (Conger & Chen, 2022), while Apple's advertising market share allegedly tripled (McGee, 2021).

Veale (2023a) writes about both of these projects. According to him, the idea is that devices no longer send lots of personal information to a server that can return a personalised ad, but instead run analytics on the device itself. This requires both complex computing and some control over the devices that users will see ads on. Therefore, such PETs are generally reserved to use by Apple and Google, as they have the resources to develop these complex computations and also control browsers, app stores, and smartphone OSes to run them on. In addition to rolling out their own privacy-preserving tools, these companies can block conventional tracking of others because they manage the environments wherein these mechanisms reside (e.g. browsers and OSes) – a phenomenon that McGuigan et al. (2023) calls *"sabotage"* (p. 10). Smaller online advertising companies without this expansive infrastructure are therefore outcompeted through confidentiality. Meanwhile, Veale (2023a) argues, user privacy might not actually be improved: *"Because this data is kept confidential, there is even a potential perverse outcome where companies try to use more sensitive data than before as part of their business models, arguing that it's fair game if not transmitted or centralised"* (p. 46). Such an interpretation of PETs interprets privacy only as confidentiality. The paper thus makes three arguments: first that parties with infrastructural control have a great advantage in rolling out PETs; second that they can do so in a way that lets them outcompete businesses dependent on this infrastructure; and third that enhancing confidentiality does not guarantee privacy, and can even undermine it. Moreover, he sketches that encryption is no longer used merely for protecting communications from state or corporate surveillance: *"This is a much more open design space, where businesses can design complex PETs to advantage them to the detriment of their competitors"* (p. 47). McGuigan et al. (2023) bring similar points.

2.3.4. Differences with Sidewalk

It follows from these cases that tech companies leverage PETs to expand their power over governments, companies, and citizens alike. However, the GAEN, CDN, and online advertising cases differ from Sidewalk in multiple ways. First, the CDN and advertising applications use PETs to mitigate a privacy problem in already existing and widespread practices. In contrast, the Sidewalk PETs solve a problem for a service that was not yet in use before its publication. Amazon conceived of Sidewalk as a crowdsourced network, and has since its inception included PETs to alleviate privacy concerns associated with including end-user devices in this network.

Second, all aforementioned cases are a reconfiguration of the companies' own CI. With this, I mean that Apple, Google, and CDN providers changed the way wherein devices that are controlled by themselves (regardless of whether they are owned by users, as phones and computers are) work to expand their power. This is also the case for Sidewalk, as it relies on an over-the-air update to gateways

in customers' houses to achieve its coverage (§4.3, §6.5.2). However, Sidewalk goes further by latching third-party devices onto their CI. As Chapter 9 elaborates, IoT manufacturers must implement specific hardware components in and 'key' their devices to support the Sidewalk PETs. After, manufacturers must necessarily use AWS to control their endpoints. Adopting Sidewalk is thus a matter of both hardware and software engineering, with hardware production and re-engineering being harder to scale. Therefore, Sidewalk has a greater effect on the way that Sidewalk customers (i.e. IoT manufacturers) produce their products and services, compared to the customers in the other cases (e.g. advertisers or content providers); although the effect on DCT is hard to measure, as GAEN was the first large-scale smartphone-based DCT infrastructure of its kind.

Third, in the advertising and GAEN cases, Google and Apple instrumentalise PETs to craft power over other actors that rely on their infrastructure. For GAEN, this is governments and public health authorities desiring DCT; in the advertising cases, these are online advertisers that want to serve ads to smartphone users. For DCT and online advertising, there are little feasible alternatives with such a high market penetration as the infrastructures of Google and Apple. Conversely, IoT manufacturers do not currently rely on Amazon's Echo and Ring devices to connect to their non-Sidewalk-enabled devices. Similarly, other IoT connectivity providers do not rely on Amazon's smart-home devices to provide third-party devices with connectivity, given the plethora of other low power wide area networking (LPWAN) technologies available (see §4.4). Amazon thus leverages its infrastructure to attract customers that, at face value, also have other feasible alternatives to choose from.

This cloud integration marks a fourth relevant distinction. IoT manufacturers adopting Sidewalk can choose to move their software production into Amazon's cloud. Thereby, adopting Sidewalk does not only change how devices work, but can influence the adopting company in more profound ways. Adopters can not only manage their devices from within AWS, but also choose to move other business logic to AWS (e.g. for general data storage and processing, or website hosting). Conversely, the GAEN, advertising, and CDN cases only pertain to one specific service: namely contact tracing, advertising, and content delivery, respectively.

Fifth, the examples in this section are mostly written about from a data perspective. For instance, McGuigan et al. (2023) conclude their paper about the online advertising case by stating that *"To make privacy meaningful, and forestall these self-interested moves by companies, policy measures have to tackle the structural harms at the root [...] ensuring that we don't face a race to the bottom as firms seek to leverage privacy rhetoric to their own gain"* (p. 11). Accordingly, they mention measures that can *"cut off firms' access to data"*, *"institute strong curbs on profiling activities"*, and prevent tech companies from *"expand[ing] their access to data flows"* (p. 11). Although such measures might prevent Amazon from peeking into adopters' business-sensitive data, such as how their endpoints work and how they use the cloud to manage the devices – a possibility not highlighted in the other three PETs-as-power stories – this will not suffice to curb Amazon's power. As reasoned, the potential concern is not in what personal data is accessible to whom; it is about Amazon reconfiguring the way that IoT manufacturers produce their devices.

Finally, the cases reflect a power position of large tech companies over different actors. The CDN case affects content providers that want to send large files to their users quickly (e.g. to stream a video). Their customer demographics will mostly consist of other businesses. The advertising cases, too, primarily affect businesses (namely other advertising service providers), and indirectly the customers of these ad providers, which could range from businesses to governments and NGOs. The GAEN case concerns power over governments and public health authorities, as use of the framework was reserved for public authorities wishing to set up DCT. For Sidewalk, the affected sector is less clear. It follows from §5.2 that most Sidewalk adopters are active in one of three domains: the smart-home, logistics and asset tracking, and utilities. While the former two spaces are occupied by businesses, utilities is a public sector. Thus, Amazon could obtain leverage over both businesses and public sector organisations with Sidewalk.

2.4. Research gap

This chapter discussed existing literature about how companies leverage digital technologies to grant them greater power. §2.1 brought in literature about how technologies can constitute a source of power. This brought into view how tech companies' roles of defining technology, contractual standards, and enforcement gives them a powerful position that eventually leads to locking third-party businesses into their environments. I established three gaps in this literature: namely a flattening of third-party businesses to *"complementors"*, obscuring power dynamics; a lack of considering the effect of power and

technology on production processes; and a lack of knowledge about how PETs enable power.

The literature widely acknowledges how tech companies utilise different elements of their CI to grow their ecosystems and constrain or enable third-parties' use thereof. Meanwhile, how 'platforms' come to be (e.g. what knowledge, hardware and software is required; how tech companies form strategic partnerships to obtain these resources and develop their services; how they market it to the public and on-board early adopters) is not often scrutinised. Similarly, how platforms affect the production by third parties and are themselves the product of production processes is not seen, meaning that the dynamics of people, software, hardware, partnerships, and technical infrastructure often go unmentioned. Following the hypothesis of the Programmable Infrastructures Project (Programmable Infrastructures Project, n.d.) that CI are environments for software production, I look at how manufacturers' production of IoT devices is (re)organised through their adoption and co-development of Sidewalk. As the results show, this brings into view another group of businesses, namely that of silicon providers, that likewise reconfigure their production to produce Sidewalk-compatible chips and as such co-produce Sidewalk. Considering these as two separate entities reveals their different roles in the Sidewalk ecosystem, with unique production processes, indicating that a generalisation to *"complementors"* is not appropriate for this case. I also look at the role of privacy, and its in interplay with boundary resources, but do not limit my view to studying SDKs and APIs, as detailed in Chapter 3.

These gaps are important to address, as it fosters an understanding of how privacy may not necessarily serve to limit the power of certain actors as we are used to (§2.2.1). Rather, and paradoxically, due to their infrastructural power, these parties can instrumentalize PETs to create a production environment that transforms production of devices and services, and therewith increase dependencies on their CI. This is demonstrated by the literature documenting examples of tech companies' PET-enabled power expansion in public health, CDNs, and online advertising. By focusing on specific actors, and changes to their production, I provide insight into how Amazon manages to not only repurpose but extend their CI, and therefore how this power manifests itself with and beyond BRs. By focusing on privacy, I demonstrate how infrastructural power could render protections afforded by design worthless, affecting competition, affordability of privacy, and public decision-making.

To address these literature gaps, I answer the following research question: *"How does Amazon's use of privacy-enhancing technologies in Sidewalk affect its power over IoT manufacturers?"* To do so first requires a more elaborate understanding of what Sidewalk is, beyond the differences of Sidewalk and priorly documented cases discussed here. This includes grasping the technologies powering Sidewalk and what convinces IoT companies to adopt the service. Special attention will be devoted to Amazon's utilisation of PETs, granted the largely unexplored dynamics that this class of technologies entails for power. The power over manufacturers can be assessed by studying their production of (non-)Sidewalk-compatible devices. Here, I interpret 'production' broadly as the ways wherein IoT companies shape how their devices work and are used, during phases of design, development, manufacturing, and post-manufacturing management and updating. Sidewalk's technologies as well as how Amazon governs the service impose requirements on device capabilities and production processes. Studying manufacturers' production can therefore reveal power dynamics, for instance if manufacturers are restricted in how their technical designs, limited in their procurement of device components, or dependent on Amazon for technical support and approving of Sidewalk products. Therefore, I ask three subquestions to answer the main research question:

1. What is Amazon Sidewalk?
2. What role do privacy-enhancing technologies play in Sidewalk?
3. How does Amazon's technical design and governance of Sidewalk affect the production of IoT devices?

3

Research approach and methods

In this chapter, I describe the approach and methods that I have taken to answer the research questions. I first discuss why a case study approach is suitable for the questions at hand, and what data is required for it, in §3.1. This section already shortly discusses the methods pursued. I then give a more thorough description of these methods in 3.2.

3.1. Approach and data requirements

The first step towards answering the research questions is choosing an approach. In §3.1.1, I reason why I have adopted a case study approach and what this entails. Next, I discuss the data that is required for the study and where this can be found, briefly mentioning the methods taken to obtain and process this data §3.1.2.

3.1.1. Case study research approach

While the research question is centred on Amazon's use of PETs to increase their power, they are not the only large tech company to do so (see §2.3). In Chapter 2 I found that there is scant literature on this development. To address this knowledge gap, I adopt an empirical approach that contributes an elaborate description of how this development plays out in practice. A case study approach is well-suited for this goal. Indeed, a case study is suitable for research into a contemporary phenomenon with a 'how' question, wherein the researcher has limited control over behavioural events (Yin, 2017). Second, it allows the researcher to rigorously study *"a unit of analysis as a bounded system (the case), over time, within its context"* (Harrison et al., 2017, p. 15). Third, a close coupling between the case study account and empirical evidence provide the research with testability, originality, and empirical validity, without having to rely on exhaustive past scholarship (Eisenhardt, 1989). More specifically, I adopt a *"no theory first"* approach to stay close to the case and unravel novel power dynamics, given the nascence of relevant literature I established in Chapter 2.

The case study will be explanatory, as answering the 'how'-question explains an empirical phenomenon (Yin, 2017); but also exploratory, as the goal is not providing conclusive answers to the problem, but posing new ideas to understand the underlying mechanisms in the absence of existing literature (Swedberg, 2020). The utility of case studies for this research is demonstrated by their extensive use in other literature about the exercise of infrastructural power in different, sometimes non-technological contexts (see, indicatively, Bakonyi, 2022; Lucas, 1998; Pinzur, 2021; Tavmen, 2020; Valdez, 2023).

A case study research design comprises five components (Yin, 2017). After articulating the question(s) to be answered (Chapter 1) comes formulating propositions, indicating the theoretical issue and where this could be investigated empirically. The research question fulfils this part by proposing a causal relationship between PETs and expansion of power. Third is selecting the case(s); a step not reported on here, because Chapter 1 already explains the case. Last are considering how to connect the findings and propositions (§3.1.2), and defining criteria for assessing the strength of the findings. It is important to conduct this final step before executing the case study, so that the data and methods can still be adjusted. Therefore, I explored methodological and data shortcomings, and subsequently iterated on the chosen data and methods. I discuss the mitigatory triangulation in §3.2.6 and the remaining limitations in §10.4.

Table 3.1: Overview of the data sources used to answer each subquestion, and how this data will be gathered and analysed

Subquestion	*Data gathering and analysis method for the listed data sources*				*Main chapters*
	Grey literature review	**Technology analysis**	**Elite interviewing and IoT conference**	**Semi-structured academic literature study**	
1. What is Amazon Sidewalk?	Articles by Amazon, manufacturers, and tech journalists	Developer documentation for AWS, Sidewalk, and similar connectivity technologies	Manufacturers' experiences	Scientific literature about similar connectivity technologies	4, 5
2. What role do privacy-enhancing technologies play in Sidewalk?	Articles by Amazon, civil society and tech journalists; legislation	Developer documentation for AWS and Sidewalk; APIs; SDKs; endpoint, gateway	Manufacturers' experiences	Scientific literature about privacy, PETs, and power in the IoT	6, 7
3. How does Amazon's technical design and governance of Sidewalk affect the production of IoT devices?	Sidewalk and AWS terms and conditions; manufacturers' blogs; Amazon's press releases	Developer documentation for AWS and Sidewalk; APIs; SDKs	Manufacturers' experiences	Scientific literature about power emergence in technology	8, 9

3.1.2. Data requirements and analysis

Looking ahead to the connection of case study propositions and findings (Yin, 2017) involves a discussion of required data and data analysis methods, techniques, and tools. The varied nature of the subquestions calls for diverse data types which, consequently, adds to the robustness of the case study by enabling triangulation (Yin, 2017). Table 3.1 lists each subquestion and, in the three or four adjacent cells, the types of data used to answer them. The four middle columns represent how the respective data types will be gathered and analysed (elaborated in §3.2), inspired by suggestions for exploratory and explanatory case study research from Yin (2017) and Swedberg (2020). The final column states in which chapters the question is answered. 'Manufacturers' refers to manufacturers of Sidewalk-compatible IoT devices, excluding Amazon, as I outline in §4.1.

For answering subquestion 1, I first investigate what the value of Sidewalk is to IoT manufacturers, gateway owners, and endpoint owners. This information is available in press releases and news articles from Amazon, IoT manufacturers, and tech journalists. Because these publications mostly serve marketing purposes, it is important to consult manufacturers themselves to assess which benefits are most important, and what other (dis)advantages exist that are not mentioned in these sources. Further, Sidewalk's value is partly defined by its technical capabilities and architecture. Understanding what sets Sidewalk apart from other low-power wide-area network (LPWAN) technologies necessitates a look into technical resources, developer documentation, and governance of both Sidewalk and other technologies. Here, I looked for sources from academia, IoT manufacturers, and standards bodies. To augment my understanding of both Sidewalk and these other technologies, I visited an IoT business conference in September 2023. Here, I listened in on presentations about contemporary developments and spoke to exhibitors about their devices, and how they connect and produce them.

For subquestion 2, I bring into view the privacy concerns that Sidewalk raises, and how Amazon addresses them using PETs. Reports about Sidewalk from civil society and tech journalists are the starting point. Further, Amazon has publications about how they themselves process data for Sidewalk. I added to these insights by examining developer documentation and APIs to see what data they expose to manufacturers. However, these materials might be biased and incomplete, as I reflect on in §3.2.6. Therefore, examining the operation of an actual endpoint and gateway to see what data they transmit and receive is helpful. In addition, I seek to gain insight into manufacturers' first-hand experience with their own and Amazon's processing of Sidewalk data, as well as their customers' perception of Sidewalk's privacy; this is not reported on in this grey literature.

To contextualise these findings, I furthermore include scientific literature about privacy concerns and PETs in digital services and the IoT more broadly, and briefly reflect on data protection legislation.

Subquestion 3 calls for information about how Amazon governs Sidewalk and integrates it with its cloud services. Scientific literature about power emergence in technology provided inspiration on where to look for this governance. I first consulted the Sidewalk terms of use (Amazon, 2023k) and qualification process (Amazon, 2023m). Examining Sidewalk technologies and documentation thereof is again relevant, by conveying how manufacturers must adjust their endpoints and software to accommodate Sidewalk adoption. Additionally, some governance measures may be implicit or otherwise not captured in these resources, necessitating insights into manufacturers' experiences in adopting Sidewalk. Second,

their experiences are valuable for learning how they produce their products and services, both those that do and do not use Sidewalk. There are close to zero publications from Sidewalk adopters about this topic, presumably because of the business-sensitive nature. This makes talking to manufacturers fundamental to the research.

3.2. Methods

In this section, I detail the different methods I adopted to analyse the data types and sources that I identified as necessary to answer the subquestions in §3.1.2. These are visiting an IoT conference (§3.2.1), reviewing grey literature (§3.2.2), performing a technology analysis (§3.2.3), studying academic literature (§3.2.4), and elite interviewing of IoT manufacturers (§3.2.5). Finally, I triangulated findings with these different methods (§3.2.6).

3.2.1. IoT conference: TechEx Europe 2023

Early in my research, I visited the *"IoT Tech Expo"* track of the TechEx Europe 2023 conference in September. Featuring approximately 175 exhibitors (TechEx, n.d.-b), it provided a rich and broad view into how businesses use IoT, what challenges they encounter, and what novel solutions exist (TechEx, n.d.-a). In preparation, I skimmed through a book by Høyer Leivestad and Nyqvist (2017), providing helpful networking and conduct advice.

Besides attending multiple presentations, I approached exhibitors in the business of long-range and low-resource IoT applications on the exposition floor. I inquired with them about who their customers are, which connectivity protocols and whose networks they use, how they process data (e.g. how much data does the device itself process 'on the edge', how much is sent to the company's own infrastructure or cloud, and which cloud provider they use), and what they thought Sidewalk could (not) mean for them.

3.2.2. Grey literature review

I performed a grey literature review largely with three objectives: to understand Sidewalk's benefits and how adopters use it; to elicit privacy and security concerns; and to assess how Amazon governs Sidewalk.

For the first goal, I set out to understand adopters' target audience, market domain (e.g. building management or logistics), and what the benefits of adopting Sidewalk are for them. I identified all third-party Sidewalk adopters mentioned in Amazon publications about Sidewalk up until the cut-off date of January 19th 2024. In addition, I performed a Google search for *"Amazon Sidewalk"* every two weeks between November 2023 and this cut-off date. By sorting results by date, lesser-known websites also came into view. This yielded blog posts, press releases, product listings, and annual reports, from actors such as Amazon, adopters, and tech journalists.

To elicit privacy and security concerns in the grey literature, I executed a Google search for *""Amazon Sidewalk" AND privacy"* in early November 2023. I excluded 63 of the 203 results for being affiliated to Amazon or their partners; not contributing an argument but merely quoting text from other websites; and not actually mentioning privacy concerns in connection to Sidewalk. The most relevant records were (technology) news websites. I distilled a list of privacy and security concerns to serve as the basis for the write-up in §6.1. For the sake of time, and because this study is not quantitative, I did not log which record mentioned which concern. I supplemented this literature with a Google Scholar search for *"Amazon Sidewalk"*, which yielded few useful results: most records only mention Sidewalk in passing.

Finally, Sidewalk policies are listed in the developer documentation (Amazon, 2023k, 2023m).

3.2.3. Technology analysis

To understand the capabilities of Sidewalk and the role of PETs herein, I first collected and archived all public technical documentation of Sidewalk. Examples include the Sidewalk homepage (Amazon, n.d.-b), Privacy and Security whitepaper (Amazon, 2023n), developer documentation for Sidewalk (Amazon, n.d.-c, n.d.-h, 2023i; Amazon Technologies, 2023a) and Sidewalk services in AWS (Amazon Web Services, n.d.-j), and the protocol specification (Amazon Technologies, 2024). To ensure that I found all relevant documentation, I used a subdomain finding tool for Amazon's *sidewalk.amazon* domain (C99, 2023). I furthermore searched the Internet Archive's n.d. Wayback Machine for older versions of the documentation to find out how Amazon has been changing Sidewalk. I also added all current

documentation to the archive, to enable future historical comparisons. I scrutinised these resources to elicit the requirements that manufacturers' production processes and endpoints must fulfil, what functionalities Amazon exposes to manufacturers, and how Amazon processes and secures Sidewalk data.

To mitigate the bias in and incompleteness of these Amazon-affiliated resources (§3.2.6), I initiated an experiment to measure network traffic going to and from a Sidewalk endpoint and gateway used in a real-world setting Because I am not trained to conduct such an analysis, I set up a collaboration with a PhD student I met during ISP 2023 working at the IMDEA Networks Institute in Spain. We prepared a network analysis experiment with a Sidewalk development kit (generally used for prototyping Sidewalk endpoint functionality), an endpoint, and a gateway. The collaborator could then sniff the data sent to and from these devices over Bluetooth and Wifi, enabling me to cross-examine these measurements with Amazon's description of their data processing practices, as well as how intertwined Sidewalk devices and AWS are. Regrettably, the measurements are not finished yet, due to differences in priorities, logistical barriers, and the development board being complicated to set up. In preparing the experiment, though, we multiple times discussed the Sidewalk developer documentation, fostering my understanding of how Sidewalk works technically and how it constrains manufacturers.

3.2.4. Semi-structured academic literature study

I studied academic literature for largely two purposes. First, to contrast Sidewalk with other LPWAN technologies, I looked for grey and scientific resources about other technologies, and their architecture and governance. I took directions for relevant technologies from interview results and grey literature mentioning protocols similar to Sidewalk.

Second, I studied literature privacy and PETs in the IoT, as well as how power can emerge herein. To this end, I performed a Google Scholar search using (variations of) the keywords 'privacy', 'privacy-enhancing technologies', 'BRs', 'platform ecosystems', and 'power', combined with forward snowballing and looking at author profiles. To gain a sense of the state-of-the-art in scholarly privacy circles, I attended the 5th Interdisciplinary Summerschool on Privacy (ISP 2023) (Hoepman, n.d.) and the Beyond Data Protection conference 2023 (INFO-LEG, 2023), too. This culminated in Chapter §2.

3.2.5. Elite interviewing

To learn how manufacturers experience their adoption of Sidewalk, I conducted elite interviews. Here, I argue for the merit of this technique, elaborate on the interviewee populations and recruitment, and explain how I executed and analysed the interviews.

Rationale

The breadth of the research questions that learning about manufacturers' experiences contributes to, led me to search interviewees that could tell me about their motivation to adopt Sidewalk, its effect on their production, Amazon's governance of Sidewalk, and the privacy and security of their service. In-depth knowledge of Sidewalk, similar technologies, and the company's production, are therefore essential. I presume C-level executives and department heads to uniquely possess comprehensive experience with all this business and technical experience.

To approach and interview such people, I adopted an elite interviewing approach. Informants are referred to as 'elite' based on possessing power, expertise, connections, and information that is unique both vis-à-vis their peers and the interviewer (Solarino & Aguinis, 2021; Undheim, 2003). Their elite nature imposes unique challenges for research design, data collection, and reporting results compared to non-elite interviews (Solarino & Aguinis, 2021; Undheim, 2003).

During arrangement of the interviews, I told prospective respondents about who I had already interviewed to build rapport, a practice that Latour (1987) refers to as claiming *"allies"* (p. 31) and Lofland and Lofland (1984) also recommend. Similarly, I informed interviewees what sector I investigate (*"novel long-range IoT technologies and the production of IoT devices"*), to entice them to provide their own perspective in addition to those of others in their field. This serves to tell interviewees how the interview benefits them or their organisations (Solarino & Aguinis, 2021; Undheim, 2003).

Interviewee populations

I recruited interviewees from two populations: IoT companies that have and have not adopted Sidewalk, with an emphasis on the first.

Population 1: Sidewalk-adopting companies Employees of the 16 identified Sidewalk-adopting companies (see §3.2.2) listed in Table B.1 constitute the first interviewee population. I initially contacted high-level executives and engineers involved in device connectivity or data processing; but soon widened the scope to other engineers and administrative departments, in hopes of them redirecting me to higher-ranking employees. I sent invitations over LinkedIn because it scales easily, email addresses were hard to come by, and it bypasses *"gatekeepers"* such as elites' secretaries (Solarino & Aguinis, 2021, p. 659). In total, I sent 94 Linkedin connection requests with a 300-character interview invitation, and 1 invitation to someone I connected following TechEx Europe 2023.

Taking a cut-off date of January 19th 2024, I received 23 responses (almost 25%), of which 8 people ultimately participated. Others stopped replying, considered themselves out of scope, or represented an organisation I already interviewed someone from.

After excluding people whose company I already conducted an interview with (to sustain a balance between the interviewed organisations), and people that stopped replying or considered themselves outside the scope of my research, I ultimately arranged 8 interviews from this batch. Of these participants, 4 hold a C-level position, 2 are department heads, and 2 are high-ranking engineers. I refer to these interviewees as [A1], [A2], ... [A8], with the *A* abbreviating 'adopter of Sidewalk' and the ascending numbers denoting the order of conducting interviews. Interviewees' products were at varying stages of maturity and Sidewalk use, as discussed in §C.1. Granted the small interviewee population and close ties between Amazon and adopters, I refrain from using identifiers when quotes might reveal an interviewee's affiliation to Amazon.

Population 2: Non-Sidewalk-adopting companies Having concluded most interviews from the first group, and establishing the contours of how Sidewalk indeed reshapes their production processes, I wondered whether US-based IoT companies that had not adopted Sidewalk, predicted this impact and therefore refrained from adopting it. To assess this, I approached 25 employees of 4 non-Sidewalk-adopting companies on LinkedIn in late December 2023. I randomly selected these companies from a tech magazine article discussing smart door lock brands, because of their technical similarity to Sidewalk devices (see Table B.1). This increases the chance that the company considered Sidewalk.

Taking the same cut-off date of January 19th 2024, I only received 3 replies, all negative. This prompted my decision to stop pursuing interviews, for three reasons: the highly time-intensive nature of arranging, conducting, and analysing interviews; the uncertainty whether these companies actually considered Sidewalk; and the fact that the predictability of the studied dynamics is not strictly necessary to answer the research question. I reflect on this decision in §10.4.

Meanwhile, I approached 4 LinkedIn contacts that I discussed Sidewalk with during TechEx Europe 2023. One person agreed to an interview. They are not an IoT manufacturer, but a C-level executive of a LoRaWAN service provider and prominent industry figure. To emphasize that they are the only interviewed non-adopter, I refer to them as [N1], the *N* denoting 'non-adopter'.

Interview execution and structure

All respondents signed an informed consent form. I stressed that they were free to skip questions or withdraw from participation at any time. I did not share interview questions beforehand, to ensure spontaneous rather than preconceived answers, and because of the semi-structured nature of the conversation (§3.2.5). The exception is one participant that I sent the questions per their request. Due to distance between me and the interviewees, I conducted all interviews in an online video call, except one that took place over telephone. Interviews were recorded to aid analysis. During the interviews, I repeated important or striking statements by the interviewees in the same words, to allow them to correct my interpretation or reinforce their points (Jorgensen, 1989). Afterwards, I shared the interview transcript to allow participants to redact or edit any statement. Nobody used this opportunity.

I conducted the interviews in semi-structured fashion, as Solarino and Aguinis (2021) recommend for one-off interviews. Beforehand, I mapped the importance of questions and established potential follow-up questions, to ensure flexibility during the interviews. I structured the interviews along the three elements that Undheim (2003) delineate: opening and rapport building, grand tour and focused questions, and closing; discussed in turn hereafter. The interview questions are given in Appendix A.

Key in elite interviewing is establishing *"a rapport that consists of both trust and respect"*, both while gaining access to the respondent and during the conversation (Ostrander, 1993, p. 8). Therefore, I dedicated

the opening of each interview to rapport building, asking how interviewees were doing and following up with a personal question, compliment, or joke. For instance, these related to a participant's recent promotion, a business trip abroad, and a virtual meeting background. The goal of these comments was to establish a comfortable atmosphere and therefore trust, as Undheim (2003) recommends.

My first actual interview question was asking respondents how they got to their current position and what their role is, asking for their ambitions and meeting their stories with admiration. Making room for introspection in the otherwise busy business days is fulfilling for elites and fosters trust with the interviewer (Undheim, 2003). I followed up inquiring about specific details of their company, referencing their corporate publications to demonstrate my knowledge of the topic and the respondent's background.

Having built rapport, I alternated between *"grand tour questions"* (giving an overview of the interview topic by posing more superficial questions or eliciting shorter answers) and *"mini-tour questions"* (homing in on specific subjects or interesting responses, eliciting longer responses) (Jorgensen, 1989, p. 86).

Prefacing sensitive mini-tour questions, I reminded participants that they are free to skip the question, but also that I process their answers anonymously, as Ostrander (1993) recommends. I also did this when interviews visibly hesitated to answer a question or pointed to non-disclosure agreements. Related is the advice to *"conduct the interview in a non-threatening way"* (p. 662), for which Solarino and Aguinis (2021) suggest positioning oneself as a curious apprentice. At times I emphasised my junior status as master student to elicit elaboration on sensitive topics or shallow answers. I did so only when necessary and having gauged that sufficient rapport had been established earlier, to not compromise the elite's respect for me as knowledgeable interviewer (Undheim, 2003).

Finally, I closed all interviews with 2 questions that Solarino and Aguinis (2021) recommend. First was whether the interviewee expected me to bring up any topic that I had not, or wanted to share any other matter. This question surfaces information that they think is important but was not discussed. Second, I asked participants who else in their network they ought me to interview. I then requested permission to mention that the interviewee referred me to those contacts when reaching out, helping to build rapport.

Interview analysis: coding

As a next step, I transcribed all interviews verbatim and coded the transcripts using ATLAS.ti 23 (ATLAS.ti, 2023), a tool commonly used for qualitative data analysis (Alasseri et al., 2018). I do not publish the codebook because of the administrative overhead. I coded the transcripts following the manual of Saldaña (2021), advising e.g. to iteratively work through two coding cycles and combine multiple coding methods, as explained below. For explanations of the coding methods, see his comprehensive book.

For the first cycle (concerned with attaching codes to parts of the transcripts), I iteratively combined initial coding, structure coding, and process coding (structuring and categorising transcripts according to identified processes, properties, dimensions, and relevant subquestions); hypothesis coding (developing hypotheses about the research questions, e.g. about how privacy manifests in interviewees' services or how their production changes after adopting Sidewalk, and attaching quotes that (dis)prove them); and evaluation coding (highlighting respondents' judgments and opinions). Thus, except for hypothesis coding, I used an inductive approach where I devised codes during the analysis of the transcripts. I defined many codes in *in vivo* fashion, to capture the respondents' own language and sentiment.

The second cycle involved *"classifying, prioritizing, integrating, synthesizing, abstracting, conceptualizing, and theory building"* with the excerpts coded in the first cycle and with the codes themselves (p. 89). I used two methods, starting with pattern coding. This entailed categorising codes and distilling higher-level themes and concepts. I first categorised codes according to their topic and higher-level themes (e.g. yielding the *"Amazon's dynamics"*, *"Industry dynamics"*, and *"Governance"* categories), and then mapped the codes and categories to the related research question(s). Second was axial coding, i.e. 'reassembling' separate codes by establishing their properties, and relating and contrasting (sub)categories to each other. For example, I contrasted opinions about the opt-in nature of Sidewalk's roll-out to gateways, and about Amazon's vantage point.

3.2.6. Triangulation

As visualised in Table 3.1 and elaborated above, I use at least two research methods and multiple data sources for each topic. This corroboration of findings with multiple data sources is known as

triangulation and recommended for case studies and interviews to add to their robustness (Rowley, 2002; Solarino & Aguinis, 2021; Yin, 2017), and especially valuable because of biases in the materials. For instance, some Sidewalk documentation is only accessible to adopters and not the public (e.g. Amazon, n.d.-h). Similarly, Amazon's press releases are obviously not always objective and written with Amazon's public reputation in mind. In addition, some interviewees accused tech journalists not comprehending the Sidewalk technology, and of being excessively negative about Amazon for the sake of *"clickbait"* [A1, A3, A6]. Finally, most interviewees are Sidewalk adopters, which could colour them more optimistic about Sidewalk. I reflect further on these biases in §10.4.

Examples of applied triangulation include that I consult technical documentation about Sidewalk and asked manufacturers what Amazon can learn about how endpoints use Sidewalk (§7.1); contextualise remarks about Amazon downscaling their hardware division and disappointing sales by finding relevant news reports (§9.3.1); cross-examine the benefits of Sidewalk advertised in Amazon's (§5.1) and manufacturers' marketing materials (§5.4), with interviewees' perceptions thereof (§5.5); and check whether Amazon implores obligations for adopters in addition to those laid out in developer documentation (§8.1).

4

What is Amazon Sidewalk?

The first step to understanding what PETs do for Sidewalk and how they potentially grant Amazon power over IoT manufacturers, is understanding what Sidewalk is. Therefore, §4.1 first explains what different actors Sidewalk involves. Next, to understand the implications of Sidewalk adoption for IoT manufacturers, we must grasp the technology underpinning it. Therefore, §4.2 studies the technical architecture of Sidewalk, and §4.3 explains how Amazon rolled out Sidewalk functionality to gateway owners. Then, §4.4 situates Sidewalk vis-à-vis other IoT connectivity methods, to see what makes Sidewalk special. §4.5 reflects on the chapter.

4.1. Actors

In Sidewalk, the following actors play a relevant role:

- *Amazon*: overarching term to refer to Amazon as an organisation, and their Amazon Web Services and Amazon Marketplace services
- *Sidewalk-adopting company, adopters, (IoT) manufacturer, IoT company*: the companies that have adopted Sidewalk for the IoT devices that they develop and produce, excluding Amazon. For the sake of simplicity, I assume that the actual development and production is in hands of the same company; even though, in practice, most IoT companies will partner with other companies for elements of the design or its actual fabrication
- *Silicon provider, chip provider*: company that develops and produces chips or low-level hardware components that the Sidewalk-adopting companies use in their products
- *Gateway owner*: individual people that own (and potentially use) one or more gateways
- *Consumer user, consumer*: individual people that own and use one or more endpoints, not in the context of a business, but for their own personal use (e.g. in a smart home)
- *Business user, business*: people that own and use one or more endpoints, in a business context, e.g. a property owner that deploys smart locks across their apartments, or a utility provider that deploys sensors at its water or electricity infrastructure
- *end-user, endpoint owner*: a person interacting with an endpoint that they own, either as consumer or business user

4.2. The technology underlying Sidewalk

This section outlines the technology that powers Sidewalk. After a brief introduction of the architecture (§4.2.1), I describe which technologies Sidewalk utilises in communication between the parts of the architecture (§4.2.2).

4.2.1. The Sidewalk architecture

Figure 4.1 pictures the Sidewalk architecture as visualised in Amazon's Privacy and Security Whitepaper (Amazon, 2023n). In its simplicity, this visualisation overlooks the role that the gateway owner's WiFi router plays; that endpoint users that want to interact with their endpoint from a browser or

smartphone must do so through the associated application server; and that the AWS IoT Wireless service is responsible for one of the three encryption layers (elaborated in §6.3.1).

Hence, I now describe my own visualisation of the hypothetical smart-home Sidewalk architecture pictured in Figure 4.2, to walk through an example of endpoints sending data uplink, i.e. to their associated application server. Sidewalk also supports downlink communication, i.e. from an application server to an endpoint, explaining the double-ended arrows. For this example, we assume that the gateway owner is opted in to Sidewalk (whether they are aware of it or not).

Sidewalk enables certain Amazon smarthome devices ("*bridges*" or "*gateways*") to share a portion of their WiFi bandwidth with other nearby IoT devices ("*endpoints*") (Amazon, n.d.-b). Besides connecting endpoints to the cloud, these gateways also scan for other gateways in their neighbourhood, to construct a map of the network topology for Amazon (Amazon Technologies, 2024, p. 16). In this example, the home owner has 2 gateways, an Echo (4th generation) and a Ring Video Doorbell, that are both connected to the home owner's router over wifi.

The endpoint may be owned by someone else than the gateway owner; therefore Sidewalk is referred to as a *crowdsourced* network (Amazon, 2023n) (more information on how this works follows in §4.3). This way, endpoints can communicate with an associated "*application server*" despite not having an internet connection themselves (Amazon, 2023n): once connected to the gateway, the gateway will relay the endpoint's messages over the gateway owner's Internet Service Provider's infrastructure to the network server. This is useful when the endpoint is outside WiFi range of the owner's router, or if the endpoint simply has no WiFi or cellular data connectivity capabilities on board.

It is the application server that endpoint owners interact with through the endpoint's accompanying smartphone or browser interface, for instance to consult their tracker's location, or to turn their light on. This connection is out of the Sidewalk scope and therefore indicated with dotted black lines. But note that to get the endpoint's information, the application server has to fetch it from the AWS IoT Wireless service using a Topic or API (Amazon Technologies, 2024, p. 46). Theoretically, manufacturers can ingest the data in their own infrastructure outside AWS, but the this is barely done in practice (see §8.3): it requires additional effort and does not negate the need for an AWS application server. Therefore, I only pictured an application server outside AWS for one manufacturer, with a dashed instead of solid arrow.

In between the gateways and application server is the "*Sidewalk Network Server*". It routes all the packets between their destinations, maintains time synchronisation of the network, and authenticates devices to maintain the integrity of the network (Amazon, 2023n).

4.2.2. Connectivity protocols

Sidewalk devices communicate using one of three connectivity technologies, namely Bluetooth Low Energy (BLE), LoRa, and Frequency-Shift Keying (FSK), depending on the distance between devices (Amazon, 2023n) and protocols supported by the endpoints and gateways (Amazon, 2023a, 2023n). BLE, FSK, and LoRa are intended for short, medium, and long ranges, respectively (Amazon Technologies, 2024, p. 11). The longer the distance, the lower the data rate; the data rates are up to 1 Mbps, 50 kbps, and 2 kbps, respectively (p. 11). Indeed, LoRa is intended for low-resource, long-range communication, as elaborated in §4.4.1.

The LoRa and FSK protocols are *"physical layer modulation techniques"* (p. 144) (also referred to as PHYs) for communication at a frequency between 902.2 and 927.8 MHz (p. 145). The Sidewalk specification also refers to these frequencies as the 900 MHz and sub-GHz band. This specific frequency band is reserved for industrial, scientific, and medical purposes (p. 202), where neither users nor manufacturers to obtain a radio license (Milarokostas et al., 2023). LoRa and FSK are similar, but differ in some low-level technical details. I refer readers interested in the differences between LoRa and FSK to the paper by Wiklundh (2019); for this research it suffices to know how Sidewalk utilises the two protocols in different ways.

Sidewalk is not the only service using these PHYs. For each, standards exist. Amazon has chosen to follow the IEEE 802.15.4g standard (2012) for FSK communication. Sidewalk's BLE implementation follows version 4.2 of the Bluetooth specification (*Core Specification 4.2*, 2014), but comes with proprietary layers on top of that, including the Alexa Mobile Accessory format for data formats (Amazon Technologies, 2024, p. 159). The LoRa implementation in Sidewalk is proprietary and not the same as the LoRaWAN standard published by the LoRa Alliance (Blackman, 2020). This is striking, because Amazon

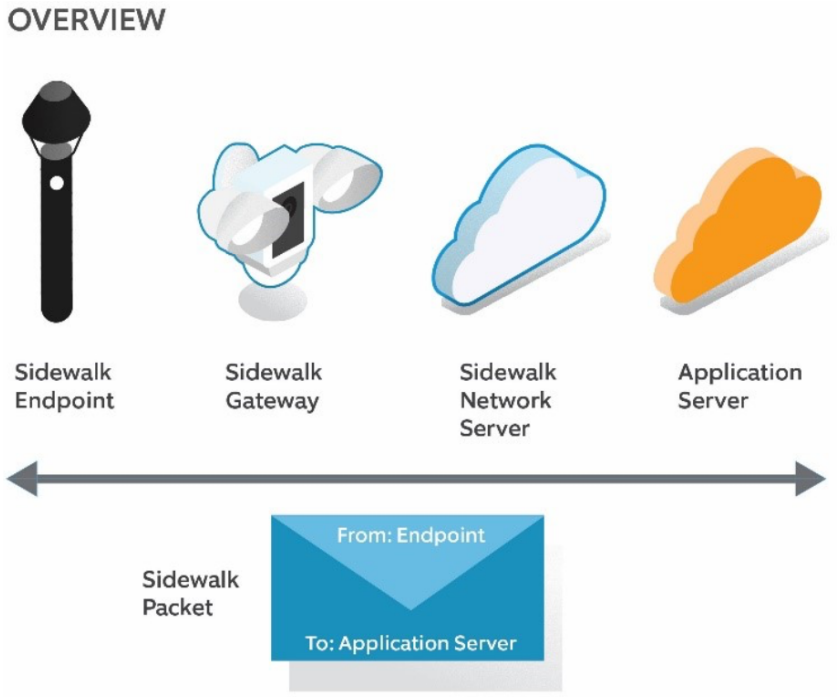

Figure 4.1: Amazon's overview of the Sidewalk architecture. Reproduced from Amazon (2023n) (p. 3)

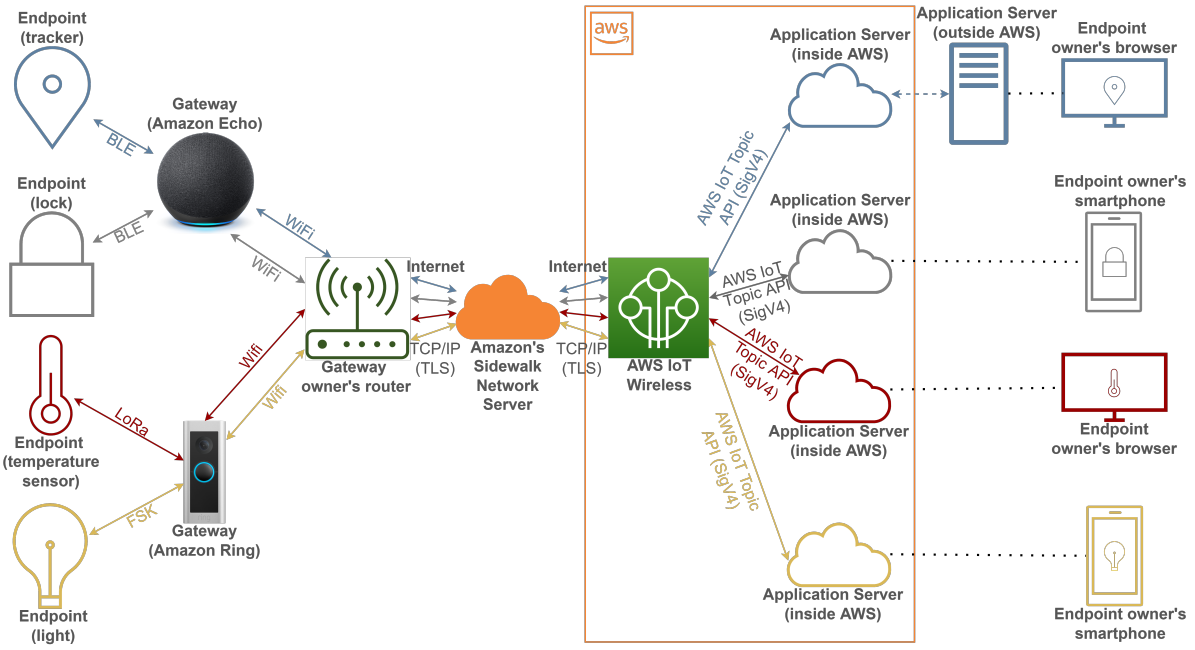

Figure 4.2: A more complete overview of the Sidewalk architecture, providing an example for a smart-home use-case. Ring image reproduced from Ring (n.d.-e). Echo image reproduced from (Amazon, n.d.-a)

is one of 15 'Sponsor' members of this standards body (LoRa Alliance, n.d.-a), employs one of its 15 Board Members (LoRa Alliance, n.d.-c), and also offers a myriad of LoRaWAN-related services in AWS (e.g. Amazon Web Services, n.d.-b). §9.3.2 discusses the tensions between Amazon and the LoRa Alliance.

Amazon caps the bandwidth used by gateways for Sidewalk traffic at 500MB per month per customer, at a rate of 80Kbps (Amazon, 2023n). In this context, Amazon differentiates between *Personal Area Networks* (PANs) and *Wide Area Networks* (WANs). A PAN is a network wherein the endpoints and gateways are linked to the same Amazon or Ring user account, with BLE-based device connections. Conversely, in a WAN, devices can be linked to different accounts and use LoRa or FSK. In a PAN, the data caps and also the Sidewalk participation opt-out of the gateway do not apply (Amazon Technologies, 2024, p. 13, 17–18).

4.3. How Sidewalk came to be

Rolling out a large-scale crowdsourced IoT connectivity network is no easy feat. This section describes how Amazon managed to do so, highlighting the limited control that owners have of their Echo and Ring devices.

The gateway role can only be performed by a selection of Amazon Echo (smart speakers) and Ring (smart cameras and doorbells) models (Amazon, 2023a). Amazon pushed the gateway functionality to devices already in use in consumers' homes with an over-the-air update in June 2021, that users were merely notified of by email 7 days before the launch of Sidewalk (Vaas, 2021). The function was enabled by default; users not willing to participate had to proactively opt out (Callas, 2021; Vaas, 2021), which users tend not to do (see §6.1.3). In March 2023, when Amazon opened the network for developer testing and made coverage testing kits available, they claimed to have coverage of over 90% of the United States population, as pictured in Figure 4.3 (Amazon, 2023o). About 10 months later, the Ring CEO (that also oversees Sidewalk) said that Sidewalk currently has 95% coverage (Bishop & Hamren, 2024). The coverage is owed to Sidewalk being *"enabled on more than 80 million Amazon and Ring devices"* (Amazon, 2024b).

Shortly after this network opening and coverage announcement in March 2023, Amazon updated the Privacy and Security Whitepaper to say that customers setting up a Sidewalk-eligible Echo or Gateway are asked whether they want to participate in Sidewalk, with the option being enabled if the setup is not completed (Amazon, 2022d, 2023n). The fact that Amazon has only adopted this more respectful approach now, without retroactively asking already opted-in users for consent, speaks volumes about the contribution of the opt-out nature to the present coverage.

Notably, not every Sidewalk gateway supports all 3 wireless technologies underlying Sidewalk. There are currently 30 different Amazon smart-home device models that can function as gateway. Of those, 4 types support all 3 protocols; 2 support LoRa and FSK; and 24 support only BLE (Amazon, 2023a). Interestingly, 4 Ring models were labelled as not supporting FSK in December 2023 (Amazon, 2023b), although the page now says that they do support FSK (Amazon, 2023a). This either means Amazon restored these incorrect listings, or is able to update gateways to have them support more protocols. Given that FSK and LoRa work in the same band, and these 4 devices already worked with LoRa, the latter sounds feasible: it would mean that supporting FSK and LoRa simultaneously is a matter of a software or firmware update as long as the hardware for either is in place.

In addition to these smart-home devices having received a dual identity to become a Sidewalk gateway, Amazon announced a dedicated gateway device called the Sidewalk Bridge Pro in early 2022 (pictured in Figure 4.4) (Amazon, 2022a). These devices are fit for outside use and support a longer range than the 'consumer' gateways. Simultaneously, this Bridge Pro signifies Amazon's public sector ambitions: it is aimed at *"businesses, municipalities, universities, and public services"* (Amazon, 2022a). In this announcement, Amazon also said they were launching pilots with a university for researching smart campus and hence smart city projects, and with an IoT start-up for forest fire detection and alerting. I could not find these Bridge Pro devices for sale. Moreover, there are no further updates about the gateway, nor the two pilot projects. In fact, the start-up project seems to be discontinued: one of the two (then-)employees has left the company according to his LinkedIn page, and emails cannot be delivered to the email address listed on their website, as I experienced during the interview invitation process.

