International Review of Law, Computers & Technology

ISSN: 1360-0869 (Print) 1364-6885 (Online) Journal homepage: www.tandfonline.com/journals/cirl20

Device sharing features: a study on software policy approaches and platform capabilities

Kalle Hjerppe, Sini Mickelsson, Jukka Ruohonen, Robin Carlsson, Timi Heino, Sampsa Rauti & Ville Leppänen

To cite this article: Kalle Hjerppe, Sini Mickelsson, Jukka Ruohonen, Robin Carlsson, Timi Heino, Sampsa Rauti & Ville Leppänen (23 Oct 2025): Device sharing features: a study on software policy approaches and platform capabilities, International Review of Law, Computers & Technology, DOI: 10.1080/13600869.2025.2575550

To link to this article: https://doi.org/10.1080/13600869.2025.2575550

Published online: 23 Oct 2025.

INTERNATIONAL REVIEW OF LAW, COMPUTERS & TECHNOLOGY
https://doi.org/10.1080/13600869.2025.2575550

Device sharing features: a study on software policy approaches and platform capabilities

Kalle Hjerppe [a], Sini Mickelsson[b], Jukka Ruohonen[c], Robin Carlsson[a], Timi Heino[a], Sampsa Rauti[a] and Ville Leppänen[a]

[a]Faculty of Technology, University of Turku, Turku, Finland; [b]Faculty of Law, University of Turku, Turku, Finland; [c]SDU Center for Industrial Software, University of Southern Denmark, Odense, Denmark

ABSTRACT

Personal computing devices are often not literally 'personal' in practice. Device sharing, i.e. two or more persons using a device, is a common phenomenon in everyday life. With multiple different layers of software and accounts, the interactions between them in a device sharing scenario become complex, leading to data protection and other risks. With the goal of gaining insight into how the industry considers this topic, in this mixed-methods study, we examine the approaches software providers take on device sharing in their policies with systematic content analysis. Furthermore, we examine the indications whether these approaches are present in the current capabilities of the devices as platforms, with systematic black-box testing. The results reveal a complex and partly ambiguous landscape of different approaches, highlighting potential areas with a lack of alignment. We identified 18 common approaches in policies to manage different aspects of device sharing and clarified the 'border' between operating systems and applications.

ARTICLE HISTORY
Received 8 April 2025
Accepted 11 October 2025

KEYWORDS
Device sharing; data protection; GDPR

1. Introduction

Device sharing is hard to design for! Consumer device and account sharing is a common practice among household members and relations, for multiple different use cases ranging from borrowing to helping others Matthews et al. (2016). The social relationships and user needs around sharing are complex and not simple to fit into technical design assumptions – a feature that serves one might be a hindrance to another (Sailaja and Fowler 2022).

Software product and service providers, whether considering platforms or applications, all have their own objectives and motives. It is safe to assume in product design that the product will be shared by some of the end users with other persons whenever convenient for the user (Matthews et al. 2016). The implications of this ought to be considered in

CONTACT Kalle Hjerppe kphjer@utu.fi Faculty of Technology, University of Turku, Vesilinnantie 3, 20500 Turku, Finland

responsible software and policy design, whereas the actual approach chosen is a business strategy decision. A provider might, for instance, try to limit sharing by service agreement terms, or manage it with explicitly supported features. Device sharing may also involve risks, which should be considered in threat models or data protection risk assessments (Levy and Schneier 2020).

Legal requirements affect software and policy design. Data protection and intermediary laws impose requirements, inter alia, concerning user consent age limits which need to be considered in the policies and user agreements (DE/BB, EDPBI:DEBB:OSS:D:2019:53 2019; Italian Supervisory Authority 2021) and in implementing technical features (Irish Supervisory Authority 2022a). In addition, the end-user licence agreements and other terms attached to the products and services are influenced by the principles of copyright, consumer, and contract law in general (Corbett 2019, 454), (Sandeen 2003, 513–526).