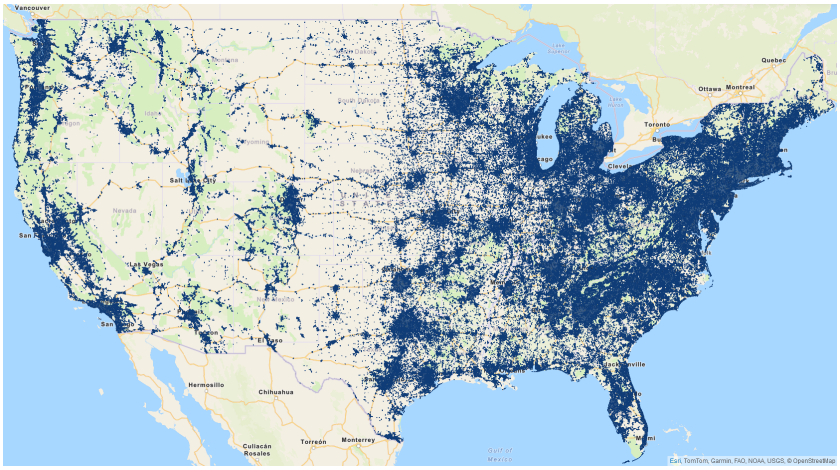

Figure 4.3: Screenshot of live Sidewalk coverage (Amazon, n.d.-g), taken March 3rd 2024. Blue dots indicate coverage. For the sake of comprehensiveness, I included only the contiguous US

Figure 4.4: Amazon's announced but not yet for sale Sidewalk Bridge Pro. Reproduced from Amazon (2022a)

4.4. Situating Sidewalk in the broader context of IoT connectivity

To understand how Sidewalk compares to other IoT connectivity methods, I here compare Sidewalk to the connectivity standards LoRaWAN (§4.4.1) and Matter (§4.4.2). I restricted the comparison to these two technologies because they have similar use-cases and architectures as Sidewalk, use radio frequencies that do not require licenses, and were each mentioned in at least four interviews, contrary to other LPWAN technologies (see e.g. Chaudhari et al. (2020) and Mekki et al. (2019) for a general comparison of LPWAN technologies). Finally, I investigate whether Sidewalk qualifies as a wireless mesh network (§4.4.3).

4.4.1. LoRaWAN

One of the three technologies that Sidewalk uses is LoRa. This radio frequency technology is widely used in LPWAN applications, commonly implemented using the LoRaWAN standard, that describes the communication formats and security measures of a networking protocol atop of lower-level LoRa radio communication (LoRa Alliance Technical Committee, 2020). Here, I contrast Sidewalk and LoRaWAN. For a brief history of LoRa(WAN) and description of a LoRaWAN architecture, see Appendix B.

A typical LoRaWAN architecture looks similar to LoRa communication in Sidewalk, with two important differences. First, the Sidewalk Network Server manages the network to ensure its integrity, route traffic, and to enable new devices to join the network. For LoRaWAN, this latter functionality is

the responsibility of a Join Server, and the former functionalities that of a LoRa-enabled Network Server (Semtech, n.d.-i). These may be operated by different companies.

This raises the second difference, namely that the LoRaWAN ecosystem is governed in a significantly more open fashion compared to Sidewalk. LoRa is patented by US-based semiconductor manufacturer Semtech Corporation (Slats, 2020), that actively invites third parties to the ecosystem by licensing the LoRa technology to them and promoting their services. Manufacturers wishing to make their endpoints LoRaWAN-compatible, can develop this functionality themselves using the developer resources, or can hire a partner company to do this for them. Similarly, they can develop their own gateways or buy them from another company (Semtech, n.d.-d). The same applies to obtaining software for network and application severs (Semtech, n.d.-f). Moreover, endpoints can be connected to networks of gateways managed by other organisations (such as [N1]'s company) (Semtech, n.d.-e), so that endpoint owners or manufacturers need not manage a gateway infrastructure and network themselves. Numerous telecom, technology, and consultancy companies offer paid proprietary networks (e.g. KPN, Cisco, and Capgemini) (Semtech, n.d.-e). There are even companies that offer wholly integrated LoRa-based solutions, covering the entire chain from endpoint to application server, for example for geolocation solutions that comprise both endpoints and an application server to control the endpoints (Semtech, n.d.-a, n.d.-b). So-called *"systems integrators"* can aid customers in building their own solutions for more specific use-cases (Semtech, n.d.-c). LoRaWAN adopters thus have significantly more degrees of freedom than Sidewalk adopters, being able to manage network components themselves, or buy them as products or services from others to save development resources (Ranjan, 2022).

The LoRaWAN standard is governed by industry body The LoRa Alliance, counting almost 400 members (LoRa Alliance, n.d.-c) across four membership tiers (LoRa Alliance, n.d.-f). Like Amazon, the Alliance helps adopters developing their products (LoRa Alliance, n.d.-d). There is also a qualification process, that is optional and signifies compliance of services with the standard (LoRa Alliance, n.d.-b, n.d.-e). Furthermore noteworthy is that the Alliance features multiple working groups, task forces, and user groups, that regularly convene to discuss the future of the specification LoRa Alliance (n.d.-f). While only the highest tier yields voting rights and the eligibility to be appointed a seat in the Board of Directors, and the two highest tiers may chair the aforementioned groups, all members get the right to attend their meetings to contribute to updates of the specification LoRa Alliance (n.d.-f). While Amazon is also open to feedback on their Sidewalk specification [A6], they retain the sole discretion to decide, and does not organise recurrent meetings with all adopters to jointly discuss modifications.

Conceiving of a sufficiently large LoRaWAN network to provide meaningful coverage, is no easy feat. This is why network providers are mostly large technology and telecom companies (Semtech, n.d.-e), but they cannot always make it work, either. For example, one interviewee told about an attempt by telecom provider Comcast at making their own LoRaWAN network in the US, named the 'MachineQ' network. This endeavour failed because of the enormous infrastructural investments required, as further described in §B.3.

Because of this, some LoRaWAN network providers deploy crowdsourced models, where people buy a gateway and open it for use by others. The Things Network bet on fostering a community of gateway operators and users. According to an interviewee, incentives to put up and manage a gateway lacked granted the purchase and electricity costs, leaving the organisation behind it to abandon this community part of the network. Helium tried to solve this by rewarding gateway operators with cryptocurrency (Roose, 2022). However, Helium's reputation is tarnished because its creators and early investors allegedly claimed an egregious part of the revenues while providing new gateway operators far less rewards than they expected (Emerson et al., 2022), and because the organisation listed companies as their customer that did not use Helium at all (Binder, 2022).

This illustrates the value of Amazon's control over Echo and Ring devices: because Sidewalk gateway owners already had gateways in their home that they used for other purposes, Amazon needed not invest in deploying dedicated LoRaWAN gateways throughout the US. Moreover, by making the Sidewalk update being opt-out, incentivising gateway operators was far less of a hurdle (as §6.1.3 explains). But telecom providers also equip their customers with devices, such as routers, that they could potentially repurpose. Comcast indeed did so to create a crowdsourced wifi network, that was not specifically targeted at IoT use and I elaborate on in §6.5.3.

4.4.2. Matter

Another technology that was mentioned repeatedly in interviews is Matter. Multiple interviewed organisations (considered to) use this technology in their IoT products. Tuohy (2023b) gives an explanation of what Matter is and how it works, that this section is based on where not indicated otherwise.

Matter is a standard specifically for the smart home that creates a local mesh network, tying smart devices together to extend their connectivity. The standard is being developed by the Connectivity Standards Alliance, wherein a wide range of smart-home manufacturers are represented. Members include big names such as Google, Apple, Samsung, and Amazon; but also chip providers and smart-home companies including Signify, Somfy, and Tuya (Connectivity Standards Alliance, n.d.). Matter acts as translator between devices of different brands, that can even use different communication protocols, namely Wi-Fi, ethernet, and Thread. Thread supports low-power, low-resource, long-range communication (Tuohy, 2022a), which makes it similar to Sidewalk. The Thread Group, that manages the technology, features many of the same members as the Connectivity Standards Alliance; again ranging from large technology companies to silicon providers and smaller smart-home oriented device manufacturers (Thread Group, n.d.-a).

Figure 4.5 illustrates a typical Matter smart-home architecture. Every Matter network requires a Matter controller, that is configured from a smartphone or tablet. This device manages the devices in the network (e.g. to add new ones or configure automation patterns). Another requirement is a WiFi network, hosted by the router in the middle of the image. Further, note how the architecture connects devices over wifi, ethernet, and Thread. All Matter devices in the network can address the internet and therefore their application servers, but also each other, using the Internet Protocol (IP).

To incorporate Thread-based devices in the architecture, there must be a Thread border router that liaises between the WiFi and Thread protocols. The Matter controller cannot by definition interface with Thread devices, although many controllers integrate Thread border routing functionality themselves (Tuohy, 2023a). Once on-boarded, Thread-based devices that qualify as Mesh Extender contribute to the network stability by acting as a traffic router. These devices can route traffic sent by others to their destination in the network. Consequently, if one device fails, other mesh extenders can take over to improve network reliability. Thread Battery Operated Devices are more resource-constrained and can therefore not route traffic for other devices. These two types are also referred to as Full or Minimal Thread Devices, respectively (OpenThread, 2023).

The similarities between Sidewalk and Matter are mostly that both connect smart-home devices, and provide users *"internet connectivity on a device that requires a gateway, without [the smart-home device manufacturer] providing the gateway"* [A2]. [A2] refers to the fact that some smarthome devices that users already own, could be updated by their manufacturer to support Matter, in some cases even becoming a Matter controller. For instance, in December 2022 Amazon pushed an over-the-air update to select Echo devices that made them Matter controllers (Tuohy, 2022b) and added support for Matter over Thread a few months later (Tuohy, 2023d). Indeed, this roll-out is akin to Echo devices becoming Sidewalk gateways; however, the Matter functionality cannot be opted out of. It might be that Amazon does not see a downside or privacy risk in Matter participation, because it is not crowdsourced. This would then, in their eyes, be a reason to restrict device owners' control over their devices.

There are also multiple differences. First and most obviously, Sidewalk is a proprietary technology managed by Amazon, which is not targeted at communication between devices, but instead at communication between an endpoint and an application server. To provide functionalities to their user, Sidewalk endpoints rely on the cloud because they can only address and be addressed by their accompanying application server (which disqualifies it as a mesh network, as §4.4.3 argues). Conversely, Matter devices can communicate with each other without needing an internet connection. The traffic routing happens locally in the Matter network, because Matter devices are themselves IP-based. [N1] compares Matter to Sidewalk as follows: *"[Matter] is set up as kind of a 'local-first' standard. So if you look at that standard, it's much more about those devices being autonomous, rather than smart; smart is when you connect them to the cloud, and autonomous is that you make sure everything keeps working, even if the cloud vendor quits"*.

Second, Sidewalk caters to a different audience than Matter. As §5.2 and §5.3 will show, adopters are primarily B2B-oriented, operating in the logistics and utilities domains. This is largely because Sidewalk supports both long and shorter ranges, and because its crowdsourced nature enables endpoints to 'roam',

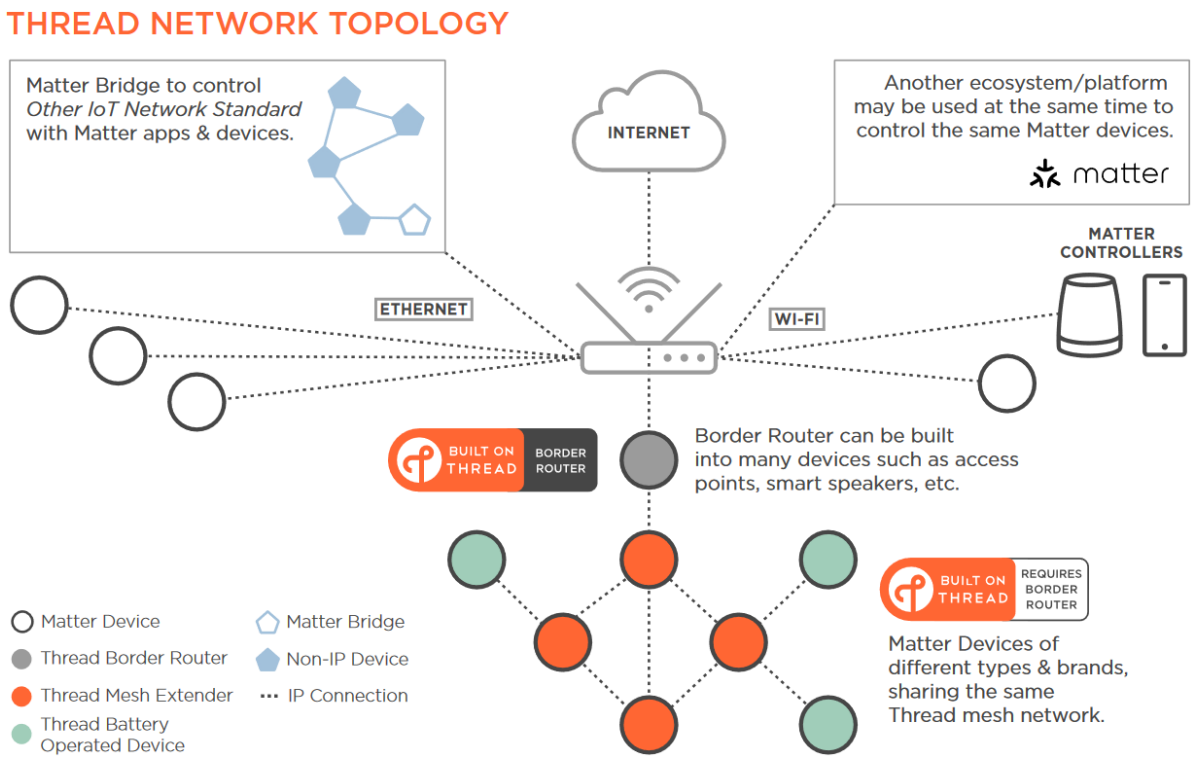

Figure 4.5: Overview of a Matter architecture. Reproduced from Thread Group (n.d.-b) (p. 2)

i.e. connect to different gateways on the move. On the opposite, Matter devices can only connect to other devices that belong to the same network and hence owner, over small distances. It is therefore marketed more towards smart-home and B2C applications, although B2B building management use-cases are not excluded.

4.4.3. Is Sidewalk just a mesh network?

Multiple grey literature sources (e.g. Callas, 2021; Lardinois, 2023; Song, 2023), and also one interviewee, refer to Sidewalk as a mesh network. However, as I show here, this is an inaccurate designation. The distinction is important, because Amazon has configured Sidewalk such that its own infrastructure (i.e. gateways, Sidewalk Network Server, and AWS IoT) is a key piece to realise the connectivity of endpoints with application servers. Conversely, in a mesh network, devices can talk locally to others in the mesh, as the discussion of Matter already alluded to.

To understand the difference, consider the book *Wireless Mesh Networks* by Akyildiz and Wang (2009). Devices that comprise a wireless mesh networks (WMNs) act both as *"host"* that generate data to be sent over the network and process data sent to them, and as *"router"* to forward packets sent from other nodes to their destination elsewhere in the mesh (p. 1). WMNs are also *"ad hoc"*: the mesh is dynamically reconfigured when devices enter and exit the network, adding to its coverage and reliability (p. 1). Further, WMNs enable data transmission between devices (*"peers"*) in the network, but also between devices and the internet (p. 6).

Following these characteristics, Sidewalk does not qualify as WMN. This is visible in the architecture in Figure 4.2. For the user to interact wirelessly with their device, their smartphone or browser has to connect to the respective application server. It is this application server that mediates between the user and their device, passing through the other Sidewalk components. While gateways function as routers that endpoints can connect to, endpoints cannot route traffic of or connect to other endpoints. Sidewalk endpoints are thus not a host and router simultaneously. Similarly, the endpoints cannot send payloads to each other locally: all Sidewalk traffic starts at an endpoint and ends at an application server (or vice versa).

Moreover, the only purpose of the connection between an endpoint and gateway is for the gateway to forward traffic to or from the endpoint. The two devices cannot communicate other information with

each other. For instance, if a Ring camera (gateway) detects motion, it cannot directly command a light to turn on.

Finally, gateways can only communicate information to and from a predefined application server (specified during manufacturing; see §8.2.2), passing through the Sidewalk Network Server. Sidewalk devices can thus not talk freely to other devices or to 'the internet' the way that devices in a WMN can.

It follows that Amazon consciously positions itself between manufacturers and their end-users with its configuration of Sidewalk. While mesh networks are decentralised and local, Sidewalk is centralised and relies on Amazon's cloud. Recall that Amazon's architecture visualisation (Figure 4.1 in §4.2.1) leaves out of the picture that endpoint owners must interact with their endpoints through the manufacturer's application server; that this server must talk to both AWS IoT and to the Sidewalk Network Server, that are controlled by Amazon; and that the gateway owner's router is fundamental for connecting gateways to the network server. This simplification obscures the centrality of Amazon's cloud, because local control of endpoints is not possible. Depicting Sidewalk as mesh network therefore implies that endpoints (and their manufacturers) have significantly more freedom than they in practice do: Amazon has cemented its own infrastructure between endpoints on the one hand, and their manufacturers and users on the other.

4.5. Chapter conclusion

The first component to answering the first subquestion of what Sidewalk is, is determining how the technology works and compares to similar LPWAN technologies. Sidewalk is remarkably different from LoRaWAN and Matter both in its governance (pitting Amazon at the centre as sole network provider) and its architecture (routing all traffic through their network server and AWS). Most salient is Amazon's ability to conceive of a network catering to at least 90% of the US population with, essentially, the push of a button that transformed Echo and Ring devices into gateways. With this scheme, Amazon avoided the enormous capital expenses that LoRaWAN network providers face, as well as the issues of user incentivisation that crowdsourced LoRaWAN networks faced.

While certain people mistake Sidewalk as a decentralised mesh network because of this crowdsourcing, this is actually far from the case. Its technical architecture is far more centralised and proprietary than Matter and LoRaWAN are, with all traffic being processed in their infrastructure. It follows that Amazon has consciously positioned itself between manufacturers and end-users through technology, and as Chapter 9 will demonstrate, also through their unilateral governance. Meanwhile, LoRaWAN's open ecosystem enables companies to leverage knowledge and services of others, and Matter's focus on local connectivity increases device reliability. Why, then, do manufacturers adopt the proprietary Amazon Sidewalk? This is the topic of Chapter 5.

5

Sidewalk adopters and products

Now that we know how Sidewalk's technology works, I survey why manufacturers adopt Sidewalk and how they use it, to answer the question what Sidewalk is. At the basis of this chapter lies the overview of all companies that (to date) have advertised their Sidewalk adoption in grey literature, given in §B.1. I start by reviewing how Amazon markets Sidewalk towards manufacturers (persuading them to make their endpoints Sidewalk-compatible) and gateway and endpoint owners (convincing them of Sidewalk's safety and that they need not opt out their gateway out of Sidewalk) (§5.1). Next is an elaboration on the market categories wherein the adopting companies operate (§5.2), followed by a discussion of whether they cater to businesses or consumers and how use cases and functional requirements differ between these contexts (§5.3). This background is essential for the next sections, wherein I expound on the advantages that move IoT manufacturers to adopt Sidewalk, as they came forward in the grey literature (§5.4) and the interviews (§5.5). These advantages differ between market categories. I present the findings from both methods separately, because interviewees expressed many unexpected incentives that push the publicly marketed advantages to the background. Further, I investigate manufacturers' discovery of and path to adopting Sidewalk (§5.6). To conclude, I provide a reflection on the chapter (§5.7). Taken together, this chapter yields an image of what Sidewalk is, providing a first step to assessing how Amazon uses it to pull manufacturers into AWS, as Chapters 9 and 8 go into.

5.1. How Amazon markets Sidewalk

Amazon promotes different aspects of Sidewalk to consumers and developers. Studying their narratives helps understand how Amazon appeals to both demographics and legitimises the opt-out schema. In Figure 5.1, I compiled numerous examples of how Amazon visualises Sidewalk's characteristics.

In consumer-facing marketing, Amazon firstly emphasizes that gateway owners need not worry about being opted in to Sidewalk, because they warrant the security of Sidewalk (Figure 5.1 **a** and **d**), and cap the amount of bandwidth that it uses (Figure 5.1 **c**). These assurances are usually made directly after the crowdsourced nature of Sidewalk is mentioned.

Amazon furthermore stresses Sidewalk's alleged 'community benefit'. For example, Sidewalk's homepage that primarily targets consumers, defines Sidewalk as *"a shared network that helps devices [...] work better at home and beyond the front door. When enabled, Sidewalk can unlock unique benefits for your device, support other Sidewalk devices in your community, and even locate pets or lost items"*. The page furthermore reads that 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"*. Similarly, the Amazon Ring CEO said that Sidewalk *"is best described as a community network"* (Bishop & Hamren, 2024, 19:51). And in one of the earliest Sidewalk announcements, an Amazon director likened the service to *"his native village in Southern Spain, where residents make their own soap"* and share it with their neighbours, because *"people feel good sharing"* (Amazon, 2021b). Amazon thus emphasises that gateways provide valuable coverage both for the owners' devices, and those of others in their community. Figure 5.1 **b** and **d** show how Amazon visualises these 'advantages'.

This framing is akin to that of the Ring Neighbors App, wherein residents can share video footage

Figure 5.1: 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** are reproduced from O'Neill (2023). **b** and **d** are reproduced from (Amazon, n.d.-b)

of their Ring cameras to warn or inform each other. Amazon has since long branded this service as having *"a strong effect of bringing neighbors together"* and making users *"feel very connected to [their] community"*, with as marketed use-cases locating pets, preventing crime, and improving cooperation with law enforcement (Ring, n.d.-a). Perhaps Amazon found success with appealing to this community notion and therefore replicates it for Sidewalk.

Further, it is striking that Amazon's press releases promote a variety of Sidewalk adopters active across the three application domains identified in §5.2. For instance, Amazon (2021a) and Amazon (2021b) mention adopters in asset tracking and building management; Amazon (2022a) demonstrates utility applications; and Amazon (2023o) references all three domains. As one interviewee formulated it: *"they used [us] as a pawn basically in the game, of showing that there's value to this network"*. The respondent noted that Amazon emphasised demonstrating Sidewalk's value to the public to divert attention from or compensate for the privacy backlash that happened around their announcements. Indeed, Amazon released a blog post detailing the value for Sidewalk end-users in September 2021, with most grey literature expressing privacy concerns (§6.1) being written in June that year.

The marketing to developers has a slightly different tone. In one piece, Amazon explains Sidewalk as *"a secure, free-to-connect, long-range and low-power shared community network designed to provide connectivity for billions of devices"* (Amazon, n.d.-c). The protocol specification (Amazon Technologies, 2024, p. 11) and press release announcing Sidewalk's opening for all developers (Amazon, 2023o) have a similar description. These pages also mention that Sidewalk is *"low cost"*, although without specifying whether this applies to end-users or IoT manufacturers.

More concretely, Amazon promises market opportunities and improved control over endpoints. The Privacy and Security Whitepaper, aimed at reassuring users, developers, and the media of Sidewalk's security, outlines Sidewalk as *"a shared network developed by Amazon to allow third-party developers to create and bring to market all types of consumer, enterprise, and public sector smart and connected devices and services"* (Amazon, 2023n, p. 2). The protocol specification (Amazon Technologies, 2024, p. 9) and Sidewalk developer documentation library (Amazon, 2023i) speak specifically of providing endpoints with *"cloud*

connectivity". Additionally, a February 2024 update to the Sidewalk protocol brought the *"Sidewalk Bulk Data Transfer"* functionality to Sidewalk, which lets manufacturers send not only simple commands, but entire firmware updates and other files to their endpoints (Amazon Technologies, 2024, p. 177). Amazon claims this contributes to security by offering remote patching, but also to *"extending their lifecycle and capabilities, cost-efficiency in maintenance from remote operation, and rapid prototyping to introduce a new firmware to their Sidewalk devices"* (p. 177).

Further, Amazon says that *"Sidewalk is a 'pipeline' that moves data back and forth between an Endpoint and its respective Application Server"* (Amazon, 2023n, p. 13). This analogy is also implied in Figure 5.1 **c** that visualises the gateway bandwidth cap. [A6] acknowledged this framing, saying that the Sidewalk team presented Sidewalk as a transport layer to them: *"[T]hey've been very clear 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. [...] Just bear in mind there are restrictions, right?'"* This framing is important for public policy discussions around net neutrality (Thierer, 2005). Classifying a connectivity provider as a *"dumb pipe"* or *"mere conduit"* that simply links an end-user to a content provider, as opposed to a *"smart cable"* network that treats data streams depending on their content, is an ongoing discussion (de Diego Martín, 2016, p. 4), that is become a partisan issue in the US (Jamison, 2018) Classifying Sidewalk as the former could exempt Amazon from certain responsibilities, such as liability for users using the connectivity for illegal purposes (Husovec & Roche Laguna, 2023; Renda & Yoo, 2015).

The discrepancy between marketing oriented at gateway and endpoint owners on the one hand, and manufacturers on the other, is curious. For the former, Amazon emphasises security, privacy, bandwidth limitations, more device coverage, and community benefit. Only the final two arguments demonstrate Sidewalk's value; the former three are aimed at taking away concerns that might incentivise gateway owners to find the opt-out button. Speaking towards manufacturers, Amazon highlights the opportunities for revenue generation and operational control. They emphasize that it is free to use, and can be used in various markets in both the public and private sector. Presenting Sidewalk as a pipeline does not do justice to the centrality of Amazon's cloud that manufacturers pursuing these opportunities must account for in their production processes, as §8.3.3 will show.

5.2. Market categories

Having mapped all Sidewalk adopters and what market categories they are active in, it became clear that each adopter focuses on one of five domains: logistics, in-home care, utilities, industrial, and building management. I tallied the number of companies per market category to assess which categories Sidewalk is most applied in (Table 5.1). Readers interested in a complete overview of Sidewalk-adopting companies, their products, and more, are referred to Table B.1 in §B.1.

Five companies target *logistics* applications, pertaining to the tracking of goods, people, and pets. One of these services also facilitates autonomous asset delivery by package drones and robots. All logistics applications cater to tracking by businesses, e.g. for companies to monitor their products' location and conditions during shipping. Two of these companies, namely Tile and CareBand, also sell to and target use by both consumers and businesses.

For CareBand, the asset tracking application for e.g. outdoors worker safety comes secondary to their primary focus of delivering *in-home care* services for people with dementia. CareBand is currently the only Sidewalk-adopting company delivering in-home care services with Sidewalk.

Next, five companies offer services for *utility* providers, namely for sensing gas or water leaks in pipelines, detecting wildfires, and for communicating information from water meters. Deviceroy's product is the broadest in this category; their product aims to communicate information from virtually any machine to servers of Deviceroy or their customers. Therefore, I added the label '*Industrial*' for them. While their device can also be used by consumers, the organisation focuses on B2B sales.

Further, eight companies offer products for *building management*. 6 of these offerings are for sensing air quality, water leaks, motion, and whether doors and windows are open or closed. 2 companies produce smart locks.

Table 5.1: Occurrences of market categories that Sidewalk adopters operate in

Market category	Subcategory (if applicable)	Occurrence
Building management		**8**
	Sensors	*6*
	Smart locks	*2*
Logistics		**5**
	Asset tracking	*5*
	Autonomous delivery	*1*
Utilities		**5**
In-home care		**1**
Industrial		**1**

5.3. Targeted audiences

It follows from Table B.1 in §B.1 that almost all Sidewalk-adopting companies are B2B-oriented. Of the 16 adopters, 15 companies design endpoints specifically for business users, of whom 9 companies simultaneously focus on consumers.

Considering that Amazon's customer-oriented marketing mostly speaks about the benefits of Sidewalk for consumer users, and not for business users (§5.1), it is striking that most Sidewalk adopters target business users. Apparently, adopters consider a business orientation better for their business model. But what explains this discrepancy?

According to [N1], smart-home business models are rarely viable. According to them, the margins in B2C sales are small. Consumers pick the cheapest device that satisfies their wishes, necessitating low retail prices and therefore cheap components. Moreover, commodity devices have a longer distribution chain, where every party (e.g. manufacturer, distributor, and retail store) takes a cut of the sale price. Manufacturers must then sell high volumes to compensate, but simultaneously, consumers only buy few devices (e.g. because they only need one smart lock for their front door). A common alternative is to offer subscription services on top of the device, but consumers tend not to buy into those [N1], which challenges the business models of companies that *"sell a [device] to a customer and then [...] run a service forever"* [A1].

Contrast that to e.g. a real estate owner that buys smart locks for all their properties in a building, or buys sensors to communicate sensor readings of industrial machinery to their cloud infrastructure. Such business users buy in greater quantities [A1, A7] and have an operational efficiency business case that makes the devices' price less important [a7, N1]. Further, enterprise consumers generally have (or obtain) more knowledge to set devices up than consumers [A6]. Moreover, business users will be less reluctant to purchase and manage additional gateways to provide coverage to their end devices; one gateway can serve multiple endpoints, which scales more efficiently when more end devices are purchased [A3]. Therefore, the majority of interviewed companies initially or mainly focused on B2B contexts, before shifting or expanding to B2C, if at all.

The technical requirements for devices thus depends on the targeted customer and their wallet, but also on their context of use more generally. This is elaborated in Table B.2 in §B.1. Consumer-oriented Sidewalk endpoints are typically intended for building management, and thus generally used in a fixed place, inside or near homes, with electricity and gateways commonplace, communicating over short ranges. Consumer asset trackers, conversely, are mobile and used on short ranges (for finding devices) and long range (for more course-grained location tracking). These requirements are similar for business users in these domains. However, utility endpoints are used on longer ranges, in less densely populated areas, and in battery-powered fashion due to a lack of electricity. Sidewalk coverage might be lower in those cases, necessitating that these devices support multiple protocols at once. Similarly, privacy and security concerns manifest differently, with business users more often being subject to relevant regulations; and consumers not often caring or wanting to buy secure devices if they are more expensive, or not knowing how to select such devices. A company's targeted customer type thus has implications for their business model and device capabilities.

5.4. Sidewalk benefits according to grey literature

The benefits of Sidewalk that adopters advertise in their press releases, and Amazon advertises in their own announcements, are listed in Table 5.2. The occurrence of each advantage was counted to assess which benefits the adopters perceive to be most valuable.

Table 5.2: Occurrences of the Sidewalk benefits mentioned in companies' marketing of their Sidewalk products and services

Occurrence	Benefit
16	Pervasive connectivity and long range
10	Reduces complexity for users and developers (because manufacturers need not manage a protocol or gateways)
8	Low costs for customers (because it is free to use and requires no additional gateway)
6	Reliability (e.g. pervasive coverage, or using Sidewalk as additional connectivity method)
6	Secure connectivity protocol
4	Additional functionalities to the endpoint (e.g. tighter integration with Alexa and/or Ring ecosystems, or opening up the opportunity to become a gateway for other devices)
4	Low power consumption
3	Easy connection to AWS, easing cloud service use
3	Low complexity for customer (because it requires no additional gateway)
2	Reducing electronic waste
1	Low political costs for customers (opposed to having *"fixed network towers and cellular gateways"*)
1	Higher data rates compared to LoRaWAN

The single most salient promise of Sidewalk is its pervasive connectivity and long range, which all 16 adopters advertise. Sidewalk's crowdsourced nature and the long-range capabilities of the LoRa protocol seem the most important contributors to this promise. The fact that endpoint users can leverage the gateways owned by others is indeed a recurring theme that enables other marketed benefits. First, it makes adopters' offerings cheaper for customers, because Sidewalk is free to use and means customers need not buy a separate hub device to connect their endpoint to, as is the case with many current-day IoT devices. One company explicitly contrasts the *"pay as you need"* model of their solution, with the upfront capital expenses that deploying one's own gateways or connectivity infrastructure incurs.

Further, according to 2 adopters, the crowdsourced nature reduces electronic waste because an endpoint needs no dedicated gateway, but leverages the Sidewalk gateways that simultaneously fulfil another purpose as smart speaker or camera. Not having to manage a hub makes the endpoint easier to use, too. Instead, the*"Frustration Free Setup"* connects the device to the cloud with little action needed from the user (§5.5.1).

Sidewalk's crowdsourcing furthermore eases the development and maintenance of endpoints by manufacturers, as they need not spend development resources on developing and maintaining a gateway. Similarly, adopters profit from not having to invest in creating a proprietary networking protocol themselves; they can instead leverage the development efforts that Amazon invested into Sidewalk. This advantage may also hold for LoRaWAN, if manufacturers partner with an end-to-end service provider that can take care of each component in the architecture (§4.4.1). However, their offering may differ in terms of pricing; governance; coverage; and technical requirements and support offered for making endpoints LoRaWAN-compatible, and for managing them from the cloud.

Finally, the crowdsourced model realises the network's pervasive coverage. As such, it helps adopters' endpoints to work reliably, that 6 adopters emphasize as advantage. Another contributor to device reliability is that adopters may use Sidewalk as redundant connectivity method, besides other protocols such as LoRaWAN (e.g. Deviceroy). However, as §9.4.2 will show, this is only feasible for developers with sufficient development resources, and for sufficiently powerful devices, which is generally not the case in the smart-home domain.

The remaining benefits are less clearly interrelated. Marketed by 6 companies is Sidewalk's security (including the end-to-end encryption). 4 adopters refer to the low power consumption of Sidewalk endpoints, which is true, but also applies for LoRaWAN (§4.4.1). For 4 companies, adopting Sidewalk brought additional functionalities to the device, for instance by enabling tighter integration with the Echo and Ring ecosystems (Tile, Level) and opening up the opportunity for endpoints to also become a gateway-like device for other devices to connect to, whether over Sidewalk or other connectivity protocols (Arrive, Deviceroy). Moreover, 3 adopters see value in Sidewalk easing the process of connecting their

endpoints to AWS, allowing them to leverage the cloud more and better. Furthermore, 1 company says Sidewalk offers higher data rates than LoRaWAN does. Finally, 1 adopter catering to utility providers said that customers need not interact with *"fixed network towers and cellular gateways"*, meaning they face lower *"political costs"* (Subeca, 2023a). Apparently, utilities face administrative burdens when putting up this infrastructure when providing connectivity to pipelines or water treatment sites.

5.5. Sidewalk benefits according to interviewees

§5.4 presented the advantages that Sidewalk adopters communicate in their own and in Amazon's marketing materials. The public and commercial nature of these resources means that certain (dis)advantages remain out of view, that the conversations with interviewees did evoke. This section describes the benefits as the interviewees described them. As I will show, these differ from the publicly marketed advantages. Potential explanations are that respondents were promised anonymity and were therefore more open-hearted, and that numerous benefits would not convey value of the adopters' services to their customers or shareholders, and therefore did not make it to their marketing resources. The advantages relate to improving the experience of adopters' customers (§5.5.1), profiting from the synergies that catering to both businesses and consumers simultaneously creates (§5.5.2), easing compliance with cybersecurity regulations (§5.5.3), profiting from Amazon's reputation (§5.5.4), and sustaining or creating business relations with Amazon (§5.5.5).

5.5.1. Customer experience

A first strand of advantages relate to the user experience.

Outsourcing the management of gateways to Amazon and their customers

Respondents expounded on and nuanced the value that using gateways already in people's homes brings about. They shared that their endpoints rely on there being a gateway nearby. For Sidewalk, it is Amazon's customers (i.e. gateway owners) that provide these gateways and hence the coverage, and Amazon that manages them (e.g. to make sure they are secure and ensure their functioning). The adopters shared that this model brings them multiple benefits.

Sidewalk's shared-use model of consumer gateways that covers at least 90% of the US population addresses *"the problem in IoT that you have gateways everywhere. And no one wants a gateway"*. In fact, gateways are still there, but the gateway owners have put them in their homes for other reasons, namely for their smart speaker or camera functionalities. The interviewees also raised that endpoint users need not buy, manage, and understand a dive additional to the endpoint, as §5.4 discussed. Moreover, given its long-range capabilities, more endpoints can be managed with fewer gateways. This is especially valuable in business settings, where interviewees expect their clients to purchase more endpoints than in consumer settings.

Sidewalk-adopting manufacturers also benefit from lower costs themselves, as their development and maintenance complexity and costs decrease: they need not build their own networks or select other network providers to do business with. In the words of [A3], *"we've been the iPhone and Verizon, we've been doing both things, which is really hard to do. And as a start-up company, you can't actually do that very well, because you can't execute both things as well. [...] But now that the Verizon part of it, or the network is kind of off to the side, with Sidewalk or Helium or other network providers that exist, we can now offset that a little bit, where we don't have to build out our own network and can kind of leverage their networks."* Their mention of Helium and other network providers implies, though, that LoRaWAN networks can also have this benefit (§4.4.1).

Frustration Free Setup

[A1, A3, A5, A6] hailed Sidewalk's *"Frustration Free Setup"* (FFS), which [A5] phrases as giving customers *"an Amazon- or Apple-like experience"*. Subeca (2023a) similarly says that FFS *"brings the Amazon shopping experience"* to their users. With FFS, users can set up their endpoint by simply scanning a QR code with their smartphone. The endpoints then rely on nearby *"helper or provisioner devices"*, that include Echo devices and routers (Amazon, n.d.-d), to finish device registration. This eases device setup significantly, especially compared to LoRaWAN where configuring the encryption measures requires more and complex actions by the user [A6].

FFS is not unique to Sidewalk, though: Amazon also lets third-party manufacturers implement it for IoT devices based on Wi-Fi, Zigbee, Bluetooth, and Matter (Amazon, n.d.-d). Implementing FFS comes

with its own governance hurdles. For instance, manufacturers must pass a certification process; print a special barcode on their packages; and have devices shipped to customers through Amazon's logistics department (Amazon, n.d.-f). Amazon impels the latter because *"Amazon scans your device's package barcode during order fulfillment and pre-registers the device with the Amazon customer's account"* (Amazon, n.d.-e). Interviewees did not bring up this requirement, although the general FFS page for developers explicitly mentions that FFS only works for devices purchased on Amazon.com (Amazon, n.d.-f).

Integration with other IoT devices

End-users furthermore benefit from their smart-home endpoints being better integrated by the Alexa (Amazon's voice assistant available on supported devices, including Echos and smartphones) ecosystem, as acknowledged by 2 interviewees. One of these interviewees sells asset trackers, for which locating devices is obviously a key point. Their devices can now be located by Alexa-enabled devices. They saw adopting Sidewalk as an experiment that might create a *"meaningful uplift in finding capabilities"*, which they indeed noticed in some cases. The other interviewee's endpoints can be controlled from within Alexa-related smartphone apps, allegedly improving the user experience.

The other way around, another company is interested in integrating third-party IoT devices into their own services. Their ambitions are to have their device become a gateway for other utilities and industrial devices, but using ethernet rather than the Sidewalk protocol. Thus, this other device connects to the endpoint over ethernet to send a message, and the interviewee's endpoint then forwards the message over the Sidewalk network as if it were a regular Sidewalk packet. As the interviewee describes it:

> *[Y]ou can connect [another device] to our device and it'll run normal TCP/IP, through the Sidewalk bridge, into our servers, and then connect to the rest of the Internet, through that bridge. So it becomes effectively almost like a cell modem, but without the expense of a cell network. [...] We're still using all the infrastructure of Sidewalk; it's just that once it hits the servers, we are relaying it out to the normal Internet on behalf of that device. And giving it TCP/IP, Ethernet, Internet, in places where they otherwise would never be able to have it.*

In essence, this company duplicates Amazon's ploy of cementing their own infrastructure between an endpoint and the manufacturer's server.

5.5.2. Catering to additional customer groups

Sidewalk changes the type of customers that adopters can cater to, enhancing their market prospects. For [A3], Sidewalk resolved a blocker that previously hampered them to expand into B2C activities. Their solution had to work both outdoors and indoors, but within buildings, coverage from the third-party LoRaWAN networks was often spotty. Therefore, they relied on consumers putting up LoRa gateways themselves. This worked for business use-cases, as only few gateways were able to cater to a heap of endpoints throughout the entire building. However, for consumers with only one or a handful of endpoints in their home, this scaled terribly. Besides the costs, consumers were less knowledgeable about managing their network than business users. The premise of Sidewalk eliminating the need for a customer-installed, IoT manufacturer-provided gateway, thus enabled the adopter's expansion to B2C markets.

By extension, Sidewalk enables catering to both consumers and businesses simultaneously, yielding adopters unique synergies that lets them improve their offerings for both demographics. This plays out as follows for [A2]: *"it's two ways. We see that we get benefits in the consumer space by having business quality in a consumer product. And then we get volume and we get testing and we get marketing and awareness and all of that from the consumer part, that helps us in the business segment"*. The company of [A7] is of the opinion that *"only by having a wide acceptance in the consumer sectors, that we could replicate the growth and the all worldwide global application, like what we see with Wi-Fi"*. However, before catering to consumers, they first had to focus on the B2B market to generate sufficient revenue to enable further expansion: *"Our first phase was to go full-speed with vertical market application. And now, we have some resources in terms of financially, because we went to our own fundraising with the success, we got a very strong round of fundraising for our bigger dream. [...A]fter so many years of implementation in the vertical market, actually this industrial customer helps us; vice versa effort that we improve the product with a very stringent power management level and a very easy barcoding scanning installation process, that we believe it is perhaps a time that we revisit our dream in the consumer market, [...] to specifically address the smarthome requirements"*.

The difference in approach between the two companies (i.e. [A2] using consumers to test and develop the product, opposed to [A7] first developing the product with businesses and then jumping into the consumer market) is striking. Generally, most interviewees expressed their B2B activities to be more profitable than the B2C, so [A7]'s statement that consumer adoption is necessary for worldwide adoption is interesting. This belief could stem from the interviewee's general advocacy for LoRa applications.

The quotes above highlight the agile production processes that manufacturers maintain. The *"testing"* and *"improv[ing] the product"* relies on manufacturers monitoring how users interact with endpoints and when crashes occur, such that they can be updated to improve the user experience or the revenue generation of the manufacturer (see §2.2.3). Sidewalk strives to make devices continuously connected, offering more opportunities for devices to communicate telemetry and receive updates. Sidewalk's tight integration with AWS (elaborated in §8.3.3) could entice manufacturers to process the telemetry data (e.g. to transform this data into knowledge) inside Amazon's cloud, which manufacturers might find convenient, too. As such, Sidewalk supports companies with shifting between B2B and B2C activities more fluidly, by rendering endpoints and how users interact with them better visible to their manufacturers.

5.5.3. Enabling lift and shift into the cloud for regulatory compliance

The promise of Sidewalk to deliver (cloud) connectivity to devices, together with Sidewalk's tight integration with the Amazon cloud (detailed in §8.3.3), can help business users to lift and shift their operations into the cloud. This is because current utility equipment (e.g. sensors or actuators) might not be connected to the cloud currently, whereas using Sidewalk-compatible sensors and actuators send data to and accept commands from the cloud.

[A5] argues that cloud use helps organisations subjected to cybersecurity regulations – as is utility providers often are – comply with these regulations, and demonstrate this compliance. They reason as follows. Cloud services improve the cybersecurity levels of utility providers because many providers are currently *"still running off of desktop computers. So they don't do patching, they don't do firmware updates, they share passwords and all that. All the no multi-factor authentication, all of the basic things, that if you just move to the cloud, you're so much more secure. [...] Amazon knows more about cybersecurity than the average [utility provider]"*. But besides actually complying, these cybersecurity regulations require companies to demonstrate their compliance. Cloud providers can also alleviate this burden: *"one of the toughest things about being in compliance with cybersecurity, in addition to actually being compliant, is actually documenting compliance. So how do you document compliance? You know, working with a cloud provider, where you can just download a report and say 'here's all my compliance data', there's just a lot of benefits to it."* Adopting Sidewalk is then one pathway to cloud adoption by utility providers, helping them attain and demonstrate regulatory compliance.

5.5.4. Leveraging Amazon's reputation

Interviewees also shared that adopting Sidewalk lets them profit from Amazon's reputation. This benefits their reputation vis-à-vis customers, silicon providers, and search engines.

First, one interviewee spoke on their customers' perception of the networking services their IoT devices utilised, comparing Sidewalk with an earlier Helium pilot. While Helium did provide connectivity well, it was harder to manage and explain to users because of its crowdsourced nature and blockchain-based incentive scheme (§4.4.1). Conversely, being able to say that the manufacturer's devices are powered by a network by Amazon, instils more trust in users, as Amazon is well-known for its technical capabilities. Interestingly, [N1] has an opposite perception: they argued that Amazon has a poor reputation concerning privacy.

Another interviewee, catering to utility providers, said Sidewalk is the wireless technology that gives them *"most traction in the market"* compared to LoRaWAN and BLE, because of its novelty. Their customers already have thousands of deployed sensors, often without connectivity; being able to connect them to a free network is attractive and something they have not seen before.

Adopters also benefit from Amazon's reputation in their relationships with their suppliers, such as silicon providers. One respondent felt that the suppliers they work with treat them better because they adopted Sidewalk. These other manufacturers consider Amazon an important client of themselves, leading them to serve Amazon well and extend that service level to Amazon's customers. Concretely, *"component manufacturers are much more likely to give us what we need, in the timeline that we need it, rather*

than putting us at the end of the line" [A6].

Finally, the externalities of Amazon's reputation extend to the *"reputability"* of manufacturers' websites. This is a metric that is inter alia used by search engines to rank websites as results for search queries. Amazon has *"one of the most credible websites on the planet"* [A6], therefore automatically increasing the reputability of websites that they link to (*"backlinks"*). Adopters' websites will be ranked higher in search results when Amazon's websites and promotional materials link to them.

5.5.5. Sustaining and creating business relations with Amazon

Numerous respondents explicitly mentioned that they adopted Sidewalk to sustain current or facilitate entering new partnerships with Amazon. One participant expressed that *"there's an aspect of an ongoing partnership with Amazon, which is a huge company"*. They elaborated over email later: *"[Our company] has had partnerships with a number of different groups in Amazon and significantly has a major retail relationship with Amazon"*. It is unclear how many or which groups this pertains to exactly, but over one tenth of this business' total 2022 revenue was obtained through from Amazon.com. Further, this organisation did a *"separate deeper integration with custom voice action"* for Alexa, wherein the interviewee believes another Amazon group was involved that they expect not to collaborate very closely with the Sidewalk division. Moreover, the interviewee's business is *"95% Amazon on cloud services"*, which another company publication actually classifies as a risk. These pre-existing relationships moved this company to accept Amazon's proposal to adopt Sidewalk, even though the interviewee explicitly mentioned that it brings them scant functional benefits. That they regardless jump through all the hoops that Sidewalk adoption entails, illustrates the importance that they place on maintaining on good footing with Amazon. While other interviewees did not acknowledge it explicitly, I expect that their reliance on AWS (see §8.3.2) will for them, too, be a reason to remain on good terms with Amazon.

Another respondent's company had no business relations with Amazon prior to adopting Sidewalk, but sees Sidewalk as *"a stepping stone towards future development, like Amazon Key and other Amazon services. 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."* This quote was a response to my question of what opportunities Sidewalk offers them, leading me to believe that this stepping stone is their major motivator for adoption. Without detailing the interviewee's business proposition to maintain their anonymity, know that the utility of endpoints would be much greater for users if the endpoints support Amazon's parcel delivery business. The company knows that Amazon is keen to deliver a similar service themselves, as they beat Amazon to the patent office for a key functionality of their device. It is this context that the participant said the following in:

> *[I]t's like befriending the giant, right? [...] So we don't want to shut them out, we want to include them, right. You want the giant to be able to [use our functionality], because now you're opening up a convenience to the end-user [...]. 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.*

An additional benefit is that partnering with Amazon creates opportunities for both companies to learn from each other; both technologically, and about planned product releases. The importance of having a good relationship for inquiring about rival products is underlined by the following quote: *"There's a whole story behind Apple, [...] we used to have a much closer partnership with Apple and it degraded, in the years prior to the [name of competing product] launch, which in retrospect was not surprising, but..."* The interviewee implies that their company was caught off guard by their launch of a competing product, which might have been prevented had their company not drifted away from Apple.

5.6. Paths to Sidewalk adoption

Because Amazon had already secured Sidewalk adopters before opening up the network to all developers, I wondered how these early adopters learnt about Sidewalk. Therefore, I inquired with interviewees about their path to adoption. Six interviewees elaborated on who initiated their adoption of Sidewalk.

The companies of three respondents approached Amazon on their own initiative. They learnt about Sidewalk by already being active in the sub-gigahertz spectrum, or in Amazon's announcements, and were convinced by the publicly marketed benefits.

The three other participants had a different path to adoption. One interviewee *"didn't really* choose *Sidewalk"*. In the context of there being pre-established business relationships, teams of the two companies met, where Amazon shared plans to adapt the existing LoRaWAN protocol in its own Sidewalk network. They invited this company to become an *"alpha partner"*, besides Ring. This partnership entailed building a range of Sidewalk-enabled smart-home devices, compatible with Amazon's Echo smart speakers. The organisation saw the potential to grow the LoRa IoT market and went ahead with the partnership.

The second interviewee's business also got involved with Sidewalk after Amazon took the initiative for a collaboration; they presume Amazon invited them to give Sidewalk an application as finding network.

The third participant was also an *"alpha partner"*, but at the invitation of their silicon provider, that they had a close relationship to (as further elaborated in §C.4). Amazon requested the silicon providers to nominate customers operating in a Sidewalk-relevant field as alpha partners. The rationale of Amazon here was that *"[t]hey want to push their technology, then of course they want to have the silicon providers provide SDK and things like that to kind of support that"*. The alpha partners of these silicon providers were thus both a guinea pig for Amazon developing Sidewalk, and for silicon providers developing Sidewalk-compatible chips and accompanying software.

Curiously, these two latter participants pursued the collaboration despite Sidewalk not contributing much functionality to their product and putting them at the risk of commoditisation (see §C.6.2 and §8.4.4); and the bandwidth restrictions making Sidewalk *"not a perfect fit for us"* (§8.4.1), respectively. They indicated that maintaining close relations with Amazon (§5.5.5), and for the final participant also their silicon provider, prevailed. This demonstrates the industrial leverage that Amazon has: they convince these companies to adopt Sidewalk, despite it not bringing much utility to them.

5.7. Chapter conclusion

Besides its technical architecture (Chapter 4), how manufacturers put Sidewalk to use shapes Sidewalk's identity and value, and is thus relevant information to answer subquestion 1 asking what Sidewalk is.

Amazon markets different features of Sidewalk depending on their audience. They assure endpoint users that the service is secure and does not infringe their privacy, despite the crowdsourced and Amazon-centralising architecture. These characteristics are also relevant to convince gateway owners not to opt their devices out of Sidewalk – granted they are aware of this option in the first place. Further arguments to this end are that Sidewalk does not eat up all their bandwidth, and that gateways come to the aid of their owners' neighbours.

The consumer- and smart-home-centred marketing is an interesting contradiction with the dominance of B2B-focused adopters, with many of them being active in utilities and logistics domains. The reason is that B2B is generally more profitable and scalable than B2C. This is an important realisation given that most coverage about Sidewalk centres consumer uses and also the power and privacy risks therein. How businesses, as well as public organisations (e.g. water utility providers or municipalities investigating smart city applications) might be captured in Sidewalk, is a blind spot.

Still, Sidewalk mitigates barriers to consumer IoT adoption (such as complicated device setups and needing a gateway to provide an endpoint with connectivity), allowing these companies to expand their B2B offerings into consumer applications, too. Simultaneously, manufacturers remarked that the added operational control over endpoints enables them to learn how customers of one type use their devices, that they can use to improve the offering to the other type. Therefore, Sidewalk lets adopters experiment with new business models.

Besides, Amazon promises manufacturers a secure, easy-to-use *"pipeline"* between their application server and endpoints. Indeed, manufacturers tout these benefits in their own marketing, too. The centrality of AWS in the architecture leads me to doubt this designation. §4.2.1 outlined the important roles of the Sidewalk Network Server and AWS to route traffic, authenticate devices, and enable application servers to interface with endpoints. Classifying Sidewalk as a dumb pipe undersells the control that Amazon exercises over the network. As 8.3.3 elaborates, Amazon indeed uses Sidewalk to funnel developers into AWS.

Triangulating the Sidewalk benefits identified in manufacturers' marketing materials, with the interviews, revealed that secure connectivity was often not the primary reason for them to adopt

Sidewalk. In fact, security did not even play a role for some interviewees, despite nearly half of the adopters advertising Sidewalk's secure nature. This underlines that marketing security affordances serve mostly to take alleviate concerns, rather than distinguishing Sidewalk from other LPWANs.

Other incentives included moving the organisation's entire operations into the cloud to ease cybersecurity regulation compliance, and making their devices easier to configure for consumers, as well as cheaper to develop. Additionally, leveraging Amazon's reputation, as well as improving the image Amazon has of them (*"befriending the giant"*), were fundamental drivers. Multiple interviewees engaged with Sidewalk because Amazon or their silicon provider invited them. By taking on the role of *"guinea pig"*, they aspire to be treated better by silicon providers and improve their reputation with customers. But more interestingly, adopters' reliance to have access to Amazon's marketplace, cloud, and logistics businesses were reason to entertain Sidewalk – even if adoption was costly and brought minimal functional benefits to their endpoints. This suggests that Amazon is able to mobilise resources of third-party developers and silicon providers to spur Sidewalk's development; a proposition investigated in Chapter 9 onwards. Before I go there, I examine the merit of the privacy and security concerns in the grey literature, and how Amazon addresses them, in Chapter 6.

6

Privacy and security concerns

In studying what Sidewalk is, I learnt that all traffic passes through Amazon's Sidewalk Network Server and AWS. Intuitively, [A3] confirms, opening up people's gateways to forward traffic to and from endpoints owned by others seems an *"inherent security risk"*, that the PETs supposedly address. In this chapter, I investigate this premise to answer subquestion 2: *"What role do privacy-enhancing technologies play in Sidewalk?"* Here, I take a consumer privacy focus, to stay with the grey literature and interviewees' remarks. Chapter 7 expands the view to confidentiality of manufacturers' business knowledge, to fully answer question 2.

To this end, I outline the privacy and security concerns that Sidewalk raises, how Amazon addresses them, and what manufacturers make of them. First is an overview of the concerns raised in the literature (§6.1). I triangulated these with the interviews, inquiring about respondents' views on their severity and how they account for this in their production. In fact, defining *"how secure"* a developed IoT device should be, is largely a financial choice determined by the customer's wishes and how sensitive the data or service is (§6.2). Adopting Sidewalk as a connectivity method that comes with its own security measures (§6.3) can then seem attractive to IoT manufacturers wishing to reduce their own development costs. However, attaining this security level also comes with costs (§6.4). When asked about how Sidewalk's PETs actually contribute to user privacy, interviewees mostly brought up the opt-out nature of Sidewalk in relation to its contribution to Sidewalk's vast coverage (§6.5). A conclusion closes the chapter (§6.6).

6.1. Privacy concerns in grey literature

Many authors have written about privacy and security complications that Sidewalk raises. A first reason is that traffic goes through Amazon's AWS IoT Wireless, Sidewalk Network Server, and through gateways potentially owned by others than the endpoint owners. Both the travelling of data between these components, and the processing of data within them, must therefore be secured (§6.1.1). Further, authors take issue with the applications that Sidewalk enables (§6.1.2) and the opt-out fashion wherein Sidewalk was rolled out to gateway owners (§6.1.3). Publications about these topics are mostly grey literature; at the time of writing, there was scant academic literature meaningfully covering Sidewalk.

6.1.1. Protocol security

The literature was cautiously positive about the effectiveness of the encryption and obfuscation methods laid out in the Privacy and Security Whitepaper (e.g. Callas, 2021), but concerns remain.

First, new technologies are rarely bug-free, making it likely that flaws will be detected when the system is already widely used (Callas, 2021; Vaas, 2021). Considering that major vulnerabilities were uncovered when industry-standard wireless technologies such as Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) already became widespread, trusting a proprietary standard to be entirely safe seems naïve (Vaas, 2021). Such bugs could be present in software and firmware developed both by Amazon and others in the ecosystem, namely adopters and silicon providers (Callas, 2021).

Second, Amazon has not published details about how precisely it implements their security measures, nor given researchers access to the technology. Independent reviews are thus not possible, making it

hard to verify that the implementation described in their Privacy and Security Whitepaper is bug-free (Callas, 2021). As Despres et al. (2022) note, *"users must place full trust in Sidewalk to deliver on their data management policies with no effective guarantee of privacy built into the system design itself"* (p. 3). And even if Amazon obeys its own privacy and security restrictions, third-party developers may abuse user data, according to a PhD candidate cited in Chase (2021). This is made clear by the Whitepaper stating that *"Third-party Sidewalk device manufacturers may maintain their own logs that are subject to their respective retention periods and privacy notices"* (Amazon, 2023n, p. 6).

6.1.2. Problematic applications of Sidewalk

Further privacy questions sprout from Sidewalk's core functionality, namely extending the connectivity of IoT devices. By increasing their connectivity, some authors argue, the privacy concerns that IoT devices inherently pose, will apply to larger areas. These concerns relate to Sidewalk enabling more pervasive tracking of endpoint users, contributing to more pervasive surveillance, and constituting a transgression of a technology into personal livelihoods.

Two concerns surfaced around the more pervasive localisation that Sidewalk enables by providing trackers with connectivity: these trackers could facilitate stalking, and be abused by Amazon to track the location of their users.

Callas (2021) and Vaas (2021) fear that Sidewalk amplifies the potential of using asset trackers for stalking by extending their coverage. 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 (Karabus, 2023). The potential of tracker-based stalking had already been widely demonstrated for trackers of Google, Tile, and Apple before this case (see, indicatively, Cahn and Galperin (2021)). While Google and Apple are spearheading an effort for an *"industry specification"* with abuse-mitigating measures (Apple, 2023) that is currently being finalised by the Internet Engineering Task Force (Ledvina et al., 2023; Vermes, 2024), there is no mention of Amazon's participation herein. Amazon has also not said that they incorporated anti-stalking measures in Sidewalk.

In addition, authors fear that Sidewalk reveals endpoint users' locations to Amazon. An analyst cited in Crist (2021) states that pet trackers tell Amazon how often, how long, and where users walk their pets, and note that pet location data could be combined with other data in unexpected ways. The analyst did not substantiate how Amazon could do this, or provide examples of such data recombination. Following his logic, I hypothesise that Amazon could advertise pet care products if they see users visit known locations of veterinary clinics, or could notify local authorities if the pet is located in an area where pets are prohibited. These examples are not to say that I subscribe to these possibilities, but merely to illustrate the nature of the analyst's concerns.

Despres et al. (2022) do demonstrate that tracking an endpoint on Sidewalk is possible for Amazon by looking at which gateways it connects to. Amazon sees the gateway that the endpoint is connected to Sidewalk through, and logs the most recently used gateway to then route downlink traffic to (Amazon, 2023n). They also point out an inconsistency in the Privacy and Security Whitepaper: *"the system claims to forget the device ID associated with a transmission after replacing it with a temporary rotating identifier. In reality, the same analysis details how 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).

Other articles are concerned about Amazon's growing surveillance infrastructure and past security vulnerabilities thereof. Amazon's Ring brand offers an extensive suite of surveillance products and services, including video doorbells, cameras, and security systems (Ring, n.d.-b). A patent from 2018 describes white- or blacklisting home visitors based on facial recognition (Holley, 2018). Another patent depicts delivery drones filming customers' homes, checking for trespassing and damages at an interval set by the users (Cook, 2019). Sidewalk expands the area wherein cameras and drones can work, both in public and private areas. Ring cameras are then no longer confined to the range of their owner's wifi router, enlarging the area that Ring owners can monitor. While the bandwidth restrictions might prevent these devices from functioning as a live camera feed, they may communicate over Sidewalk in case of alerts, e.g. when motion is detected.Sidewalk then functions as the thread connecting smaller patches of surveillance products into one great surveillance network (Hanley, 2021), potentially enabling Amazon to monitor entire neighbourhoods and cities.

As such, Sidewalk amplifies the traditional critiques concerning the surveillance that Ring enables.

This backlash comes from their ambitions of working with law enforcement (detailed in Appendix B.4) and history of giving employees too liberate access to customer's videos (Brodkin, 2023). Meanwhile, there are reports that refute Ring's alleged contribute to combating crime (Farivar, 2020; Guariglia, 2020; Harris, 2018). Further, Nguyen and Zelickson (2022) argue that Ring lets Amazon convert a labour cost of monitoring their delivery drivers and parcels themselves, into a source of income by giving Ring users the ability to monitor deliverers with cameras and sanction them through reviews or sharing recordings on social media. Sidewalk could also extend this kind of surveillance.

In addition, Ring has a history of security issues. For example, a vulnerability exposed wifi network credentials (Ng, 2019); Ring took poor security measures against brute-force login attempts that eventually let strangers log into other people's devices (Guariglia, 2020); and Ring only applied end-to-end encryption to camera footage sent from cameras to the cloud starting in 2021 (Guariglia et al., 2021), while presently being on opt-in basis and removing access to other Ring features (Ring, n.d.-d). Echo devices have generated similar backlash for allowing employees access to user voice recordings (Patterson & Simon, 2019).

Finally, several authors write that Sidewalk tightens Amazon's grip over citizens' personal households and physical livelihoods. Chatting et al. (2021) note that 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. In their opinion, a shift in control over IoT devices results, from gateway owners to Amazon (further discussed in §6.1.3). I personally question how much control device owners had in the first place. Cleave (2021) contrasts digital services confined to cyberspace with Sidewalk reaching into the personal and physical family space of citizens. Similarly, Humphry and Chesher (2021) remark that traditional physical privacy boundaries, such as curtains and fences, do not affect connectivity travelling to or from gateways. With connectivity enabling digital services that reach beyond the range of one's home router(s), i.e. into the yard or streets, Sidewalk bridges further blur the borders between private and public spaces around people's homes (Humphry & Chesher, 2021), scaling smart homes up to smart neighbourhoods (Crist, 2021).

6.1.3. Sidewalk's inception: opt-out functionality on gateways

Grey literature publications following Amazon's (muted) announcement that Sidewalk would be enabled in opt-out fashion, sees three disadvantages for gateway owners: that Amazon undermines their control over their devices is undermined, puts their privacy at risk because of the opt-out fashion and crowdsourced nature, and might cause issues with their ISPs (e.g. Callas, 2021; Chase, 2021; Goodin, 2021; Newman, 2021; Patterson, 2021). This is exemplified in Figure 6.1. Authors speculate that Amazon did so to increase participation, as users tend not to opt out but are hesitant to opt in to services (Callas, 2021; Goodin, 2021; Newman, 2021; Patterson, 2021). Indeed, extensive scientific research demonstrates that people tend not to deviate from default settings, because they find it convenient, consider it the recommended option, are indifferent about it, or are unaware of the option to change settings; with tech companies encouraging the latter by hiding settings away (e.g. Acquisti et al., 2015, 2016) In the eyes of Callas (2021), this opt-out scheme violates *"the most important principle in respectful design"*, namely user consent: *"People must be free to autonomously choose whether or not to use a technology"*. This philosophy is a stark difference from Amazon's approach of justifying gateways' participation in Sidewalk after the fact by pointing to the bandwidth and security protections (§5.1). Most sources claim that gateway owners had less than two weeks before Sidewalk went live (e.g. Goodin, 2021; Vaas, 2021). Gateway owners allegedly received an in-app notification about Sidewalk going live, and Echo owners were additionally notified a month before launch with an email (Moorhead, 2021). It is unclear why Amazon used two different communication channels. I question how many users will have seen the in-app notification; this will depend on how often they use their device apps in the first place. Similarly, not all Echo owners might be interested to read an email titled *"Echo Update: Amazon Sidewalk is coming soon"* (Budd, 2020), which does not mention the crowdsourced and opt-out nature.

The privacy and security issues sketched above exacerbate this lack of gateway owners' control over their devices. Other concerns include the risk that gateway owners violate the terms of service agreements with their ISP, as an ISP representative quoted in Chase (2021) argues is the case; and that Sidewalk also snoops away bandwidth from users that are on metered contracts, potentially without being aware of it (Baker, 2023; James, 2023).

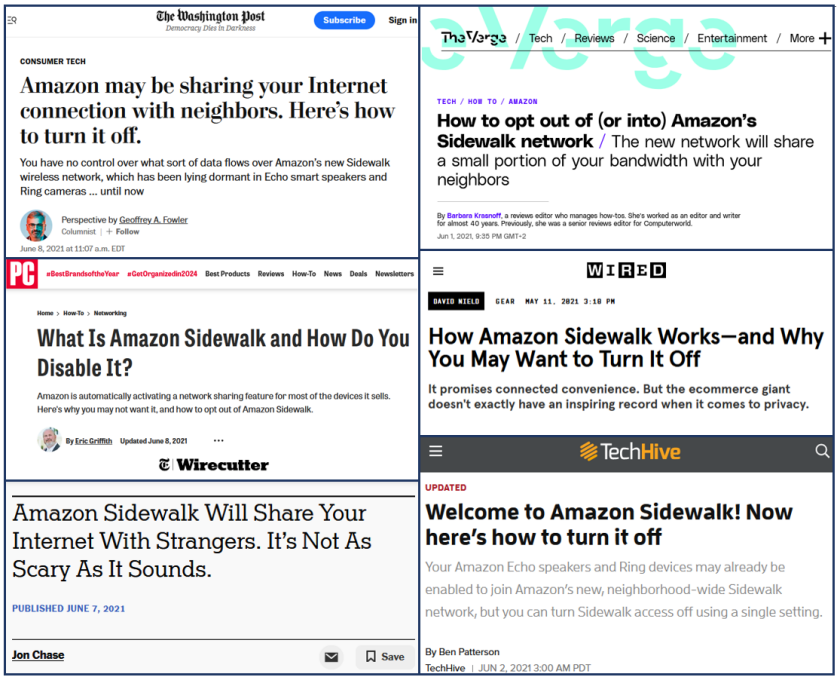

Figure 6.1: Examples of grey literature around Sidewalk's opt-out roll-out

6.2. Security level as a financial choice

As many things in corporate life, how secure manufacturers develop their IoT device to be is firstly a financial choice, largely influenced by the customer's context. The type of customer targeted, as well as their context and the sensitivity of transmitted data, inform manufacturers' choice for adopting a certain level of security [A1, A6, A7]. For instance, end-users will see it more problematic if their smart lock or a water shut-off valve can be operated by a threat actor, than if a threat actor could view the humidity in their living room. Additionally, recall from §5.3 that smart-home IoT consumers value device cost in their purchases higher than business customers do. According to one respondent, these factors come together in customers' willingness to pay:

> *I would take this question to the market: how much is the user willing to pay for a premium security or entry-level security, right? [...] I let them make the decision. Because for us, to embed more encryption technology, is easy. Either the hard encryption or soft encryption: we have the software, we know how to embed a chip for the encryption into the circuitry. But are you willing to pay €10 more per unit, for encrypting your garbage data?*

It is relevant that this interviewee works for a large technology corporation that seemingly has sufficient resources to make adding more security *"easy"*. In fact, as other interviews also made clear, encryption requires setting up a public key infrastructure. This is a demanding technological and administrative endeavour, especially for companies with less experience in doing so.

Similarly, multiple interviewees reported that some business customers want to control the entire architecture out of security concerns. One example is this quote of [A7]: *"the early adopters of LoRaWAN networks are actually big corporates that understand the importance of the data points that they need. And this data is important, and some level of confidentiality to them. They want to analyse themselves. So they want a proprietary network owned by themselves, managed by themselves, by using your [own] devices"*. The desired level of confidentiality is the stimulus for choosing such a private solution: *"For enterprise, that's why they want proprietary network, 'is my network, by me, for me, and I own everything. No one is going to crack'"* [A7]. Using Sidewalk is then not an option [A6, A7]. The organisations of [A6] and [A7] can cater to these demands: they sell end-to-end LoRaWAN solutions, where customers can deploy gateways themselves to host their own private network that directly connects the endpoints to the company's servers, be that in a cloud or on-premise. All data then stays within the local infrastructure of the customer. However, these applications require the IoT company to take on a consultative role, wherein

they elicit their client's requirements and tailor their application to it. This seems to be an expensive endeavour, that will not scale easily for B2C-oriented companies; selling to consumers usually entails selling few cheap devices to many clients, rather than selling many cheap or few expensive devices to few customers, as is the case for B2B.

6.3. Sidewalk's security measures and PETs

The Privacy and Security whitepaper (Amazon, 2023n) describes how communication over the Sidewalk network is secured in its travel through a gateway and the Sidewalk Network Server. This boils down to a combination of end-to-end encryption (§6.3.1) and device identifier obfuscation (§6.3.2). Amazon does not refer to these measures as PETs, but does speak of them in the context of protecting data, information, customers, privacy, and security.

6.3.1. End-to-end encryption

Sidewalk applies an end-to-end encryption setup with 3 *"layers"*. Figure 6.2 shows how this works for an endpoint communicating to an application server. This image is taken from the whitepaper (Amazon, 2023n, p. 7). The *endpoint* encrypts the payload data (here the detection of motion) with an Application Server Key (only known to the endpoint and application server), and encrypts the result 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 inspects the packet. This entails checking whether the packet complies with protocol format specifications, and that the device is not on a blocklist that the network server shares with the gateway. After approval, the gateway adds a third layer of encryption using the Gateway Network Server Key (only known to the gateway and Sidewalk Network Server). The *network server* then decrypts the second and third layers and inspects the package. Here, the inspection serves to authenticate the endpoint and verify that it is not blocked from Sidewalk or reported as lost or stolen by the application server. Finally, the network server forwards the packet (with only one encryption layer remaining) to the appropriate *application server*, that decrypts the final layer and processes the payload (e.g. sending a motion detection alert to the endpoint user's phone).

The whitepaper also contains a schematic visualising downlink traffic (Figure B.2), included in §B.6. The application server knows which endpoint the data should be routed to (e.g. which light should be turned on), and sends a packet with the command to the network server submits the endpoint's Sidewalk-ID to the network server along with the twice-encrypted payload. This ID is created during the device fabrication. The network server then looks up which gateway the endpoint last used to communicate uplink, and sends the packet there. The gateway then forwards the packet to the endpoint.

There are some nuances to this scheme, that become clear upon reading the protocol specification (Amazon Technologies, 2024). For instance, in the case of downlink communication where the endpoint is no longer within range of the last-used gateway, another process is triggered. This is out of scope for the current argument.

6.3.2. Device identifier obfuscation

All endpoints and gateways carry unique credentials for Amazon to authenticate them and combat illicit use. To *"minimize data tied to customers"* (Amazon, 2023n, p. 11), Amazon uses temporary identifiers. For instance, transmission and gateway identifiers are renewed every 15 minutes. Amazon clears information used for routing packets over their network every 24 hours. Amazon distances itself from the practices of adopters, though, as mentioned in §6.1.1.

While specifying how data is deleted and rotated, the whitepaper is unclear about what data is retained. For example, to deny abusers and endpoints marked as stolen from accessing the network, Amazon must store persistent identifiers of devices, as well as which manufacturer these are associated to. Amazon does not mention this explicitly.

6.4. Interviewees' perceptions of Sidewalk security

§6.3 explored the PETs that Sidewalk employs, as described by Amazon themselves. For triangulation, I asked interviewees for their opinions on the security of Sidewalk applications. §6.4.1 presents respondents' perception of how secure Sidewalk is. §6.4.2 follows with a comparison with the security level of other technologies the respondents used, finding that Sidewalk's security level did not play a

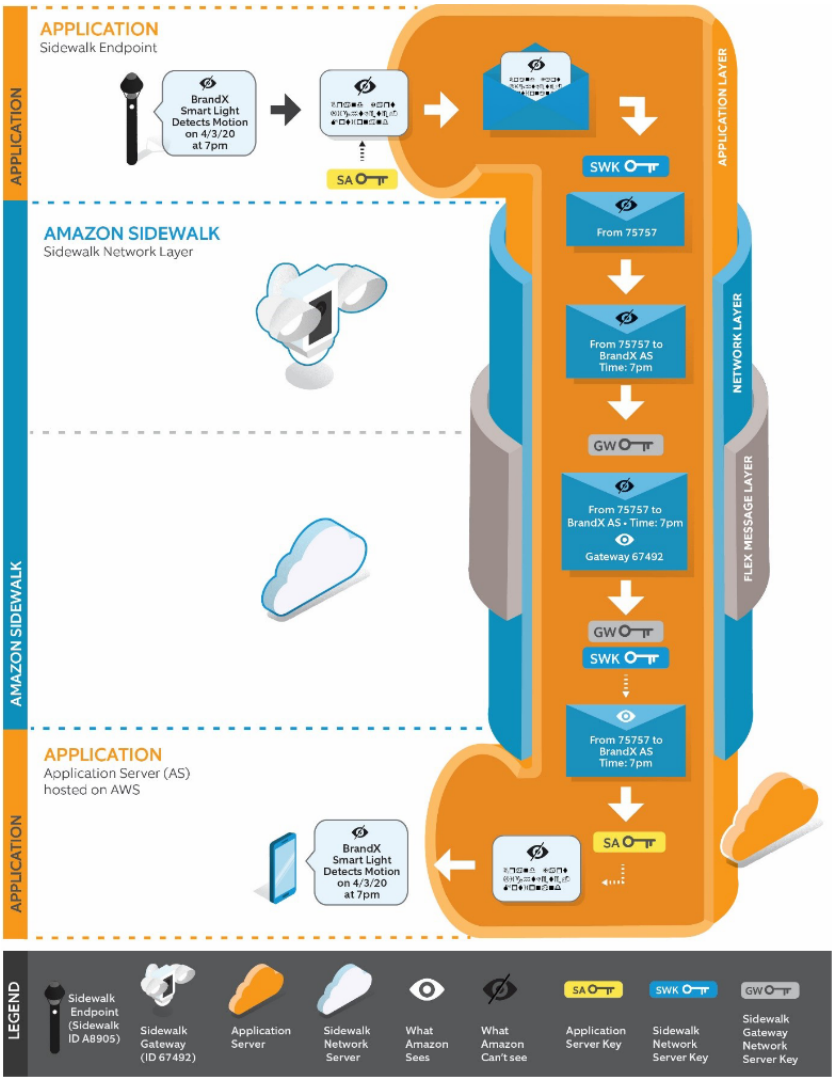

Figure 6.2: Overview of Sidewalk's end-to-end encryption scheme for uplink traffic. Reproduced from Amazon (2023n) (p. 7)

decisive role for manufacturers to adopt Sidewalk over other technologies.

6.4.1. Security of the Sidewalk protocol and architecture

There was consensus among interviewees that Amazon's security measures do what they promise, in the sense that neither Amazon, nor a gateway owner can access or tamper with an endpoint's payload data. Multiple interviewees had backgrounds in cybersecurity, and were confident in the security of Sidewalk gateways, packets in transit, and the back-end in AWS. This trust comes from Amazon's Privacy and Security whitepaper (Amazon, 2023n), and their vested reputation in the cloud computing sector, but also the fact that Amazon is open to adopters' feedback and even adjusted their security scheme after a suggestion of one of the interviewees. Only [N1] said that Amazon has a bad name and a history of damaging people's trust. Therefore, the interviewee surmises that other big companies such as Samsung will *"never ever endorse"* Sidewalk.

As §6.1 made clear, the grey literature was not as appreciative of Sidewalk's security level. Authors pointed out that Sidewalk is a novel and proprietary protocol, preventing independent scrutiny and introducing the risk that security flaws are only detected once the technology is used extensively in the field. Remarkably, these concerns did not surface in the interviews. Multiple explanations exist. First, the interviewees might be oblivious to these woes. This sounds unlikely, granted the cybersecurity background of multiple interviewees. Moreover, many were aware of grey literature criticising Sidewalk's opt-out nature, meaning that other negative articles are probably also on their radar.

Second, it could be that Amazon grants adopters exclusive access to the security protocols to convince them of their soundness. However, I doubt that Amazon would proactively provide all adopters insight into something that Amazon is shielding from the public, considering that open-sourcing the technology would also improve public trust in the technology. Third, and most probable, interviewees might brush off the concerns because of the business incentive to adopt Sidewalk and prioritise a low device price over security (following §6.2).

A number of interviewees justified the crowdsourced and AWS-centred architecture with their faith in the security measures. For instance, [A2] said *"I don't see an issue with sending data over someone else's hub. Because this is end-to-end encrypted, and it's like, everything is secure"*. In fact, [A1, A6] argue that the public fears and *"paranoia"* [A6] discussed in §6.1 are misplaced because of the security (and bandwidth restrictions) that Sidewalk incorporates. [A6] even dismissed articles that critique Sidewalk as clickbait:

> *These are topics that some companies, they'll try and put articles out that say that it's not secure, or that they're using up your Internet. But they're just doing that as what we call "clickbait", right? They're trying to scare people into reading an article, and now that they've got you, they're going to keep going down the story of paranoia, even though it's not based in any kind of reality. I mean, when I read them, I just shake my head and I say, "man, these people have not, they haven't researched anything", right. Because they're just saying silly things that are just not true, but they're just trying to play into getting people to read their articles.*

Even if grey literature authors were to conduct more research, as this interviewee desires, they would run into the limitations of Amazon only offering limited insight into the technical implementation of Sidewalk's security measures and the connection between gateways, the network server, and AWS; as I reflect on in §10.4.

[A1] also points to an, in their opinion, discrepancy between reality and public perception. They think that the public may be led to an imbalanced or inaccurate opinion because of biased and incorrect media coverage:

> *It was definitely difficult. There's like a PR piece of it that was hard, where it was like "oh, we're gonna allow people to use your Internet connection for the Sidewalk network". I didn't actually mind that personally, as a customer, I was sort of like "it's minuscule amounts of bandwidth. It's all super secured. You're, firewall between your data and the other person's data". It seemed like a pretty good architecture in some ways... But as soon as it came out, immediately the story and the media was "here's how to turn off this, like, network that's spying on you". So it's like... That's not really what's happening, but that was the perception, at least. [...] Really, the story had nothing to do with "here's this neat new network that's going to give you free Internet for emergency services or things like that". It was more like "here's this thing that Amazon's trying to get around on you, and how to turn it off". And it was like, okay, well, that's gonna be hard to get around in the future.*

This quote exemplifies what I stated in the introduction of this chapter, namely that Amazon and interviewees depict the only stakes of Amazon's remote control over gateways to be bandwidth usage and security of gateway and endpoint users. This respondent argues that with these obstacles alleviated, there is no objection to Amazon repurposing gateway owners' devices for their own financial gain.

6.4.2. Sidewalk's security vis-à-vis security of other connectivity protocols

Amazon believes that Sidewalk improves the security level of adopters in multiple ways. One road is that making devices connected to the manufacturers' servers, allows them to deploy patches and monitor devices for anomalous behaviour while they are being used (Amazon Web Services, n.d.-c). Also, in Amazon's words, using their supposedly secure communication protocol reduces the need for IoT manufacturers to obtain knowledge of and implement security measures themselves, making secure communication feasible for companies that would otherwise lack resources to make their own (Rubin, 2021). This reasoning is similar to the cases described by van Hoboken and Fathaigh (2021), where Apple and Google put regulators at ease by saying they protect privacy, while in fact leveraging control over their smartphone OSes to outcompete third-party developers. Sidewalk promises to improve security, but in the meantime expands Amazon's hold over IoT manufacturers.

In practice, the latter argument does not hold. As §8.2.2 will elaborate, ensuring that endpoints comply with the security measures (e.g. to accommodate the end-to-end encryption) significantly

complicates the production process. And none of the interviewees brought Sidewalk's security up as an argument for adopting Sidewalk. For instance, one participant said the Sidewalk privacy and security levels simply had to be on par with their existing solution before adopting Sidewalk. Another participant said that Sidewalk's security was a benefit, but not a decisive one that distinguished the protocol from others. Interviewees that use both Sidewalk and other technologies reported that even if Sidewalk traffic would be more secure than that of others, these others were still sufficiently secure for their use cases, e.g. because they use similar encryption schemes [A1, A2, A4, A5, A6, A7], or because all data is already encrypted on the device before it is sent uplink [A3, A6]. [N1] stated that Sidewalk does obscure more metadata than LoRaWAN network providers do, but never heard from LoRaWAN customers that considered this a problem.

Rather, it seems that the encryption scheme is necessary to enable Sidewalk's crowdsourced setup: because Amazon is inserting more components between the end device and cloud server (i.e. gateways, the network server, and AWS IoT), it must necessarily protect the detour.

6.5. Interviewees' perception of Sidewlak's opt-out nature

The interviewees also references the backlash from the general public that the opt-out nature of gateway functionality caused (§6.5.1), as well as potential reasons for Amazon to make Sidewalk opt-out (§6.5.2), but normalise Amazon's remote control over consumer devices by only considering user benefits and privacy risks.

6.5.1. "PR incident"

[A2] referred to the opt-out nature of Sidewalk as a *"major issue"* causing *"quite a large PR incident"*. [A3] thinks Amazon's reputation played a part in this: *"I think many people were already out to get Amazon for their, you know, buying all these companies, data, they have the entire stack. I think there are a lot of people out there already looking for something to attack, and this was a perfect... I mean, everything was there to attack it."* This respondent thus views Sidewalk concerns from a privacy as confidentiality lens, reckoning that the trove of data that Amazon processes with its myriad services and companies generates the negative reactions.

In the opinion of [N1], though, *"it's not a media storm; they've done a press release every year the past 4 years, and in fact they've sent out the same press release every year. [...] And they've been saying the same thing for 4 years. In the end, nothing has happened every time"*. That same interviewee said *"I still find it super fascinating that there is no... I think if you had done this in Europe or Germany, all hell would have broken loose. [...] I also find it very special that they can get away with [this opt-out method] in America"*. It is unclear to me, though, what the interviewee would consider to be a reasonable public reaction, beyond the negative press. Did the respondent expect a massive opt-out campaign? A boycott of Amazon's services? Regulatory intervention forcing Amazon to make Sidewalk opt-in? Regardless, I think they mean to say that Amazon has managed to normalise their remote control over and repurposing of consumer devices for their own financial gain; a sentiment I can only agree with.

6.5.2. Rationale behind the opt-out

This backlash begs the questions whether Amazon foresaw the criticism and what motivated them to pursue the opt-out scheme. [A2] thinks Amazon was well aware of a potential *"adverse reaction"* of the public, basing their belief on Amazon's early communication strategy around Sidewalk. Judging by their press releases preceding and accompanying Sidewalk becoming public, the respondent hypothesises that *"maybe that was the plan all along, to make people aware of how good the security was so that people wouldn't mind doing the opt-out approach. And then that backfired. I honestly don't know. But that might be one way"*. The interviewee then echoed the grey literature (§6.1.3) in surmising that the opt-out nature was fundamental for Sidewalk's vast coverage throughout the US, but said Amazon had to justify it with the security measures.

[A3] similarly thinks the opt-out scheme was fundamental for realising Sidewalk's pervasive coverage. Their hypothesis is that consumers' knowledge of what Sidewalk is, how it could be turned on, and how it can benefit themselves and others would be too low to achieve a meaningful number of participating devices: *"if you ask the consumers, 'do you want to have [Sidewalk] on', their level of consumer knowledge is so low that they don't really know what it means."* Today, the interviewee still sees a lack of awareness when interacting with their customers: *"The consumer level of understanding of [Sidewalk] is not very high,*

typically. The fact that you just say that it works with your Echo is usually good enough." This interviewee thus first dismissed the security concerns by security experts in popular media, and subsequently dismissed consumers for a supposed lack of expertise about how Sidewalk works and what it has to offer. They did not elaborate which other actor could, in their eyes, present a fair and unbiased assessment of Sidewalk. Surely, it cannot be the interviewee themself; despite their cybersecurity background making them able to understand the technology, they have an obvious economic incentive to trust Sidewalk.

[N1] also notices the limited consumer awareness. They ascribe it to a scarcity of marketing by Amazon, leaving customers uninformed about the possibility to leverage Sidewalk connectivity from their own or someone else's nearby Echo and Ring devices. This lack of marketing can, according to the respondent, be explained by Amazon *"operating very much in a grey area. They are building a network... No, they are not building a network; they are* using *a network that is not theirs and that they also have not asked consent for"*. [N1] thus seems to be the only interviewee that does not excuse the problems they see with Sidewalk – probably because they are the only non-adopting respondent.

A consequence of this lack of marketing, that [N1] has heard about from other parties in the market, is that consumers are unaware of what Sidewalk is and that it likely works in their homes, too. Consequently, smart-home-oriented Sidewalk adopters have a hard time selling their endpoints to consumers. It could be that the lack of consumer-oriented awareness creation by Amazon about Sidewalk is deliberate, as this participant surmises, to not draw attention to Amazon's control over consumer devices. The downside would be that Amazon then misses out on end-users buying Sidewalk-compatible devices, as [N1] indicates. This might be less of a problem for Amazon than it seems. After all, the majority of Sidewalk adopters is B2B-oriented, which interviewees reported is a more scalable business model (§5.3). Hence, the volume of business users (or the amount of endpoints they use) might compensate for the lack of consumer users.

6.5.3. Normalisation of infrastructural power

[A4] contrasted the Sidewalk backlash with Apple's roll-out of their Find My network: a crowdsourced, Bluetooth-based, and PET-using network wherein Apple's phones, tablets, desktops, and laptops report the approximate locations of lost devices to Apple's cloud or to other participating devices, to help the owner locate it (Apple, n.d.-a; Edwards, 2021; Fleishman, 2021). Apple rolled out this functionality in opt-out fashion (Fleishman, 2021). The opt-out means both that the device cannot be found by others, and that the device does not contribute to the network by locating the reports of other devices (Edwards, 2021). [A4] found this opt-out strategy *"actually quite surprising, but nobody has really pushed back against that. Whether or not you ever own an AirTag, your phone is reporting information about AirTags"*. The respondent did not clarify where they think this difference comes from. A potential explanation is that Apple markets itself as a privacy-friendly company (see e.g. Apple's privacy webpage Apple (n.d.-d), showing in big font *"Privacy. That's Apple."*), giving it a better public reputation concerning privacy. On top of that, Find My benefits not only AirTag owners, but also iPhone and Mac owners, as these can also be localised with the network. Conversely, gateway owners' benefit of Sidewalk might be less, if their own gateways already have connectivity, and if they have no other endpoints.

Another interviewee saw the latter happening in the case of Xfinity Connect, where the US telecommunications company Comcast remotely updated their customers' routers to become *"Xfinity WiFi hotspots"* in opt-out fashion, that other customers could connect to (Comcast, n.d.-b). The respondent implies that its users experience cognitive dissonance and choose to ignore the security benefits because the service makes expensive data plans redundant: *"it was a Trojan Horse, but it provided a lot of positive benefit for people. But people don't wanna acknowledge that it was a Trojan Horse and that it is an inherent security risk"*. However, they also think this benefit would not have been realised without its opt-out roll-out, and notes that many people are therefore not even aware of the security risks: *"I have a lot of friends that use it, my wife uses it, a lot of people use this Xfinity Connect thing and they have no idea where it comes from. They think it's just out there in the world or something. But it's really on everyone's individual routers. [...] they didn't ask anyone, they just turned it on. And then a year later when they had this massive network, then they said 'now you can use Xfinity Connect anywhere you go'"*. The public *"didn't attack it from a security perspective. They just kind of trusted it, and they just used it. And then it became real."* They also referred to Sidewalk as a *"Trojan Horse"*, that has its benefits but also security risks. This is an interesting frame, because the interviewee had said earlier that they trust the security mechanisms that Amazon has put in place.

These cases differ from Sidewalk, though. The interviewees imply that Amazon incurred backlash because the public despises Amazon, or because its roll-out was more visible and less beneficial to gateway owners. However, Sidewalk is a much more elaborate ecosystem. Amazon uses gateway owners' devices to offer a whole new service to IoT manufacturers and, through that, pull manufacturers to their cloud environment. Sidewalk affects the way wherein manufacturers produce their devices and software, requiring grand effort from them to become compatible (demonstrated in Chapter 9). This is similar to Apple Find My (as I explore in §10.5.2), but the cloud environment and hardware re-engineering burdens are presumably lower. And as for Xfinity Connect, only Comcast benefits by increasing customer value and by selling separate plans for wifi access 'on the go' (Comcast, n.d.-a). Therefore, reducing Sidewalk concerns to questions of privacy and security does not cut it.

In sum, these respondents only evaluate the desirability of Apple, Comcast, and Amazon to repurpose consumer devices by weighing user benefit with privacy and security concerns. This demonstrates an apparent normalisation of their construction of build crowdsourced infrastructures, and hence of their infrastructural power.

6.6. Chapter conclusion

Amazon's materials about privacy and security, limit these concerns to a matter of keeping endpoint and gateway user data and identities confidential. With this reductionist frame, Amazon manages to present privacy as something that can be solved through technology; namely PETs. And they have steered the discourse successfully: when I asked interviewees about Sidewalk's privacy and security, they took a user privacy angle (§6.4.1, §6.5.1). Similarly, literature about Sidewalk almost exclusively takes concern with Sidewalk from a user privacy lens, at most bringing its possibilities for surveillance into view (§6.1).

This frame benefits Amazon in multiple ways. First, it is necessary to proclaim that the opt-out roll-out and crowdsourced architecture pose no risk to gateway and endpoint owners (§5.1). Both Amazon and interviewees used this argument to justify the opt-out scheme, saying that the benefit of Sidewalk's huge coverage combined with its PETs (and bandwidth limitations) leave no harm to consumers (§6.5).

Second, Amazon touts privacy and security as unique advantages of Sidewalk that could improve the security of the IoT, presumably much to the liking of regulators (cf. van Hoboken and Fathaigh (2021)). Offering a ready-to-use, secure technology allegedly reduces development efforts, while enabling patching of live devices. In practice, while interviewees trust the security level, it does not distinguish Sidewalk from other LPWAN protocols (§6.2, §6.4).

Third, adopting Sidewalk is not an easy feat. Amazon repeatedly submits privacy and security as reasons to justify its strict governance and instruct manufacturers on configuring their production, as subquestion 3 and Chapter 8 will assert.

Largely absent from public discourse is the skewed distribution of gains between Amazon and gateway owners. The many use cases of Sidewalk for Amazon, endpoint manufacturers, and endpoint users (5), are only possible thanks to gateway owners not opting out. These people are crucial contributors to Sidewalk, by purchasing the gateway, placing it somewhere throughout the US, providing it with electricity and WiFi, and replacing it when it is faulty. While Amazon and manufacturers reap the business opportunities that gateway owners' participation generates, gateway owners are compensated with only a sense of community (§5.1) – granted they are even aware of their device's dual use.

This is a broader trend, as interviewees pointing to a lack of backlash about Apple's Find My network signifies. If this is indeed due to Apple's self-proclaimed reputation as privacy guardian, or the utility of finding devices outweighing the perceived small harm that crowdsourcing this service brings end-users, then this represents a grave oversight in popular and academic literature, because user privacy is not the only value at stake. For instance, neither literature nor interviewees mentioned that confidentiality of manufacturers' business practices might be visible to Amazon, unless I asked them about it. This is the subject of Chapter 7. Other concerns are that Amazon grows their power through this privacy focus, as the rest of the thesis will elaborate.

7

Amazon's unique vantage point

In Chapter 6, I found that privacy and security concerns about Sidewalk are generally reduced to confidentiality of user data and identities. However, Amazon routing all Sidewalk traffic through AWS, suggests they can learn how endpoints operate. On top of that, they manage AWS, and can therefore learn how manufacturers configure the back-end, i.e. manage their Sidewalk endpoints. In this chapter, I examine whether Sidewalk's PETs protect the confidentiality of manufacturers' business-sensitive knowledge, providing the final component to answering subquestion 2 (*"What role do privacy-enhancing technologies play in Sidewalk?"*).

First, §7.1 discusses the Sidewalk and AWS *"usage information"*, i.e. data endpoints' attributes and interaction with Sidewalk, and associated business logic in the cloud, that Amazon has insight into. §7.2 elaborates that interviewees had highly varying perceptions of the value of this usage data for Amazon. Abuse of this position as an awkward *primus inter pares* looms, given Amazon's of leveraging their vantage point on their Marketplace to unfairly compete with third-party sellers (§2.2.4). Therefore, I asked interviewees whether they expect Amazon to leverage insight into their usage data to fuel development of competing endpoints, as §7.3 explores. To conclude, §7.4 reflects on the chapter, and assesses what purpose the usage data contributes most significantly to.

7.1. Usage data visible to Amazon

Before the interviews, I examined the technical documents of Sidewalk and AWS mentioned in 3.2.3 to determine which Sidewalk data Amazon can see. These documents express both the information that Amazon (allegedly) needs to make Sidewalk work, and what variables are in a Sidewalk packet. I verified and supplemented this list during the interviews, because the interviewees have first-hand experience with developing towards Sidewalk and working with the technologies. Based on these exercises, it can be stated that the information Amazon can see about endpoints, includes at least the endpoint's manufacturer; a persistent identifier, recorded during device provisioning (Amazon Technologies, 2024, p. 54) (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"* (Amazon, 2023n, p. 14)); the identifier of the gateway that the device uses to connect to Sidewalk; the endpoint location (by knowing the associated gateway's location (see §C.6.2 for details)) and therefore also how many devices are in a certain area; the endpoint's communication mode, profile, and parameters (see §8.2.1 for what this entails); the signal quality; unspecified *"auxiliary device and user data"* that the *"IoT asset services"* provides the application server with (Amazon Technologies, 2024, p. 46); and the amount of and interval between data transmissions; and an identifier of the application server (Amazon Technologies, 2024, p. 53). I further refer to this data as *"usage data"*, after [A3] labelling it as such.

7.2. Value of usage data for Amazon

What is the use of this usage data for Amazon? Interviewees saw multiple applications, namely enhancing the reliability of Sidewalk (§7.2.1), improving Amazon's IoT offerings (§7.2.2), and most significantly, improving AWS to make it more attractive to both Sidewalk adopters and IoT companies more generally (§7.2.3).

7.2.1. Enhancing Sidewalk's reliability

Logically, usage data provides Amazon insight into the integrity and reliability of Sidewalk. In [A2]'s eyes, usage data being available to Amazon *"is inherent. I mean, they need that in order to drive, to operate. So they need that. Just as we need some metrics to see if things actually work, then they need metrics to see if things actually work. You can't really get away with it, I think."* Similarly, [A6] says: *"as far as network operations, yeah, I'm sure they could glean some information. They certainly are able to see, for example, the location of the device, the interval of data, the quality of the signal. These are important things for making sure the network is reliable, though, so those types of network metadata I'm not really concerned about. They even know which Echo is transporting the data. We don't. That type of thing is hidden from even us, as operators, and that's just for, you know, identity protection of the people that are part of the network."* These manufacturers understand Amazon's desire for metadata, as they collect metadata to improve their endpoints, too.

7.2.2. Enhancing Amazon's IoT offerings

Further, Amazon can leverage their vantage point to improve their own IoT offerings. They can both learn the demand for certain types of third-party devices, and learn how they function to enhance their own products, although two respondents think this benefit is negligible.

Four interviewees mentioned the value of Amazon seeing which products are popular. [A3] thinks *"there's probably a lot of value in that kind of data. [...] I think it's brilliant. [... Y]eah, of course they're gonna learn about it and learn what markets are hot, and maybe build devices or solutions for those markets, like any other company would do"*. [A8] expressed a similar expectation. [A1] said *"it's possible. I mean definitely, I wouldn't put it past Amazon. They definitely have used data about their partners to come up with products to compete with them"*), referring to the Amazon Marketplace case (§2.2.4).

[A7] and [A4] not only expect Amazon to utilise usage data for this purpose, but confidently asserted that they are already doing so: *"What you say is still happening right now. They're looking at all the traffic. They are forcing people, or definitely to funnel people to use Amazon Cloud for the service. Right. And then looking at who is selling better, and then reprice whatever they OEM from Asia, again to fight against you. This is going to happen, and there's no doubt. Even if I were an Amazon manager, I'll do the same. This is the privilege, right? I have all the intelligence in front of me, why wouldn't I make use of it?"* [A7]. [A4] made the same argument, and also raised the Amazon Marketplace example: *"[T]hey of course are also collecting data on what kind of engagement they're getting and is this a viable product. Amazon is turning... You know, if you're familiar with Amazon Basics, they take high-volume competing products and rebrand them for themselves all the time. So I'm mentioning this, just because this is the recurring pattern with these large companies."*

[A2] nuanced that Sidewalk usage data does not enable Amazon to analyse the total IoT market, because Sidewalk is not used by all IoT devices: *"it's quite natural that Amazon use the information that they get from this. Like, they probably have people looking at the total available market for certain types of devices to see if they want to go into that field of business. And then that's something that they can see. But again, they would only see a snapshot of it, right? Because not everything is on Sidewalk. Quite few things are on Sidewalk, actually, so..."* Regardless, Sidewalk adopters are active in such a wide range of market categories (see Table B.1 in §B.1) that the insights need not represent the *"total available market"* for them to be useful to Amazon.

In addition to learning what endpoints are popular, monitoring their behaviour informs Amazon how they work under the hood. This could help them in developing their own endpoints. For example, the usage data might teach Amazon about *"power usage, connectivity usage, and data transfer"* patterns [A8], and *"might help them if they were gonna do things like [design] their battery model for their [device] and figure out, you know, how many times someone [triggers the device] or something like that"* [A1].

Three interviewees suppose that the encryption of payload data inhibits their learning of how IoT devices work. According to [A2], *"it's quite a lot of interesting data for Amazon. But it's the fact that we are a device, not our data, that they would see"*. [A1] believes that Amazon would have to do *"a lot of inferring"* if it wanted to learn from Sidewalk devices, because of the encryption scheme. And even then, they think the information is not as valuable that it would warrant what the interviewee calls *"stealing information"*, rather than figuring it out themselves.