The design of consumer device and software features nevertheless has implications beyond convenience and meeting regulations. While there has been progress in multi-user features in recent years, providers often consider devices entirely personal and households as single units. Neglecting this, home devices with misguided features can end up facilitating abuse (Levy and Schneier 2020; McKay and Miller 2021) and compromise vulnerable users' rights (Buitelaar 2018; Piasecki and Chen 2022). Furthermore, their use can simply be burdensome to users (Chen, Hengartner, and Khan 2022). Software platforms have an important role in defining how application providers can handle these issues (van Hoboken and Ó Fathaigh 2021). The practice of sharing devices, e.g. smartphones, is especially common in non-Western contexts where privacy expectations are different because of the cultural, religious, and familial structures (Naveed et al. 2022).

In recent years, the industry has made advances around the device sharing features. Many service providers have implemented their own technological solutions for shared accounts and enabled devices to better integrate multiple accounts (Karlson, Brush, and Schechter 2009), for instance, but there are also naive implementations that either fail to consider the issue or fail to solve users' practical challenges (Sailaja and Fowler 2022). Some business decisions have been made actively against consumer preferences, too (Zhang and Challis 2022). Viewing the consumer device and service domain as a whole, solutions for sharing are immature in many ways; there are problems with usability and data protection, among other things. One vision to ease these issues is a more integrated, proactive device sharing awareness on platforms (Chen, Hengartner, and Khan 2022).

Much of the academic literature considers the perspective, rights, and needs of users around device sharing. There are proposals with merit for solutions for users, but are the product and service providers on board? Making conclusions for industry providers requires a nuanced approach.

This paper begins from the perspective of providers by surveying their *policies*, i.e. how they would prefer their software to be used in the *as-is* state of a sample of the ecosystem. The crux of this paper is exploring the junction of these two assumptions: Firstly, that the users *will* share their devices and software, while requiring a good user experience, data protection, and privacy. Secondly, that the software platform and service providers have expectations and limitations for this sharing (and express them in their policies and agreements).

The paper presents a systematic analysis of common and codified policy strategies of popular software products and services, following existing guidelines (Assarroudi et al. 2018; Elo et al. 2014), with content analysis and systematic mapping. The results from the analysis are then used as the input for preliminary use case elicitation and test definition for the software artifacts themselves. Subsequently, we review the current popular consumer device platforms for their capabilities to support the use cases.

The results are twofold: we firstly present a mapping of industry policies for sharing, and secondly, a gap analysis of the current platform capabilities to the use cases. The core findings are a list of policy approaches, their prevalence in the industry, a conceptual map of the implications to platform design, and an indicative view of the gap in practice. The frictions identified in this research are not necessarily critical errors in usability or data protection. Rather, we present ways to further align industry actors while also considering user needs for sharing and privacy.

We note that the device sharing features can both support software product and service providers' business strategies and promote data protection by design to further users' privacy, also in household device sharing situations.

The objective of the study is to map the state of practical device sharing related considerations, including data protection and privacy, through the many layers of different software products and services, especially focusing on the capabilities of the common consumer technology platforms. Before visions for a future where most needs are met, it is important to know what the different stakeholders (consumers, platform providers, and application developers) are each currently doing and what they are striving for. This study elucidates the current situation of the technology providers from two dimensions.

On one hand, we envision that providers and producers of software products use End User Licence Agreements *(EULAs)* and terms of use to specify *how they prefer their services to be used* and privacy policies to specify *how they process personal data*. On the other hand, functionalities of the software products reveal *how device sharing is impacted by provider and platform choices in practice*.

Achieving our objective of providing a wide picture of the current state of device sharing capabilities, both the policy document dimension and the technological dimension are covered in two separate research phases. Two research questions (RQs) are asked and answered, to this end:

RQ1: What are the common assumptions and strategies employed by software product and service providers to account for device sharing in their policy documents?