[A8] said *"they could definitely use it. I mean, the one thing that they were very interested in with their development is, they wanted that data from our sensor. And so they* have *that, they have access to that, so they can see what we're doing with it. But they can't necessarily see what we transfer* with *it, right? They just see the activity. Which is probably going to drive their developments for other sensors. [...] But they don't get the back-end, like how we're triggering things with it, or what we're connecting to it, necessarily"*. Amazon's interest in their

sensor can be explained by Amazon selling an IoT device that offers a subset of the functionalities of the interviewee's endpoint. Moreover, I doubt the accuracy of the latter statement, because Amazon also sees how companies use AWS. While perhaps not seeing the exact operations performed on the data and how precisely devices are managed, Amazon can see what IoT services manufacturers use, and as such infer what logic is needed to operate this back-end.

[N1] disagrees that the payload encryption prevents Amazon from distilling knowledge from payloads. They think Amazon can still do so using machine learning techniques: *"[a]nd with all these neural networks and things like that: everybody also knows that, you can protect that data, but of course, with all these neural networks, you can actually extract so much data from the metadata already. So yes, you can say 'well, you can't see the payloads', but of course that's not enough."*

7.2.3. Enhancing AWS for IoT applications

Only [A4] explicitly pointed out what is, to me, perhaps the largest benefit of Amazon's vantage point. Having stated that Amazon can learn about which device types are popular, they continued that Amazon has previously managed to cater their AWS services aptly to the needs of their customers, based on their interactions with AWS. Thus, the usage data could come in handy for seeing how services in AWS could be improved:

> *To credit Amazon, with AWS in particular, they were early, 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.*

By monitoring both how endpoints interact with the cloud (leveraging their control over Sidewalk), and how manufacturers set up the back-end to manage these endpoints (leveraging their control over AWS), Amazon can optimise their AWS offering for IoT use-cases. Not only does this streamline the experience of Sidewalk adopters; it also improves the operations of IoT companies that use Amazon's IoT services without Sidewalk.

[A5] implicitly hints at the significance of this premise. They did not explicitly point out the importance of making AWS attractive to IoT manufacturers, but did doubt the value of usage data for Amazon's business model: *"I don't know, really logically, what they would get out of that. You know, and again, you have to... The ultimate AWS business model, if I had to boil it down to one single statement, the business model is 'data has gravity'. So they want the data coming to AWS. [...] That's where they make their money"*. While I argue that AWS' promise to manufacturers goes far beyond 'data', by offering services for operational control and flexibility in developing and managing devices (see §9.2.1), this interviewee underlines that selling endpoints is not Amazon's main revenue generation model. Rather, Sidewalk is an exercise for Amazon to optimise their cloud infrastructure for the entire IoT, regardless of how the devices are connected to AWS.

7.3. Potential of leveraging usage data to compete with manufacturers

Numerous interviewees mentioned Amazon's ability to leverage usage data to launch competing products. Presently, Amazon's only endpoints are the Echo and Ring devices that double as a gateway (see §4.3). Based on Amazon's press releases around Sidewalk, technology watcher blogs, an interviewee's experiences inside Amazon, and interviewee's expectations about Amazon's Sidewalk ambitions, I argue in §C.7 why Amazon is likely to launch more endpoints in the future. Granted this observation, I inquired with respondents whether Amazon potentially informing their endpoint development with usage data that manufacturers generate, causes them concern. For most participants, this was not the case (§7.3.1); only 1 participant expressed worry (§7.3.2).

7.3.1. Not concerned

5 participants were not concerned about Amazon potentially launching endpoints that would compete with their own. Some think Amazon will not enter their line of business in the first place. [A5] thinks Amazon is not interested in their market, because they think AWS' business model is *"data has gravity"*, as elaborated in §7.2.3: *"I mean, AWS is not gonna go out and build [competitors to our products], you know, it's just not their business"*. [A3] thinks Amazon is more likely to compete with other Sidewalk devices

in *"commoditized spaces"*, i.e. *"dumb sensors"* that *"all do the same thing"* with *"very little differentiation"*; contrary to their own devices that qualify as *"smart"* because of their capabilities and security model. Still, it does not seem unlikely that Amazon's very advantage as a service provider allows them to learn how these *"smart"* devices work and copy them.

Others believe strongly that their company's capabilities (e.g. *"Bring them on!"* [A2]), intellectual property and patents [A3], and time that their company has been active in their respective market (*"[W]e've been doing this since the beginning. They know that we've been doing it since the beginning, there's enough stuff on the internet around us doing it since the beginning, that I'm not worried about that"* [A3]) will let them outcompete Amazon. I personally doubt that consumers will care which company 'did it first', and mostly think with their wallets. Compared to the interviewee's company, Amazon could sell the devices at a lower price point: both because they have deeper pockets to finance selling below cost price in order to gain an edge in the market, and because they could produce at a far larger and more efficient scale to drive the cost price down. Moreover, Amazon could sell endpoints under their established brands to leverage their reputation. As such, the reputation of [A3] might put them above a new, no-name copycat, but this might not hold for Amazon.

Further, multiple interviewees think Amazon might compete with them, but not on the short term. They think that Amazon's offering of Sidewalk and their own endpoints help to grow the market, spurring revenues. This is yet another unmentioned benefit that Sidewalk brings, besides the promise of connectivity. The respondents did not provide definitions for the markets they refer to, but it seems to be the market of low-resource IoT devices, as well as connectivity protocols for them, in their respective market domains.

One of these interviewees is [A2], that only sees risks for their own competitive position on the long term. Their organisation prioritises short-term revenue over long-term profit:

> *you have this curve basically* (pictures bell curve with fingers) *that if you have a market that is immature and people aren't really aware of it, the only thing that would happen if Amazon entered the market would be that the market grows. And then eventually when that phase is over, then you get competitiveness in pricing and stuff like that. And that's long-term hurting our profit. But short-term increasing revenue, because more people get aware, and we get kind of pulled along the marketing machine of a bigger company. So that's nice.*

The argument of Sidewalk growing the market and increasing customer awareness was echoed by other interviewees [A7, N1]. [A7] termed Amazon's launch of their own endpoints and connectivity network a *"double-edged sword"*: *"Without them, I think there is a level of market education that we would not be able to achieve. With them, we are using it as an advertising expense, to bring the market up with the knowledge of LoRaWAN."* For this reason, they think LoRaWAN cannot compete with other technologies such as wi-fi and cellular: *"we are peanuts, in terms of values, right. Very honest. Because these are all multi-billions, tens of billions of dollars sectors. But LoRaWAN is not. So there's no reason to compete, and not much to compete. But more of a missionary effort as a market pioneer like us, or like LoRaWAN side or like Sidewalk side, we are all doing effort of acting like a missionary to the market, to tell them that this is available."* Similarly, according to [N1], the market is not a *"zero-sum game"*, so that *"the benefit of them growing the market, is much bigger than the most negative scenario of them replacing technology"*.

[A7] acknowledged that their organisation might at one point find themselves competing with Amazon, but they actually see benefits in what they termed *"coopetition"*. The interviewee thinks they need Amazon to reach the aforementioned market education and growth, to what could be called 'grow the pie'; but they could then start to compete with Amazon to grow their own share of the pie:

> *We don't prevent that, we* use *that, to a certain level of resource investment. You know, either way, we need to spend money, right? We need to invest. So, either I invest in R&D, or more product; or we invest in cooperation with Sidewalk and salvage whatever intelligence we can have, as an entry level cooperation, right. "Come on, let's share. We build this for you, and then you share some information for me, in exchange." So this is more of a business* coopetition *mindset. You cooperate, while compete, and so don't expect that you win all; you give and take something in between. And then let time flows, if things all went well, you know, we are married happily ever after; if things didn't go well, well, we are two independent entities, that we could spread and find our own roads. So at this moment I would say the next 3 years, 3-5 years, it will still be a stage for our cooperation with Amazon for sure.*

> *And then maybe by the 5th year, there might be a crossroad, that we have to review the status of the cooperation,* perhaps*. I'm just guessing, don't take it for granted, okay?*

These quotes signify that IoT companies operate mostly with short-term visions. Either they (wishfully) think they can outcompete the giant Amazon, or they accept the risk of Amazon outcompeting them as the cost of doing business.

7.3.2. Concerned

Only 1 interviewee reported concern about Amazon competing with them. This concern did not pertain specifically to competition by Sidewalk endpoints, but by *"platform moves"* generally. The interviewee stated that *"things that the company has done with success are encroached on by Apple and Google and Amazon over time"*. When asked whether they defend themselves from this in the case of Sidewalk, the reply sounded powerless:

> *No, I mean, it's been a fairly open, transparent partnership. I think they do ask, of course, when the business development teams would meet up, they're like, "Hey, we hear you're launching a [similar] product, when do you think you might do that?" But no, we don't... We're concerned, of course, but in the end there's not a whole lot we can do about it, you know, aside from government action or lawsuits.*

It sounds as if the company can at most hear from Amazon's plans and adapt their own business in response, while relying on legal or regulatory action to combat this encroachment. This speaks volumes about the power dynamics between Amazon and their adopters, especially when realising that this same respondent adopted Sidewalk primarily for their multiple business relations with Amazon rather than the functionalities that Sidewalk provides (§5.6).

7.4. Chapter conclusion

Whereas the literature on Sidewalk and interviewees consider privacy and security of Sidewalk from a user angle ((§6.6), the interviews and technology of Sidewalk also reveal the trove of usage data that Amazon has insight to. This includes at least device's location, battery level, connectivity, communication mode, manufacturer, and persistent identifier (§7.1). Striking is that the interviewees that agreed that Sidewalk's PETs do not protect the confidentiality of how their devices work. Interviewees never raised this when I asked their opinions about Sidewalk's privacy and security level, meaning they had either not considered this, or did not have it top-of-mind; the latter being the result of Amazon's reductionist reframing of privacy to confidentiality of user identity and data.

The utility of this vantage point to Amazon is threefold. First, this usage data enables improving Sidewalk itself. Second, it may fuel Amazon's development of their own endpoints. Amazon has an edge over adopters, because as the network provider, they could self-preference their endpoints. In this context, multiple interviewees referenced Amazon's previous (ab)use of third-party vendor data and self-preferencing on their marketplace (§7.2.2, cf. §2.2.4) However, Amazon need not even go that far: the usage data already informs them which device types are popular in what regions, as well as how they have to communicate with the cloud and be managed therein.

Not all interviewees were concerned about this possibility for competition, which is striking given how many interviewees pointed out the Amazon Marketplace example. I sensed some naivety and pride in adopters' own products. In addition, some interviewees focussed on short-term rather than long-term profitability, and others think the profit for Amazon is not in selling devices but in *"data"*. Interviewees that were concerned, accepted this risk as the cost of doing business with the tech giant Amazon, and hoped for regulatory protection.

This brings me to the third benefit: Amazon can further tailor their AWS offerings to suit IoT manufacturers' needs. As such, they can make AWS a more attractive production environment not only for Sidewalk adopters, but for any IoT company. Here, the combination of seeing Sidewalk and AWS usage simultaneously is of great benefit to Amazon. §9.2.1 will detail further why I expect this aspect of the vantage point to yield Amazon the most value; in connection to Amazon's main business not being hardware sales.

Whereas I pointed out a lack of conversation about the fairness of resource distribution in §6.6, this Chapter is reason to call for making manufacturers aware about how Amazon learns from their practices to better their own business; whether that is for directly competing with them or not.

8

The effect of adopting Sidewalk on manufacturers' production

So far, I have established both the benefits for manufacturers, and the privacy and security concerns for manufacturers and users that Sidewalk brings about. To address these concerns, Amazon has designed PETs and governance mechanisms for Sidewalk. Complying with these mechanisms, which is necessary for aspiring adopters to attain the benefits of Sidewalk, requires them to invest significant efforts into the production of their endpoints. I examine this effect in this chapter, as a first step to answering subquestion 3: *"How does Amazon's technical design and governance of Sidewalk affect the production of IoT devices?"* The second step in answer the question is assessing how these efforts craft a dependency relation between manufacturers and Amazon, as Chapter 9 investigates.

For the first part, I start by sketching how Sidewalk is governed. Following Van Hoboken and Fathaigh (2021), I classify Amazon's governance of Sidewalk as taking shape through policy and enforcement measures (§8.1) and through technology (§8.2), although Amazon also effectuates the former using the latter. I devote special attention to the centrality of AWS, and whether manufacturers and end-users have alternatives to managing endpoints using Amazon's cloud services (§8.3). In fact, Sidewalk's governance disadvantages adopters in multiple ways (§8.4). Last is a conclusion (§8.5).

8.1. Governance of Sidewalk through policy and enforcement

Companies that want to adopt Sidewalk cannot get all the information they need right off the bat; Amazon first needs to approve them (§8.1.1). In addition, several obligations come into view for aspiring adopters. Amazon organises periodic meetings with each adopter (§8.1.2) and audits their organisation and the partnered factories (§8.1.3). Further, Amazon created Sidewalk usage requirements that define (non-)functional requirements for endpoints during their operation (§8.1.4). Finally, when the adopter has finished designing a device prototype, it has to pass a qualification process (§8.1.5).

8.1.1. Not publishing requirements until manufacturers have contacted Amazon

In its early stages, Amazon maintained secrecy about how Sidewalk worked. Only companies admitted to Amazon's closed alpha and beta programs received information they needed to manufacture their devices. While confidentiality during development phases is common industry practice, it resulted in one interviewee's company having to change which chip OS they used; they already anticipated Sidewalk adoption but did not know which OS to use.

After this modification, they had to change to yet another OS, *"for whatever reason, the powers that be, whether it's due to the company that makes the processor that we use, or something internal of Amazon, or something else; we were required, specifically because of our hardware setup, to then switch into another RTOS [Real-Time Operating System] that they were adding in for support."* The interviewee understands that *"[t]hese are kind of the pain points of going through beta processes with companies as they iron out how they want the long-term experience to be for everybody else"*, resulting from the interviewee's role as *"their guinea pig"*.

It should be noted that Sidewalk is now in a public stage and the developer documentation is mostly public. Still, for some information, prospective adopters must contact Amazon by email or sign up for a

development console that requires approval of the Sidewalk team (e.g. Amazon, n.d.-h). Thus, Amazon has been, and still is hiding information from prospective adopters. This practice slows manufacturers slowed down in their product development, and even causes them to invest into the wrong technology, as the RTOS example illustrates. Apparently, manufacturers simply accept this as an acceptable hoop they have to jump through in order to become Sidewalk-compatible, demonstrating the leverage that Amazon has.

8.1.2. Periodic meetings

Amazon hosts periodic check-in meetings with their adopters, where they elicit feedback from manufacturers. These meetings are a good opportunity for Amazon to resolve issues that manufacturers run into, and receive their feedback, as §9.5 elaborates upon. However, I conjecture that these meetings also pose an avenue for Amazon to keep close tabs on the manufacturer's product plans, and learn from their development processes to inform their own product and service development. For instance, Amazon may learn what AWS functionalities adopters desire. They can then tweak AWS not only for this adopter, but generally for IoT companies using AWS. This way, Amazon makes good on the costly endeavour of structurally conducting meetings with each individual adopter.

8.1.3. Organisational auditing

Amazon also scrutinises prospective adopters to determine if they are fit to be allowed onto Sidewalk , as one respondent, an early adopter of Sidewalk, elaborated on: *"[Amazon] audited the company, they audited the objectives of the company [... T]hey 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. They also needed to understand what our technical capabilities were, because these, especially in the very beginning, the efforts to make it work were pretty complex."* The interviewee also shared that after passing the tests, Amazon reserves the right to re-audit or recertify the organisation at later stages.

It seems probable that Amazon was specially looking for technical capabilities and financial sustainability because Sidewalk was still in an early stage when the interviewee adopted it. The interviewee indicated that *"we were their guinea pig"* that necessarily had to be receptive to and able to deal with frequently occurring changes. But Amazon also verified their *"market potential"* to contribute to Sidewalk's marketability: they considered the interviewee's company *"a very strong opportunity for Sidewalk to show off what it can do"*. Thus, Amazon wanted to make sure that the resources they invested in on-boarding the company to Sidewalk were not in vain, while in that very process burdening manufacturers with changing technical requirements (see §8.1.1).

It should be noted that this information was shared by a participant that was involved with Sidewalk from an early stage. It could be that Amazon only went to this extent of organisational auditing because Amazon wanted to tread carefully while Sidewalk was still in a developmental phase, looking for partners that would last until their adoption was finalised.

8.1.4. Usage policies and program requirements

Amazon furthermore regulates how endpoints in operation may use Sidewalk and should be managed by manufacturers. With Amazon being the sole party to govern the network, I asked participants about their awareness about, opinion on, and experiences with these policies and usage requirements. I show here that these policies constitute more examples of how Amazon asserts itself in production and deployment of IoT devices, using the arguments of privacy and security.

Before I go there: what do the usage requirements govern? For one, endpoints must be reliable and contribute to *"an overall good customer experience"* (Amazon, 2023l). As illustration, the Sidewalk qualification may be revoked if a device or adjacent service suffers from repeated disruptions or latency (Amazon, 2023l). Second, Amazon wishes to protect the integrity of Sidewalk (devices). For instance, endpoints must comply with the Sidewalk technical specification, e.g. respecting the uplink rate limits (Amazon, 2023d). Manufacturers must provide security updates for endpoints as long as Amazon says so (currently *"no less than 4 years from the last shipping date of the device"* (Amazon, 2023f)), and also address any encountered vulnerabilities within a time period that Amazon defines (Amazon, 2023l). Further, if the manufacturer finds a vulnerability, they must immediately notify Amazon and *"take all appropriate steps to remedy such vulnerability, including cooperating with [Amazon]"* (Amazon, 2023e). Third, specified

in Amazon (2023e), manufacturers must propagate Sidewalk updates that Amazon publishes to all endpoints, again within a certain period. Amazon may use this content for *"firmware update, reporting, or debugging purposes"* and requires manufacturers to share the metrics collected with Amazon. Somewhat ironically, the terms forbid manufacturers to monitor *"the availability, performance, or functionality of any of [Amazon's] products or services"* (Amazon, 2023e). Finally, the policies are prone to change over time (Amazon, 2023l). For example, in the February 2024 version of the protocol specification (Amazon Technologies, 2024, p. 18; Amazon, 2023h), Amazon changed the uplink traffic rates (i.e. how many messages an endpoint may send within a certain time) and added a daily limit compared to the March 2023 version (Amazon Technologies, 2023b, p. 19), that had (different) traffic rates and lacked this daily limit. Finally, manufacturers may not charge customers for using Sidewalk (Amazon, 2023d). Manufacturers found to infringe these policies can see their keys revoked by Amazon, meaning their endpoints can no longer connect to Sidewalk.

Some interviewees were not aware of the requirements imposed. The respondents that did know about them, found the obligations they lay down reasonable. One commented: *"The first time [Amazon] notice[s] the customer doing something they don't want to, then it's a discussion, and then they might throw them out, and then they will tell others that 'we're gonna throw you out if you do this'"* [A2]. This quote highlights that the terms are subject to change; that adopters rely on others not to abuse the service so that their own autonomy is not restricted; and that Amazon indeed holds a powerful position by being able to kick anyone that they deem an 'abuser' off the network. When I remarked to [A2] that Amazon then has a great responsibility to not abuse this power, e.g. for competitive reasons, the interviewee replied with a deadpanned *"Yep"*. They then went on to discuss the reciprocity that they presume will prevent Amazon from doing so. Chapter 8 will elaborate this point, but find that the Sidewalk ecosystem lacks reliable checks and balances, and that manufacturers rely more on Amazon than vice versa.

Another interviewee downplayed the risk of Amazon abusing their power, because they have close communications with them. Allegedly, they could communicate any issues they have with Amazon's governance: *"if they propose something that's going to negatively affect our customers, we're able to communicate that. And the amount to which we communicate that, is how seriously they'll take it. If we just say, 'hey, we don't like that', they may say, 'well, you're gonna need to come up with a reason better than 'you just don't like it'', right? 'Explain it better. Help us understand.' And if we do, and we have a very clear reason for it, they'll actually understand it and appreciate, they'll escalate it, and they'll try to actually protect our interest in that, which is, it's really nice."* This demonstrates yet again that the adopters' relation with Amazon strongly defines how Amazon treats them, perhaps causing inequality between adopters. There is no formal guarantee (e.g. in the form of a code of conduct or contract), though, that Amazon will consider all feedback openly, thus the adopter still relies on Amazon's attitude. [N1] explicitly pointed out this risk in collaborating with Amazon, claiming that *"the nice thing about Amazon is that you know that you can't trust them"*.

Finally, Amazon retains the ability to adjust the pricing model for all these services, if they so desire [A1]. Garnering a sizeable adopter group by offering a service for free, to then monetise the service, is indeed a popular business model (Pauwels & Weiss, 2008; Witell & Löfgren, 2013).

8.1.5. Qualification process

When a Sidewalk adopter has finished developing their device prototype, it must pass through the Sidewalk qualification process. Only then are the devices allowed on the network, and may the adopter advertise their compatibility with the Works With Amazon Sidewalk badge (Figure 8.1). The qualification process entails requesting Amazon to provide development keys, so that the prototype can connect to the Sidewalk network during testing; requesting a Sidewalk360 account; shipping three prototypes to a test facility (that may be a third party), that runs the tests laid out in the Test Specification (Amazon Technologies, 2023c); and submitting the facility's proof that the prototypes passed all test cases to Amazon, along with a qualification fee (Amazon, 2023f, 2023m).

I asked interviewees about their experiences with this mandatory process. The interviewees generally considered the qualification process to be reasonable, but as the quotes show, the process was actually more invasive than the documentation makes it out to be.

One respondent remarked that their prototypes were tested by Amazon's team, that kept on testing and retesting the devices because they were not finding anything wrong with it. I interpret this as a demonstration that Amazon was at the time still experimenting with how to best govern Sidewalk devices, which incurred a delay at the expense of the interviewee's company. The effect is similar to

how manufacturers were and are kept in the dark about the Sidewalk requirements (§8.1.1). Amazon furthermore performed in-person security inspections of the factory [A6] worked with to manufacture devices, although this is not mentioned in the qualification documentation.

Moreover, while written up as a uniform process for all adopters, Amazon recurrently gave manufacturers a favourable treatment depending on their relation with them and their involvement in Sidewalk. One respondent shared that their organisation has only *"done the parts of [the qualification process] that was required for us to make our devices updatable"*, i.e. to enable Sidewalk functionality on devices later (see §C.1). They noted this is *"not typically how you do it"* and ascribed their privilege to *"the world [being] a small place"*; they were acquainted with someone leading Sidewalk (see §C.3). Another interviewee described that Amazon was also more lax towards them than usual: *"Because we've been working kind of hand-in-hand with them for a while, our process has been a little bit different, but we have had to go through a similar process around getting on-boarded to their network"*. Finally, the company that has not integrated the entire Sidewalk stack in their endpoints but got Amazon to develop a custom version (elaborated in §8.4.3), will not even undergo qualification for this reason. Regardless, both the company and Amazon actively advertise their Sidewalk adoption.

Figure 8.1: The Works With Amazon Sidewalk badge. Reproduced from Deviceroy (n.d.)

8.2. Governance of Sidewalk through technology

On the technical side, Sidewalk endpoints must have certain hardware components on board. Amazon prescribes that adopters must procure these parts from selected silicon providers. The devices must furthermore be engineered such that manufacturers can get sufficient data to or from the device, accounting for e.g. the data rate and availability restrictions that the Sidewalk specifications lay down (§8.2.1). The production processes of the endpoints must also be configured in a certain way, to ensure that the security certificates and encryption keys (§6.3) are properly embedded in each device (§8.2.2).

8.2.1. Technical measures

The technical requirements for endpoints that Amazon has defined in the Sidewalk protocol specification (Amazon Technologies, 2024) constitute a form of governance through technology. As I contend more in-depth in §C.2, the specification limits the degrees of freedom that manufacturers have concerning the fabrication and operation of their endpoints. A brief selection of salient requirements presented in that section, is that manufacturers must select which connectivity protocol they want their device to use during device development already, as endpoints can only support one at a time and cannot switch during operation; predict the usage conditions of endpoints, as each connectivity method has its own maximum capabilities, e.g. in terms of whether endpoints communicate *"synchronously"* or *"asynchronously"*, and at what rate they can send and receive data; and embed endpoints with at least BLE or FSK capabilities, which is necessary for registering them to the Sidewalk network. One developer publicly posted on their silicon provider's forum that these stringent requirements led them to pivot back to a more flexible BLE and LoRaWAN solution rather than Sidewalk (jcesnik, 2024).

Amazon effectuates these requirements through the qualification process (see §8.1.5), only allowing aspiring Sidewalk adopters that are qualified onto the network. An example is that the qualification process obliges manufacturers to use hardware development kits from approved silicon providers (Amazon, 2023m). At the moment, Amazon lists 4 companies in its developer documentation that sell *"qualified development kits"* (Amazon, 2023j).

Amazon thus also has the power to reorganise business relations between device manufacturers and silicon providers, undermining the profitability of chip companies without a close partnership with Amazon. This could move manufacturers to adopt these chips in their other device models, too: one interviewee said that knowing what you can do with a chip is helpful, implying that shifting to another chip provider would first require learning how their technology works and what it offers.

8.2.2. The effect of encryption measures on the manufacturing of IoT devices

In the interviews, *"keying devices"* surfaced as the security functionality with the biggest impact on production processes of endpoint manufacturers. This is the process that ensures that the endpoints can encrypt their messages with the appropriate keys (§6.3.1). Adopting Sidewalk therefore impacts manufacturers' production, as [A2] states:

> *it affects production, 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. [...] For us, it was a minor change. But it was still a minor change. It was not, like, you just plug and play.*

[A5] also notes that compared to provisioning a LoRaWAN endpoint, for Sidewalk, *"a couple of things are a little bit different [...T]hey don't add too much to the manufacturing process. I just think it's a little different"*. This section substantiates this argument, by explaining how manufacturers must implement the encryption resources in endpoints and why this process poses a larger burden for companies that are smaller or produce less sophisticated devices.

To understand what the workload of *"get[ting] keys into devices"* entails, I dug into the manufacturing section of the Sidewalk documentation (Amazon, 2023c, 2023g). Endpoints use a collection of cryptographic measures (i.e. certificates and key pairs) to communicate privately with their associated application server, and to be authenticated by the Sidewalk Network Server (Amazon, 2023n). These keys are unique for every application server. The keys must be embedded into the endpoints during their production, to ensure the integrity of the devices throughout their entire lifespan. To realise this, device factories must use a 'YubiHSM' specifically programmed to sign the device certificate with the private key of the manufacturer. The YubiHSM is a Hardware Security Module (HSM) sold by Yubico, which plugs into a USB-A port of the computer used in manufacturing (pictured in Figure 8.2). The IoT company must purchase the HSM (currently priced at €650 excluding VAT (Yubico, n.d.)), and then send it to the Sidewalk team for *"factory support"* (Amazon, 2023c). This entails Amazon programming a *"device attestation key"* and the *"Sidewalk certificate chain"* onto it and returning the key to the IoT company (Amazon, 2023c). The company then sends it to the factory for the actual production. The factory then has to maintain a series of logs of manufactured devices and share those with Amazon, so that the Sidewalk Network Server knows the serial numbers of the new endpoints.

For smaller companies that are only just starting up their IoT product development [A2], or are not used to producing secure devices [A1, A2], implementing this *"keying"* workflow is *"a big change. It's a big step up in security. [... I]f you don't have these kind of systems from before when you do production, then it's a significant change. [... I]t will take some while to get the production of this up."* [A2]. [A1] thinks especially manufacturers of less sophisticated devices might struggle: *"Provisioning I don't think is* that *crazy of a step for a somewhat experienced electronics company to handle. But it's definitely a hurdle to get over, if you're trying to do something, especially if it's something simple like a light or something, like 'I just want to make a light and I have a really cool industrial design. Why do I have to figure out how to like provision all this stuff in order to make it work', you know?"*. For instance, it is not standard for factories to use computers in their actual manufacturing process: *"In order to do this stuff, you generally need to have a computer on your factory line with an internet connection; or if not with an Internet connection, it has to have a fair amount of setup in order to make it work without an Internet connection"* [A1].

An anecdote from another respondent reinforces this point. They found themselves having to set up two separate product lines: their products had the same functionalities, but would either be Sidewalk-based, or LoRaWAN-based. Setting up an additional production line was not problematic for this large and experienced IoT company: *"when it comes to hardware, is the same thing. The hardware itself, is the RF, the baseband, to MCU, and some memories; is the same. So by using the same silicon vendor to build [our] Sidewalk version, and [our] LoRaWAN version, they are all combined to one scale. So that's why we're not so against it. I don't mind, just, you know, using the same ingredients to make a salty pancake and a sweet pancake: there's still a pancake."* Conversely, companies with a small kitchen, so to say, might lack the resources for manufacturing two product lines, at scale, simultaneously. Consequently, they may struggle to adopt Sidewalk.

The takeaways from this part are as follows. Amazon inserts their partner company Yubico (Amazon Web Services, n.d.-g) into the production environment of endpoint manufacturers. They leverage the argument of security to do so. In addition, recall that related literature posited that only large technology

companies might be fit to effectively deploy PETs (for they have the expertise and infrastructure necessary to do so), and that they may be so expensive that only their largest customers can afford buying services implementing them 2.3. Both dynamics apply for Sidewalk, too. Devising the encryption scheme and realising the logistical side (i.e. providing the 'factory support) requires resources that smaller tech companies wishing to set up such a security ecosystem might not have to spare. On the side of the adopters, the expertise and resources required might make Sidewalk adoption infeasible for smaller companies.

Figure 8.2: The YubiHSM 2 that Amazon prescribes as Hardware Security Module. Images reproduced from Yubico (n.d.)

8.3. Entanglement of Sidewalk and AWS

Another way wherein manufacturers become dependent on Amazon's services is that Sidewalk funnels them to use Amazon's cloud services. To preface this argument, I explain why cloud use is important for manufacturers (§8.3.1). The next part delves into interviewees' current use of AWS (§8.3.2), and how Sidewalk data can be accessed by servers outside AWS, which exposes the tight integration between Sidewalk and AWS (§8.3.3). Further, I examine how Sidewalk data can be sent directly to and from business customers' servers, bypassing manufacturers' infrastructure (§8.3.4). Finally, I inquired with two interviewees about how reliant they consider themselves to be of AWS, and also reflect on why Amazon's marketing of Sidewalk as a *"pipeline"* is inaccurate (§8.3.5).

8.3.1. Importance of the cloud for manufacturers

All interviewees use cloud services for their business. This can be explained by considering the technology of Sidewalk endpoints: they are limited in processing power and battery constraints, for instance because they are designed to minimise costs or to last for years (§5.3). Therefore, many endpoints rely on remote servers to interpret the data they gather. As [A2] illustrates, *"we move complexity from the devices to the cloud, and we made sure that, we kind of... We crunch the numbers. So you get raw data from the devices, more or less. And then we crunch the numbers and we provide something to the user from our cloud. [...] But the devices are basically sending raw sensor values and accepting configuration or commands. So everything is cloud driven, yeah."* Cloud integration is therefore crucial for low-resource IoT devices, as Sidewalk endpoints are.

Amazon capitalises on this cloud dependency by offering a range of AWS services around managing IoT devices. For instance, these can be combined to automatically connect endpoints to the cloud upon their first boot; send and receive data from and to devices; visualise metrics in a dashboard (see Figure 8.3); inspect and access individual devices (e.g. to assess their status or reboot it); mirror the status of devices into a digital counterpart (*"device shadow"*); analyse and sift through all devices (e.g. to select all devices with a certain firmware version); push updates to devices; and monitor device behaviour to detect and act on anomalies for security purposes (e.g. *"quarantining"* devices from the rest of the fleet). AWS thus allows processing data that devices send uplink, but also managing the devices and issuing commands or updates to them in downlink traffic (Amazon Web Services, n.d.-f).

The *"AWS IoT Core for Sidewalk"* bundles a range of IoT-related tools, including for device provisioning, logging, and monitoring, and routing data between the *"IoT Core Rules Engine"* and other AWS services (Amazon Web Services, n.d.-j). This bundling aims to reduce development efforts.

Clearly, AWS serves manufacturers to know the status of their devices, and the ability to remotely manage them, aiding their production. I further refer to this as *"operational control"*. Indeed, [A2] said they use Sidewalk both for allowing end-users more control over their devices (through the additional coverage), and for *"operational purposes"*: *"We typically log things regarding like the functionality of the device, like, did it reboot and why did it reboot. Basically, did it crash, and why did it crash; so that we can fix it. And then there are some battery lifetime things and things like that. But we don't monitor a lot of things in our devices. It's purely for, like, operational purposes"*. [A6] and [A8] similarly utilise Sidewalk for operational control, mentioning remotely rebooting and updating their endpoints, and assessing which functionalities

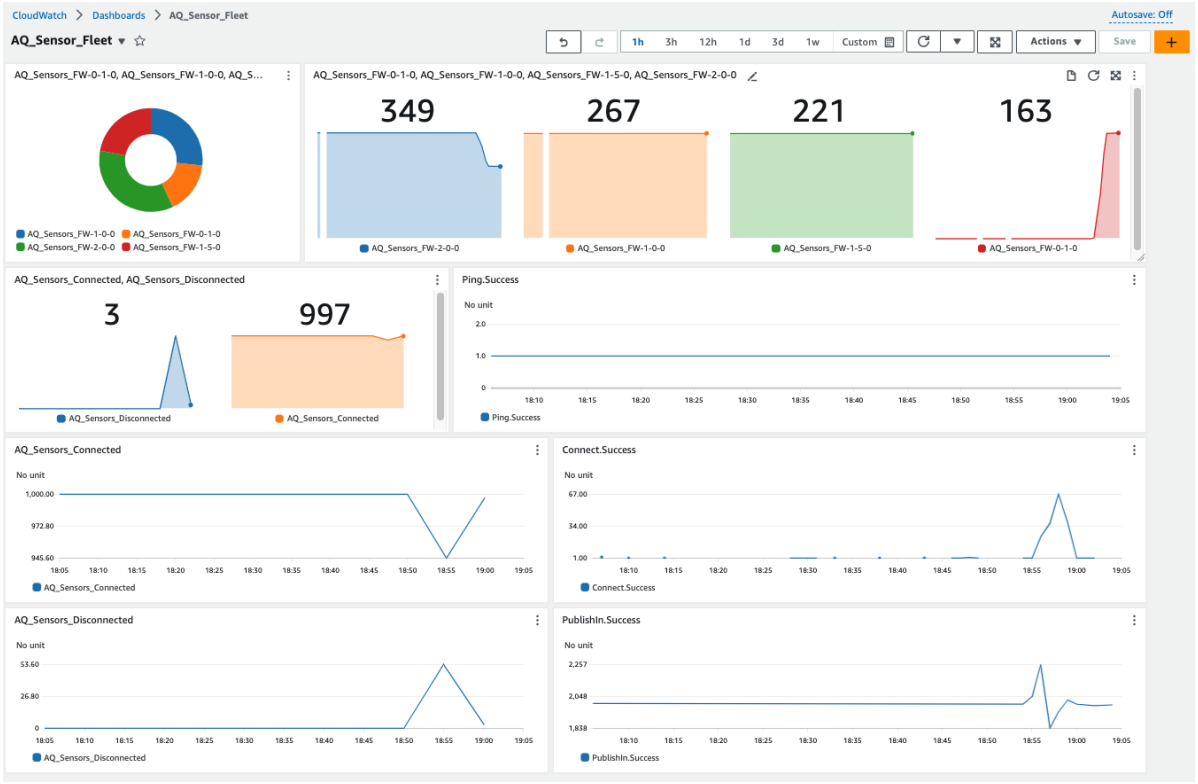

Figure 8.3: Example of an AWS dashboard showing multiple metrics about 1000 deployed endpoints, illustrating the operational control that AWS can yield manufacturers. Reproduced from Amazon Web Services (n.d.-e)

end-users use most. As such, manufacturers' production becomes significantly more flexible (and agile) than if devices could only be updated by e.g. plugging them into a laptop or even not at all.

8.3.2. Manufacturers' adoption of AWS

All eight interviewed Sidewalk adopters use AWS. This was already the case prior to adopting Sidewalk, meaning their adoption did not prompt a migration to Amazon's cloud. However, their prior experience with or investments in AWS might have eased their adoption of Sidewalk or entrenched AWS further in their practices.

Six of them use AWS for all their cloud-hosted IT. The seventh respondent did not elaborate on the extent to which they use AWS vis-à-vis other cloud vendors. The final respondent's company combines cloud services from a cloud vendor they are partnered with, with AWS. The partnered vendor's infrastructure *"works very well"*, but they did not attempt migrating to one cloud entirely. Both cloud infrastructures expose APIs to enable communication between the two. All Sidewalk-related data is stored in AWS in a Mongo database, that both the adjacent AWS services they use, and the infrastructure in the other cloud can talk to. They also use AWS as a *"man-in-the-middle"* to authorise users trying to interact with endpoints: *"you have to talk to our AWS cloud, get tokens, and then the cloud talks to our unit. [...] So long as you can get through and talk authorised through AWS and our cloud services, then those cloud services are actually what sends commands to our [endpoint]. You can't command it locally"*. This company uses Sidewalk primarily for endpoint maintenance, troubleshooting, and telemetry; users' interaction with the endpoint might not rely on this authentication. This exemplifies that Sidewalk is more used for operational control purposes, than bringing end-users value (e.g. enhanced coverage).

I furthermore asked Sidewalk-adopting interviewees whether they leverage AWS IoT Core. Four interviewees reported using this service. Three respondents said they do not use IoT Core, but manage their devices elsewhere in AWS. This means that they have to undertake extra steps to pick up the data from the Sidewalk network and process it there. The company of one participant sells multiple wirelessly connected products, of which some are equipped with Sidewalk functionality. To process

data of all devices the same way, they *"need to do some glue things. In the sense that we have slightly different entry points into our cloud depending on if we use our ecosystem or Sidewalk. But in the end it just goes into the same software. [...] It's ingestion, basically. So ingestion of data is different."* Thus, even if manufacturers have all business logic inside AWS, managing Sidewalk devices poses a hurdle when not using IoT Core. But apparently, this service comes with its own challenges: this same person indicated that IoT Core did not yield sufficient benefit to warrant migrating their working solution to IoT Core, such that both Sidewalk and non-Sidewalk devices are interfaced with through IoT Core.

The eighth interviewee did not know whether they use IoT Core, but expressed that processing data sent over Sidewalk is more complicated than processing data sent over LoRaWAN. Their company has a LoRaWAN and Sidewalk product line, and attribute this difference to Sidewalk being a closed network, whereas LoRaWAN is open-source and has a large community developing for it. LoRaWAN adopters can therefore leverage third-party solutions to interface with LoRaWAN data, saving development efforts. In sum, choosing to refrain from using the native Sidewalk AWS service (i.e. IoT Core for Sidewalk) complicates managing Sidewalk devices, but also requires development efforts that might not be worth migrating from a current solution.

8.3.3. Managing Sidewalk endpoints outside AWS

With this entanglement of Sidewalk and AWS, how can Sidewalk devices be managed outside AWS? The interviewee that has their own business logic in both an AWS and non-AWS cloud, answered that *"you just create APIs, right? And the APIs are what's going to create the communication between the two. And as long as they can align up, whether it's a call or a push, that's going to drive your connection."*

Moreover, [A5, A6, A7] have APIs inside AWS 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, you know, a fraction of a millisecond. [... Y]ou 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. [...] You know, moving data around is a pretty solved problem these days, so it's not that complicated."* [A7] said something similar, but does not find it as easy: *"[A7:] [Y]ou have to find your own way to cultivate it out, extract it out to the next one. There's still a copy and paste effort, but I think it's not easy. Yeah. [Author:] Okay. So you ingest the data in AWS, and then you copy-paste it into your own cloud? [A7:] Yes, yes. It's not as easy as is said, okay. But it's still doable."* Whether moving data around is easy or not, key is that the data has to be moved around in the first place, because Amazon has made avoiding AWS impossible [A5, A6]: *"the data has to come into AWS, yeah. So there's no option for the data not going to AWS. That's how Sidewalk works"* [A5]. This means a duplication of data and processing, increasing complexity, security risks, and costs for business customers and manufacturers that wish to use a non-AWS server. [A7] therefore claims that Amazon *"funnel[s] people"* into using AWS. Indeed, only one out of eight interviewed adopters use a non-AWS environment, illustrating how unappealing this duplication is. This demonstrates that SW is not *"just a pipe"* (cf. §5.1): the Sidewalk *"network protocol"* is not technology-agnostic because of the funnelling towards AWS. As Renda and Yoo (2015) note, infrastructure providers' claim to being a dumb pipe will become weaker the more they manage and regulate traffic and utilise usage data. Resultingly, Sidewalk provides AWS a competitive edge over other cloud providers, leaving manufacturers with less alternatives and Amazon with greater power.

8.3.4. Routing Sidewalk data directly to a business customer's server

Some business customers want endpoint data to be processed or visualised data for them, while others want the manufacturer to forward the data to process it in their own infrastructure [A5, A6]. Recall from §8.2.2 that Amazon ties the HSM, and thus endpoints specifically to the application server of the manufacturer. Endpoints can therefore only send data to and receive data from the manufacturer's infrastructure. One solution is to provide APIs for business customers to fetch the data from [A5, A6]. But what if a business user does not want their data to pass through the manufacturer's infrastructure, for security reasons? In these cases, endpoints can be *"keyed"* to communicate with the customer's own application server, without passing through the manufacturer's instance [A6]:

> *[I]t is keyed specifically by Amazon and then delivered to the factory, and it is uniquely keyed to that company. So [if] we need devices that need to go through just to their instance, or to that other company's instance, that key then will uniquely set those devices up to where even we cannot decode the data that's coming through; it's unique to that company, they're responsible for it. They will have*

> *to run their own Amazon instance, because Sidewalk is decoded and decrypted in Amazon's cloud. [... I]n those cases, they have to buy in volume, because there's a set-up time for the factory to do that uniquely for their lot of devices. And we certainly don't want those to get mixed in with our normal devices.*

Thus, these customers must manage their own application server in AWS, because all Sidewalk traffic ends or begins in AWS (see Figure 4.2 in §4.2, and §8.3.5) and a YubiHSM, that Amazon then links to this server. Because of these hurdles, that exist to facilitate Sidewalk's PETs, business users might not feel comfortable asking their Sidewalk manufacturer to route traffic to their own premises. Even if they would, the manufacturer might not have the resources to guide their customers in this process; liaise between the customers, factory, and Amazon; arrange the HSM logistics; and support custom endpoint setups on the long term. And even if the manufacturer would support the customer, then the customer must buy a sufficiently large volume to warrant the factory to temporarily adjust its production process, posing another hurdle. For these reasons, it seems unfeasible for customers to circumvent the Sidewalk manufacturer's infrastructure. Alternatively, this may be reserved for customers with sufficient knowledge and time to jump through the hoops themselves. But at that point, other, non-Sidewalk options might provide less cumbersome and expensive. For instance, LoRaWAN is more flexible in this regard: customers of [A6] *"can connect [their LoRaWAN-compatible endpoints] directly to their own LoRaWAN accounts, connect that directly to their own servers"*

Note that Amazon's funnelling of manufacturers to use AWS, extends to the customers that do not want their data to pass through the endpoint manufacturer's infrastructure. The data is still routed to an AWS instance, that it has to be pulled from if the customer wants to process it in another infrastructure.

8.3.5. Manufacturers' perceived reliance on AWS

I asked [A5] and [A8] whether they perceive their use of AWS as a reliance. [A5] said *"We are relying on AWS. To an extent, right, to an extent"*. They think their aforementioned ability to *"mov[e] data around"* alleviates their reliance; overlooking that they still need an AWS instance and depend on it for *inter alia* device provisioning (§8.2.2). [A8] similarly pointed to APIs enabling communication between their AWS and non-AWS cloud, but acknowledged that this setup still presents a single point of failure, because they use AWS for *"a lot of [their] use cases"*. It is interesting that this interviewee interprets the reliance primarily as a technical risk, implying it only needs addressing to improve their service reliability, rather than seeing the power it yields Amazon.

8.4. Disadvantages for Sidewalk adopters

Besides the uncertainties around Sidewalk's lifespan, adopting Sidewalk comes with other disadvantages for IoT manufacturers. These are the bandwidth restrictions (§8.4.1), having to support customers with debugging Amazon infrastructure (§8.4.2), the costs of developing Sidewalk-compatible endpoints (§8.4.3), and the risk of commoditisation (§8.4.4).

Two other downsides that interviewees mentioned are that Amazon over-promises the range of Sidewalk devices and causes confusion about underlying radio technologies, and that one interviewee doubted the utility of Sidewalk as finding network. I discuss these in §C.6, because they are less impactful.

8.4.1. Bandwidth restrictions

Manufacturers must carefully engineer their devices such that they can communicate and receive sufficient information within the confines of the Sidewalk specification (§8.2.1). [A2] indicated that the bandwidth limitations force manufacturers to ensure that transferred packets contain *"exactly what [they] want"* with marginal room for error [A2]. In fact, their devices typically send more data than Sidewalk's bandwidth constraints allow, meaning that using Sidewalk *"would kind of limit how much data we could send"*. [A6] also mentioned that their endpoints perform some filtering before sending data uplink, to reduce bandwidth consumption.

8.4.2. Manufacturers and silicon providers debugging Amazon's infrastructure

Besides the benefits that the crowdsourced nature yields Sidewalk, two interviewees reported a practical issue with it. Manufacturers repeatedly had to troubleshoot Amazon's gateways when users'

endpoint was not working properly, because most users running into trouble *"come to us because we're the manufacturer, we're the maker, and we maintain that relationship with them"* [I3]. This is especially because the *"consumer level of understanding"* of Sidewalk is typically low (§6.5.2). The debugging is challenging if the endpoint owner does not have access to the problematic gateway, for instance if the gateway is owned by a neighbour. Amazon might even see manufacturers encourage end-users to buy a Sidewalk gateway themselves, to ensure coverage – be that a residential gateway as currently on the market, or the announced Bridge Pro for industrial use (§4.3).

A similar dynamic applies for silicon providers. In a forum conversation, a manufacturer expresses to that their endpoint is not time synchronising. Their silicon provider responds that the gateway might be the issue, but that they cannot identify the problem without involving Amazon, because the operation of gateways is hidden to them: *"If your setup is stuck in this state, we can investigate with Amazon ([gateways] are basically black box for us)"* (rsoc16 & silabs-Lucie, 2024). Thus, at times, the burden to troubleshoot gateways undermining Sidewalk's reliability lands with manufacturers and silicon providers, rather than Amazon itself.

8.4.3. Costly hardware requirements and governance

The shadow side of Sidewalk's PETs is the computational resources required for them. Interviews showed that the Sidewalk stack requires hardware that is relatively powerful and therefore costly for IoT applications, in order to implement the security protocols. [A6] elaborates that *"there are only certain processors that 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."* This B2B-oriented respondent did not state that the costs are inhibitive for them.

[N1] considers the implied high hardware costs a barrier for other IoT companies to adopt Sidewalk, especially in the B2C domain. While triangulating this statement is challenging given the interview sample mostly constituting Sidewalk adopters (see §10.4), one interviewee did indicate that the hardware costs were too high for them. They are, indeed, active in the B2C domain. The Sidewalk firmware stack was larger than the endpoints' chips' memory and flash memory permitted. The limited benefits that Sidewalk brought for their products, did not outweigh the costs of incorporating more powerful and thus expensive hardware in their endpoints. This was reason for them to not implement the full firmware stack in their devices, after which Amazon created a custom version: *"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."* A consequence of not adopting the full stack is that their endpoints do not use the Sidewalk authentication and security scheme, which Amazon apparently permits for the sake of onboarding this organisation. Moreover, it is plausible that this custom implementation incurs additional development effort or costs on Amazon's side, leading them to *"occasionally nudge us to implement the full stack, [even though] it kinda doesn't make sense"* for the respondent to do so.

The other governance measures that Amazon employs from a security motivation also pose security-related expenses. Device makers must spend time and money on interacting with the governance measures that Amazon employs, for instance to accommodate the device keying workflow and to have Amazon qualify their device; this is elaborated in §8.2.2. These costs are both monetary (e.g. staff salary) and temporal (e.g. complying with Sidewalk's governance instruments takes up staff capacity). This is illustrated by an interviewee whose devices do not support Sidewalk yet, despite having the necessary hardware and software on board. When I asked them when they expect to turn Sidewalk on for their endpoints, they said *"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"*.

Thus, while Sidewalk might at first glance seem attractive for IoT companies that want to minimise the costs of their device (because of being free to use and not requiring customers to buy a gateway), the hardware costs will drive up the development costs and hence potentially the cost prices of endpoints.

8.4.4. Risk of commoditisation

One respondent brought up that Sidewalk adopters risk being commoditised. They saw this unfolding for the asset tracking company Chipolo in making themselves compatible with Apple's Find My network: *"Chipolo and others have started to introduce Find My devices, and that's interesting because they almost completely relinquish control. They become Apple devices, in a way commodity providers to Apple. [... T]hey're a bit*

on a leading curve of this trend, 'I used to have my own device, I had a mobile app. Now, I'm on Find My, and I'm just a hardware provider'". They see a similar future for IoT manufacturers adopting Sidewalk, noting that as an IoT or hardware company, *"if you're just selling hardware, you're always in an uphill battle against commoditization. And so the typical path is to pursue subscription services"*. This is no different for the interviewee's company: subscriptions made up about two-thirds of their 2022 revenues, almost three times as much as the contribution of hardware sales, as I found in a recent annual report. The interviewee continued that *"if you hand that control off to Amazon or Apple, your opportunities are diminishing. [...] So it's interesting, it could give you better reach. But you may be giving away things if you're not careful. We were always mindful of that."* The better reach is the additional coverage that Sidewalk provides, but by conforming to Amazon's standards, adopters run the risk of becoming mere hardware providers. This quote is another demonstration of why the viability of B2C-based business models is under pressure (5.3), and that Amazon shapes the business opportunities and business models of third parties.

8.5. Chapter conclusion

This chapter brings into view how manufacturers' production of IoT devices changes after adopting Sidewalk, forming the first part to answering subquestion 3. On the one hand, Amazon has carefully set things up to make Sidewalk appealing to manufacturers, promising them a plethora of benefits while offering help with adopting Sidewalk (Chapters 4 and 5). On the other hand, aspiring adopters must actively adjust their production process to make their products Sidewalk-compatible, as I showed in this chapter. Manufacturers must invest significant resources (including time, money, and skilled staff) to *inter alia* arrange the elaborate endpoint keying workflow; procure expensive device components while minimising device costs; comply with Amazon's processes, such as for organisational audits and qualification; and troubleshoot Amazon's infrastructure if endpoint users run into trouble (as silicon providers also do when manufacturers experience issues). Meanwhile, Amazon cements AWS in the production processes of manufacturers, through its entanglement with AWS. If manufacturers wish to use a server on their own premises or in another cloud, they must resort to *"moving data around"*, incurring significant complexity, security risks, and costs. These barriers suggest that Sidewalk adoption is most feasible for large or well-funded IoT manufacturers, willing to engage with AWS. This effect extends to business users that want data routed to their own premises directly: the overhead and costs that *"keying"* endpoints to their servers incur, means that most will have to accept their data travelling through their manufacturer's infrastructure. Even then, using AWS cannot be avoided, meaning Sidewalk is not appropriate for business use-cases with highly sensitive data.

The implications are as follows. First, Amazon funnelling manufacturers to use AWS and comply with the myriad technical and organisational requirements for the sake of *"security and privacy"* means Sidewalk is clearly not just a *"dumb pipe"*. Manufacturers making their endpoints Sidewalk-compatible, in practice latch them onto Amazon's CI. They are contractually forced by Amazon to relay updates that Amazon publishes for Sidewalk to the endpoints. Meanwhile, manufacturers can only manage their devices from within AWS, and are implicitly nudged to move their other business logic into AWS to reduce duplication, complexity, and security risks. Therefore, Sidewalk captures both endpoints and application servers into Amazon's span of control.

The fact that Amazon manages to make all these manufacturers jump through all these hoops, demonstrates the industry leverage that Amazon has. The disadvantages (including bandwidth limits and costs) negated many of Sidewalk's claimed functional benefits (such as coverage and cheap IoT development), implying that manufacturers deemed *"befriending the giant"* and leveraging their reputation is worth the trouble. Consequently, studying this change in production processes lays bare the power asymmetry between Amazon and manufacturers.

PETs play a central role in Amazon's reconfiguration of adopters' production. Privacy and security are the arguments that Amazon wields to justify their discretionary power. This ranges from usage terms laying all decision-making power about Sidewalk with Amazon, to obligating manufacturers to buy chips from certain silicon providers and to buy an HSM that Amazon must sign. Amazon thus even inserts other companies in manufacturers' production. These PETs, then, serve to justify Sidewalk's crowdsourced nature, that was brought about with an opt-out update. Even if one argues that the effect on individual gateway owners is small – setting my opinion on this matter aside, the gain for Amazon is clearly enormous.

Meanwhile, manufacturers are seemingly unaware that they risk commoditising themselves and

becoming to rely on Amazon; reducing the latter to a technical concern that can be solved by *"moving data around"*. To investigate this further and definitively answer subquestion 3, I scrutinise the dependencies that these changes in production bring about in Chapter 9.

9

How adopting Sidewalk makes IoT manufacturers dependent on Amazon

Chapter 8 expounded on how adopting Sidewalk requires manufacturers to invest significant resources in making their endpoints Sidewalk-enabled, showing the tangible affects on their production processes. The necessary reconfiguration suggests that these efforts make manufacturers dependent on Amazon. This chapter demonstrates the complexity of this dependency relationship and surfaces the power dynamics that it creates.

First, Amazon does not allow third parties to offer gateways and network servers, meaning that only Amazon can provide Sidewalk connectivity to manufacturers (and endpoint users) (§9.1). With Amazon being the sole provider, manufacturers rely on their ambitions and investments into Sidewalk. Therefore, I examine what motivates Amazon to offer Sidewalk (§9.2), as well as which dynamics within Amazon put its longevity at risk (§9.3). Manufacturers attempt to mitigate this risk, as well as the drawbacks of Sidewalk (found in §8.4), by implementing other connectivity protocols in their endpoints, too, but the impact of adopting Sidewalk on their production means this is not always feasible (§9.4). Curiously, Amazon simultaneously depends on manufacturers to get the most value out of Sidewalk (§9.5). Finally, I conclude the chapter (§9.6).

Together with Chapter 8, this Chapter shows the lasting dependencies and power dynamics that manufacturers' reshaping of organisational and production processes to bring them in line with Sidewalk's requirements. This helps answer the third subquestion (*"How does Amazon's technical design and governance of Sidewalk affect the production of IoT devices?"*).

9.1. Sidewalk's closed nature

A final dependence of manufacturers on Amazon is that only a selection of Amazon IoT devices contribute to Sidewalk coverage as gateway (see §4.3). Thus, if Amazon were to ever remove gateway functionality from these devices, endpoints cannot connect to other third-party gateways instead. While [A8] bets on Amazon eventually opening up the technology stack for third parties to implement gateway functionality in their endpoints (§9.1.1), [A4] does not see this happening any time soon (§9.1.2).

9.1.1. Lack of third-party gateways and network servers

[A8] is anticipating and developing towards equipping their endpoints with Sidewalk gateway functionality. Because their devices are generally placed outdoors, close to homes and office buildings, they see a rich future in becoming a gateway for other devices over Sidewalk or other sub-gigahertz protocols:

> *Amazon does not want to quite open up their gateway service yet, right? [...]. You know, there's not many [gateways] out there. But they are in the works of creating a development kit to be able to do that. So our thinking is, once they cross that threshold to allow that development, and we can... the way we want to integrate with them, we wanna be Sidewalk access points. Because if you start thinking about the infrastructure and how many of [our devices] start getting out there, what's gonna happen is, you're now going to have the ability to create this additional network, right? So if we fill*

> *this entire neighbourhood with our units, well, now everybody's going to have access to connecting of Sidewalk, which will extend their... It's kind of like a mesh network at that point.*

The statement that *"there's not many [gateways] out there"* seems contradictory to Amazon's claim of covering 90% (Amazon, 2023o) or 95% (Bishop & Hamren, 2024) of the US population. Considering that the interviewee's device uses both LoRaWAN and Sidewalk, they could be referring to the fact that only 6 of the 30 gateway models support LoRa (4.3). When asked why Amazon would not want the devices to contribute to Sidewalk's coverage, the participant replied:

> *I can't say that they've ever given us a true answer, you know, there's a lot of vagueness in there. So I'm sure that there's meanings behind it. And I'm wondering if it's because they still wanna hold that control under their umbrella, to be like "oh, you have to have these devices". [... I]'m wondering if they're trying to eyeball their best path to be able to create that. I see it happening eventually, I just can't give you a timeline, because they don't give us a timeline.*

Amazon is keeping the participant's company in the dark on this aspect, which the participant simply has to stomach, because of the power asymmetry, speaking volumes about Amazon's power over them:

> *I mean, if they shared a little bit more, then we could develop a gateway with them. But you know, we're not there. There's always about, you know, who's holding the more power on which side of that? And we just kind of play ball the way they play ball, and hopefully develop an innovation that can drive the growth. That's all.*

Until then, manufacturers depend on Amazon supporting the gateway functionalities of current Echo and Ring devices, and on their end-users having gateways nearby. The same dependency applies to the fact that there is only one Sidewalk Network Server, managed by Amazon. If Amazon were to pull the plug, all endpoints would lose Sidewalk connectivity, unless Amazon would make the network server technology open-source. Even then, Sidewalk's integrity might be compromised by the lack of an actor to organise the governance (i.e. to manage the encryption schemes, qualification process, usage policies, and so on).

9.1.2. Closed networks as industry practice

The expectations of another respondent are in stark contrasts with those of [A8]. They believe Amazon will not allow third parties to incorporate gateway functionality, based on earlier experiences around standardisation with Google and Apple. At one point, the interviewee's company proposed open standards for a finding network, but *"[w]e've only seen that [Apple] want[s] to have nothing to do with that. They want to have complete control, top to bottom. It's a similar thing with Google: as they create their network, they want to have complete control. [... W]ill something emerge that everybody agrees is actually a really nice standard that should be generalized, that still seems years away. But that looks like the opportunity. And for now, all these large companies want to completely own it themselves."* The interviewee believes that Google pursues a walled garden out of privacy concerns that inviting third parties to a finding network could induce. Google supposedly faces more public scrutiny than Apple, because Google's business model is historically vested on advertising and data, as opposed to Apple's business model of hardware. Another difference is that Apple is generally more restrictive in granting access to their technologies (e.g. Mossberg (2016)), making it harder to scrutinize Apple's technical implementations. Comparing this separate network situation to the early telecom days, the respondent thinks only government regulation establishing regional monopolies could move these companies to open their networks for each other.

I speculate that Amazon might open up the network to third-party gateways if LoRaWAN adoption gains traction in areas where Sidewalk's LoRa coverage is limited. If Amazon would let others develop gateways, they could still keep a tight rein on the network. For instance, Amazon could choose to only allow third-party gateways to use the LoRa PHY, force manufacturers to route all traffic through Amazon's Sidewalk Network Server, or demand some connection to AWS for authentication purposes. Then, all the dependencies of manufacturers on Amazon, and effects of adopting Sidewalk on the production processes of endpoint manufacturers that I demonstrated in this chapter, will extend to gateway manufacturers, too; further cementing Amazon's infrastructure at the centre of Sidewalk. Until then, manufacturers rely on the availability of gateways by Amazon.

9.2. What's in it for Amazon? Amazon's motivation to deploy SW

[A3] brought up the tremendous time and money that Amazon has invested into Sidewalk until this stage. They therefore believe that Sidewalk will be around a long time, at least the coming 5 or 10 years. It is unclear whether [A3] thinks Amazon will not want to abandon these sunk costs, or that their amount of resource investment reflects their belief in the project. This begs the question why Amazon does not directly monetise Sidewalk use to earn back on these investments. This section assesses how Amazon is set to benefit from their efforts. First, Sidewalk could increase Amazon's turnover (§9.2). Second, partnering with silicon providers saves Amazon the effort of (obtaining knowledge about) manufacturing secure chips (§9.2.2).

9.2.1. How Sidewalk could generate revenue for Amazon

In essence, Sidewalk constitutes an environment for the development of new and enhancement of current IoT products. [A1] thinks that Sidewalk *"was something where Amazon really wanted to generate an ecosystem that other people would develop hardware for"*. This implies that such an ecosystem requires an active generation effort by Amazon, and that the resulting ecosystem promotes hardware development that can eventually generate revenues for Amazon.

According to [A3], Amazon was not the only player eyeing to provide such an ecosystem. They say Amazon pitted itself in a *"fight against the big telecom"*, and aims to cement itself as intermediary for third-party digital applications. In their words, *"everybody wanted to own the smart home. So if you can build the IoT network to own the smart home, that unlocks a massive amount of revenue and opportunity. So that was the intent from everyone"*. Similarly, Sidewalk could fulfil Amazon's ambition to facilitate smart cities [A3] as well as next-generation utilities that are increasingly digitally managed, both within homes and in utility infrastructures [A6]. [A3] saw both big tech companies and telecom providers *"trying to figure out how to bring LoRa to consumers"*. However, while *"everyone was kind of having similar ideas around the same time, but nobody [succeeded]"* due to the massive capital expenses that building such an infrastructure calls for (§4.4.1). This points out that only resource-rich companies stand a chance to successfully generate this ecosystem.

Having established this ecosystem, the question rises how Amazon profits from it. Four avenues arose in the interviews, demonstrating the versatility of the Sidewalk project for Amazon's bottom line. First and most obviously, Amazon could start to charge end-users or manufacturers for their Sidewalk usage [A1]. §9.5 reflects on this possibility.

Second, Sidewalk improves Amazon's own products and services. For example, their shipping division could benefit from more intensive shipment tracking [A4]. Additionally, Sidewalk adds functionality and coverage to Amazon's smart-home products [A4], enabling Amazon to sell them at a higher price. [A4] noted that although Amazon already enables IoT companies to integrate with Alexa software and devices, Amazon is *"struggling a bit, because after all this work, people mostly use Alexa for the news and the weather and timers. [...] They enabled this ecosystem and it hasn't really taken off in the way they hoped."*. This raises the point that there is a massive unattained opportunity to improve Alexa, namely *"there being thousands of things to integrate"*, for instance allowing users to control third-party devices from within the Ring app and with the Alexa voice assistant. Amazon could leverage this enhanced third-party integration, as well as the extra connectivity that Sidewalk brings to their current and future endpoints (§C.7), to increase their device prices or offer these functionalities as add-on subscriptions.

Third, manufacturers' AWS use generates direct revenue for Amazon [A1, A7]. The IoT-related functionalities are monetised in various ways, for instance charging per number of API calls, queries, connected devices, messages sent or analysed, and amount of data processed (Amazon Web Services, n.d.-d). Recall from §8.3.1 that AWS lets manufacturers both improve the endpoint end-user experience by improving connectivity, and improve their operational control over devices by enabling remote maintenance and assessing which functionalities end-users use most. Amazon has lined the Sidewalk and AWS integration up in such fashion that there is little to no incentive for manufacturers to migrate this data and operational control out of AWS (§8.3.3). What is more, adopters might be inclined to also move other components of their business logic (e.g. for miscellaneous data storage or running a website) to AWS, to have everything in one place and reduce complexity.

Finally, learning how manufacturers use AWS to manage Sidewalk devices (§9.5), enables Amazon to learn how to make AWS as attractive a production environment for IoT developers as possible

(§7.2.3). Sidewalk would then function as a vehicle for Amazon to assess the needs of a specific group of developers, and knit close relations with them, to garner insight into how AWS can fulfil their needs.

9.2.2. Hardware development connections and knowledge

To attract Sidewalk adopters that will manufacture end devices, Amazon must ensure the availability of modules that support the Sidewalk radio protocols and the security mechanisms. Collaborating with silicon providers to develop such chips is thus necessary for Amazon to conceive the Sidewalk ecosystem. Being designated as Sidewalk-qualified chip provider lets these companies sell to Sidewalk adopters; an attractive proposition, especially with Amazon limiting the number of qualified silicon companies (§8.2.1). It is not public whether Amazon has negotiated additional returns from the resulting partnerships with silicon providers, such as preferential treatment for Sidewalk adopters or a commission of chip sales to them. But [I3] signifies that there is more to this business relation:

> *It's very interesting from a policy economic perspective, the kind of interconnectedness of all of these different folks around the stack. Because a lot of people think about just the cloud side, they're just kind of "once we have the data, where does it go?" But the other side of that, the manufacturing and the development of it, is super interesting because there's a lot of cash associated with that.*

This interviewee underlines the point of §9.2.1: that the value for Amazon is not only in *"data"*, but also in *"manufacturing"* (production and hardware) and *"development"* (operational control). Consider, for example, this quote from the same interviewee that sheds light on the aforementioned interconnectedness:

> *There's 3 companies that Amazon worked with initially and still invests a lot of time and a lot of resources into. It's TI [(Texas Instruments)], Nordic and Silicon Labs. [... T]here's a lot of people that are now creating modules and chips, which I think was part of the Amazon strategy, but those core three were the ones that have been working on it since when I was involved with it, kind of helping to inform Amazon and teach Amazon around how you actually build security within, for example, or how you actually put this thing together.*

When I confirmed with the participant whether silicon companies indeed taught Amazon about the mentioned topics, they replied with *"Yes, correct"*. In addition to knowledge, Amazon gets valuable connections in the field:

> *[I]t's very interesting from a strategic standpoint for Amazon to leverage those people and the intelligence or services or resources that those silicon providers have. Because if you get the silicon providers to endorse you, for example, or to support you, that's a lot of power. Because those guys make a lot of money and only have a specific amount of time that they want to spend on certain things, they are looking to optimize profits. So getting them to really sign with [Amazon] and do some of the work, is a really big signal to the market, I believe.*

The silicon providers' buy-in thus signals to IoT companies that Sidewalk might be the next big thing they should develop towards. Meanwhile, Amazon obtains state-of-the-art knowledge about developing and manufacturing secure hardware. This knowledge benefits both their Sidewalk endeavours and their hardware development more broadly. More importantly, this proves that Amazon has recruited silicon companies to *"do some of the work"* of enabling IoT companies to manufacture Sidewalk-compatible endpoints, namely by supplying them with appropriate silicon. Thus, these connections save Amazon the enormous effort of obtaining knowledge, setting up a chip development and manufacturing infrastructure, and operating it to produce Sidewalk-capable chips themselves.

On top of that, by asking partnered silicon providers to nominate a lead customer (§5.6), Amazon outsourced the labour of advertising Sidewalk, recruiting early adopters, and testing developmental versions. One interviewee received limited support from Amazon to comply with Sidewalk's security and production requirements; the silicon provider that nominated them as *"lead customer"* had to provide guidance. This is also visible in a prospective adopter resorting to the customer support forum of their silicon provider upon failing a qualification test, rather than asking Amazon or the test facility for help (netvoxrd & silabs-Lucie, 2024).

Over time, the larger the ecosystem, the more other chip providers will want to get involved to grow the pie or claim their share of it. This is already happening, as Amazon partnered with a fourth silicon

provider (Amazon, 2023j), in addition to the *"core three"* that Amazon initially involved [A3]. Amazon is betting on integrating more chip providers, evidenced by a recent job opening listing this as one of the duties (Amazon, 2024a). This allows Amazon to scale up the production of Sidewalk silicon further, while being able to have silicon providers bid against each other.

9.3. Risks to Sidewalk's longevity

While still being positive about their relationship with Amazon, [A7] was aware of the time sensitivity of Amazon's goodwill: *"they're very friendly, and they're willing to help – at this moment, because they need us too, right?* (laughs)"; a sentiment shared by [A2]. But multiple risks to Amazon's long-term commitment to Sidewalk exist. Amazon has recently had multiple lay-off rounds (§9.3.1). Further, rolling out Sidewalk put Amazon in a bad light for the LoRa Alliance (§9.3.2); there is a lack of communication within Amazon could hamper them getting the most out of Sidewalk (§9.3.3); and a roll-out of Sidewalk outside the US is complicated, limiting opportunities for expansion (§9.3.4).

9.3.1. Lay-offs and downscaling hardware activities

Much like many other technology companies in 2022, 2023 and 2024 (see e.g. Lee (n.d.) and Stringer and Corrall (2024), Amazon has been downscaling their activities in less profitable sectors. Some grey literature publications ascribe the cuts in less profitable divisions to the end of low-interest rates (e.g. Hern, 2023; Streitfeld, 2023). One interviewee discussed Amazon's downscaling. A potential explanation is, in their eyes, a *"fear that regulators may split Amazon into a bunch of companies because it's gotten so big"*. The reason behind the lay-offs is out of scope; it matters here that Sidewalk is not immune to this downscaling movement, as multiple participants alluded to.

Organisation-wide, this respondent that has worked as hardware developer within Amazon earlier, noticed a change in Amazon's attitude towards customers:

> *Amazon has its own problems. I feel like Amazon... They've spent many years in this customer obsession mode, of not really worrying too much about profits, and really being focused on the customer and growing the business. Something happened in the last few years where they really... Maybe it was Jeff [Bezos] stepping down, or whatever it was, but yeah, it just feels much more like they're on that... I don't know if you ever read the article, or the essay about the "enshittification" of everything. But they're starting to head down that path of "let's put ads on everything", "let's charge a monthly fee for everything". I just noticed my Fire TV, I turned it on and there's like full-screen loud ads now playing the second you turn it on. These are not customer-obsessed activities. These are "we're trying to squeeze our customers for a few more dollars" kind of activities. And that's kind of a bummer, because, it did feel like for all Amazon's faults, they were really good toward their customers. And that seems like that's finally kinda evaporating.*

The participant then related the consequences of these tighter reins to Amazon's hardware department:

> *Amazon, it feels to me like they're trying to reduce their hardware business a lot. And so you never know what they're gonna do. Like, they could just say "forget it, the Sidewalk thing didn't work out, we're abandoning it". And there's not a lot that you could do about that. [... T]hey've been doing so many lay-offs, they've been cutting features, they've been trying to charge for other features. They've definitely been cutting product lines of hardware.*

For context, I looked up relevant recent lay-offs at Amazon by Ortakales and Kim (2024). In November 2022, Amazon laid off about 10,000 employees, with the devices division being one of the three divisions most affected. January 2023 saw 18,000 lay-offs, also hitting the People Experience and Technology Solutions division (although their precise involvement with Sidewalk is unclear). In March 2023, 9,000 employees were laid off company-wide, that according to Sundar (2023) also affected the AWS department. Most recently, in November 2023, *"several hundred"* employees in the Alexa division were fired (Ortakales & Kim, 2024). The respondent discussed the question marks surrounding the profitability of Amazon's hardware activities, to explain the rationale behind this downscaling:

> *It's probably good. When I was there, at one point we were shipping like 75 hardware products every year. That's ridiculous, that was way too much. Hardware I don't think has ever been a very good business for Amazon, like in terms of a profit centre. And for many years, they kind of justified the*

> *hardware business with a lot of hand-waving and sort of math tricks, of like "Well, if someone buys an Echo device, they're more likely to buy content, or they're more likely to sign up for a monthly service or become a Prime customer". And "if you're a Prime customer, you're more likely to buy more things on Amazon" and... You know, Amazon talks about these "flywheels" and all these things that keep these other flywheels moving. I think over the last couple years in the hardware business, the leadership has said "OK, enough of all that. Hardware needs to actually be a profitable business, on its own." [...] Part of it could be just other portions of the business saying "hey, it's not fair that the hardware team gets to sort of hand-wave away all of their losses. And we don't get that". Or maybe they just realise it's not actually that true.*

Another participant too expects Amazon to eventually bring more focus into their product lines, but did not directly relate this to a pursuit for revenue. This is part of their argument for why they expect that *"at the end of the day, LoRaWAN Alliance would prevail"* (§9.3.2).

> *[I]f you look at Sidewalk now in Amazon, comparing to other business units and the overall group, business unit is peanuts. So they always, you know, for a big giant, a rich guy, they have a lot of pets. Or for a king, they have a lot of artists, right? Then eventually, only one artist can stay; the other artists are all too small or not famous, they have to go away. Something like this, right? So this is what I'm very concerned and worried about. But if LoRaWAN prevail, I don't see a problem for that. I envision more and more people joining the bandwagon of LoRaWAN for different application.*

[N1] similarly acknowledged that Amazon has scaled down their Alexa and device divisions. This participant related this to Matter, that has tuned down their smart-home ambitions and now takes a different focus with their standard. [N1] generally doubts the feasibility of a smart-home oriented business model, meaning that a reduction of Sidewalk activity would not surprise them. This underlines again that Sidewalk's value to Amazon is most likely in attracting IoT developers to AWS (§9.2.1).

> *And actually what they have done is that they kind of let go of the smarthome part. [...] And what it actually means to me, is that you're in the IoT market, that everyone is taking a step back to not the wishful thinking, of "okay, we're going to smarthome, make people's lives better, and people are going to take out subscriptions for that", or "hey, we're going to smarthome, and then we'll suck the whole house dry in terms of data and we'll be able to offer you better ads and products". Actually what you see is that, for both hypotheses, that business case is not there.*

9.3.2. Tensions with the LoRa Alliance

§7.3.1 argued that interviewees believe Amazon's entry into the LoRa and IoT domain to increase customer awareness and grow the market that they operate in. However, Sidewalk also poses an alternative to LoRaWAN (§4.4.1). This caused tensions between Amazon and the LoRa Alliance, which is especially striking considering that Amazon is a Sponsor member and holds one seat in the board (§4.2.2), as [A6] elaborated:

> *Amazon is a member of the LoRa Alliance. The LoRa Alliance is the, I would say, the governing body on what the LoRaWAN specifications are. So to have a company that is using the LoRa radio, but not using LoRaWAN in their main implementation... Again, they do have a LoRaWAN network server, but Sidewalk does not use LoRaWAN, it's a proprietary approach. You know, that was an interesting complication. And that's something that we have to deal with sometimes delicately, with the LoRa Alliance, is that we do both LoRaWAN, and we also use what they feel is a competing communication stack. They really want Sidewalk to use LoRaWAN. That's between those two organizations. [...] And I'm sure there were valid reasons that Amazon did it, right. I mean, just infrastructure alone could be pretty complicated. I can't really comment much, beyond just speculation.*

The Alliance tried to persuade Amazon to switch Sidewalk to the LoRaWAN standard, even establishing a *"LoRaWAN-Versus-Proprietary"* working group to tailor the standard more to Amazon's wishes (Blackman, 2020). To no avail: Sidewalk presently relies on a proprietary LoRa implementation (Amazon Technologies, 2024). Another interviewee (that holds a high position in the Alliance) predicted a joint future: *"I think at the end of the day, LoRaWAN Alliance would prevail. Reason being that it is an open platform that anyone can participate. And this is a pool, that encourage, and actually supports entrepreneur spirit. Whereas Sidewalk is owned by someone, right? [...] I think it is a great idea to have Sidewalk, but I*

think at the end of the day, they will have to move back to LoRaWAN". Here, the respondent argued that Sidewalk is now just one project of Amazon, that will be eliminated at some point, in typical fashion for a large technology company (see §9.3.1). They therefore expect that Sidewalk and LoRaWAN will *"maybe 5 or 8 years later [...] be all unified to one universal standard"*. This implies that current Sidewalk devices would become compatible with this standard, thus not necessarily putting Sidewalk-adopting companies at risk. However, the interviewee did not speak on their expectation of the crowdsourced nature remaining in place, which is one of Sidewalk's key value propositions (§5.5.1).

9.3.3. Lack of communication within Amazon

Two interviewees provided anecdotes wherein different divisions of Amazon insufficiently communicated with each other, causing the miss of a business opportunity, and a waste of resources, respectively. As a consequence of this lacking communication, Sidewalk might not be used to its fullest potential within Amazon, or its value might not be clear to higher-ups that have power to cut its development. This puts Sidewalk at a specially precarious position within Amazon when considering their hardware business downscaling.

The first anecdote concerns the potential benefit for Amazon's logistics business if it were to leverage Sidewalk coverage for tracking their own assets (i.e. shipments). The interviewee suggested the Sidewalk team to put Bluetooth trackers with GPS in Amazon's last-mile delivery trucks, for pinpointing their locations in residential neighbourhoods that typically have high Sidewalk coverage. However, this suggestion made the team *"laugh, because that's the fulfilment part of the company, right? It's not Sidewalk. They basically don't talk to each other"*, except potentially *"at the VP level"*.

The second anecdote comes from an interviewee that has worked on Sidewalk and Sidewalk-enabled products. Here, the lack of communication is between product engineers and their higher-ups. Their story about the development of *"a Tile type of device that would use the Sidewalk network"* is detailed in §C.7.2. The partnership that made Tile trackers compatible with Sidewalk, is *"what killed the project, right? We were in the middle of it, and then they cut a deal, you know, the executives cut a deal with Tile. And we're like 'yeah, well, then, we don't need this other thing'. [... O]nce they got Tile deal, then it was sort of, 'what's the point here?'"* This quote demonstrates that Amazon's higher-ups can leave product developers in the dark about their business initiatives, effectively laying their efforts to waste.

9.3.4. Complications to expanding Sidewalk outside the US

If Sidewalk is successful in the US, Amazon could consider rolling it out in other regions to make more revenue off of it. [A6] confidently said that this is indeed Amazon's intention. This statement conveys a belief that Sidewalk will be around for a while.

However, different legislations hinder an expansion of Sidewalk to Europe. [N1] brought up that the EU's GDPR might prevent Amazon from transforming Echo and Ring devices into gateways on opt-out basis. This claim was not verified for scope reasons. On a more technical note, interviewees consider the European LoRa regulations to inhibit Sidewalk from attaining a similar level of functionality as in the US. In §B.5.2, I elaborate that Europe regulates how often a device may communicate at a certain frequency per hour (known as *"duty cycle"*), which the US does not regulate. As such, duty cycle regulations limit both how much bandwidth devices can process (both up- and downlink), and how often they can 'listen' for incoming downlink traffic, when using the LoRa protocol in Sidewalk. These limitations directly undermine Sidewalk's premise of 'continuous connectivity'. IoT manufacturers would then be up to the challenge of providing their customers enough value (i.e. sufficient information transmitted by their endpoints, or commands sent to it) with a less powerful network than in the US. [N1] considers these regulations as prohibitive for Amazon to bring Sidewalk to Europe: he does not even know *"how exactly they plan to do that"*.

Theoretically, Amazon could bring Sidewalk to other territories without duty cycle regulations. In the eyes of [A2], though, the globally fragmented regulatory landscape of radio frequencies quickly makes this messy. This incurs overhead for both Amazon and manufacturers. I elaborate this in §B.5.3.

Finally, Sidewalk's coverage relies on the amount of active Echo and Ring devices, and hence on their usage numbers per country.

9.4. Manufacturers' struggles with adopting additional connectivity protocols

The uncertainty of Sidewalk's longevity (§9.3) and its other disadvantages (§8.4) lead manufacturers to adopt other connectivity protocols besides Sidewalk, such as Matter and LoRaWAN (§4.4). Other reasons include extending the coverage for their endpoints and enhancing the customer experience (§9.4.1). However, adopting Sidewalk hampers IoT companies' ability to do so, contributing further to manufacturers' dependence on Amazon (§9.4.2). Consequently, companies' bargaining position vis-à-vis Amazon weakens, with Amazon knowing that pivoting to other protocols and cloud infrastructures incurs significant overhead for manufacturers.

9.4.1. Rationale for implementing multiple protocols

A plethora of reasons pleading for compatibility with various communication methods surfaced in the interviews. [A1] neatly captures the three reasons that manufacturers provided, namely improving the customer experience, extending coverage, and mitigating reliance on a single closed technology.

> *It is sort of a "hedging your bets" kind of thing. I don't know if the final end state of this will be that one of these protocols wins, but, you know, the more you can support, the better it is for your customers. If you say "Oh well, you can buy this [product], but it only works with Sidewalk", I think that - even if that's fine for the customer, and that'll do what they need - just the perception of "well, I'm kind of locked into this one ecosystem", I think doesn't feel good. Especially because, you never know. [... Amazon] could just say "forget it, the Sidewalk thing didn't work out, we're abandoning it". And there's not a lot that you could do about that. And especially if you're a little company, if you based your whole company around that, that's a bad spot to be in.*

First, two companies mentioned making their endpoints compatible with other protocols, so that they can communicate with third-party IoT devices that customers also use [A1, A6, A7]. As such, they improve the customer experience, akin to how Amazon aims to integrate third-party devices in their Alexa ecosystem (§9.2.1). For one interviewee, it is currently Matter that promises them interoperability with different platforms of IoT devices their users might control their endpoints from: *"[W]e want different wireless technology product that we build now, to, you know, simultaneously or concurrently working on one platform. And Matter seems to offer that kind of possibility"*.

Second, using more connectivity protocols generally increases coverage [A6, A8]. Some technologies are more widely adopted in one industry or area than another. For instance, LoRaWAN is not available across the entire US, and cellular coverage has dead zones. The fact that Sidewalk does not restrict itself to a set of states but operates nation-wide was hailed, although interviewees also pointed out that the coverage is not as pervasive in less urban areas (see Amazon (n.d.-g)). And with Sidewalk only being available in the US, companies with international ambitions must necessarily invest into other communication technologies. This argument is aptly summarised by the following quote, that conveys a sentiment shared by multiple interviewees: *"Our objective is connectivity. We're not trying to say that we are a purely LoRaWAN company, or purely Sidewalk company. Our objective is to make sure that that device connects"*. However, this quote leaves all the advantages that adopters mentioned next to connectivity (e.g. sustaining business relations with Amazon; §5.5) out of view.

Third, manufacturers fear reliance on one single technology governed by one single company for business reasons [A1, A2, A3]. As I established in §9.3, nothing guarantees Sidewalk's long-term viability, nor that Sidewalk will outlive other LPWAN protocols [A1, A7]. Manufacturers are practically stuck in a perpetual state of uncertainty. As the quote opening this section highlights, adopters think customers are also wary of being locked into a closed, proprietary network. This reliance concern steers companies towards more open protocols, including LoRa, Matter, and BLE [A1, A7, A8]. [A7] said that *"if I want to play this kind of 'owned by someone'-game, I would go to T-Mobile, you know, I'll go to the KPN, you know. They have a bigger network for coverage, and they are financial, even financial rich, and they're very good with the government regulation and all this."* In this quote, it seems the interviewee would prefer a closed network by a telecom provider because they deem their solutions or them as a company to be more reliable, which is understandable given the risks to Sidewalk's longevity elicited in §9.3.

9.4.2. Difficulty to support multiple protocols at once

Sidewalk's powerful hardware requirements and extensive governance regime do not only imply high development and product costs for manufacturers (§8.4.3). The hardware requirements further hamper companies' ability to adopt multiple protocols in their endpoints. The resource-heavy Sidewalk stack may not leave room in the device to support other communication protocols, too. In principle, any hardware component (e.g. compute power, battery, memory, radios) can be the bottleneck. For two respondents, their devices' memory prohibited them to support Matter over Thread, and LoRaWAN, in addition to Sidewalk. Conversely, two B2B-oriented participants said their devices do support LoRaWAN simultaneously, although one found this *"pretty complicated"* to realise. It follows that the business orientation influences the ability to adopt multiple protocols, because business users are less cost-oriented than consumers are (5.3).

Besides the technical resource requirements, Sidewalk's many governance measures are taxing on organisational resources, as I argued in §8.4.3. Manufacturers must have sufficient knowledge and staff to understand the multiple protocols, and entertain multiple production lines (e.g., remember the anecdote of making *"a salty pancake and a sweet pancake"* in §8.2.2). Simultaneously appeasing Amazon's governance measures makes it difficult to adopt multiple protocols.

As such, adopting Sidewalk crafts a path dependency for adopters on both a device and organisational level. Companies pursuing Sidewalk-compatibility surrender both resources of their device (e.g. memory and battery), and of their organisation (e.g. *"R&D bandwidth"* and staff time), that cannot be dedicated to adopting other protocols. This is especially problematic for smaller companies. Over time, organisations adapt their devices and development processes to support this limited set of protocols, meaning that knowledge about and flexibility to develop for other protocols fades away over time. This aligns with what Cutolo and Kenney (2021) say happens with third-parties becoming locked into a platform ecosystem when the ecosystem necessitates asset-specific investments.

9.5. Dependency of Amazon on manufacturers

Chapter 9 outlined the myriad ways wherein IoT manufacturers grow dependent on Amazon when adopting Sidewalk. I asked interviewees how they perceive their relation with Amazon and deem this problematic. To their own surprise, they were positive about these relations, which they explain by saying that the success of Sidewalk relies on the success of adopters. [A6] nicely illustrates this:

> *[T]hey don't just provide a service and then say "don't call us". It's very much an interactive process, it's really a partnership, which is surprising coming from such a large company. Normally in a large company scenario, they say "here it is, take it or leave it, don't bother us". But they're very, very different. It's been a very unusually positive experience for us. I mean, we worked in our careers with many other companies that have been much less than that. So to have such a big company be so friendly and supportive, it's very helpful for our company success.*

Other Sidewalk-adopting interviewees agreed, referring to their relationship with Amazon as *"transparent"* and *"fairly open"*. A respondent mentioned having access to Sidewalk's senior engineers. [A2] phrased it as: *"it's a relationship. It's not a 'fire and forget' kind of thing. We are part of their ecosystem."* This implies an asymmetry and hierarchy in [A2]'s relationship, with Amazon 'owning' the ecosystem and [A2] merely being a part of it. This opinion also appeared when they mentioned that the Sidewalk security is arranged in *"almost an identical way"* as their own product security scheme that already existed before Sidewalk was published. [A2] saw this as *"a pat on the back. But it just showed that we've made the same analysis and selected the same tools, as someone who has more bandwidth and more resources to do the correct choices. That just validates that the choices that we made, based on what we knew, is the same as someone who probably knows more."* [A2] thus considers themselves inferior to the big Amazon.

Given their earlier experiences with large tech companies, [A2], [A6], and [A8] were surprised that Amazon actually invests in their relation. Apparently, smaller companies typically make do with whatever big companies give them. What motivates Amazon's remarkably friendly attitude?

[A6] gives the answer: *"[T]hey want us to be successful, because our success equals their success. And the last thing they want to do is have it all fall apart because they didn't help people out"*. Sidewalk's success indeed depends on the adopters' success. Manufacturers must obtain sufficient customers to run a healthy business, which prolongs the manufacturers' use of Sidewalk and therefore fuels Amazon's

revenue generation opportunities. For this reason, Amazon *"consider[s] both my customer and me to be their customer"*, as one interviewee said. Simultaneously, a good public reception of manufacturers' products and services could attract more manufacturers or motivate gateway owners to opt in. Indeed, Amazon pursued different partnerships to *"show off what Sidewalk can do"* [A6] across the three application domains, simultaneously diverting from privacy backlash (§5.1).

It is this reciprocity that [A2] expects to protect their company from a sudden price hike for AWS or Sidewalk usage: *"if Amazon wanted to have the best quarter ever in revenue, they'd just crank up the prices on AWS and no one could do anything about it basically, and they would make a lot of money. But people will start to migrate away. So every action has a consequence here, right? So we also have to trust that Amazon as a company wants customers."* This interpretation is too simplistic, though. The interviewee contradicts that *"people will start to migrate away"* by saying that *"no one could do anything about it basically"*. Migrating away from AWS to another cloud infrastructure is cost-intensive, as it requires moving data and processes, and getting familiar with the newly chosen infrastructure. Also, the entanglement of Sidewalk and AWS practically forces manufacturers to use AWS for managing Sidewalk devices (§8.3.3). Similarly, if Amazon would charge for Sidewalk access, then the investments of manufacturers to adopt the service (including developing a compatible device, buying compatible silicon, going through the qualification process) would be in vain. Moreover, as §9.4 argued, path dependencies limit manufacturers' ability to switch to other connectivity methods. The sunk costs, path dependency, and loss of Sidewalk advantages might lead customers to stomach a price increase.

Besides needing successful adopters to make Sidewalk a success, Amazon relies on them to improve Sidewalk itself. The periodic check-in meetings (§8.1.2) provide Amazon valuable feedback from their manufacturers and, through them, their end-users. For instance, Amazon improved Sidewalk's cybersecurity by adopting designs suggested by [A6]. Moreover, one interviewee helped Amazon shape the testing procedure of the qualification process. Thus, while Amazon uses these meetings to help adopters with how to best utilise Sidewalk, address issues, and roll out new features to endpoints [A6], these provide a forum for tapping into manufacturers' experiences and encouraging co-development of both Sidewalk and AWS.

9.6. Chapter conclusion

Having established how manufacturers must The reconfigurations that manufacturers must endure in their production environment to adopt Sidewalk (Chapter 8), suggests that they make themselves dependent on Amazon. This was the premise of this Chapter. In both chapters, I showed the myriad ways wherein these dependencies occur. Manufacturers rely on Amazon's choices regarding *inter alia* which chips they can buy; how the production line (and HSM) must be set up; which Amazon devices can function as gateway; how endpoints must be managed (i.e. from within AWS); how prototypes are qualified; how Sidewalk devices may be marketed; and the bandwidth constraints.

Manufacturers give up all this autonomy, even though there is a curious asymmetry between Sidewalk's value to them, and to Amazon. Sidewalk is clearly aligned with the revenue-generating activities of Amazon (§9.2): it most tangibly spurs use of their cloud services, and enables them to sell their IoT devices at higher prices or offer additional services on top of them. Further, they could choose to monetise Sidewalk use. Conversely, §8.5 concluded that the main benefits for adopters are befriending Amazon, rather than improving their devices or enabling end-users to contribute to their community, as the marketing material revolves around. Meanwhile, it is the manufacturers that invest efforts and resources, that ultimately has the effect of expanding Amazon's cloud infrastructure and market power.

To redeem these opportunities, Amazon relies on Sidewalk adopters to become successful, leading Amazon to maintain a friendly attitude (§9.5). However, multiple uncertainties in Amazon's business put Sidewalk's longevity at risk (§9.3). In this context, mind that Amazon manages to mobilise the knowledge and development resources of both adopters and silicon providers to improve their services: both for Sidewalk (e.g. its security, and the qualification process), and for AWS more generally. As such, it is imaginable that Amazon does not envision Sidewalk as a key profit maker, but rather as a vehicle to making AWS as attractive for IoT developers as possible. Consequently, if Amazon's direct revenue generation (e.g. through selling endpoints, or monetising AWS or Sidewalk itself) is insufficiently profitable, Amazon can pull the plug out of Sidewalk when they decide they have sufficiently learnt

how to improve AWS for IoT developers.

Conversely, manufacturers generally resort to subscription-based business models (§5.3); they might not have had long enough time to earn back their significant investments into becoming Sidewalk-compatible. Granted the sketched dependencies, they will then be left empty-handed. Even if Amazon open-sources the network server technology, it remains to be seen whether an organisation can successfully take over Amazon's governance measures to secure the network, including running an encryption infrastructure and qualifying manufacturers.

To make matters worse, adopting Sidewalk hampers manufacturers' abilities to implement other connectivity protocols. Both hardware constraints and limited organisational resources and *"R&D bandwidth"* necessitate them to reduce the amount of protocols they adopt (§9.4). Therefore, manufacturers face a path dependency.

In sum, manufacturers that adopt Sidewalk must adjust their organisational processes and infrastructure, to accommodate its PETs and the strict governance aimed at protecting the service's security. Meanwhile, these very efforts craft a myriad of long-lasting, self-reinforcing dependencies of manufacturers on Amazon.

10

Conclusion and discussion

To conclude the thesis, in this section I answer the research questions (§10.1); explicate my scientific contributions (§10.2); sketch the societal implications of my findings and provide recommendations for policy makers, scholars, and Sidewalk adopters (§10.3); elaborate limitations in the research data and methods (§10.4); and point out interesting avenues for further research (§10.5).

10.1. Conclusion

In this research, I set out to answer the question *"How does Amazon's use of privacy-enhancing technologies in Sidewalk affect its power over IoT manufacturers?"*

To do so, I formulated three subquestions, that I answer in turn hereafter:

1. What is Amazon Sidewalk?
2. What role do privacy-enhancing technologies play in Sidewalk?
3. How does Amazon's technical design and governance of Sidewalk affect the production of IoT devices?

Sidewalk is a crowdsourced network giving connectivity to IoT devices. It covers a vast 90% or 95% of the United States population, which it thanks to Amazon pushing a software update to Echo and Ring devices that were already in people's homes, to transform them into Sidewalk gateways. Crucially, all Sidewalk traffic passes both through gateways owned by people that might not even be aware that their device is used for Sidewalk, and through Amazon's Sidewalk Network Server, that is closely tied to AWS. Contrary to other connectivity protocols that interviewees' companies use (e.g. LoRaWAN and Matter), both the governance and technical architecture of Sidewalk put Amazon at the centre.

Then, I dug into Amazon's and adopters' marketing of Sidewalk. In their communication to gateway owners, Amazon emphasizes that Sidewalk is secure, protects their privacy, and does not consume all their bandwidth.

I also studied manufacturers' (rationales for their) use of Sidewalk. Adopters are active in the domain of utilities, logistics, and building management. The majority of adopters focuses on B2B or both B2B and B2C sales. This highlights an interesting oversight in the current literature: most authors only consider Sidewalk from a consumer perspective. For instance, they may hail the additional functionality that Sidewalk's connectivity brings to consumers' devices, or express worries about Sidewalk's implications for the privacy of gateway or endpoint users. The effect on the way wherein business customers can create value, is overlooked.

Furthermore, while Sidewalk seemingly revolves around making devices *"work better at home and beyond the front door"* (Amazon, n.d.-b), interviewees reported many other incentives, such as leveraging Amazon's reputation, not needing to sell gateways to customers, and most remarkably, sustaining business relations with Amazon (*"befriending the giant"*). With regards to the latter motivator, staying in conversation with Amazon allows both parties to remain updated on business developments and (competing) product launches. Interviewees also reported that they rely on Amazon for their cloud services, marketplace, or logistics business. They expected that adopting Sidewalk, and in that process

helping Amazon shape and expand the service, puts them on a good footing with Amazon.

The fact that all Sidewalk data is processed by gateways and the Sidewalk Network Server, has raised privacy and security questions in the literature. In most communication, Amazon boasts its use of PETs (primarily a combination of encryption and device identifier obfuscation) as protecting the confidentiality of data sent to and from endpoints, which in their eyes protects user privacy. Privacy is thus reduced to confidentiality, sidelining the privacy as control and privacy as practice paradigms (see §2.2.2). The name of Amazon's Privacy and Security Whitepaper is therefore, in my opinion, deceptive. With this guarantee, and the bandwidth limitations, Amazon justifies Sidewalk's opt-out nature, thus managing to take these privacy concerns and instrumentalising them to fend for their use of consumer devices. In fact, multiple interviewees imitated this reasoning. Respondents furthermore excused the opt-out nature of Sidewalk because of the functional benefits it brings to end-users. With an opt-in update of Echo and Ring devices, the current grand coverage would presumably not be achieved. Gateway owners' concerns were dismissed on the ground of them not understanding the value that Sidewalk could bring them in a 'secure' and 'privacy-protecting' way.

Furthermore, Amazon claims that Sidewalk, as a secure connectivity service, can enhance the security of the IoT. The interviews showed that this was not a reason for manufacturers to adopt it. Instead, they saw Sidewalk's security as a necessary characteristic, that did not distinguish it from other protocols (e.g. LoRaWAN) because these are also secure.

Besides the fact that Amazon's privacy and security discourse (and grey literature coverage thereof) reduces privacy to confidentiality, this confidentiality is narrowed down even further to apply only to gateway and endpoint users. Confidentiality worries of manufacturers, i.e. secrecy of business-sensitive data of how their devices operate and interact with the cloud, are not addressed. In fact, the possibility for Amazon to leverage this information to compete with manufacturers lies wide open. Interviewees that were aware of this, seemingly accepted it as a part of doing business with Amazon, thinking that the benefits of Sidewalk outweigh this risk.

I have furthermore demonstrated that Amazon's technical design and governance of Sidewalk affects the production processes of manufacturers. They impact both the design and the deployment phases of their endpoints. First, the technological architecture funnels adopters to use AWS for managing endpoints. All Sidewalk data ends or begins in AWS, meaning that adopters that want to use another cloud service, must manually pull data out of AWS and ingest it in their other infrastructure, and vice versa. This also hampers business consumers who want to have their data routed directly to their own infrastructure. As a side effect, I expect that manufacturers might adopt AWS services additional to that for managing Sidewalk devices, so that they have all business logic in one place. This reasoning also applies the other way around: if manufacturers were already using AWS, their familiarity with it could ease the adoption of Sidewalk.

Second, contrary to Amazon's claims of their secure service making it less necessary for adopters to have know-how about and resources for securing their devices, keying endpoints during fabrication surfaced as a not insignificant hurdle. Similarly, Amazon inserts other companies they have partnered with into the production process (including Yubico and silicon providers) using security as an argument. This means that silicon providers that Amazon has not partnered with are disadvantaged because IoT manufacturers cannot use their chips for their Sidewalk endpoints. Adopters may then choose to use their silicon in other device models, too, as manufacturers must learn what a chip can do.

Third, adopting Sidewalk leads to path dependency. Its hardware footprint limits how many other protocols a device can support besides Sidewalk. Moreover, all technical and governance aspects of Amazon consume resources of adopters (technical, financial, and organisational), leaving less bandwidth for using other protocols.

Meanwhile, adopters not only invest resources to become Sidewalk-compatible, but also to help Amazon optimise Sidewalk. Consider, for example, Amazon showcasing one organisation's product to demonstrate the service's value and divert attention from the privacy backlash; and the fact that adopters gave feedback on the protocol specification and security.

In sum, I demonstrated *inter alia* that Amazon manages to insert other companies in the production process of manufacturers; subjugate manufacturers by instantiating a mandatory qualification process and reserving the right to kick manufacturers off of the network; restrict manufacturers in using

non-AWS cloud providers; determine how often devices can communicate with the cloud and in what power profiles; refrain from giving manufacturers all information that they need for becoming Sidewalk-compatible and keeping the technology under proprietary control; impose terms of use and mandatory organisational audits; and have adopters be kind to Amazon because they see them as a giant that they rely on for multiple other services beyond connectivity (e.g. cloud, logistics, and retail). Especially the latter point implies that power begets power. As a result, the way wherein manufacturers develop and deploy their devices, changes. Being funnelled into AWS could spur other AWS usage. Amazon curbs autonomy in procuring hardware components, as well as in determining how the endpoints work.

These manifestations of power are only possible because of the privacy assurances that Amazon gives, that are enabled by PETs. Amazon recurrently uses privacy and security as reasons to funnel manufacturers into AWS, to oblige manufacturers to buy components from certain companies, to enact its stringent governance measures, and to justify the opt-out approach that was fundamental to reaching Sidewalk's current coverage. Curiously, in doing so, they reduce privacy to confidentiality for endpoint and gateway users. This leaves confidentiality of how endpoints work entirely out of view, exposing manufacturers to the risk of Amazon learning sensitive business information and using this knowledge for competition. Privacy as control and privacy as practice are also not respected. The PETs thus mainly serve a role as marketing device and a justification for Sidewalk's opt-out crowdsourced setup, while granting Amazon insight into usage data generated by endpoints. PETs, together with Amazon's current CI as well as strategic partnerships and marketing, are thus important contributors to the further expansion of their CI.

10.2. Scientific contributions

Looking back on the related literature in Chapter 2, this thesis makes the following scientific contributions. Methodology-wise, this thesis demonstrates that scrutinising technology, contractual standards, and enforcement (cf. van Hoboken & Fathaigh, 2021); developer documentation (cf. van der Vlist et al., 2022); and interdependencies between technologies from both Amazon and third parties (cf. Rodon Modol & Eaton, 2021) is a valuable exercise to identify sources and exertions of power. The results also illustrate the merits of combining a technology analysis with elite interviewing. While initially hard to enter into this world of tech elites, these conversations enable a cross-analysis of the barriers that the technology documentation hints at, and offer unique insights into the typically hidden world of B2B arrangements that a behemoth such as Amazon makes. In this process, it proved worthwhile to not only look for the materialisation of an *ex ante* defined form of power in the case: staying close to the materials brought into view the myriad manifestations of power, that is e.g. of market, disciplinary, and infrastructural nature. I suggest this approach for the future research proposals in §10.5.

Further, I corroborated numerous concepts and mechanisms in the literature. For instance, by establishing that Sidewalk is a way for Amazon to combine its control over the cloud with control over edge devices, the thesis illustrates how a *"twinned power with new capacities for subjectivation and governance"* (Munn, 2022, p. 975) can materialise. Moreover, I showed that the *"agile turn"* in software production that Gürses and van Hoboken (2018) point to, is both what makes Sidewalk possible, and attracts manufacturers. IoT companies' desire to be able to learn how their device is used and performs, and to update it remotely, drives them to the connectivity and operational control that the intertwining of Sidewalk and AWS promises. Simultaneously, Amazon could only attain the enormous coverage by shipping an over-the-air, opt-out update to Echo and Ring devices, and knowing what their locations are to assess the coverage. This illustrates both that Amazon has the ability to redefine user devices for their own financial gain, and that user privacy (or rather: confidentiality) is dynamic and not at all sufficient to capture or justify the complex of power dynamics at play.

This remote control highlights how Amazon is able to leverage their CI to create entirely new markets, namely that of integrated connectivity and cloud. Manufacturers are not primarily concerned with offering digital goods or services to users 'on top' of an established digital user base or service, as is often the assumption in literature about power in online advertising and digital platforms. Neither are endpoint end-users solely interested in using the Sidewalk service. Rather, end-users want to enjoy the functionalities that endpoints bring them, in a reliably way; and manufacturers develop their own endpoints to sell products or services with, and have to reckon with Amazon's infrastructure to do so. Therefore, I contribute to present literature about technology as a source of power, that mostly

looks at tech companies gatekeeping how third parties can access users or user data that the tech company has garnered, to claim more of their current markets; and how tech companies leverage their infrastructures to creep further into other existing markets. Moreover, granted the demonstrated industrial leverage of Amazon and the path dependencies that adopting Sidewalk carves out, we cannot assume that manufacturers only assess their adoption of Sidewalk on the merits of its functionalities and are otherwise free to enter the infrastructure (cf. Hurni et al., 2021).

Finally, I have contributed to the nascent literature on how tech companies leverage PETs to obtain power over other parties, by thoroughly studying the Sidewalk case that is distinctive from priorly documented cases. Amazon repeatedly uses PETs to justify its remote control over gateways; instil trust with manufacturers and endpoint and gateway owners about the security of the network; and to warrant their influence over the production processes of manufacturers. I hope to build momentum for this field and provide a recommendation for follow-up research into a similarly contemporary topic in §10.5.2.

10.3. Societal implications and recommendations

The consequences of the established power dynamics are grand. First, Sidewalk raises a range of competition problems. The barriers to using non-AWS cloud services hampers competition between cloud providers. Because of Sidewalk's proprietary nature, rival cloud companies cannot integrate their services with Sidewalk as neatly as Amazon can. Moreover, Amazon hampers competition between silicon providers and between hardware security module providers. The mandatory qualification process, combined with Amazon's partnerships with select companies, prevents businesses outside these privileged groups from catering to the group of aspiring Sidewalk adopters. Furthermore, the resources and costs that adopting Sidewalk incurs (e.g. with relation to knowing how to key devices, and to keep up with Amazon's repeated check-ins) might hamper Sidewalk adoption by smaller IoT manufacturers. Additionally, these same costs inhibit IoT companies from supporting other IoT protocols, crafting a path dependency. And if history repeats itself, adopters should prepare for competition by Amazon informed by their unique vantage point as Sidewalk provider.

Second, the literature oversees the utter disregard that Amazon has for the concept of 'personal' devices. Amazon has made Echo and Ring owners a fundamental part of changing the ecosystem of the IoT, creating a valuable business proposition for themselves, without meaningful notice nor compensation towards these device owners. As such, they appropriate gateway owners' efforts and money spent on buying their consumer device, placing it in their homes, providing it with electricity and wifi, and troubleshooting it when it is faulty. Proponents of Sidewalk and other opt-out crowdsourced services (e.g. Apple Find My) predominantly evaluate the ethics of tech companies' reconfiguration of consumer devices on the basis of the harm this could bring them. As such, they generally default to user privacy, which is a too constrained focus. As I have demonstrated, this is not the only value at stake. Rather, I encourage a dialogue about fair distribution of gains and personal control over devices.

Third, the more IoT companies within an application domain steer towards adopting Sidewalk, the more these domains will become homogenised. Manufacturers will conform their devices' functioning to the capabilities supported by the Sidewalk protocol, approved chips, and AWS functionalities (e.g. AWS IoT Core for Sidewalk). With that, Amazon could become the standard setter for low-resource long-range networking, and customers will have a less diverse array of IoT devices or services to choose from. It is even imaginable that Amazon leverages this market share argument and technical conformation of Sidewalk adopters, to steer the LoRaWAN standard towards Amazon's advantage, using their position in the board.

These issues remain out of view when, or can perhaps even be partially ascribed to, advocating only for privacy (or confidentiality) protection in digital products and services. While Amazon's (supposed) protection of privacy and security for endpoint and gateway owners is in principle admirable, I have demonstrated the far-reaching implications it has for the production of IoT devices, as well as competition. Therefore, I call upon privacy scholars, advocates, and regulators, to converse with their competition colleagues and jointly consider ways wherein privacy protection augments a company's power.

In this dialogue, it is vital to not only consider end-users' privacy. As I have demonstrated, power especially emerges with respect to the production environments of companies grappling with a CI (i.e. manufacturers adopting Sidewalk), as well as the confidentiality of their business practices. Civil society, researchers, and policymakers traditionally oriented at protecting end-users should therefore pivot to

talking to businesses that adopt services rolled out on top of CI leveraging PETs, to properly lay bare the power emergence and its effects on their production. Ultimately, this ploy also affects consumers, as argued above. I provide suggestions for two example cases in §10.5.1 and §10.5.2.

In addition, I recommend Sidewalk adopters to establish a community; in essence becoming a bottom-up alliance. Interviewees said that the current contact with other adopters is at this point only limited, but because Amazon also depends on their success and feedback to make Sidewalk a success, they have more bargaining power than they might be aware of. While I am under no illusion about manufacturers being able to pull themselves out of AWS, given the path dependencies that Sidewalk adoption incurs and especially their tendency to stay on good footing with Amazon, undertaking effort to constitute a bottom-up interest group might give them a stronger bargaining position vis-à-vis Amazon. As such, they could attempt to alleviate the stringent governance measures and argue for alterations to the technical specification that they desire; much like the LoRaWAN alliance (on paper) allows its members to do (§4.4.1).

10.4. Limitations

The following limitations should be minded when interpreting the research results. First, interviewing has as disadvantage that it is time-consuming, necessitating a limit on the number of interviews. Consequently, the generalisability of the findings deteriorates (Alshenqeeti, 2014). While I interviewed employees from half of the companies that have adopted Sidewalk, which yielded a diverse set of results while also at some points reaching saturation, other adopters might have yet other stories about how they experience Sidewalk adoption. The interviews showed that Amazon gave multiple companies a custom treatment, which additional interviews could provide more insight into. Still, the impact of this shortcoming is limited, because the interviews are not conducted to infer something about a general population (cf. a quantitative approach), but to check whether the presumed power asymmetries between Amazon and IoT manufacturers hold up in practice and how they are perceived (cf. a qualitative approach).

Second, and relatedly, only one interviewee from the group of non-Sidewalk-adopting companies was interviewed. This participant does not work for an IoT manufacturer, but for a LoRaWAN service provider. Hence, the interview sample is likely to be biased towards positive attitudes about Sidewalk, because most participants strongly rely on their Sidewalk offerings for their business or at least had invested significant resources into it. Conversely, while I sought to include the perspectives of IoT companies that decided not to adopt Sidewalk, these lack from the study for reasons of time and trouble in contacting them (elaborated in §3.2.5). While hearing their reasons for not motivating Sidewalk are not necessary to answer the present research question, it would be interesting to hear whether companies refrain from adopting Sidewalk out of fear of falling into the power of Amazon, as I describe in this thesis.

Third, the thesis uses a holistic single-case design, i.e. analysing one 'unit' in one case. A multiple-case design would allow comparing cases across contexts, aiding theory building (Yin, 2017). Yet, the proposition of this thesis of limited duration is already novel and time-consuming to study, making an elaborate exploration within a holistic single-case design more valuable than superficially investigating multiple cases.

Finally, considering data quality, grey literature and technologies have proven biased, inaccessible, and incomplete. For one, Amazon restricts access to certain documents and development portals to Sidewalk-authorised developers. Additionally, Amazon-affiliated reports do not disclose the full details of technical implementations. As illustration, neither Amazon's privacy and security whitepaper (Amazon, 2023n) nor the Sidewalk protocol specification (Amazon Technologies, 2024) provide full details on what (meta)data is processed how for service optimisation. The latter explicitly says that a "*Detailed specification of Gateways and the Amazon Sidewalk Cloud*", and interactions between them, are outside the scope of the specification, without arguing why or referring to other documents that do cover this topic (p. 10).

This limitation applies especially to the argument that Amazon could learn from how endpoints interact with Sidewalk. Triangulation with first-order evidence from a network analysis would strengthen the merit of this argument, that is currently based on knowledge by interviewees and a reading of

descriptive technical documentation. The envisioned network analysis of how and when an endpoint and gateway interact with each other and the cloud, was not finished due to time constraints of the collaborator and logistical challenges (see §3.2.3). I recommend proceeding with this experiment. Currently, this reasoning is based on knowledge or assumptions by interviewees, and a reading of technical documentation.

10.5. Future research

Based on the thesis findings, I see three interesting avenues for future research: extending the Sidewalk case study to involve silicon providers (§10.5.1); replicating the case study by investigating the PET-leveraging finding network Find My by Apple that has similarities with Sidewalk (§10.5.2); and extending the case study into Amazon's expansion of their CI and power by investigating Amazon's other connectivity-related endeavours and their relation to AWS (§10.5.3).

10.5.1. Silicon providers

First, the research could be repeated with a focus on silicon providers instead of on IoT manufacturers. Demonstrating how Amazon accumulates power over IoT manufacturers that adopt Sidewalk, at times shone light on the role of silicon providers in enabling Amazon to do so. For instance, recall that an interviewee stated that silicon providers taught Amazon about manufacturing IoT devices and hardware-level security (§9.2.2).

As demonstrated in §2.3.4, one of the characteristics that sets the Sidewalk case apart from other examples of large tech companies leveraging PETs to expand their power, is the large role that hardware plays: Sidewalk affects physical production of IoT devices. Investigating how Amazon influences silicon providers, who manufacture the lowest level of hardware, contributes to a more thorough understanding of this phenomenon. The stakes for Amazon to be allied to silicon providers are high, as [A3] noted, *"the manufacturing and the development [...], there's a lot of cash associated with that"*. This respondent also thinks Amazon is appealing to more silicon providers to manufacture hardware for Sidewalk chips.

I expect some differences with the present case. Contrary to IoT manufacturers, where connecting devices for their users is the primary purpose of Sidewalk, silicon providers do not need to enable their own products (i.e. chips and radios) to communicate with the cloud. At best, they could configure their firmware such that it periodically sends telemetry data to the silicon provider, and enables over-the-air updates. Silicon providers can then better monitor their chips' performance and address bugs even during use. However, this is hypothetical; the feasibility of this remote control and monitoring, especially considering endpoints' hardware constraints (§8.4.3), would have to be verified with silicon providers.

The consequence of not processing as much data is that silicon providers' cloud use for Sidewalk applications will be lower or even non-existent compared to IoT manufacturers. Therefore, Amazon could have less leverage over silicon providers, because I presume their production to be less reliant on software and data processing than that of IoT manufacturers.

Another difference is that chip production is much more capital-intensive than IoT device production, presumably making it harder for Amazon to outcompete silicon providers by manufacturing chips themselves. To the best of my knowledge, Amazon does not produce its own IoT chips, although they do make their own high-performance compute chips for cloud computing (Amazon, 2022c) and more specifically to power AI models (Wiggers, 2023).

For this extension, the interview questions for interviewing manufacturers can be largely reused. For example, it would be interesting to learn how silicon providers discovered Sidewalk; what moved them to develop for Sidewalk (e.g. did business relations with Amazon play a role, or was it mostly the prospect of being a vital supplier in the Sidewalk ecosystem); and do the benefits outweigh the costs (e.g. educating Amazon, nominating lead customers, educating customers, and developing the actual hardware and SDKs). While the number of eligible companies is lower (as only 4 silicon providers are known to manufacture Sidewalk-eligible hardware (Amazon, 2023j)), these companies are typically larger than Sidewalk adopters, meaning there are more employees to invite for interviews.

10.5.2. Crowdsourced finding networks by Apple and Google

Next, one interviewee alluded to the Apple Find My network. Apple's own devices (e.g. earbuds, phones, and laptops) can be found as part of this network (Apple, n.d.-a), but third-party developers can also make their devices findable by this network (e.g. third-party earbuds, a smart backpack, an electric bike, a smart mug, and trackers similar to Airtags (Bowe, 2022; Menon, 2023)). To do so, they need to join Apple's MFi program (Apple, n.d.-b), that also spans technologies such as Apple's CarPlay, HomeKit, and a module for audio accessories (Apple, n.d.-c). Only enrolled developers can access technical specifications and other resources necessary to develop towards Find My compatibility (Apple, n.d.-b). Similar to Sidewalk, third-party Find My devices must first be certified by Apple, a process that entails submitting a product plan, developing a prototype, and having the prototype and packaging reviewed by Apple (Apple, n.d.-c). For the prototype development, Apple tells adopters to *"Procure any MFi components as needed"* (Apple, n.d.-c), so it could be that adopters are forced to buy certain components from selected silicon providers.

The benefit for third-party adopters is twofold. First, manufacturers can embed finding functionality in devices or services that do not intrinsically revolve around finding (e.g. the earbuds, backpack and bike), reducing development costs while adding value for their users. Second, devices that do revolve around tracking (e.g. those of Chipolo (n.d.-a) and Pebblebee (n.d.-b)) can tap into a finding network much larger and more pervasive than that of their own. These parties typically run on a similar crowdsourced model as Apple Find My, but only users that have the app installed to locate their own tracker report the location of other trackers to the service. Thus, the finding power of the network is limited to the company's user base.

The appeal for tracker manufacturers to join the Apple network is thus clear. Without joining Apple's network, the utility of their devices is dwarfed when compared to Apple's tracker that run on its huge finding network, leaving them to be outcompeted. However, as an interviewee remarked, these companies then essentially become hardware providers to Apple (argued in §8.4.4). With their finding power no longer being a competitive feature, they must distinguish themselves in other ways, such as through the tracker design, price, or add-on services. For instance, Pebblebee offers a business solution with a dashboard to manage multiple trackers at once (Pebblebee, n.d.-a).

The tracker-producing company Chipolo provides another interesting example. They seemingly pivoted their business after becoming Find My-compatible. In addition to selling trackers, Chipolo now caters to other parties that want to join Apple's or Google's finding networks, and offer them consultancy services, a firmware solution, and advice on hardware integration (Chipolo, n.d.-b). They advertise that being one of the first businesses to become compatible with these networks grants them valuable experience they can share with prospective adopters, as well as a firmware solution that is already extensively tested and externally approved (presumably referring to Google's and Apple's certification processes) because they used it for their own products (Chipolo, n.d.-b). It thus appears that Apple's launch of their finding network caused Chipolo to adjust their business model, by also offering consultancy services and sell their own firmware as a service to others, potentially to compensate for reduced sales.

Researching the experiences with and motivation for tracking companies to (not) engineer towards Apple Find My compatibility, similar dynamics as I showed in this thesis could be found. Google is initiating a similar finding network, that also allows third parties, but it is not officially released and opened for third parties yet (Vermes, 2024).

10.5.3. Amazon's other telecom- and connectivity-related endeavours

With Sidewalk, Amazon takes on a role somewhat similar to that of a telecom company that provides connectivity to devices. There are numerous differences that make this an awry analogy (e.g. the fact that Sidewalk is far from a 'neutral pipe' for traffic, but uses it to funnel IoT traffic into AWS, as argued in §8.3.3). Designating Amazon as one for the sake of this exploration brings their other ambitions in this domain into view.

M. Day (2023) writes about Amazon's Project Kuiper. This project entails Amazon making satellites to offer internet connectivity from a low-earth orbit. He notes that Kuiper is a serious bet, with Amazon already having invested over 10 billion US dollars in hopes of becoming a telecom giant selling internet both to home users, business users, and telecom operators that want to connect remote cell towers (see Amazon, 2023p) from 2025 onwards. According to a project head, Amazon *"want[s] to serve enterprise, governments, schools, hospitals, mobile operators, so [they] don't have a single channel, or segment, on which [they]*

make money". But a representative of a space sustainability organisation cited in Grush and Day (2023) questions how many customers Kuiper will have, granted that it might be an expensive alternative, especially for citizens that already have good broadband. This could imply that Amazon's primary bet is selling connectivity to businesses that can afford it. Indeed, M. Day (2023) notes that *"AWS, the largest seller of rented computing power and data storage, will in the coming years be able to offer packages of products that include internet access, a perk that Amazon's cloud-computing rivals can't match on their own"*. While it is not clear how this bundling of connectivity with cloud compute will look in practice, the Kuiper project resembles the way wherein Amazon lures IoT manufacturers into AWS with the promise of connectivity.

An interviewee pointed out that there exist companies who offer LoRaWAN connectivity by Low Earth Orbiting satellites with LoRa gateways inside them. Examples include EchoStar Mobile (n.d.), Lacuna Space (2022), and Wyld Networks (n.d.). To the best of my knowledge, no materials exist that discuss the possibility of Kuiper satellites offering LoRaWAN coverage besides broadband internet access; but it could be a way to expand the Sidewalk network further.

Besides leveraging connectivity to spur AWS usage, Amazon seemingly encroaches on telecom companies in other ways. The Dutch government also recognises that cloud providers *"are increasingly moving into the traditional domain of telecom companies"*, expanding on the current services they offer to telecom providers (Dutch Ministry of Economic Affairs and Climate Policy, 2024, p. 39). As illustration, AWS offers a plethora of services *"empowering telcos to reinvent themselves – transforming from telco to tech-co while moving their core workloads to the cloud"* (Amazon Web Services, n.d.-i). The AWS Marketplace also offers services to *"modernize infrastructure and processes, optimize security operations, and deploy new technologies to drive business initiatives"* (Amazon Web Services, n.d.-h). Investigating these other telecom-related endeavours and how they could grant Amazon power over citizens, businesses, and governments, would be a worthwhile extension of this research.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Acquisti, A., Taylor, C., & Wagman, L. (2016). The Economics of Privacy. *Journal of Economic Literature*, *54*(2), 442–492. https://doi.org/10.1257/jel.54.2.442

Adelantado, F., Vilajosana, X., Tuset-Peiro, P., Martinez, B., Melià-Segui, J., & Watteyne, T. (2017). Understanding the Limits of LoRaWAN. *IEEE Communications Magazine*, *55*(9), 34–40. https://doi.org/10.1109/MCOM.2017.1600613

Agahari, W., Ofe, H., & de Reuver, M. (2022). It is not (only) about privacy: How multi-party computation redefines control, trust, and risk in data sharing. *Electronic Markets*, *32*, 1577–1602. https://doi.org/10.1007/s12525-022-00572-w

Agre, P. E. (1994). Surveillance and capture: Two models of privacy. *The Information Society*, *10*(2), 101–127. https://doi.org/10.1080/01972243.1994.9960162

Airthings. (n.d.). *Airthings*. Airthings. Retrieved January 21, 2024, from https://www.airthings.com/en/

Airthings. (2023, March 29). *Annual Report 2022*. Airthings. Oslo, Norway. https://www.airthings.com/hubfs/Website/investors/reports/Airthings-Annual-Report-2022.pdf

Akyildiz, I. F., & Wang, X. (2009, March 2). *Wireless Mesh Networks* (1st ed., Vol. 3). Wiley. Retrieved February 8, 2024, from http://ebookcentral.proquest.com/lib/delft/detail.action?docID=437489

Alasseri, R., Joji Rao, T., & Sreekanth, K. J. (2018). Conceptual framework for introducing incentive-based demand response programs for retail electricity markets. *Energy Strategy Reviews*, *19*, 44–62. https://doi.org/10.1016/j.esr.2017.12.001

Alshenqeeti, H. (2014). Interviewing as a Data Collection Method: A Critical Review. *English Linguistics Research*, *3*(1), 39–45. https://doi.org/10.5430/elr.v3n1p39

Amazon. (n.d.-a). *Amazon Devices: Echo Smart Speakers & Displays*. Amazon India. Retrieved March 2, 2024, from https://www.amazon.in/amazon-echo/b?ie=UTF8&node=14156834031

Amazon. (n.d.-b). *Amazon Sidewalk*. Amazon. Retrieved February 28, 2024, from https://www.amazon.com/Amazon-Sidewalk/b?ie=UTF8&node=21328123011

Amazon. (n.d.-c). *Amazon Sidewalk Test Kit*. Amazon Sidewalk. Retrieved February 12, 2024, from https://sidewalk.amazon/testkit

Amazon. (n.d.-d). *Frustration-Free Setup*. Amazon Developer. Retrieved March 12, 2024, from https://developer.amazon.com/frustration-free-setup

Amazon. (n.d.-e). *Frustration-Free Setup: Provisionee Barcode Specification*. Amazon Developer. Retrieved March 12, 2024, from https://developer.amazon.com/docs/frustration-free-setup/provisionee-1d-barcode-specification.html

Amazon. (n.d.-f). *Getting Started with Amazon Frustration-Free Setup*. Amazon Developer. Retrieved March 12, 2024, from https://developer.amazon.com/frustration-free-setup/getting-started

Amazon. (n.d.-g). *Sidewalk Coverage Maps*. Sidewalk Coverage Maps. Retrieved March 3, 2024, from https://coverage.sidewalk.amazon/

Amazon. (n.d.-h). *Sidewalk360*. Sidewalk360. Retrieved February 23, 2024, from https://360.sidewalk.amazon/

Amazon. (2021a, May 7). *Echo, Tile, and Level devices join Amazon Sidewalk*. About Amazon. Retrieved January 21, 2024, from https://www.aboutamazon.com/news/devices/echo-tile-and-level-devices-join-amazon-sidewalk

Amazon. (2021b, September 27). *CareBand and Life360 tap Amazon technology to help people stay connected*. About Amazon. Retrieved January 21, 2024, from https://www.aboutamazon.com/news/devices/careband-and-life360-tap-amazon-technology-to-help-people-stay-connected

Amazon. (2022a, January 6). *Amazon Sidewalk Bridge Pro offers professional-grade connectivity*. About Amazon. Retrieved March 4, 2024, from https://www.aboutamazon.com/news/devices/amazon-sidewalk-bridge-pro-offers-professional-grade-connectivity

Amazon. (2022b, July 1). *Amazon Response to Senator Markey*. Senator Edward Markey of Massachusetts. https://www.markey.senate.gov/imo/media/doc/amazon_response_to_senator_markey-july_13_2022.pdf

Amazon. (2022c, August 11). *Take a look inside the lab where AWS makes custom chips*. About Amazon. Retrieved February 25, 2024, from https://www.aboutamazon.com/news/aws/take-a-look-inside-the-lab-where-aws-makes-custom-chips

Amazon. (2022d, September). *Amazon Sidewalk Privacy and Security Whitepaper*. Retrieved March 28, 2023, from https://web.archive.org/web/20230328145953/https://m.media-amazon.com/images/G/01/sidewalk/final_privacy_security_whitepaper.pdf

Amazon. (2023a). *Amazon Sidewalk Gateways*. Amazon Sidewalk Documentation. Retrieved January 8, 2024, from web.archive.org/web/20240302142350/https://docs.sidewalk.amazon/introduction/sidewalk-gateways.html

Amazon. (2023b). *Amazon Sidewalk Gateways*. Amazon Sidewalk Documentation. Retrieved December 11, 2023, from http://web.archive.org/web/20231211071017/https://docs.sidewalk.amazon/introduction/sidewalk-gateways.html

Amazon. (2023c). *Amazon Sidewalk manufacturing setup and workflow*. Amazon Sidewalk Documentation. Retrieved January 9, 2024, from https://docs.sidewalk.amazon/manufacturing/sidewalk-manufacturing-setup-works.html

Amazon. (2023d). *Amazon Sidewalk Program Requirements*. Amazon Sidewalk Documentation. Retrieved March 16, 2024, from https://docs.sidewalk.amazon/sidewalk-terms-and-agreements/sidewalk-program-requirements.html

Amazon. (2023e). *Amazon Sidewalk Program Security Requirements*. Amazon Sidewalk Documentation. Retrieved March 16, 2024, from https://docs.sidewalk.amazon/sidewalk-terms-and-agreements/security-program-requirements.html

Amazon. (2023f). *Amazon Sidewalk Qualification Concepts*. Amazon Sidewalk Documentation. Retrieved March 16, 2024, from https://docs.sidewalk.amazon/qualification/works-with-sidewalk/sidewalk-qualification-concepts.html

Amazon. (2023g). *Components of Amazon Sidewalk manufacturing*. Amazon Sidewalk Documentation. Retrieved January 9, 2024, from https://docs.sidewalk.amazon/manufacturing/sidewalk-manufacturing-components.html

Amazon. (2023h). *How Amazon Sidewalk Works*. Amazon Sidewalk Documentation. Retrieved March 15, 2024, from https://docs.sidewalk.amazon/introduction/sidewalk-how-works.html

Amazon. (2023i). *Introduction to Amazon Sidewalk*. Amazon Sidewalk Documentation. Retrieved February 10, 2024, from https://docs.sidewalk.amazon/introduction/

Amazon. (2023j). *Qualified development kits*. Amazon Sidewalk Documentation. Retrieved February 3, 2024, from https://docs.sidewalk.amazon/getting-started/Qualified-Development-Kits.html

Amazon. (2023k). *Terms and Agreements*. Amazon Sidewalk Documentation. Retrieved February 23, 2024, from https://docs.sidewalk.amazon/sidewalk-terms-and-agreements/

Amazon. (2023l). *Works with Amazon Sidewalk Qualification Guidelines*. Amazon Sidewalk Documentation. Retrieved March 16, 2024, from https://docs.sidewalk.amazon/sidewalk-terms-and-agreements/wwas-sidewalk-qualification-guidelines.html

Amazon. (2023m). *Works With Amazon Sidewalk Qualification Process*. Amazon Sidewalk Documentation. Retrieved February 6, 2024, from https://docs.sidewalk.amazon/qualification/works-with-sidewalk/qualification-works-path.html

Amazon. (2023n, March). *Amazon Sidewalk Privacy and Security Whitepaper*. Retrieved March 19, 2024, from https://m.media-amazon.com/images/G/01/sidewalk/final_privacy_security_whitepaper.pdf

Amazon. (2023o, March 28). *Amazon Invites Developers to Test Sidewalk and Build the Next Billion Connected Devices*. About Amazon. Retrieved January 13, 2024, from https://press.aboutamazon.com/2023/3/amazon-invites-developers-to-test-sidewalk-and-build-the-next-billion-connected-devices

Amazon. (2023p, September 5). *Here's how Project Kuiper's satellite network can help telecom partners like Vodafone and Vodacom enhance reliability and extend reach*. About Amazon. Retrieved February 26, 2024, from https://www.aboutamazon.eu/news/innovation/heres-how-project-kuipers-satellite-network-can-help-telecom-partners-like-vodafone-and-vodacom-enhance-reliability-and-extend-reach

Amazon. (2024a, January). *Software Development Manager, Ring*. Amazon Jobs. Retrieved February 13, 2024, from https://web.archive.org/web/20240213094920/https://www.amazon.jobs/en/jobs/2523471/software-development-manager-ring

Amazon. (2024b, February 6). *Embedded Software Engineer - Amazon Sidewalk, Amazon Sidewalk*. Amazon Jobs. Retrieved February 13, 2024, from https://web.archive.org/web/20240213093646/https://www.amazon.jobs/en/jobs/2553181/embedded-software-engineer-amazon-sidewalk-amazon-sidewalk

Amazon Technologies. (2023a, March 26). *Amazon Sidewalk Sid API Developer Guide* (Protocol Stack 1.0, Document Revision A). Retrieved February 28, 2024, from https://docs.sidewalk.amazon/assets/pdf/Amazon_Sidewalk_Sid_API_Developer_Guide-1.0-rev-A-032623.pdf

Amazon Technologies. (2023b, March 28). *Amazon Sidewalk Specification* (Protocol Stack 1.0, Document Revision A). Retrieved February 28, 2024, from https://docs.sidewalk.amazon/assets/pdf/Amazon_Sidewalk_Specification-1.0-rev-A-032823.pdf

Amazon Technologies. (2023c, July 25). *Amazon Sidewalk Test Specification* (Protocol Stack 1.0, Document Revision A.1). Retrieved March 18, 2024, from https://docs.sidewalk.amazon/assets/pdf/Amazon_Sidewalk_Test_Specification-1.0-rev-A.1.pdf

Amazon Technologies. (2024, February 8). *Amazon Sidewalk Specification* (Protocol Stack 1.0, Document Revision A.1). Retrieved February 28, 2024, from https://docs.sidewalk.amazon/assets/pdf/Amazon_Sidewalk_Specification-1.0-rev-A.1-020824.pdf

Amazon Web Services. (n.d.-a). *AWS IoT Core Device Location*. AWS IoT Core Developer Guide. Retrieved February 11, 2024, from https://docs.aws.amazon.com/iot/latest/developerguide/device-location.html

Amazon Web Services. (n.d.-b). *AWS IoT Core for LoRaWAN*. Amazon Web Services. Retrieved March 23, 2024, from https://aws.amazon.com/iot-core/lorawan/

Amazon Web Services. (n.d.-c). *AWS IoT Device Defender*. Amazon Web Services. Retrieved March 20, 2024, from https://aws.amazon.com/iot-device-defender/

Amazon Web Services. (n.d.-d). *AWS Pricing: Internet of Things*. Amazon Web Services. Retrieved March 16, 2024, from https://aws.amazon.com/pricing/?awsf.tech-category=tech-category%23iot

Amazon Web Services. (n.d.-e). *Manage a Connected AWS IoT Device Fleet*. Amazon Web Services workshop studio. Retrieved March 1, 2024, from https://catalog.workshops.aws/aws-iot-device-fleet-management/en-US/setup-fleet-metrics

Amazon Web Services. (n.d.-f). *Manage a Connected AWS IoT Device Fleet*. Amazon Web Services workshop studio. Retrieved March 1, 2024, from https://catalog.workshops.aws/aws-iot-device-fleet-management/en-US

Amazon Web Services. (n.d.-g). *Partners: Yubico*. Amazon Web Services. Retrieved February 28, 2024, from https://partners.amazonaws.com/partners/001E00000101DhfIAE/

Amazon Web Services. (n.d.-h). *Telecom solutions in AWS Marketplace*. Amazon Web Services. Retrieved February 26, 2024, from https://aws.amazon.com/marketplace/solutions/telecom

Amazon Web Services. (n.d.-i). *Transforming Telcos*. Amazon Web Services. Retrieved February 26, 2024, from https://aws.amazon.com/telecom/transforming-telcos/

Amazon Web Services. (n.d.-j). *What is AWS IoT Core for Amazon Sidewalk?* AWS IoT Core Developer Guide. Retrieved February 26, 2024, from https://docs.aws.amazon.com/iot/latest/developerguide/amazon-sidewalk-intro.html

Apple. (n.d.-a). *Find My*. Apple Support. Retrieved February 26, 2024, from https://support.apple.com/find-my

Apple. (n.d.-b). *Find My network*. Apple Developer. Retrieved February 25, 2024, from https://developer.apple.com/find-my

Apple. (n.d.-c). *How It Works*. Apple MFi Program. Retrieved February 25, 2024, from https://mfi.apple.com/en/how-it-works

Apple. (n.d.-d). *Privacy*. Apple. Retrieved February 27, 2024, from https://www.apple.com/privacy/

Apple. (2023, May 2). *Apple and Google lead initiative for an industry specification to address unwanted tracking*. Apple Newsroom. Retrieved February 24, 2024, from https://www.apple.com/newsroom/2023/05/apple-google-partner-on-an-industry-specification-to-address-unwanted-tracking/

Arrive. (n.d.). *Arrive Campaign on PicMii Crowdfunding*. PicMii Crowdfunding. Retrieved January 21, 2024, from https://www.picmiicrowdfunding.com/deal/arrive/

Arrive. (2023, July 31). *Arrive Announces Successful Integration with Amazon Sidewalk*. Arrive. Retrieved January 21, 2024, from https://www.arrive.tech/news/arrive-announces-successful-integration-with-amazon-sidewalk

Arrive. (2024). *Arrive*. Arrive. Retrieved January 21, 2024, from https://www.arrive.tech

ATLAS.ti. (2023, May 9). *ATLAS.ti Desktop* (Version 23.1.2). Retrieved February 28, 2024, from https://atlasti.com/atlas-ti-desktop

Baker, R. (2023, January 17). *Everything You Should Know About Amazon Sidewalk*. SlashGear. Retrieved February 28, 2024, from https://www.slashgear.com/1169639/everything-you-should-know-about-amazon-sidewalk/

Bakonyi, J. (2022). Modular sovereignty and infrastructural power: The elusive materiality of international statebuilding. *Security Dialogue*, *53*(3), 256–278. https://doi.org/10.1177/09670106211051943

Ballance, L. (2024a, January 13). *Wave: Understanding the connectivity and compatibility of your Wave*. Airthings Help Center. Retrieved January 21, 2024, from https://help.airthings.com/en/articles/6009826-wave-understanding-the-connectivity-and-compatibility-of-your-wave

Ballance, L. (2024b, January 13). *What's the difference between Airthings smart products?* Airthings Help Center. Retrieved January 21, 2024, from https://help.airthings.com/en/articles/5161848-what-s-the-difference-between-airthings-smart-products

Baur, A. (2023). European Dreams of the Cloud: Imagining Innovation and Political Control. *Geopolitics*. https://doi.org/10.1080/14650045.2022.2151902

Binder, M. (2022, July 29). *Web3 darling Helium has bragged about Lime being a client for years. Lime says it isn't true.* Mashable. Retrieved March 21, 2024, from https://mashable.com/article/helium-lime-web3-crypto

Bishop, T. J., & Hamren, L. (2024, January 13). *'Unfinished business': Ring CEO Liz Hamren leads Amazon's home monitoring products into the AI era*. GeekWire. https://www.geekwire.com/2024/unfinished-business-ring-ceo-liz-hamren-leads-amazons-home-monitoring-products-into-the-ai-era/

Blackman, J. (2020, December 8). *LoRa Alliance in talks with Amazon to switch Sidewalk over to LoRaWAN*. RCR Wireless News. Retrieved February 7, 2024, from https://www.rcrwireless.com/20201208/internet-of-things/lora-alliance-semtech-in-talks-with-amazon-to-switch-sidewalk-over-to-lorawan

Blancato, F. G. (2023). The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem. *Policy & Internet*, Advance online publication. https://doi.org/10.1002/poi3.358

Blanke, T., & Pybus, J. (2020). The Material Conditions of Platforms: Monopolization Through Decentralization. *Social Media + Society*, *6*(4). https://doi.org/10.1177/2056305120971632

Bowe, T. (2022, August 25). *All the Non-Apple Gadgets the "Find My" App Can Find*. Gear Patrol. Retrieved February 25, 2024, from https://www.gearpatrol.com/tech/g36063168/apple-find-my-compatible-gadgets/

Boyne, S. M. (2020). Data Protection in the United States: U.S. National Report. In D. Moura Vicente & S. de Vasconcelos Casimiro (Eds.), *Data Protection in the Internet* (pp. 409–455, Vol. 38). Springer International Publishing. https://doi.org/10.1007/978-3-030-28049-9_17

Brodkin, J. (2023, June 1). *FTC: Amazon/Ring workers illegally spied on users of home security cameras*. Ars Technica. Retrieved February 24, 2024, from https://arstechnica.com/tech-policy/2023/06/ftc-amazon-ring-workers-illegally-spied-on-users-of-home-security-cameras/

Budd, C. (2020, December 12). *Amazon Sidewalk rollout shows the future of 'forced opt-in,' taking lessons from Xfinity Wifi*. GeekWire. Retrieved March 14, 2024, from https://www.geekwire.com/2020/amazon-sidewalk-rollout-shows-future-forced-opt-taking-lessons-xfinity-wifi/

Bundesverfassungsgericht. (1983, December 15). *Urteil des Ersten Senats vom 15. Dezember 1983 - 1 BvR 209, 269, 362, 420, 440, 484/83* (ECLI:DE:BVerfG:1983:rs19831215.1bvr020983). Retrieved October 3, 2023, from https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html

Busch, C. (2021, September). *Regulation of digital platforms as infrastructures for services of general interest*. Friedrich-Ebert-Stiftung. Bonn, Germany. https://library.fes.de/pdf-files/wiso/17836.pdf

C99. (2023, October 29). *Subdomain Finder scan of sidewalk.amazon*. Subdomain Finder. Retrieved October 29, 2023, from https://subdomainfinder.c99.nl/scans/2023-10-29/sidewalk.amazon

Cahn, A. F., & Galperin, E. (2021, May 13). *Apple's AirTags Are a Gift to Stalkers*. Wired. Retrieved February 15, 2024, from https://www.wired.com/story/opinion-apples-air-tags-are-a-gift-to-stalkers/

Callas, J. (2021, June 22). *Understanding Amazon Sidewalk*. Electronic Frontier Foundation. Retrieved February 28, 2024, from https://www.eff.org/deeplinks/2021/06/understanding-amazon-sidewalk

CareBand. (n.d.-a). *Products*. CareBand. Retrieved January 21, 2024, from https://carebandremembers.com/products/

CareBand. (n.d.-b). *Technology*. CareBand. Retrieved January 21, 2024, from https://carebandremembers.com/powered-by-third-wave/

Casadesus-Masanell, R., & Hervas-Drane, A. (2015). Competing with Privacy. *Management Science*, *61*(1), 229–246. https://doi.org/10.1287/mnsc.2014.2023

Chase, J. (2021, June 7). *Amazon Sidewalk Will Share Your Internet With Strangers. It's Not As Scary As It Sounds.* Wirecutter. Retrieved February 28, 2024, from https://www.nytimes.com/wirecutter/blog/amazon-sidewalk-review/

Chatting, D., Taylor, N., & Rogers, J. (2021). Design for Reappearance in Smart Technologies. *CSCW 2021 Workshop on Designing for Data Awareness*. www.nick-taylor.co.uk/wp-content/uploads/chatting_cscw21_workshop.pdf

Chaudhari, B. S., Zennaro, M., & Borkar, S. (2020). LPWAN Technologies: Emerging Application Characteristics, Requirements, and Design Considerations. *Future Internet*, *12*(3), Article 46. https://doi.org/10.3390/fi12030046

Chipolo. (n.d.-a). *Chipolo*. Chipolo. Retrieved February 26, 2024, from https://chipolo.net/en/

Chipolo. (n.d.-b). *Integrations*. Chipolo. Retrieved February 25, 2024, from https://chipolo.net/en/pages/integrations

Ciovacco, R. (2020, September 21). *Amazon Sidewalk paves the way for more connected communities*. Alexa Device Makers Blog. Retrieved January 22, 2024, from https://developer.amazon.com/en-US/blogs/alexa/device-makers/2020/09/amazon-sidewalk-paves-the-way-for-more-connected-communities.html

Cleave, P. (2021). Two Suns? Data Doppelgangers and the Construction of the Digital Self. *Te Kaharoa*, *14*(1). https://doi.org/10.24135/tekaharoa.v17i1.352

Cohen, J. E. (2013). What Privacy Is For. *Harvard Law Review*, *126*(7), 1904–1933. https://doi.org/https://heinonline.org/HOL/LandingPage?handle=hein.journals/hlr126&div=88

Comcast. (n.d.-a). *Wifi on the Go: How does a hotspot work?* Xfinity. Retrieved February 27, 2024, from https://www.xfinity.com/hub/internet/internet-on-the-go

Comcast. (n.d.-b). *Xfinity WiFi hotspots overview*. Xfinity. Retrieved February 7, 2024, from https://www.xfinity.com/support/articles/about-xfinity-wifi-internet

Comcast. (2021, April 13). *Comcast's MachineQ Updates Platform-as-a-Service for IoT Solutions at Scale*. Comcast. Retrieved January 29, 2024, from https://corporate.comcast.com/press/releases/comcasts-machineq-updates-platform-as-a-service-for-iot-solutions-at-scale

Conger, K., & Chen, B. X. (2022, February 3). *A Change by Apple Is Tormenting Internet Companies, Especially Meta*. The New York Times. Retrieved February 28, 2024, from https://www.nytimes.com/2022/02/03/technology/apple-privacy-changes-meta.html

Connectivity Standards Alliance. (n.d.). *Our Members*. CSA-IOT. Retrieved February 11, 2024, from https://csa-iot.org/members/

Cook, J. (2019, June 19). *Amazon drones could be used to film your home and spot intruders, patent reveals*. The Telegraph. Retrieved February 22, 2024, from https://www.telegraph.co.uk/technology/2019/06/19/amazon-drones-could-used-spy-home-spot-intruders-patent-reveals/

Core Specification 4.2. (2014, December 2). Bluetooth SIG. Retrieved March 2, 2024, from https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=441541

Crist, R. (2021, June 8). *Amazon Sidewalk will create entire smart neighborhoods. Here's what you should know*. CNET. Retrieved February 22, 2024, from https://www.cnet.com/home/smart-home/amazon-sidewalk-will-create-entire-smart-neighborhoods-faq-ble-900-mhz/

Cutolo, D., & Kenney, M. (2021). Platform-Dependent Entrepreneurs: Power Asymmetries, Risks, and Strategies in the Platform Economy. *Academy of Management Perspectives*, *35*(4), 584–605. https://doi.org/10.5465/amp.2019.0103

Day, G., & Stemler, A. R. (2019). Infracompetitive Privacy. *Iowa Law Review*, *105*, 61–106. https://doi.org/https://ilr.law.uiowa.edu/print/volume-105-issue-1/infracompetitive-privacy

Day, M. (2023, December 18). *Inside Amazon's Effort to Challenge Musk's Starlink Internet Business*. Bloomberg. Retrieved February 26, 2024, from https://www.bloomberg.com/news/features/2024-02-25/comac-steals-the-limelight-in-singapore-with-first-peek-inside-c919-jet

Day, M. (2024, January 24). *Amazon's Ring to Stop Letting Police Request Doorbell Video From Users*. Bloomberg. Retrieved February 24, 2024, from https://www.bloomberg.com/news/articles/2024-01-24/amazon-s-ring-to-stop-letting-police-request-video-from-users

de Diego Martín, M. Á. (2016, March). *Net Neutrality: Smart Cables or Dumb Pipes? An overview on the regulatory debate about how to govern the network*. College of Europe. Brugge, Belgium. Retrieved March 20, 2024, from https://aei.pitt.edu/85831/1/researchpaper_3_2016_miguel_angel_de_diego_martin.pdf

de Reuver, M., Sørensen, C., & Basole, R. C. (2018). The Digital Platform: A Research Agenda. *Journal of Information Technology*, *33*(2), 124–135. https://doi.org/10.1057/s41265-016-0033-3

de Reuver, M., van Wynsberghe, A., Janssen, M., & van de Poel, I. (2020). Digital platforms and responsible innovation: Expanding value sensitive design to overcome ontological uncertainty. *Ethics and Information Technology*, *22*(3), 257–267. https://doi.org/10.1007/s10676-020-09537-z

Despres, T., Patil, S., Tan, A., Watson, J.-L., & Dutta, P. (2022). Where the Sidewalk Ends: Privacy of Opportunistic Backhaul. *Proceedings of the 15th European Workshop on Systems Security*, 1–7. https://doi.org/10.1145/3517208.3523757

Deviceroy. (n.d.). *Aria*. Deviceroy. Retrieved March 4, 2024, from https://deviceroy.com/aria/

Deviceroy. (2023a, January 5). *Connectivity Revolution: Deviceroy's Aria Integrates with Amazon Sidewalk at CES*. Deviceroy. Retrieved January 21, 2024, from https://deviceroy.com/connectivity-revolution-deviceroys-aria-integrates-with-amazon-sidewalk-at-ces/

Deviceroy. (2023b, April). *Aria Spec Sheet*. Deviceroy. Retrieved January 21, 2024, from https://deviceroy.com/wp-content/uploads/2023/04/Aria-Spec-Sheet-1.pdf

Diaz, C., & Gürses, S. F. (2012). Understanding the landscape of privacy technologies. *Proceedings of the 2012 Information Security Summit*. https://doi.org/https://lirias.kuleuven.be/1662140

DLA Piper. (2023a, January 26). *DLA Piper's Data Protection Laws of the World Handbook: Collection & Processing*. DLA Piper. Retrieved January 8, 2024, from https://www.dlapiperdataprotection.com/index.html?t=collection-and-processing&c=US&c2=CA

DLA Piper. (2023b, January 26). *DLA Piper's Data Protection Laws of the World Handbook: Definitions*. DLA Piper. Retrieved January 8, 2024, from https://www.dlapiperdataprotection.com/index.html?t=definitions&c=US&c2=CA

Dutch Ministry of Economic Affairs and Climate Policy. (2024, January 22). *De staat van de digitale infrastructuur: De ruggengraat van onze digitale economie*. The Hague, The Netherlands. Retrieved March 18, 2024, from https://www.rijksoverheid.nl/documenten/rapporten/2024/01/22/staat-van-de-digitale-infrastructuur

Eaton, B., Elaluf-Calderwood, S., Sørensen, C., & Yoo, Y. (2015). Distributed Tuning of Boundary Resources: The Case of Apple's iOS Service System. *MIS Quarterly*, *39*(1), 217–243. https://doi.org/10.25300/MISQ/2015/39.1.10

EchoStar Mobile. (n.d.). *LoRa® Enabled Massive IoT Network*. EchoStar Mobile. Retrieved February 26, 2024, from https://echostarmobile.com/services/pan-european-lora-iot-network/

Edwards, B. (2021, May 9). *What Is Apple's Find My Network?* How-To Geek. Retrieved February 26, 2024, from https://www.howtogeek.com/725842/what-is-apples-find-my-network/

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. *The Academy of Management Review*, *14*(4), 532–550. https://doi.org/10.2307/258557

Emerson, S., Jeans, D., & Liu, P. (2022, September 23). *Crypto Darling Helium Promised A 'People's Network.' Instead, Its Executives Got Rich.* Forbes. Retrieved March 21, 2024, from https://www.forbes.com/sites/sarahemerson/2022/09/23/helium-crypto-tokens-peoples-network/

ETSI Technical Committee Electromagnetic compatibility and Radio spectrum Matters. (2018, June). *ETSI EN 300 220-2 V3.2.1 (2018-06): Short Range Devices (SRD) operating in the frequency range 25 MHz to 1 000 MHz; Part 2: Harmonised Standard for access to radio spectrum for non specific radio equipment* (REN/ERM-TG28-535). ETSI. Retrieved January 7, 2024, from https://www.etsi.org/deliver/etsi_en/300200_300299/30022002/03.02.01_60/en_30022002v030201p.pdf

European Commission. (2022, December 20). *Antitrust: Commission accepts commitments by Amazon barring it from using marketplace seller data, and ensuring equal access to Buy Box and Prime*.

European Commission. Retrieved February 18, 2024, from https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7777

European Commission. (2023, September 6). *Digital Markets Act: Commission designates six gatekeepers*. European Commission. Retrieved February 21, 2024, from https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328

European Union Agency for Cybersecurity. (2022, January 27). *Data Protection Engineering: From Theory to Practice*. European Union Agency for Cybersecurity (ENISA). https://doi.org/10.2824/09079

Fahmida, S., Modekurthy, V. P., Ismail, D., Jain, A., & Saifullah, A. (2022). Real-Time Communication over LoRa Networks. *Proceedings of the 2022 IEEE/ACM Seventh International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 14–27. https://doi.org/10.1109/IoTDI54339.2022.00019

Fahy, R., van Hoboken, J., & van Eijk, N. (2018). Data Privacy, Transparency and the Data-Driven Transformation of Games to Services. *Proceedings of the 2018 IEEE Games, Entertainment, Media Conference (GEM)*, 1–9. https://doi.org/10.1109/GEM.2018.8516441

Farivar, C. (2020, February 15). *Cute videos, but little evidence: Police say Amazon Ring isn't much of a crime fighter*. NBC News. Retrieved February 22, 2024, from https://www.nbcnews.com/news/all/cute-videos-little-evidence-police-say-amazon-ring-isn-t-n1136026

Fleishman, G. (2021, May 28). *How to opt out of the Find My network*. Macworld. Retrieved February 26, 2024, from https://www.macworld.com/article/347243/how-to-opt-out-of-the-find-my-network.html

Frankel, D. (2018, June 28). *6 executives quietly pulling the strings on cable's convergence into wireless*. StreamTV Insider. Retrieved January 29, 2024, from https://www.streamtvinsider.com/cable/six-execs-quietly-pulling-strings-cable-s-convergence-into-wireless

Fukuyama, F., Richman, B., & Goel, A. (2021). How to Save Democracy from Technology: Ending Big Tech's Information Monopoly. *Foreign Affairs*, *100*, 98–110. https://doi.org/https://heinonline.org/HOL/LandingPage?handle=hein.journals/fora100&div=14

Ghazawneh, A., & Henfridsson, O. (2013). Balancing platform control and external contribution in third-party development: The boundary resources model. *Information Systems Journal*, *23*(2), 173–192. https://doi.org/10.1111/j.1365-2575.2012.00406.x

Ghazawneh, A., & Henfridsson, O. (2015). A paradigmatic analysis of digital application marketplaces. *Journal of Information Technology*, *30*(3), 198–208. https://doi.org/10.1057/jit.2015.16

Gonsalves, A. (2023, April 4). *OnAsset logistics service taps Amazon Sidewalk*. TechTarget. Retrieved January 21, 2024, from https://www.techtarget.com/searchnetworking/news/365534914/OnAsset-logistics-service-taps-Amazon-Sidewalk

Goodin, D. (2021, May 29). *Amazon devices will soon automatically share your Internet with neighbors*. Ars Technica. Retrieved February 28, 2024, from https://arstechnica.com/gadgets/2021/05/amazon-devices-will-soon-automatically-share-your-internet-with-neighbors/

Google. (n.d.-a). *Exposure Notifications: Using technology to help public health authorities fight COVID-19*. Google COVID-19 Information & Resources. Retrieved February 28, 2024, from https://www.google.com/intl/en_ie/covid19/exposurenotifications/

Google. (n.d.-b). *The Privacy Sandbox: Technology for a More Private Web.* The Privacy Sandbox. Retrieved February 13, 2024, from https://privacysandbox.com/

Grush, L., & Day, M. (2023, October 6). *Amazon's SpaceX Duel Heats Up as Tardy Satellites Set to Fly*. Bloomberg. Retrieved February 26, 2024, from https://www.bloomberg.com/news/articles/2023-10-05/amazon-to-launch-long-delayed-satellites-in-race-with-spacex

Grynwajc, S. (2020, December 17). *Privacy at the Crossroads: A Comparative Analysis of Regulation in the U.S., the EU and Canada*. Law Office of S. Grynwajc: Transatlantic Legal Services. Retrieved January 8, 2024, from https://www.transatlantic-lawyer.com/privacy-laws-focus-on-a-transatlantic-perspective/

Guariglia, M. (2020, February 4). *What to Know Before You Buy or Install Your Amazon Ring Camera*. Electronic Frontier Foundation. Retrieved February 22, 2024, from https://www.eff.org/deeplinks/2020/02/what-know-you-buy-or-install-your-amazon-ring-camera

Guariglia, M. (2024, January 24). *Victory! Ring Announces It Will No Longer Facilitate Police Requests for Footage from Users*. Electronic Frontier Foundation. Retrieved February 24, 2024, from https://www.eff.org/deeplinks/2024/01/ring-announces-it-will-no-longer-facilitate-police-requests-footage-users

Guariglia, M., & Maass, D. (2021, February 16). *LAPD Requested Ring Footage of Black Lives Matter Protests*. Electronic Frontier Foundation. Retrieved February 22, 2024, from https://www.eff.org/deeplinks/2021/02/lapd-requested-ring-footage-black-lives-matter-protests

Guariglia, M., Portnoy, E., & Budington, B. (2021, February 2). *Amazon Ring's End-to-End Encryption: What it Means*. Electronic Frontier Foundation. Retrieved February 24, 2024, from https://www.eff.org/deeplinks/2021/02/amazon-rings-end-end-encryption-what-it-means

Gürses, S. (2010, May). *Multilateral Privacy Requirements Analysis in Online Social Network Services* [Doctoral dissertation, KU Leuven]. https://www.esat.kuleuven.be/cosic/publications/thesis-177.pdf

Gürses, S., Shrishak, K., van Gend, T., Bertulfo, D., & Troncoso, C. (2024, January 24). *Privacy is Big business: How Big Tech instrumentalizes PETs to expand its infrastructural power* (Conference panel). Privacy Camp 24, Brussels, Belgium. Retrieved February 22, 2024, from https://www.youtube.com/watch?v=X3ryzl5aCec

Gürses, S., Troncoso, C., & Diaz, C. (2015). Engineering Privacy by Design Reloaded. *Amsterdam Privacy Conference 2015*. https://doi.org/https://www.esat.kuleuven.be/cosic/publications/article-2589.pdf

Gürses, S., & van Hoboken, J. (2018, April 18). Privacy after the Agile Turn. In E. Selinger, J. Polonetsky, & O. Tene (Eds.), *The Cambridge Handbook of Consumer Privacy* (pp. 579–601). Cambridge University Press. https://doi.org/10.1017/9781316831960.032

Hanley, D. A. (2021, July 1). *Eyes Everywhere: Amazon's Surveillance Infrastructure and Revitalizing a Fair Marketplace*. Open Markets. Retrieved February 22, 2024, from https://papers.ssrn.com/abstract=4089858

Harris, M. (2018, October 19). *Video doorbell firm Ring says its devices slash crime—but the evidence looks flimsy*. MIT Technology Review. Retrieved February 22, 2024, from https://www.technologyreview.com/2018/10/19/103922/video-doorbell-firm-ring-says-its-devices-slash-crimebut-the-evidence-looks-flimsy/

Harrison, H., Birks, M., Franklin, R., & Mills, J. (2017). Case Study Research: Foundations and Methodological Orientations. *Forum: Qualitative Social Research*, *18*(1), Article 19. https://doi.org/10.17169/fqs-18.1.2655

Haskins, C. (2019a, July 25). *Amazon Requires Police to Shill Surveillance Cameras in Secret Agreement*. Vice. Retrieved February 22, 2024, from https://www.vice.com/en/article/mb88za/amazon-requires-police-to-shill-surveillance-cameras-in-secret-agreement

Haskins, C. (2019b, August 2). *US Cities Are Helping People Buy Amazon Surveillance Cameras Using Taxpayer Money*. Vice. Retrieved February 22, 2024, from https://www.vice.com/en/article/d3ag37/us-cities-are-helping-people-buy-amazon-surveillance-cameras-using-taxpayer-money

Haskins, C. (2019c, August 9). *Ring Told People to Snitch on Their Neighbors in Exchange for Free Stuff*. Vice. Retrieved February 22, 2024, from https://www.vice.com/en/article/ne8wqx/ring-told-people-to-snitch-on-their-neighbors-in-exchange-for-free-stuff

Hein, A., Schreieck, M., Riasanow, T., Setzke, D. S., Wiesche, M., Böhm, M., & Krcmar, H. (2019). Digital platform ecosystems. *Electronic Markets*, *30*(1), 87–98. https://doi.org/10.1007/s12525-019-00377-4

Hern, A. (2023, April 11). *TechScape: The end of the 'free money' era*. The Guardian. Retrieved March 17, 2024, from https://www.theguardian.com/technology/2023/apr/11/techscape-zirp-tech-boom

Higginbotham, S. (2021, January 7). *You've got mail! The Ring Mailbox sensor reviewed*. Stacey on IoT. Retrieved January 23, 2024, from https://staceyoniot.com/ring-mailbox-sensor-review-amazon-sidewalk-network/

Higginbotham, S. (2023, April 25). *CareBand bet on Amazon Sidewalk. How will it turn out?* Stacey on IoT. Retrieved January 21, 2024, from https://staceyoniot.com/careband-bet-on-amazon-sidewalk-how-will-it-turn-out/

Hoepman, J.-H. (n.d.). *The 5th Interdisciplinary Summerschool on Privacy (ISP 2023)*. The 5th Interdisciplinary Summerschool on Privacy (ISP 2023). Retrieved October 4, 2023, from https://isp.cs.ru.nl/2023/

Holley, P. (2018, December 18). *This patent shows Amazon may seek to create a 'database of suspicious persons' using facial-recognition technology*. The Washington Post. Retrieved February 22, 2024, from https://www.washingtonpost.com/technology/2018/12/13/this-patent-shows-amazon-may-seek-create-database-suspicious-persons-using-facial-recognition-technology/

Høyer Leivestad, H., & Nyqvist, A. (Eds.). (2017, June 21). *Ethnographies of Conferences and Trade Fairs: Shaping Industries, Creating Professionals*. Springer International Publishing. https://doi.org/10.1007/978-3-319-53097-0

Humphry, J., & Chesher, C. (2021). Visibility and security in the smart home. *Convergence: The International Journal of Research into New Media Technologies*, *27*(5), 1170–1188. https://doi.org/10.1177/13548565211030073

Hurni, T., Huber, T. L., & Dibbern, J. (2021). Power dynamics in software platform ecosystems. *Information Systems Journal*, *32*(2), 310–343. https://doi.org/10.1111/isj.12356

Husovec, M., & Roche Laguna, I. (2023, September 7). Digital Services Act: A Short Primer. In M. Husovec & I. Roche Laguna (Eds.), *Principles of the Digital Services Act* (advance online publication). Oxford University Press. Retrieved March 20, 2024, from http://dx.doi.org/10.2139/ssrn.4153796

IEEE Standard for Local and metropolitan area networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 3: Physical Layer (PHY) Specifications for Low-Data-Rate, Wireless, Smart Metering Utility Networks (802.15.4g). (2012, April 27). IEEE. New York, United States. Retrieved March 2, 2024, from https://doi.org/10.1109/IEEESTD.2012.6190698

INFO-LEG. (2023). *Beyond Data Protection Conference: Regulating Information and Protection against Risks of the Digital Society*. INFO-LEG. Retrieved November 30, 2023, from https://web.archive.org/web/20231130100523/http://infolegproject.net/beyond-data-protection-conference-2023/

Information Commissioner's Office. (2023, May 19). *Privacy-enhancing technologies (PETs)*. Information Commissioner's Office. Retrieved February 18, 2024, from https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies-1-0.pdf

Internet Archive. (n.d.). *Wayback Machine*. Retrieved March 2, 2024, from https://web.archive.org/

ITU. (n.d.). *Regionally harmonized bands*. ITU. Retrieved February 7, 2024, from https://www.itu.int:443/en/ITU-R/information/Pages/emergency-bands.aspx

Iyer, B., & Getchell, K. (2018, February 13). *Why APIs Should Be Regulated*. MIT Sloan Management Review. Retrieved February 19, 2024, from https://sloanreview.mit.edu/article/why-regulate-digital-organizations-apis/

James, M. (2023, August 24). *How To Turn Off Sidewalk on Alexa (and Why You Should)*. All About Cookies. Retrieved February 1, 2024, from https://allaboutcookies.org/opt-out-amazon-sidewalk

Jamison, M. A. (2018). Net Neutrality Policies and Regulation in the United States. *Review of Network Economics*, *17*(3), 151–173. https://doi.org/10.1515/rne-2018-0041

jcesnik. (2024, January 29). *SX126x radio HAL/SID source access*. Silicon Labs. Retrieved March 13, 2024, from https://siliconlabs.my.site.com/community/s/question/0D58Y0000B0Vr6rSQC/sx126x-radio-halsid-source-access

Jones, D. (2019, September 26). *Amazon Intros 'Sidewalk' Protocol for Low-Power IoT Networks*. Light Reading. Retrieved January 30, 2024, from https://www.lightreading.com/network-platforms/amazon-intros-sidewalk-protocol-for-low-power-iot-networks

Jorgensen, D. L. (1989). *Participant observation: A methodology for human studies* (Vol. 15). Sage. Retrieved February 14, 2024, from https://tudelft.on.worldcat.org/oclc/781976430

Kalra, A., & Stecklow, S. (2021, October 13). *Amazon copied products and rigged search results, documents show*. Reuters. Retrieved February 18, 2024, from https://www.reuters.com/investigates/special-report/amazon-india-rigging/

Karabus, J. (2023, August 17). *Stalking victims sue Tile and Amazon for negligence over tracking tech*. Retrieved February 24, 2024, from https://www.theregister.com/2023/08/17/tile_and_amazon_lawsuit/

Klinge, T. J., Hendrikse, R., Fernandez, R., & Adriaans, I. (2023). Augmenting digital monopolies: A corporate financialization perspective on the rise of Big Tech. *Competition & Change*, *27*(2), 332–353. https://doi.org/10.1177/10245294221105573

Kostova, B., Gürses, S., & Troncoso, C. (2020, July 16). *Privacy Engineering Meets Software Engineering. On the Challenges of Engineering Privacy By Design*. arXiv: SSRN. https://doi.org/10.48550/arXiv.2007.08613

Kuan, F. (2023, April 26). *Extend Your IoT Devices Range with Amazon Sidewalk Devices from MOKOSmart*. MOKOSmart. Retrieved January 21, 2024, from https://www.mokosmart.com/amazon-sidewalk-devices-from-mokosmart/

Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: A review. *Journal of Big Data*, *6*, Article 111. https://doi.org/10.1186/s40537-019-0268-2

Lacuna Space. (2022, January 11). *Lacuna and Semtech Expand LoRaWAN® Coverage through IoT to Satellite Connectivity*. Lacuna Space. Retrieved February 26, 2024, from https://lacuna.space/lacuna-and-semtech-expand-lorawan-coverage-through-iot-to-satellite-connectivity/

Lardinois, F. (2023, January 5). *Amazon Sidewalk adds new partners, plans to open to developers soon*. TechCrunch. Retrieved February 8, 2024, from https://techcrunch.com/2023/01/05/amazon-sidewalk-adds-new-partners-plans-to-open-to-developers-soon/

Latour, B. (1987). *Science in action: How to follow scientists and engineers through society*. Harvard University Press. Retrieved February 14, 2024, from http://archive.org/details/scienceinaction0000unse

Ledvina, B., Eddinger, Z., Detwiler, B., & Polatkan, S. P. (2023, December 20). *Detecting Unwanted Location Trackers* (IETF Draft No. draft-detecting-unwanted-location-trackers-01). Internet Engineering Task Force: Network Working Group. Retrieved February 27, 2024, from https://datatracker.ietf.org/doc/draft-detecting-unwanted-location-trackers

Lee, R. (n.d.). *Tech Layoff Tracker and Startup Layoff Lists*. Layoffs.fyi. Retrieved February 12, 2024, from https://layoffs.fyi/

Level. (n.d.-a). *Multifamily*. Level. Retrieved January 21, 2024, from https://level.co/multifamily/

Level. (n.d.-b). *Smart Lock Catalog*. Level. Retrieved January 21, 2024, from https://level.co/smart-lock/

Level. (n.d.-c). *Support: Home Integrations: Sidewalk*. Level. Retrieved January 21, 2024, from https://level.co/support/sections/Sidewalk03

Lofland, J., & Lofland, L. H. (1984). *Analyzing Social Settings: A Guide to Qualitative Observation and Analysis* (2nd ed.). Wadsworth. Retrieved February 14, 2024, from http://archive.org/details/analyzingsocial00lofl

LoRa Alliance. (n.d.-a). *Board, Chairs & Staff*. LoRa Alliance®. Retrieved January 13, 2024, from https://lora-alliance.org/board-officers/

LoRa Alliance. (n.d.-b). *Certification*. LoRa Alliance®. Retrieved March 20, 2024, from https://lora-alliance.org/lorawan-certification/

LoRa Alliance. (n.d.-c). *Member Directory*. LoRa Alliance®. Retrieved January 13, 2024, from https://lora-alliance.org/member-directory/

LoRa Alliance. (n.d.-d). *Membership Benefits*. LoRa Alliance®. Retrieved January 13, 2024, from https://lora-alliance.org/become-a-member/

LoRa Alliance. (n.d.-e). *Product Marketplace Search*. LoRa Alliance®. Retrieved March 20, 2024, from https://lora-alliance.org/marketplace/search/

LoRa Alliance. (n.d.-f). *Tiers & Costs*. LoRa Alliance®. Retrieved January 13, 2024, from https://lora-alliance.org/membership-benefits/

LoRa Alliance Technical Committee. (2020, October). *LoRaWAN® L2 1.0.4 Specification (TS001-1.0.4)*. LoRa Alliance. Retrieved January 7, 2024, from https://resources.lora-alliance.org/technical-specifications/ts001-1-0-4-lorawan-l2-1-0-4-specification

LoRa Alliance Technical Committee Regional Parameters Workgroup. (2023, September 17). *LoRaWAN® Regional Parameters RP002-1.0.4*. LoRa Alliance. Retrieved January 7, 2024, from https://resources.lora-alliance.org/technical-specifications/rp002-1-0-4-regional-parameters

Lucas, J. (1998). The tension between despotic and infrastructural power: The military and the political class in Nigeria, 1985–1993. *Studies in Comparative International Development*, *33*(3), 90–113. https://doi.org/10.1007/BF02687493

Lyons, K. (2021, January 31). *Amazon's Ring now reportedly partners with more than 2,000 US police and fire departments*. The Verge. Retrieved February 22, 2024, from https://www.theverge.com/2021/1/31/22258856/amazon-ring-partners-police-fire-security-privacy-cameras

MachineQ. (n.d.). *Platform*. MachineQ. Retrieved January 29, 2024, from https://machineq.com/platform

Mahieu, R. (2021). The right of access to personal data: A genealogy. *Technology and Regulation*, *2021*, 62–75. https://doi.org/10.26116/techreg.2021.005

Mattioli, D. (2020, April 23). *Amazon Scooped Up Data From Its Own Sellers to Launch Competing Products*. The Wall Street Journal. Retrieved February 18, 2024, from https://www.wsj.com/articles/amazon-scooped-up-data-from-its-own-sellers-to-launch-competing-products-11587650015

McGee, P. (2021, October 17). *Apple's privacy changes create windfall for its own advertising business*. Financial Times. Retrieved February 22, 2024, from https://www.ft.com/content/074b881f-a931-4986-888e-2ac53e286b9d

McGuigan, L., West, S. M., Sivan-Sevilla, I., & Parham, P. (2023). The after party: Cynical resignation in Adtech's pivot to privacy. *Big Data & Society*, *10*(2). https://doi.org/10.1177/20539517231203665

McIntosh, D. (2019). We Need to Talk about Data: How Digital Monopolies Arise and Why They Have Power and Influence. *Journal of Technology Law & Policy*, *23*, 185–213. https://doi.org/https://heinonline.org/HOL/LandingPage?handle=hein.journals/jtlp23&div=11&id=&page=

Mekki, K., Bajic, E., Chaxel, F., & Meyer, F. (2019). A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express*, *5*(1), 1–7. https://doi.org/10.1016/j.icte.2017.12.005

Menon, P. (2023, October 30). *Best Find My devices for iPhone in 2023*. XDA Developers. Retrieved February 25, 2024, from https://www.xda-developers.com/best-find-my-devices-iphone/

Merrick, R., & Ryan, S. (2019). Data Privacy Governance in the Age of GDPR. *Risk Management*, *66*(3), 38–43. Retrieved January 8, 2024, from https://www.proquest.com/magazines/data-privacy-governance-age-gdpr/docview/2215472110/se-2?accountid=27026

MerryIoT. (n.d.). *Product*. MerryIoT. Retrieved January 21, 2024, from https://www.merryiot.com/Product

MerryIoT. (2023, July 24). *MerryIoT Sensors & MerryIoT for Amazon Sidewalk: Quick Installation Guide*. MerryIoT. https://www.merryiot.com/Product/P_12/C_Install/V_1.0/MerryIoT%20Sensor%20Home%20Kit%20QIG%20Sidewalk%2020230724(BQW_02_0045.001).pdf

Meshify. (n.d.-a). *About*. Meshify. Retrieved January 21, 2024, from https://meshify.com/about/

Meshify. (n.d.-b). *Meshify Defender S*. Meshify. Retrieved January 21, 2024, from https://meshify.com/products/defender-s/

Milarokostas, C., Tsolkas, D., Passas, N., & Merakos, L. (2023). A Comprehensive Study on LPWANs With a Focus on the Potential of LoRa/LoRaWAN Systems. *IEEE Communications Surveys & Tutorials*, *25*(1), 825–867. https://doi.org/10.1109/COMST.2022.3229846

Moorhead, P. (2021, June 7). *Amazon Sidewalk Focuses On Security And Privacy For All IoT Users*. Forbes. Retrieved November 8, 2023, from https://www.forbes.com/sites/patrickmoorhead/2021/06/07/amazon-sidewalk-focuses-on-security-and-privacy-for-all-iot-users/

Mossberg, W. (2016, March 16). *Mossberg: The false debate between open and closed in tech*. The Verge. Retrieved March 16, 2024, from https://www.theverge.com/2016/3/16/11242266/walt-mossberg-open-vs-closed-software-apple-os-x-google-android

Mukherjee, S. (2024, January 12). *Microsoft offers to store all personal data of cloud customers in EU*. Reuters. Retrieved February 18, 2024, from https://www.reuters.com/technology/microsoft-offers-store-all-personal-data-cloud-customers-eu-2024-01-11/

Munn, L. (2020). Red territory: Forging infrastructural power. *Territory, Politics, Governance*, *11*(1), 80–99. https://doi.org/10.1080/21622671.2020.1805353

Munn, L. (2022). Twinned power: Formations of cloud-edge control. *Information, Communication & Society*, *25*(7), 975–991. https://doi.org/10.1080/1369118X.2020.1808043

National Archives and Records Administration. (2022, October 1). *Radio Frequency Devices*. 47 Code of Federal Regulations pt.15. Retrieved January 8, 2024, from https://www.ecfr.gov/current/title-47/chapter-I/subchapter-A/part-15

Netvox. (n.d.). *Products: Amazon Sidewalk: S315 Series*. Netvox. Retrieved January 21, 2024, from http://www.netvox.com.tw/protest.asp?pro=a1

Netvox. (2023, March 28). *New Netvox S315 series Devices integrate with Amazon Sidewalk technology*. Netvox. Retrieved January 21, 2024, from http://www.netvox.com.tw/news2.asp?pro=107

netvoxrd & silabs-Lucie. (2024, March 14). *Sidewalk qualification for Netvox*. Silicon Labs. Retrieved March 25, 2024, from https://community.silabs.com/s/question/0D5Vm000005K5rVKAS/sidewalk-qualification-for-netvox

New Cosmos USA. (n.d.-a). *Amazon Sidewalk Smart Natural Gas Detector*. DeNova Detect. Retrieved January 21, 2024, from https://denovadetect.com/pages/amazon-sidewalk

New Cosmos USA. (n.d.-b). *DeNova Detect*. DeNova Detect. Retrieved January 21, 2024, from https://denovadetect.com/

New Cosmos USA. (2023, February 3). *DeNova Detect 807NAS Spec Sheet*. DeNova Detect. Retrieved January 21, 2024, from https://cdn.shopify.com/s/files/1/0679/6270/0053/files/DeNova_Detect_807NAS_Spec_Sheet--NC0013D.pdf?v=1684865150

Newman, L. H. (2021, June 8). *How to Turn Off Amazon Sidewalk*. Wired. Retrieved February 24, 2024, from https://www.wired.com/story/turn-off-amazon-sidewalk/

Ng, A. (2019, November 7). *Ring doorbells had vulnerability leaking Wi-Fi login info, researchers find*. CNET. Retrieved February 22, 2024, from https://www.cnet.com/home/smart-home/ring-doorbells-had-vulnerability-leaking-wi-fi-login-info-researchers-found/

Nguyen, A., & Zelickson, E. (2022, October). *At the Digital Doorstep: How Customers Use Doorbell Cameras to Manage Delivery Workers*. Data & Society. Retrieved December 17, 2022, from http://dx.doi.org/10.2139/ssrn.4225083

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, *79*(1), 119. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10

Ofe, H., Minnema, H., & de Reuver, M. (2022). The business value of privacy-preserving technologies: The case of multiparty computation in the telecom industry. *Digital Policy, Regulation and Governance*, *24*(6), 541–557. https://doi.org/10.1108/DPRG-10-2021-0132

OnAsset Intelligence. (n.d.). *Products*. OnAsset Intelligence. Retrieved January 21, 2024, from https://www.onasset.com/products/#sentinel100

OnAsset Intelligence. (2023, March 28). *OnAsset Intelligence launches dedicated supply chain monitoring device on Amazon Sidewalk*. OnAsset Intelligence. Retrieved January 21, 2024, from https://onasset.com/sentinel200-amazon-sidewalk/

O'Neill, S. (2023, April 1). *Everything you need to know about Amazon Sidewalk, the secure, low-cost network that can connect devices up to half a mile away*. About Amazon. Retrieved May 27, 2023, from https://www.aboutamazon.com/news/devices/everything-you-need-to-know-about-amazon-sidewalk

OpenThread. (2023, September 7). *Node Roles and Types*. OpenThread. Retrieved March 3, 2024, from https://openthread.io/guides/thread-primer/node-roles-and-types

Ortakales, J., & Kim, E. (2024, January 23). *Amazon layoffs: A timeline of the company's hiring freezes, restructuring efforts, and staff reductions into 2024*. Business Insider. Retrieved January 29, 2024, from https://www.businessinsider.com/amazon-layoffs

Ostrander, S. A. (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), 7–27. https://doi.org/10.1177/089124193022001002

Patterson, B. (2021, June 2). *Welcome to Amazon Sidewalk! Now here's how to turn it off*. TechHive. Retrieved November 8, 2023, from https://www.techhive.com/article/579021/how-to-turn-off-amazon-sidewalk.html

Patterson, B., & Simon, M. (2019, August 3). *How to keep Amazon, Apple, and Google from listening to your Alexa, Siri, and Assistant recordings*. TechHive. Retrieved February 24, 2024, from https://www.techhive.com/article/583911/how-to-keep-amazon-and-google-from-listening-to-your-alexa-and-assistant-voice-recordings.html

Pauwels, K., & Weiss, A. (2008). Moving from Free to Fee: How Online Firms Market to Change Their Business Model Successfully. *Journal of Marketing*, *72*(3), 14–31. https://doi.org/10.1509/JMKG.72.3.014

Pebblebee. (n.d.-a). *Business Solutions*. Pebblebee. Retrieved February 26, 2024, from https://pebblebee.com/pages/business-solutions

Pebblebee. (n.d.-b). *Pebblebee*. Pebblebee. Retrieved February 26, 2024, from https://pebblebee.com/

Petrik, D., & Herzwurm, G. (2020). Boundary Resources for IIoT Platforms – a Complementor Satisfaction Study. *ICIS 2020 Proceedings*, Paper 2. https://aisel.aisnet.org/icis2020/iot_smart/iot_smart/2

Pinzur, D. (2021). Infrastructural power: Discretion and the dynamics of infrastructure in action. *Journal of Cultural Economy*, *14*(6), 644–661. https://doi.org/10.1080/17530350.2021.1913212

Porter, J. (2019, September 25). *Amazon announces Fetch pet tracker that uses new Sidewalk networking*. The Verge. Retrieved January 3, 2024, from https://www.theverge.com/2019/9/25/20883874/amazon-fetch-sidewalk-wireless-standard-ultra-low-power-devices-developers

Primax Electronics. (n.d.). *Primax Electronics Ltd. Launches a New Smart Door Lock That Works With Amazon Sidewalk*. Primax Electronics. Retrieved January 21, 2024, from 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

Programmable Infrastructures Project. (n.d.). *Programmable Infrastructures Project*. TU Delft. Retrieved February 28, 2024, from https://www.tudelft.nl/tbm/onze-faculteit/afdelingen/multi-actor-systems/onderzoek/projects/programmable-infrastructures-project

Ranjan, K. (2022, May 16). *Buy Versus Build: Options for LoRa Cloud™ Geolocation Integrations*. LoRa Developer Portal. Retrieved February 28, 2024, from https://tech-journal.semtech.com/buy-versus-build-options-for-lora-cloud-geolocation-integrations

Renda, A., & Yoo, C. (2015, January 1). Telecommunications and the Internet: TTIP's digital dimension. In D. S. Hamilton & J. Pelkmans (Eds.), *Rule-Malers or Rule Takers? Exploring the Transatlantic Trade and Investment Partnership* (pp. 371–422). Rowman & Littlefield International. https://scholarship.law.upenn.edu/faculty_scholarship/2621/

Ridder, H.-G. (2017). The theory contribution of case study research designs. *Business Research*, *10*, 281–305. https://doi.org/10.1007/s40685-017-0045-z

Ring. (n.d.-a). *Neighbors by Ring*. Ring. Retrieved March 4, 2024, from https://ring.com/neighbors

Ring. (n.d.-b). *Products*. Ring. Retrieved February 24, 2024, from https://ring.com/collections/all-products

Ring. (n.d.-c). *Ring Mailbox Sensor*. Ring. Retrieved January 23, 2024, from https://ring.com/products/ring-mailbox-sensor

Ring. (n.d.-d). *Understanding Video End-to-End Encryption (E2EE)*. Ring. Retrieved February 24, 2024, from https://ring.com/support/articles/7e3lk/Understanding-Video-End-to-End-Encryption-E2EE

Ring. (n.d.-e). *Video Doorbell Pro 2*. Ring Netherlands. Retrieved March 3, 2024, from https://nl-nl.ring.com/products/video-doorbell-pro-2

Rodon Modol, J., & Eaton, B. (2021). Digital infrastructure evolution as generative entrenchment: The formation of a core–periphery structure. *Journal of Information Technology*, *36*(4), 342–364. https://doi.org/10.1177/02683962211013362

Roose, K. (2022, August 3). *Maybe There's a Use for Crypto After All*. The New York Times. Retrieved March 20, 2024, from https://www.nytimes.com/2022/02/06/technology/helium-cryptocurrency-uses.html

Rowley, J. (2002). Using case studies in research. *Management Research News*, *25*(1), 16–27. https://doi.org/10.1108/01409170210782990

rsoc16 & silabs-Lucie. (2024, March 4). *Issues with Timesync over CSS*. Silicon Labs. Retrieved March 12, 2024, from https://siliconlabs.my.site.com/community/s/question/0D5Vm000004Haw1KAC/issues-with-timesync-over-css?language=en_US

Rubin, R. (2021, June 4). *Amazon Sidewalk is about infrastructure, not intrusiveness.* ZDNET. Retrieved December 8, 2023, from https://www.zdnet.com/article/amazon-sidewalk-is-about-infrastructure-not-intrusiveness/

Saelens, M., Hoebeke, J., Shahid, A., & de Poorter, E. (2019). Impact of EU duty cycle and transmission power limitations for sub-GHz LPWAN SRDs: An overview and future challenges. *EURASIP Journal on Wireless Communications and Networking*, *2019*, Article 219. https://doi.org/10.1186/s13638-019-1502-5

Sahib, S. K. (2023). Trust issues. In C. Cath (Ed.), *Eaten by the Internet* (pp. 35–42). Meatspace Press. Retrieved February 18, 2024, from https://archive.org/details/eaten-by-the-internet

Sahmim, S., & Gharsellaoui, H. (2017). Privacy and Security in Internet-based Computing: Cloud Computing, Internet of Things, Cloud of Things: A review. *Procedia Computer Science*, *112*, 1516–1522. https://doi.org/10.1016/j.procs.2017.08.050

Saldaña, J. (2021). *The Coding Manual for Qualitative Researchers* (4th ed.). SAGE. https://tudelft.on.worldcat.org/oclc/1233312600

Sawers, P. (2023, October 25). *AWS announces 'sovereign cloud' to support data residency in Europe*. TechCrunch. Retrieved February 18, 2024, from https://techcrunch.com/2023/10/25/aws-to-launch-sovereign-cloud-to-support-data-residency-in-europe/

Scassa, T. (2020). Data Protection and the Internet: Canada. In D. Moura Vicente & S. de Vasconcelos Casimiro (Eds.), *Data Protection in the Internet* (pp. 55–76, Vol. 38). Springer International Publishing. https://doi.org/10.1007/978-3-030-28049-9_3

Semtech. (n.d.-a). *Ecosystem: Hardware*. LoRa Cloud. Retrieved January 12, 2024, from https://www.loracloud.com/ecosystem/hardware

Semtech. (n.d.-b). *Ecosystem: Solution Providers*. LoRa Cloud. Retrieved January 12, 2024, from https://www.loracloud.com/ecosystem/solution-providers

Semtech. (n.d.-c). *Ecosystem: Systems Integrators*. LoRa Cloud. Retrieved January 12, 2024, from https://www.loracloud.com/ecosystem/system-integrators

Semtech. (n.d.-d). *LoRa Ecosystem: Gateways*. Semtech. Retrieved January 12, 2024, from https://www.semtech.com/lora/ecosystem/gateways

Semtech. (n.d.-e). *LoRa Ecosystem: Network Providers*. Semtech. Retrieved January 12, 2024, from https://www.semtech.com/lora/ecosystem/networks

Semtech. (n.d.-f). *LoRa Ecosystem: Software*. Semtech. Retrieved January 12, 2024, from https://www.semtech.com/lora/ecosystem/software

Semtech. (n.d.-g). *Network Server*. LoRa Developer Portal. Retrieved January 12, 2024, from https://lora-developers.semtech.com/build/network-server/

Semtech. (n.d.-h). *Products: Wireless RF*. Semtech. Retrieved January 12, 2024, from https://www.semtech.com/products/wireless-rf

Semtech. (n.d.-i). *What are LoRa® and LoRaWAN®?* LoRa Developer Portal. Retrieved January 12, 2024, from https://lora-developers.semtech.com/documentation/tech-papers-and-guides/lora-and-lorawan/

Semtech. (n.d.-j). *What Is LoRa®?* Semtech. Retrieved January 12, 2024, from https://www.semtech.com/lora/what-is-lora

Semtech. (2023, March 30). *Fiscal Year 2023 Annual Report: Technology for a smarter more sustainable planet*. Camarillo, United States. https://investors.semtech.com/media/document/bb99fbd8-0fa1-4379-95ce-3e514cd2579f/assets/Semtech_AR_2023_Final_web.pdf

Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering*, *2017*, Article 9324035. https://doi.org/10.1155/2017/9324035

Slats, L. (2020, August 1). *A Brief History of LoRa: Three Inventors Share Their Story*. Semtech. Retrieved January 22, 2024, from https://blog.semtech.com/a-brief-history-of-lora-three-inventors-share-their-personal-story-at-the-things-conference

Smart Water Watch. (2023, July 20). *Subeca aims to bring Amazon experience to water sector*. Global Water Intelligence. Retrieved January 21, 2024, from https://www.globalwaterintel.com/global-water-intelligence-magazine/24/7/smart-water-watch/subeca-aims-to-bring-amazon-experience-to-water-sector

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

Solove, D. J. (2008, May 5). Privacy: A Concept in Disarray. In *Understanding Privacy* (pp. 1–11). Harvard University Press. Retrieved October 3, 2023, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888

Song, V. (2023, April 8). *Are Amazon Sidewalk's privacy protocols ready for the real world?* The Verge. Retrieved November 8, 2023, from https://www.theverge.com/2023/4/8/23671594/amazon-sidewalk-privacy-echo-ring-smart-home

Srouji, J., & Mechler, T. (2020). How privacy-enhancing technologies are transforming privacy by design and default: Perspectives for today and tomorrow. *Journal of Data Protection & Privacy*, *3*(3), 268–280. Retrieved March 21, 2024, from https://ideas.repec.org/a/aza/jdpp00/y2020v3i3p268-280.html

Steed, R., & Acquisti, A. (2024, February 19). *Adoption of 'Privacy-Preserving' Analytics: Drivers, Designs, & Decoupling*. SSRN. https://doi.org/10.2139/ssrn.4718865

Streitfeld, D. (2023, January 23). *For Tech Companies, Years of Easy Money Yield to Hard Times*. The New York Times. Retrieved March 17, 2024, from https://www.nytimes.com/2023/01/23/technology/tech-interest-rates-layoffs.html

Stringer, A., & Corrall, C. (2024, January 25). *A comprehensive list of 2023 & 2024 tech layoffs*. TechCrunch. Retrieved February 12, 2024, from https://techcrunch.com/2024/01/25/tech-layoffs-2023-list/

Subeca. (2023a, June 13). *Subeca, Inc. Joins Forces with Amazon Sidewalk to Innovate and Simplify Water Metering*. Subeca. Retrieved January 21, 2024, from https://www.subeca.com/blogs/subeca-inc-joins-forces-with-amazon-sidewalk-to-innovate-and-simplify-water-metering

Subeca. (2023b, July 24). *Enhancing Water Utility Surveillance and Response (SRS) with Subeca - Subeca*. Subeca. Retrieved January 21, 2024, from https://www.subeca.com/blogs/enhancing-water-utility-surveillance-and-response-srs-with-subeca

Sundar, S. (2023, March 20). *Amazon is laying off another 9,000 employees — read the email CEO Andy Jassy sent to staff*. Business Insider. Retrieved January 29, 2024, from https://www.businessinsider.com/amazon-layoffs-second-round-9000-job-jobs-2023-3

Swedberg, R. (2020, March 11). Exploratory Research. In C. Elman, J. Gerring, & J. Mahoney (Eds.), *The Production of Knowledge: Enhancing Progress in Social Science* (pp. 17–41). Cambridge University Press. https://doi.org/10.1017/9781108762519.002

Tag-N-Trac. (n.d.). *Smart Sensing*. Tag-N-Trac. Retrieved January 21, 2024, from https://www.tagntrac.com/smart-sensing/

Tavmen, G. (2020). Data/infrastructure in the smart city: Understanding the infrastructural power of Citymapper app through technicity of data. *Big Data & Society*, *7*(2), 2053951720965618. https://doi.org/10.1177/2053951720965618

TechEx. (n.d.-a). *Accelerating the IoT & Edge Computing track*. IoT Tech Expo Europe. Retrieved September 24, 2023, from https://web.archive.org/web/20230924064648/https://www.iottechexpo.com/europe/track/day-1-free-accelerating-the-iot-edge-computing/

TechEx. (n.d.-b). *Exhibitors*. Edge Computing Expo Europe. Retrieved September 28, 2023, from https://web.archive.org/web/20230928095633/https://edgecomputing-expo.com/europe/exhibition/

Texas Instruments. (2020, December 4). *Connect: Amazon Sidewalk chat with Airthings and Tag-n-Trac*. YouTube. Retrieved January 21, 2024, from https://www.youtube.com/watch?v=qIXSgGq2iKw

The Things Industries. (n.d.). *Regional Limitations of RF Use in LoRaWAN*. The Things Network: Documentation. Retrieved January 7, 2024, from https://www.thethingsnetwork.org/docs/lorawan/regional-limitations-of-rf-use/

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

Thingy-IoT. (n.d.). *Home*. Thingy-IOT. Retrieved January 21, 2024, from https://thingy-iot.au/

Thread Group. (n.d.-a). *Thread Group: Members*. Thread Group. Retrieved February 11, 2024, from https://www.threadgroup.org/thread-group#OurMembers

Thread Group. (n.d.-b). *Thread Smart Home Fact Sheet* (Network diagram). California, United States. Retrieved March 3, 2024, from https://portal.threadgroup.org/DesktopModules/Inventures_Document/FileDownload.aspx?ContentID=834

Tile. (n.d.). *Tile + Amazon Sidewalk*. Tile Support. Retrieved January 29, 2024, from https://support.thetileapp.com/hc/en-us/articles/1500009711121-Tile-Amazon-Sidewalk

Tile. (2021, May 7). *Amazon Sidewalk is About to Strengthen the Finding Power of Your Tiles*. Tile. Retrieved January 21, 2024, from https://www.tile.com/blog/sidewalk-strengthening-the-power-of-your-tiles

Tiwana, A. (2014). Platform Architecture. In A. Tiwana (Ed.), *Platform Ecosystems: Aligning Architecture, Governance, and Strategy* (pp. 73–116). Morgan Kaufmann. https://doi.org/10.1016/B978-0-12-408066-9.00005-9

Tiwana, A., Konsynski, B., & Bush, A. A. (2010). Platform Evolution: Coevolution of Platform Architecture, Governance, and Environmental Dynamics. *Information Systems Research*, *21*(4), 675–687. https://doi.org/10.1287/isre.1100.0323

Troncoso, C., Bogdanov, D., Bugnion, E., Chatel, S., Cremers, C., Gürses, S., Hubaux, J.-P., Jackson, D., Larus, J. R., Lueks, W., Oliveira, R., Payer, M., Preneel, B., Pyrgelis, A., Salathé, M., Stadler, T., & Veale, M. (2022). Deploying decentralized, privacy-preserving proximity tracing. *Communications of the ACM*, *65*(9), 48–57. https://doi.org/10.1145/3524107

Tuohy, J. P. (2022a, July 29). *Thread is Matter's secret sauce for a better smart home*. The Verge. Retrieved February 11, 2024, from https://www.theverge.com/23165855/thread-smart-home-protocol-matter-apple-google-interview

Tuohy, J. P. (2022b, November 3). *Matter arrives on Amazon Echo smart speakers next month*. The Verge. Retrieved March 12, 2024, from https://www.theverge.com/2022/11/3/23438286/amazon-matter-support-alexa-echo-smart-home-platform

Tuohy, J. P. (2023a, January 27). *All the smart home products that work with Matter*. The Verge. Retrieved March 3, 2024, from https://www.theverge.com/23568091/matter-compatible-devices-accessories-apple-amazon-google-samsung

Tuohy, J. P. (2023b, January 27). *What Matters about Matter, the new smart home standard*. The Verge. Retrieved February 11, 2024, from https://www.theverge.com/22832127/matter-smart-home-products-thread-wifi-explainer

Tuohy, J. P. (2023c, April 1). *Amazon just opened up its Sidewalk network for anyone to build connected gadgets on*. The Verge. Retrieved February 11, 2024, from https://www.theverge.com/2023/3/28/23659191/amazon-sidewalk-network-coverage

Tuohy, J. P. (2023d, May 2). *Amazon's latest Matter update brings support for Thread*. The Verge. Retrieved March 12, 2024, from https://www.theverge.com/2023/5/2/23707900/amazon-matter-smart-home-thread-support

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

Vaas. (2021, June 2). *Amazon Sidewalk Poised to Sweep You Into Its Mesh*. Threatpost. Retrieved November 8, 2023, from https://threatpost.com/amazon-sidewalk-to-sweep-you-into-its-mesh/166581/

Valdez, J. (2023). The politics of Uber: Infrastructural power in the United States and Europe. *Regulation & Governance*, *17*(1), 177–194. https://doi.org/10.1111/rego.12456

van der Vlist, F. N., & Helmond, A. (2021). How partners mediate platform power: Mapping business and data partnerships in the social media ecosystem. *Big Data & Society*, *8*(1). https://doi.org/10.1177/20539517211025061

van der Vlist, F. N., Helmond, A., Burkhardt, M., & Seitz, T. (2022). API Governance: The Case of Facebook's Evolution. *Social Media + Society*, *8*(2), 20563051221086228. https://doi.org/10.1177/20563051221086228

van Dijck, J., Nieborg, D., & Poell, T. (2019). Reframing platform power. *Internet Policy Review*, *8*(2). https://doi.org/10.14763/2019.2.1414

van Hoboken, J., & Fathaigh, R. Ó. (2021). Smartphone platforms as privacy regulators. *Computer Law & Security Review*, *41*, Article 105557. https://doi.org/10.1016/j.clsr.2021.105557

Veale, M. (2022, February 25). *Future of online advertising: Adtech's new clothes might redefine privacy more than they reform profiling*. netzpolitik.org. https://netzpolitik.org/2022/future-of-online-advertising-adtechs-new-clothes-might-redefine-privacy-more-than-they-reform-profiling-cookies-meta-mozilla-apple-google/

Veale, M. (2023a). Confidentiality washing in online advertising. In C. Cath (Ed.), *Eaten by the Internet* (pp. 43–48). Meatspace Press. Retrieved February 18, 2024, from https://archive.org/details/eaten-by-the-internet

Veale, M. (2023b, November 19). Denied by Design? Data Access Rights in Encrypted Infrastructures. In J. Ausloos & S. P. de Souza (Eds.), *Research Access to Digital Infrastructures* (advance online publication). Retrieved September 28, 2023, from https://doi.org/10.31235/osf.io/94y6r

Vermes, K. (2024, February 5). *Don't hold your breath for Google's new Find My Device network*. Android Police. Retrieved February 25, 2024, from https://www.androidpolice.com/google-android-find-device-network-delay/

Waller, S. (2022, January 6). *Thingy and Sidewalk for Wildfire Smoke and Air Quality*. Thingy-IoT. Retrieved January 21, 2024, from https://web.archive.org/web/20220705152429/https:/thingy.us/thingy-and-sidewalk-for-wildfires/

Walters, R., & Novak, M. (2021a). Canada. In R. Walters & M. Novak (Eds.), *Cyber Security, Artificial Intelligence, Data Protection & the Law* (pp. 321–355). Springer. https://doi.org/10.1007/978-981-16-1665-5_13

Walters, R., & Novak, M. (2021b). Comparison, Challenges and a Way Forward. In R. Walters & M. Novak (Eds.), *Cyber Security, Artificial Intelligence, Data Protection & the Law* (pp. 405–454). Springer. https://doi.org/10.1007/978-981-16-1665-5_15

Walters, R., & Novak, M. (2021c). The United States. In R. Walters & M. Novak (Eds.), *Cyber Security, Artificial Intelligence, Data Protection & the Law* (pp. 357–404). Springer. https://doi.org/10.1007/978-981-16-1665-5_14

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193–220. https://doi.org/10.2307/1321160

Westin, A. F. (1970). *Privacy and Freedom*. Atheneum.

Wiggers, K. (2023, November 28). *Amazon reveals two new chips for AI models: Trainium2 and Graviton4*. TechCrunch. Retrieved February 25, 2024, from https://techcrunch.com/2023/11/28/amazon-unveils-new-chips-for-training-and-running-ai-models/

Wight, L. (2023, January 25). *The Promised Growth of IoT*. Meshify. Retrieved January 21, 2024, from https://meshify.com/the-promised-growth-of-iot/

Wiklundh, K. C. (2019). Understanding the IoT technology LoRa and its interference vulnerability, 533–538. https://doi.org/10.1109/EMCEurope.2019.8871966

Wimsatt, W. C. (2007, June 30). Robustness and entrenchment: How the contingent becomes necessary. In W. C. Wimsatt (Ed.), *Re-Engineering Philosophy for Limited Beings: Piecewise Approximations to Reality* (pp. 133–145). Harvard University Press. https://doi.org/10.2307/j.ctv1pncnrh

Witell, L., & Löfgren, M. (2013). From service for free to service for fee: Business model innovation in manufacturing firms. *Journal of Service Management*, *24*(5), 520–533. https://doi.org/10.1108/JOSM-04-2013-0103

Witkowski, B. (2017, December 20). *Comcast's MachineQ Deploys Smart City Solution in Philly Holiday Hotspots*. Comcast. Retrieved January 29, 2024, from https://corporate.comcast.com/stories/comcasts-machineq-deploys-smart-city-solution-in-philly-holiday-hotspots

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

Wyld Networks. (n.d.). *Wyld Connect*. Wyld Networks. Retrieved February 26, 2024, from https://wyldnetworks.com/wyldconnect

Yin, R. K. (2017, October). *Case Study Research and Applications: Design and Methods* (6th ed.). SAGE Publications, Inc. https://us.sagepub.com/en-us/nam/case-study-research-and-applications/book250150

Yubico. (n.d.). *YubiHSM 2 v2.3.2*. Yubico. Retrieved March 4, 2024, from https://www.yubico.com/product/yubihsm-2/

Zatz, D. (2022, November 1). *Amazon's Ring Car Alarm Nears Launch*. Zatz Not Funny! Retrieved February 15, 2024, from https://zatznotfunny.com/2022-11/amazon-ring-car-alarm/

Zuboff, S. (2023). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. In *Social Theory Re-Wired* (3rd ed.). Routledge. https://doi.org/10.4324/9781003320609-27

A

Interview questions

This appendix contains a compilation of all the prepared interview questions. As I conducted the interviews in semi-structured fashion (described in §3.2.5), and because some questions were not applicable for some respondents, I did not ask everyone all questions. Similarly, I might have formulated some questions differently or in a different order during the interviews, to adapt to the flow of the conversation. Clarifications appended to the question between parentheses were only given to the interviewee if they did not understand the question, to prevent inducing bias in their answer. The personal questions used for rapport building are not included to protect anonymity of the participants.

A.1. Rapport building

Background and expertise of interviewee

1. Can you tell me about your company and your role there?

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.2. Grand tour and mini-tour questions

Adoption and motivation

7. How did you discover Sidewalk?
8. What novel opportunities does Sidewalk provide? *(E.g. compared to other connectivity protocols)*
9. How important is Sidewalk to your product 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 3 connectivity protocols of Sidewalk do you use (i.e. LoRa, FSK, BLE)?
12. What other connectivity methods than Sidewalk did you consider? *(E.g. LoRaWAN, Bluetooth, Matter)*
13. How does Sidewalk compare to these other methods?
14. I found blog posts mentioning your company's adoption of Sidewalk, hailing the promise of Sidewalk for your business case. However, your product pages currently do not mention that you support Sidewalk, and also lack the 'Works with Amazon Sidewalk'-badge that you get after completing the qualification process. So I was wondering, is Sidewalk currently supported by your products? Are they already out on the market? Is there a specific reason for this low visibility of your adoption? Or what is the current status of your product/service?

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. 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 Alliance and Amazon? I assume that the LoRa Alliance side-eyes Amazon's Sidewalk efforts, because it is LoRa-based, but also a closed, proprietary network. Meanwhile, Amazon is also a Sponsor of the Alliance and they have a board member.

Confidentiality of business-sensitive data, and competition with Amazon

32. I imagine there might be usage data that gives away how your device functions. For example, how big are the payloads; how quick does the battery deplete; how often does the device communicate with the cloud. What information do you think Amazon is able to see about your devices and cloud use?
33. Do you think Amazon could use this information to improve their own offerings? *(E.g. their own IoT devices, or their AWS services)*
34. Do you have insights into whether Amazon is developing new endpoints themselves?

Reliance

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

A.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

Additional details from grey literature

B.1. Overview of Sidewalk adopters

Table B.1 displays the results of the grey literature review into Sidewalk adopters (§3.2.2. Note that these results were at points supplemented with information obtained during the interviewee recruitment phase and during the actual interviews. To protect the participants' anonymity, no references to interviewees are included in Table B.1.

Note that the devices of Netvox, Primax, and MOKOSmart, are designed for both business and consumer use, although the companies are B2B-oriented. This is because these companies are Original Equipment Manufacturers, meaning that other companies can white-label their products or buy their technology and implement it as part of their own product.

Finally, while catering to business or consumer users is usually not a fully binary choice, I categorised offerings based on companies' marketing strategies as they appeared in public materials and private correspondence. For instance, devices by consumer-oriented brand MerryIoT can also be used in business contexts such as offices, but their marketing signifies a focus on consumers.

Based on these findings, Table B.2 typifies the market categories and captures the differences in the functional requirements that they pose for endpoints. For instance, building management devices are assumed to be used in a fixed place inside or nearby the owner's building, where WiFi networks, electricity, and other smart devices are commonplace. Conversely, in the utilities category, devices may be scattered across large industrial sites or attached to water and gas pipelines, implying communication over longer ranges with battery-powered devices that must last for months or years on end.

The observations in each category should be interpreted relative to those in other categories. For instance, even if Sidewalk-enabled building management sensors utilise a longer range than similar non-Sidewalk devices, their range will generally still be shorter than that of utilities sensors scattered across streets or industrial sites. Moreover, I merged the 'industry' and 'in-home care' categories into the 'building management' and 'utilities' classes, respectively, because of only having 1 observation and being most similar to these larger categories.

Finally, utilities-oriented Sidewalk devices are strictly seen not only sold to businesses and does not only have business users as end-users, because Denova Detect's devices are sold to and used by both consumers and businesses. However, this company is predominantly B2B oriented. Moreover, the 4 other utilities-oriented companies all sell only to businesses with business users as envisioned end-users, warranting the present characterisation of the utilities domain.

B.2. LoRaWAN

B.2.1. A brief history of LoRa(WAN)

The patent of the LoRa radio frequency technology is in hands of the United States-based semiconductor manufacturer Semtech Corporation. How they obtained the patent is described by Slats (2020). LoRa was originally invented and patented in 2010 by the company Cycleo, that was also found in that year. The communication technology was designed for low-power communication of resource-constrained

Table B.1: Overview of Sidewalk adopters. 'B' denotes business users, and 'C' consumer users.

Nr	Company name	Product name (if available): functionality	Market category	Business orientation of Sidewalk offering	Intended user type	Other communication protocols supported by the Sidewalk endpoint	References
1	CareBand	CareBand: primarily panic button and location and activity detection for elderly people and people with dementia; also applied for contact tracing and outdoors worker safety	In-home care; logistics (asset tracking) (secondary to in-home care)	B2B, B2C	B, C	LoRaWAN	(CareBand, n.d.-a, n.d.-b; Higginbotham, 2023)
2	Arrive	Arrive Point, Bank, Convey, Package Tower: Smart mailbox(es), Mailbox as a Service	Logistics (asset tracking, autonomous delivery)	B2B	B	Cellular (unknown whether simultaneously)	(Arrive, n.d., 2023, 2024)
3	OnAsset	Sentinel 200: asset tracking (condition and location monitoring)	Logistics (Asset tracking)	B2B	B	BLE, LoRaWAN	(Amazon, 2023o; Gonsalves, 2023; OnAsset Intelligence, n.d., 2023)
4	Tile	Tile: finding device	Logistics (Asset tracking)	B2B, B2C	B, C	BLE	(Amazon, 2021a; Tile, 2021)
5	Tag-n-Trac	Smart Sense: Asset tracking, condition monitoring (e.g. temperature, tampering, acceleration), last-mile transport	Logistics (Asset tracking)	B2B	B	BLE, cellular (LTE-Cat.M1 and NB-IoT), Sub-GHz	(Tag-N-Trac, n.d.; Texas Instruments, 2020)
6	MOKO-Smart	Motion detection, asset and person tracking, smart plug	Building management (sensors), logistics (asset tracking)	B2B (OEM)	B, C	LoRaWAN (unknown whether supported simultaneously)	(Kuan, 2023)
7	Primax	Woody: Smart lock	Building management (smart locks)	B2B (OEM)	B, C	Unknown	(Amazon, 2023o; Primax Electronics, n.d.)
8	Level	Level: smart door lock	Building management (smart locks)	B2B, B2C	B, C	BLE, Matter over Thread	(Amazon, 2021a; Level, n.d.-a, n.d.-b, n.d.-c)
9	Netvox	S315 series: integrates modular sensors, so can support sensing temperature, humidity, motion, water leaks, vibration, light, and door contact	Building management (sensors)	B2B (OEM)	B, C	Supports only LoRa or FSK at one time (unknown if these can be used in addition to Sidewalk, or are used as Sidewalk protocol)	(Amazon, 2023o; Netvox, n.d., 2023)
10	MerryIoT (by Browan Communications)	4 devices with a combination of CO2, motion, door/window open/close, water leak, temperature, and humidity sensing capabilities	Building management (sensors)	B2C	C	None	(MerryIoT, n.d., 2023)
11	Airthings	CO2, radon, temperature, humidity, and air quality monitors	Building management (sensors)	B2B, B2C	B, C	Wifi, BLE, Matter (underlying protocol unknown)	(Airthings, n.d., 2023; Ballance, 2024a, 2024b; Texas Instruments, 2020)
12	DeNova Detect (by New Cosmos)	807NAS: natural gas alarm	Building management (sensors); utilities	B2B, B2C	B, C	None (other devices using e.g. LoRa(WAN))	(New Cosmos USA, n.d.-a, n.d.-b, 2023)
13	Meshify (by HSB)	Defender S: water leak and water pipe freeze/break detection	Building management (sensors); utilities	B2B	B	None	(Meshify, n.d.-a, n.d.-b; Wight, 2023)
14	Deviceroy	Aria: relaying an industrial device's readings to the internet	Utilities, industrial	B2B	B	LoRa(WAN), BLE, Ethernet	(Deviceroy, 2023a, 2023b)
15	Thingy	Air quality monitoring, specifically for early detection of wildfires (only pilot stage)	Utilities	B2B	B	LoRaWAN, unknown if both	(Thingy-IoT, n.d.; Waller, 2022)
16	Subeca	Pin: Advanced Meter Infrastructure sensor	Utilities	B2B	B	BLE, LoRaWAN	(Smart Water Watch, 2023; Subeca, 2023a, 2023b)

Table B.2: Typical characteristics of the three main Sidewalk device categories

Market category	Business orientation of Sidewalk offering	Range	Location	Mobility	Sensing (uplink traffic) and / or actuating (downlink traffic)
Utilities	B2B	Long-range (e.g. on large industrial sites)	Indoors and outdoors	Stationary	Sensing (leaks, wildfires, machine status) and actuating (only in Subeca's case: shutting down a valve)
Logistics	B2B and B2C	Long-range (for devices out on the streets) and short-range (for help in finding things, if sufficiently pervasive coverage [A4])	Indoors and outdoors	Mobile	Sensing (location, conditions) and actuating (only in Arrive's case: opening a mailbox)
Building management	B2B and B2C	Short-range	Indoors	Stationary	Sensing (air quality, motion, temperature, leaks) and actuating (opening / closing locks)

devices over long ranges (hence its name); more specifically for communicating gas, water, and electricity meter readings. Semtech acquired Cycleo in 2012. In 2015, the 1.0 version of the LoRaWAN specification was published and the standards body LoRa Alliance was established.

Currently, licensing the technology to third parties, and offering LoRa products and the LoRa Cloud platform are amongst the most important contributors of Semtech's 'IoT systems' and 'IoT connected services' product groups, that amounted to about 30% of its 2023 net sales (i.e. 30% of approximately $767 million) (Semtech, 2023). Semtech is active in the LoRa ecosystem by offering products and services. For example, Semtech offer chips and reference designs for other companies to manufacture LoRa gateways and end devices with (Semtech, n.d.-h), but also has its own network server (Semtech, n.d.-g) and applications and data portals (Semtech, n.d.-j).

B.2.2. LoRaWAN technical architecture

Semtech (n.d.-i) visualises what an archetypical LoRaWAN network architecture looks like. Figure B.1 illustrates that a LoRaWAN-compatible "*end device*" ("endpoint" in Sidewalk lingo) connects to one or more *gateways* using the LoRa radio communication technology. The gateway liaises between the end device and the *LoRaWAN network server* over a wifi, ethernet, or cellular connection. This network server has the same responsibilities as the Sidewalk network server: it manages the network, which includes both ensuring integrity of the network and transmitting data to and from end devices to the appropriate *application server*. These application servers host the business logic of end devices, i.e. they process their data or issue messages to them. This processing may take place using *dashboards or data portals*. Finally, the *join server* enables new end devices to join the network, for instance by informing the network server which application server it should communicate with.

B.3. MachineQ: A failed attempt at a nationwide LoRaWAN network

One interviewee told about a failed attempt by telecom provider Comcast at making their own LoRaWAN network in the US. This example illustrates that rolling out such a network, as Amazon has accomplished with Sidewalk, is challenging.

The respondent signed up for a pilot of the 'MachineQ' network, where Comcast tried to build out a nation-wide network by *"putting up big gateways in different cities as well as providing some of that Trojan Horse kind of stuff"*. The pilot was terminated two years later, as the project team failed to obtain sufficient funding from Comcast. Indeed, older announcements announce them *"set[ting] up wireless networks in 10 US smart cities, each running on the LoRa wireless network standard and designed for internet of things (IoT) uses"* (Frankel, 2018; see also e.g. Witkowski, 2017); whereas their websites now speak of enabling the deployment of LoRaWAN networks by customers through their end-to-end suite, including end devices, gateways, and a platform to analyse data (Comcast, 2021; MachineQ, n.d.).

The interviewee continued that the LoRa market was still *"in its infancy"* back then, although Amazon managed to deploy Sidewalk just an estimated 6 to 12 months later. The context was both big tech companies and telecom providers *"trying to figure out how to bring LoRa to consumers"* and *"want[ing] to own the smart home"*. MachineQ's aspirations seemingly went further than the smart home, though:

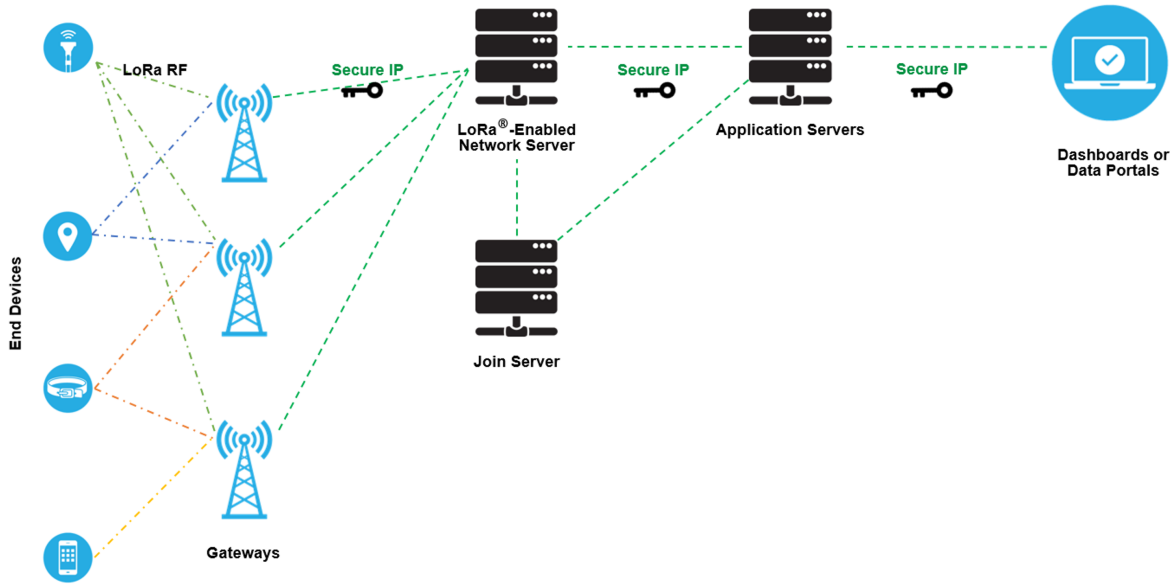

Figure B.1: Overview of a LoRaWAN architecture. Reproduced from Semtech (n.d.-i)

the interviewee mentioned that their early partnerships were for smart city applications, meaning that LoRa was then already envisioned for both B2B and B2C applications. But how could Amazon manage to roll out Sidewalk, while Comcast could not? The interviewee continues:

> *Everyone was kind of having similar ideas around the same time, but nobody... The execution part is the hard part, obviously. No one could really figure out how to execute it in a way that made sense. The thing is, you need a lot of capital to make it work, early on, before it can really take off. So you gotta have a company that's willing to invest that kind of R&D, for many years, at a high level, before it can happen.*

The interviewee seems to explain Comcast's failure and Amazon's success with a difference in resources. Perhaps Amazon had more money to invest in R&D, more skilled engineers, or more experience in networking and IoT. But I think their control over Echo and Ring devices was a crucial factor. By reconfiguring the Echo and Ring devices that were already in use in people's homes, Amazon realised a vast gateway infrastructure, without having to put up and maintain the gateways themselves. It is the gateway owners that purchase one, put it in their home, provide it with WiFi and electricity, and replace it when it stops working. This gives Amazon a huge financial and operational edge. Conversely, the interviewee said that MachineQ had to invest in and build their network infrastructure themselves.

B.4. Amazon's cooperation with law enforcement

§6.1 mentioned grey literature concerned about Sidewalk contributing to an extension of Amazon's private surveillance infrastructure. The company has a history of actively initiating collaborations with the police to foster adoption of their cameras and camera doorbells. One reference reports that Amazon counts over 2,000 US police and fire departments as their partners (Lyons, 2021). Examples of such partnerships are that Amazon had law enforcement departments hand out devices to citizens for free as long as they also encourage citizen adoption hereof, while simultaneously training officers in PR and handling press questions (Haskins, 2019a). Amazon also persuaded municipalities to subsidise residents' purchases of Ring products (Haskins, 2019b). Citizens would also receive discounts or free products from Amazon when when grouping up in *"Digital Neighborhood Watches"* and reporting crime (Haskins, 2019c).

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 without a warrant that Ring owners could approve in a smartphone app (Lyons, 2021). Even though Amazon has now removed the footage request button, authorities can still obtain footage with a warrant or by demonstrating to Amazon that they need it for an ongoing emergency (M. Day, 2024). Indeed, Amazon

has disclosed video feeds without warrants to authorities when their emergency request was critical enough in terms of *"imminent danger of death or serious physical injury to any person"*, based on Ring's own *"good-faith determination"* (Amazon, 2022b, p. 4), a practice that some authors take issue with (e.g. Guariglia, 2024). The sensitivity of these requests is illustrated by the Los Angeles police requesting Ring feeds of Black Lives Matters protests (Guariglia & Maass, 2021).

B.5. LoRa(WAN) and radio regulations

LoRa works on radio frequencies that do not require operators to obtain a radio license from a regulatory body (Milarokostas et al., 2023). Still, these frequencies are subject to local regulations that differ across regions. Therefore, the LoRaWAN general specification (LoRa Alliance Technical Committee, 2020) that details how the protocol works, is supplemented by a separate regional specification (LoRa Alliance Technical Committee Regional Parameters Workgroup, 2023) that fills in the parameters to comply with regional regulations (Saelens et al., 2019). This section briefly surveys the regulations and regional specification for Europe and the US, as this is where the author and Sidewalk are currently oriented, respectively. The LoRa regional specification informs us that many other countries have their own frequencies and regulatory bodies, too, but these are outside the scope here.

B.5.1. Available bands in Europe and North-America, and their accompanying regulations

In the EU, the sub-gigahertz band (i.e. between 25 MHz and 1000 MHz) has been harmonised by the European Telecommunications Standards Institute (ETSI) at the request of the European Commission (ETSI Technical Committee Electromagnetic compatibility and Radio spectrum Matters, 2018). Compliance with the resulting ETSI EN300 220-2 standard is not mandatory, but grants the manufacturer a *"presumption of conformity"* with the EU's relevant radio regulations that must otherwise be demonstrated by the manufacturer more elaborately (ETSI Technical Committee Electromagnetic compatibility and Radio spectrum Matters, 2018; Saelens et al., 2019). For an elaborate overview of actors involved in the conception of the ETSI standard, see Saelens et al. (2019).

Within the frequencies made available by ETSI, the LoRaWAN standard designates the bands between 433.05 MHz and 434.79 MHz (also referred to as band *"EU433"*) and between 863 MHz and 870 MHz (*"EU863-870"*) as suitable for LoRaWAN. The prescribed parameters as well as the applicability differ between the bands. The specifications for the EU433 band apply for territories in ITU Region 1; this includes inter alia Europe, Africa, and Russia (ITU, n.d.)). The EU863-870 details apply for countries covered by the mentioned ETSI standard, which includes the EU.

The relevant US regulation is Part 15 (*"Radio Frequency Devices"*) of Title 47 (*"Telecommunication"*) of the Code of Federal Regulations (National Archives and Records Administration, 2022). This chapter is governed by the Federal Communications Commission (FCC) and imposes inter alia technical, administrative, and marketing requirements on radios used in unlicensed bands (§15.1). The sub-gigahertz frequencies suitable for LoRaWAN are in the 902-928 MHz band (*"US902-928"*). The LoRaWAN specification defines parameters for *"the USA, Canada, and all other countries in ITU Region 2 adopting the entire FCC 47 CFR Part 15 regulations in the 902-928 ISM band"*.

The author theorises that this overlap could prompt Amazon to roll out Sidewalk in Canada before entering Europe, as it would require less product re-engineering. However, it is unknown whether Echo and Ring adoption differs between Canada and Europe. Also, while Canada's data protection and privacy regimes are considered to be less strict than the EU's; they are still perceived more stringent than the US, which might hamper a roll-out. For instance, in comparison to the US, the Canadian scheme defines 'personal information' more broadly, and generally forces more requirements on companies regarding informing users about data processing, asking their consent in opt-in fashion, and generally limiting data processing as far as possible (see e.g. DLA Piper (2023a, 2023b), Grynwajc (2020), Merrick and Ryan (2019), and Walters and Novak (2021b) that directly compare the regulatory schemes. See also the book chapters by Walters and Novak (2021a) vis-à-vis Walters and Novak (2021c), and Scassa (2020) vis-à-vis Boyne (2020); with each pair representing an edited book with the first-mentioned reference writing about Canada, and the second-mentioned about the United States). Therefore, an almost-silent opt-out transformation of Echo and Ring devices into Sidewalk gateways might not be in the cards for Canadian device owners. Moreover, the regulations differ between the private and public sector (Walters & Novak, 2021b, p. 410); this might bring administrative complications for Sidewalk adopters

targeting both public and private deployments, such as in the utilities or smart city sectors.

Sidewalk also works on the US902-928 band (Amazon Technologies, 2024, p. 145).

B.5.2. LoRa in Europe: a closer look

Thus, according to the LoRaWAN specification, both the EU433 and EU863-870 bands are available. Indeed, the ETSI standard also allows the former band to be used. In practice, the EU433 band is barely used for LoRaWAN (Milarokostas et al., 2023) and not investigated further in this thesis.

Duty cycle regulations

As mentioned, the US and EU have different regulatory regimes for the radio frequencies at hand. The FCC regulates the maximum strength of electric fields and harmonics of devices operating at these frequencies (Saelens et al., 2019). Additionally, devices may only spend 400 ms in a channel consecutively, before they must go offline or change to another channel (Fahmida et al., 2022; LoRa Alliance Technical Committee Regional Parameters Workgroup, 2023). This is referred to as devices' maximum 'dwell time' (The Things Industries, n.d.).

The EU regulates other aspects. Rather than dwell time and strength of electric fields and harmonics, devices' duty cycle and maximum transmission power are limited (Saelens et al., 2019). The sub-bands that the ETSI standard splits the EU863-870 band into, each come with varying maximum effective radiated power (i.e. 5 mW, 25 mW, or 500 mW) and duty cycle requirements (i.e. 0.1%, 1%, or 10%) (ETSI Technical Committee Electromagnetic compatibility and Radio spectrum Matters, 2018, p. 22)

Here, the duty cycle is the percentage of time that a *"device can occupy a channel"* per hour (Adelantado et al., 2017, p. 36). For instance, a 1% duty cycle means that a certain device may only transmit packets in a specific channel for 36 seconds per hour (Adelantado et al., 2017). A lower duty cycle will reduce the capacity of a LoRaWAN deployment, in terms of reducing transmission frequency, number of endpoints, or distance between devices (Adelantado et al., 2017). Devices switch between eligible channels on a pseudo-random basis to remain under this limit (Adelantado et al., 2017).

How problematic the radiated power limits are for Sidewalk or LoRaWAN devices will depend on their use cases. While stronger signals provide more range, they also draw more power, which is specially problematic for battery-powered devices intended to last for long times [A1]. In any case, the duty cycle requirements limit both the up- and downlink availability of endpoints, as endpoints can then only check their channel for incoming messages or send outgoing messages at fixed rates. Besides affecting functionality, this might also make devices harder to develop as engineers will have to work around this constrained availability while still getting all relevant data to and from the device.

B.5.3. Global fragmentation of LoRa regulations

Theoretically, Amazon could bring Sidewalk to other territories without duty cycle regulations. In the eyes of [A2], though, this might quickly become messy, because of a globally fragmented regulatory landscape of radio frequencies. §B.5.2 showed that the regulatory landscape of radio frequencies is globally fragmented, and that LoRa is permitted in different frequency bands. For instance, the LoRa frequencies in the EU (ETSI Technical Committee Electromagnetic compatibility and Radio spectrum Matters, 2018) differ from the LoRa and Sidewalk frequencies in the US (Amazon Technologies, 2024; LoRa Alliance Technical Committee Regional Parameters Workgroup, 2023). Catering to other countries might thus require US-oriented manufacturers to *"rebuild some radio parts"*, increasing development complexity [A2]. Against that backdrop, a benefit of bringing Sidewalk to Europe is that the applicable radio regulations are harmonised across the EU, granting Amazon access to a large market. Other countries might not have harmonised their frequency plans with neighbouring countries [A2]. If Amazon were to bring Sidewalk to non-European countries without duty cycle regulations, the LoRa frequencies may thus still differ.

B.6. End-to-end encryption: downlink traffic

In addition to Figure 6.2 visualising the encryption of uplink Sidewalk traffic, Figure B.2 visualises downlink traffic.

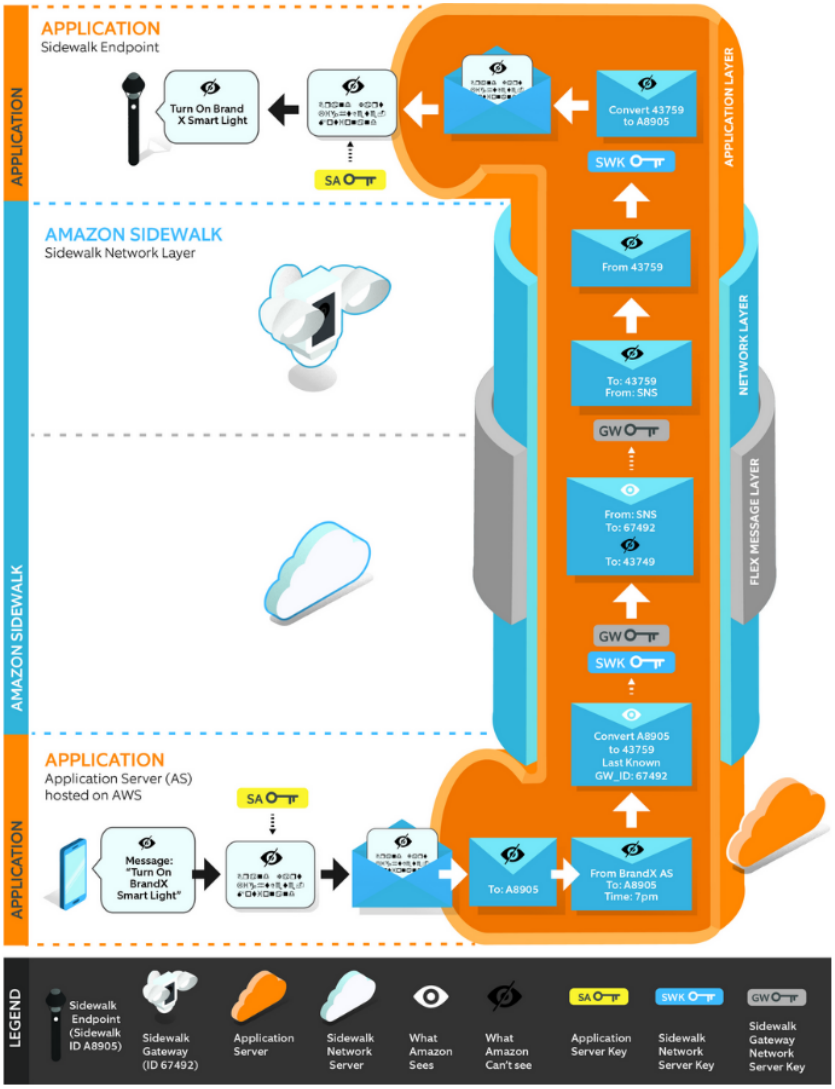

Figure B.2: Overview of Sidewalk's end-to-end encryption scheme for downlink traffic. Reproduced from Amazon (2023n) (p. 9)

C

Additional details from elite interviews

C.1. Status of interviewees' adoption

Interviewees' products were at varying stages of maturity and Sidewalk use. The 8 respondents that work at a Sidewalk-adopting company reported different levels of Sidewalk adoption and use. The products of 4 companies are currently out in the field and using Sidewalk, although one company barely markets its functionality. 3 organisations are using Sidewalk, but are still in a product trial phase, so their use is constrained to pilots. 1 company has publicly announced that they have adopted Sidewalk; however, in reality their devices do not use Sidewalk yet. Devices that are already in use by customers can be made to use Sidewalk with an over-the-air update issued by the company. The interviewee says that most of the work to turn their devices into Sidewalk endpoints has been done, but still requires some research and development bandwidth that the organisation is currently spending differently. In response to me asking if and when this update will be published, the interviewee said *"it's a timing, it's a resource, and it's a 'do we want to' question"*.

C.2. How the Sidewalk protocol specification constrains how endpoints can work

The requirements laid out in the Sidewalk protocol specification (Amazon Technologies, 2024) significantly hamper Sidewalk adopters' autonomy in determining how their IoT devices function.

To start, the specification prescribes the minimum qualities that a device must support, such as a BLE version number, number of concurrent connections, and data rate of the Bluetooth channels (p. 148). Devices complying with these qualities must then be configured in line with a certain set of parameters. An important choice for manufacturers is whether their endpoints communicate in synchronous or asynchronous fashion (p. 9). In the former mode, an endpoint only talks with its application server after a connection has been established with a single gateway. In the latter mode, endpoints send messages that can be forwarded by multiple gateways. FSK can only be used in synchronous connections, and LoRa in asynchronous connections (p. 13).

An additional complication is that *"Currently, Endpoints may use only one of these wireless technologies. Dynamic switch between these three modulations and consequently data rates are not currently supported on the Endpoint side"* (Amazon Technologies, 2024, p. 11). Manufacturers must thus predict the usage conditions of their devices before manufacturing, to pick the technology most suitable for these conditions. This restriction is visualised in Figure 4.2 by displaying only one connectivity protocol for each endpoint-gateway connection. Still, all devices must support BLE or FSK, because endpoints cannot be registered to the Sidewalk network using LoRa (Amazon Technologies, 2024, p. 60, 165–168). Before the revision of the Sidewalk specification in February 2024, only BLE was supported (Amazon Technologies, 2023b, p. 62, 161–164), necessitating endpoints to have a BLE radio on board.

For endpoints in synchronised mode (and thus use FSK), the rate wherein they can try to establish new connections to gateways, and how often they can send data uplink, is defined in the specification

(p. 114-117). Manufacturers must choose how to trade off latency and power consumption by choosing one of two *"connection profiles"*, that each have different *"transmission opportunities"* and their own set of parameters that can be tweaked (p. 131, 134). A post on a silicon provider's forum shows that these options insufficiently enabled the power management scheme that one developer's organisation envisioned themselves, leading them to pivot back to a more flexible non-Sidewalk solution (jcesnik, 2024).

The specification furthermore prescribes how often synchronised endpoints will monitor whether it is still synchronised by sending commands to the Sidewalk cloud, too (p. 140-141). An additional benefit is that the Sidewalk cloud then knows which gateway the endpoint is connected to, and thus how it should route downlink traffic destined for the endpoint (p. 141).

Endpoints configured as asynchronous can in principle send data uplink whenever they desire. Downlink traffic can only be received in synchronous fashion, i.e. after an uplink transmission has taken place that the downlink message can be sent as a response to (p. 122-123). For transmissions in both directions, the specification details how often they can take place.

C.3. Motivators for silicon providers to produce for Sidewalk

§9.2 demonstrated that the yields of Sidewalk for Amazon are clear. In §9.2.2, it also seemed that silicon providers invest significant resources to enable Amazon to attain those yields: the silicon providers develop compatible chips, test them, nominate lead customers, and teach Amazon about chip development. The question is then how the silicon providers benefit. [A3] provided insights:

> *[I]f Amazon approaches you and says "I wanna work with you because X, Y, and Z", it would be stupid, or any board of advisors would advise that company to say "Yes, I will help however I can".*

The prospect of Sidewalk adopters buying the silicon providers' silicon is an obvious pro as it generates revenue. Being endorsed by Sidewalk brings visibility to the products; both through Amazon's marketing efforts, and through their requirement that adopters buy components from one of 4 approved silicon providers (see §8.2.1).

But there might be more dynamics at play, caused by Semtech's powerful position in the LoRa ecosystem. [A7] commented on the relations between silicon providers and Semtech:

> *[I]f you are like Wi-Fi, you have Broadcom, you have Qualcomm, you have Realtek, you have MediaTek, you name it. So there's a lot of people in it. [...] In the world of LoRaWAN, because of the relatively small segment, there's only one silicon vendor, which is Semtech, who license it to STMicro and Murata. The IP licensing, which is the same thing; different brand name, with a different outfit; the same chipset, but with a different name.*

Recall from §4.4.1 that the intellectual property rights of LoRa are owned by Semtech; here referred to as the *"one silicon vendor"*. The author assumes that the interviewee's mentioning of STMicro and Murata does not constitute an exhaustive list, but was meant to illustrate their point that ultimately, the chipsets barely differ: both are based on a technology licensed to them by Semtech. Semtech thus has a strong position in the LoRa ecosystem, with LoRa chipset manufacturers and end-users depending on their licensing terms and configuration of the technology. The result is that silicon providers can only add so much unique functionality on top of how Semtech has defined the LoRa technology for them, potentially making it hard to compete with other LoRa chipset manufacturers. Entering into the Sidewalk ecosystem then not only brings revenue generation, but also a way to differentiate one's offerings from that of LoRa silicon providers without Sidewalk functionality.

Finally, one respondent pointed out that the low-resource IoT landscape is a *"small world"*. In the process of approaching interviewees, the author noticed that a number of former silicon provider employees now work at Sidewalk manufacturers that use the products of this same silicon provider. This was also the case for this one respondent. When the author inquired about this overlap, the interviewee replied with this remark and then noted that *"the guy who's in charge of Sidewalk is also a former colleague"* from this silicon provider. They did not find this strange: *"the people that I'm talking about are all working within the low-power RF business of [the silicon provider]. And if you think of Sidewalk, what that is, is low-power RF kind of stuff. It's just, the industry isn't that large. It's not that many people who do this and can do it and move around, so it's quite natural that there is overlap."*

C.4. Rationales for choosing a silicon provider

In §C.3, it was mentioned how one interviewee deemed the low-resource IoT landscape a *"small world"*, after the author noticed that multiple employees the interviewee's organisation worked at one certain silicon provider before. Now, that organisation uses the chips of this chip provider, for which the interviewee provided three reasons. From a product point of view, *"it's nice to first build the chip and then see what you can do with it"*. A social perspective is that staying in contact with former colleagues through business relations is *"fun"*. And if the silicon provider *"wants a customer who is... well, easy-going and that they can trust, and that they know the relationship well with, then of course they lean towards the customer like that, that can understand if there are delays and then there won't be issues if something goes wrong"*. The context of this latter quote is Amazon inviting silicon providers to nominate a lead customer to develop Sidewalk with, as discussed in §5.6.

Some companies purchase from a variety of manufacturers. Reasons mentioned include minimising costs, diversifying the supply chain, and the silicon provider being able to produce from multiple locations around the world which makes them more reliable.

A partnership between a manufacturer and silicon provider constitute a positive feedback loop. This is because the longer the manufacturer works with the provider's chips, the better they understand how to get the most functionality out of them [A2].

C.5. Bidirectional relations

Relationships between IoT manufacturers and silicon providers were often typified as bidirectional. As one interviewee put it, a silicon provider *"sells hardware and gives away software. [...] Part of [their] business with Amazon is dependent on if the software works, so they had to put quite a lot of effort into that, and then [the interviewee's company] get[s] to leverage that"* [A2]. Therefore, the silicon provider of [A2] gives them *"a lot of support"* and *"a dedicated person working with Amazon in [the silicon provider] working with [them]"*. Other participants also reported being a *"guinea pig"* for their silicon providers, aiding them to *"firm up their code"* [A6] and *"helping them with their test setup process"* as they were the silicon provider's first Sidewalk-adopting customer. This help concerned development of their firmware and SDK, and the addressing of bugs. [A5]

C.6. Additional disadvantages for Sidewalk adopters

C.6.1. Over-promising of range and confusion about underlying radio technologies

[A1] argues that Amazon over-promises the range that Sidewalk endpoints could operate over in their marketing. A usual disclaimer is that the range in practice depends on the radio communication protocols used, and environmental factors, such as obstruction of the signal. However, transmitting and receiving over longer ranges also requires more powerful hardware, and consequently a more powerful battery, which low-resource endpoints might lack. Relatedly, Amazon uses Sidewalk as umbrella term for the three different radio technologies with varying data transmission capabilities (see §4.2.2). In fact, a Sidewalk-enabled device might not support all three. Both factors may result in users misunderstanding their device's range, availability, and bandwidth [A1].

C.6.2. Doubts about the appropriateness of using Sidewalk as finding network

One participant questioned the appropriateness of Sidewalk as a network for finding devices in the context of the Tile and Sidewalk partnership. This is striking, given the many adopters that offer asset tracking solutions (see Table B.1). They elaborated that conventional consumer asset trackers (e.g. Tile Mate, Chipolo ONE, Apple AirTag, Samsung SmartTag) are located by mobile phones, that both sense that a tracker is nearby, and know their own location.. They then report both to their associated cloud service. Conversely, Sidewalk gateways only sense the Bluetooth IDs that Tile trackers emit; *"the interesting thing is, none of the Amazon Sidewalk devices really know where they are"* as they lack GPS. Sidewalk gateways only report the sensed IDs to Amazon's cloud, which then has to derive the location of the gateway. The interviewee believes Amazon does so by using the addresses that gateway owners report in their account, that are often incorrect. For instance, the owner might put an incorrect address out of privacy concerns.

This argument contrasts with what two other interviewees said, namely that Amazon does know

gateway locations, and did not mention that being inaccurate. Amazon's marketing materials imply the same, stating that gateway owners can *"help [their] neighbors by sharing [their] Bridge's approximate location to provide benefits like helping them locate their pet"* (Amazon, n.d.-b). Because gateways are themselves connected to the internet, it seems likely that Amazon has other ways of localising them. For instance, AWS offers a service for locating (IoT) devices by (inter alia) analysing their IP address or nearby wi-fi access points or cellular radio towers (Amazon Web Services, n.d.-a).

C.7. Amazon as a Sidewalk adopter

Amazon is not only the provider of the Sidewalk service; they use the service for their own endpoints, too. They have developed a number of endpoints, although not all of them are currently for sale (§C.7.1). Interviewees reported on a dog tracker and an asset tracker that were at one point developed, but never hit the market (§C.7.2). Two interviewees spoke on their expectations of Amazon launching more Sidewalk-enabled endpoints (§C.7.3). While Amazon can increase the usage and visibility of the Sidewalk network with these devices, Amazon could also develop products that compete with those of third-party Sidewalk adopters (discussed in §7.3).

C.7.1. Sidewalk-enabled products on the market and in development

Currently, only two Amazon device types can function as Sidewalk endpoint. These are select Echo and Ring models; and that is because all gateways can also leverage Sidewalk as endpoint (Amazon, n.d.-b). There are hints, though, that Amazon has been producing other Sidewalk-enabled endpoints. A recent job opening seeks for somebody to *"Collaborate and Work with Ring as well Echo products to launch Sidewalk End points and Sidewalk Gateways"* (Amazon, 2024a). This phrasing makes it unclear whether Amazon will put out new gateways that double as endpoints, or devices that are only an endpoint. Multiple examples of Amazon developing the latter kind of products surfaced in the interviews.

First is the Ring Fetch, which Amazon's (then-)vice president of devices described as *"a dog tracker that will use Sidewalk and ping you if your dog leaves a certain perimeter"*, supposedly coming to market in 2020 (Jones, 2019; Porter, 2019). Announced during the same press conference as Sidewalk itself, this application seemed intended to demonstrate Sidewalk's value for end-users, to convince manufacturers to join the network. Indeed, Amazon also said the Fetch would serve as reference design for developers (Jones, 2019; Porter, 2019).

At the time of writing, the device has not been brought to retail. Amazon told a journalist in early 2023 that there was *"no update"* on the device (Tuohy, 2023c). Perhaps Amazon does not see enough value in the product compared to other trackers on the market, including Tile trackers that can also be localised by Sidewalk gateways (Amazon, 2021a; Tile, n.d., 2021).

Note, though, that calling the Fetch a *"dog tracker"* oversells its capabilities. The Fetch alerts the user when the dog crosses a geofence, but neither the press release nor any second-hand journalistic coverage of the press event make mention of the Fetch informing the owner where the dog has run off to. The device does not track the dog's location, but merely whether it is inside or outside a preconfigured area.

A while after revealing the Fetch, Amazon announced a pilot with the American Red Cross for tracking supplies, with Amazon providing the necessary devices and personnel (Ciovacco, 2020). The announcement does not mention any other company that could be delivering the tracking devices, implying that Amazon also was or is developing asset tracking endpoints. At the moment of writing, no update has been shared about this project.

Late 2022, Zatz (2022) wrote about a rumoured Ring Car Alarm. He pointed to a product support page, a product image that made its way into the Ring smartphone app, and FCC and Bluetooth filings. Allegedly, the alarm could share its GPS location and alerts about detected movement of or impact on the vehicle with the owner's phone. Zatz (2022) says that the release date is uncertain and that the support page and product image were already pulled offline at the time of publication. At present, the product is not for sale.

A product that is actually on the market in the US is the Ring Mailbox Sensor, that informs users when their mailbox has been opened or when mail arrives (Ring, n.d.-c). Ring said in 2021 that it would become Sidewalk-enabled in that year (Higginbotham, 2021), but that has not happened yet. There is no

public release date either, as I confirmed in a virtual chat with Ring's customer support in January 2024. In a podcast published slightly before my inquiry, the Ring CEO did mention the sensor directly after saying that the team is *"using [Sidewalk] internally for testing different kinds of sensors that make sense to be on the Sidewalk network"* (Bishop & Hamren, 2024, 21:07). This statement implies Sidewalk compatibility is yet to come. The CEO's mention of this mailbox sensor, and not the Fetch dog tracker, seemingly confirms the role of the latter as reference design and not of actual retailed product. After all, the Fetch has been the poster child of early Sidewalk coverage; not mentioning it anymore would be odd if Amazon still planned to release it.

C.7.2. Amazon's development of their own asset tracker

Despite – or perhaps because of – the Sidewalk integration with Tile, Amazon had plans to deploy its own Sidewalk-based consumer asset tracker. One participant unveiled that Amazon was *"working on like a Tile type of device that would use the Sidewalk network"*, besides the dog tracker. For this, the team initially evaluated a LoRa tracker with a coin cell battery. However, attaining the range benefits of LoRa required more transmission power than the small battery allowed, bringing them back to ranges akin to Bluetooth. Note that I had not raised Tile in the interview up until that point, so the interviewee comparing their product to Tile is curious. The interviewee might simply consider Tile an accurate comparable example to illustrate their work-in-progress, or the team might have taken Tile (and Apple) as inspiration and referred to the project as such internally. The latter seems plausible; when I brought up the fact that Tile is now compatible with Sidewalk, they compared their project to both Tile and Apple:

> *That's what killed the project, right? We were in the middle of it, and then they cut a deal, you know, the executives cut a deal with Tile. And we're like "yeah, well, then, we don't need this other thing". I mean, we were doing some other cool things with it that were different than a Tile, that would have had... But probably the main, most important feature would have been a "Find My" type of feature. And so once they got Tile deal, then it was sort of, "what's the point here?"*

What, then, prompted Amazon to cancel this tracker and their Fetch? The Tile partnership seems the most logical explanation. If the proprietary tracker was intended to demonstrate Sidewalk's value to consumers by enabling finding applications, as was the case with the Tile partnership and the Fetch (§9.5), then the Tile integration made the development efforts redundant. Moreover, the developed tracker and the Fetch would obviously compete with Tile. Amazon might have considered the development costs to overshadow the potential revenue. Additionally, competing with Tile so directly would tarnish Amazon's reputation as trustworthy business partner, seeing how they explicitly partnered with Tile to integrate their devices in Sidewalk. This is not a completely unimaginable scenario, though, seeing how Apple has its own AirTags that effectively compete with third-party trackers (e.g. from Chipolo) that have integrated themselves with Apple's Find My network; this dynamic is further explored in §10.5.2.

Another potential explanation is the disputed utility of Sidewalk as a finding network, as elaborated in §C.6.2. The interviewee that formulated the latter point, stated that *"if [Amazon] were to launch a tracking device of their own, they don't really have an effective network to track the devices"*. On the contrary, Apple and Google can leverage smartphones' (Google, Apple) and computers' (Apple) GPS capability by baking finding functionality into the their smartphone and desktop OSes, as they do with their Find My networks (see §10.5.2).

C.7.3. Interviewees' expectations of more Sidewalk-enabled devices coming to market

Because Amazon typically stay quiet about products they have in development, I asked interviewees whether they know about or expect Amazon to bring more endpoints to market later.

[A1] noticed Amazon barely marketing Sidewalk-forward devices: *"I know they were working on some Sidewalk-based products. It seems like, I don't know if any of those have ever come to fruition. Like a Sidewalk-only product, or at least a Sidewalk-forward product"*. [A8] said they do not know if Amazon plans to release more of such products, but *"would have to imagine they will be, because if [the CEO]'s in that podcast already mentioning that [...]. I would be a fool to say they won't"*. [A7] expects Amazon to release competitive products when the Sidewalk market has matured more: *"I have no doubts that they are doing the same thing, right? Because this is still small, so their tolerance is higher, so they invite more people to join, 'you do it,*

I'm not gonna do anything', until it comes to a level where they say, you know, 'we will do it better than you do'". This interviewee thus seems to fear Amazon at one point bringing their own versions of third-party Sidewalk endpoints onto the market, potentially outcompeting them. This is the subject of §7.3.