RQ2: To what extent does the model of RQ1 map into current technical capabilities and limitations of the software platforms for device sharing use cases, and to what extent have application developers themselves implemented features to facilitate device sharing use cases?

The rest of this paper is formatted as follows. Section 2 describes the background of the study and elaborates on related work in academic literature with the identified research gap. The research method, setting, and data analysis employed are described in Section 3. The results are presented in Section 4, with discussion in Section 5.

2. Background and related work

We examine within this study the use case of device sharing in typical consumer use through various technologies, including operating systems, web browsers, web applications, and mobile applications. Simplifying the terminology, in what follows, these are together referred to simply as software products and services (SPSs). The term *device* can refer to a large range of hardware, from Internet of Things sensors to smart cars. In this study, we focus our scope on general-purpose computing devices, i.e. PCs and smartphones, even if many of the themes could be applicable to a wider range as well.

The consumer device space consists of an ecosystem of different software operating on different abstraction levels, which compose a system with many products and services (Hein et al. 2020). One perspective on the relationships between different SPS is the distinction between platform providers and application developers, which both compete and co-create value for users. A software can simultaneously be both a platform provider and a platform consumer, forming a 'stack'.

It is important to consider what the term device sharing actually entails. We refer to Matthews *et al.* for this purpose: simply put, the practice of device sharing involves two or more persons using a single device (Matthews et al. 2016). More interestingly, they present six *sharing types* that categorize *how* devices are shared. The most common type is *borrowing*, where a device is temporarily lent to another in order for the sharee to benefit. In contrast, *mutual use* refers to a regular sharing arrangement of a device, whereas *broadcasting* means that many people view a device simultaneously. Sharing types *setup* and *helping* benefit the sharer instead of the sharee. Finally, *accidental* sharing refers to the unintentional disclosure of data to another party when sharing a device. As noted previously, sharing devices and accounts is common whether or not SPS providers consider it in their design (Matthews et al. 2016).

The objective of the previous exposition is to highlight the need for nuance in assessing these issues. In 'device sharing', there is no single type of act of 'sharing', other than as an umbrella term, and 'device' can, in practice, include various different technical configurations of sharing accounts, applications, data, or features. Considering the different sharing types, it can be imagined how each could be applied when operating at a different level of the technology stack. This highlights the delicate nature of the entire digital system of a device, and how it is not trivial to identify what exactly is being shared when a device is e.g. borrowed to watch a video. There is a difference between helping an elderly parent set up a smartphone OS or just setup a profile into a *Netflix* account. This interplay of many stakeholders with differing goals motivates the need for subtle and careful consideration when designing device sharing features.

There are a few different perspectives when considering the issues raised in device sharing. To begin with, there are the aforementioned business requirements of the SPS providers to mention, with different goals for platform providers and application developers. The 'business need' of the users in this context can be considered to contain, for instance, receiving the product or service they are customers of, *while meeting their sharing practice of whichever sharing type they engage in*. However, the users have various needs and interests, which they may prioritize in different ways. For example, users may value easy sharing, but at the same time prioritize privacy over easy use.

Privacy self-management has also been shown to be difficult, and the users often resort to 'hopeful trust' for the SPS providers (Knowles and Conchie 2023). Some users are also in a vulnerable position where sharing a device may not be voluntary or may impose threats to the users' privacy and safety. The present work limits itself to considering the issues concerning shared use, while, naturally, not each user needs every use case, or shares their devices at all.

Device sharing involves both data protection and privacy issues to consider, and these – again – have competing interests. One role of the platform providers is to provide a secure and privacy-preserving product for their users (van Hoboken and Ó Fathaigh 2021). Whereas an application provider could want to keep the issue between them and their users. As a whole, the system *ought* to protect the rights and freedoms of all the persons involved, customers or not. Privacy as a concept is contextual, and what is appropriate to share depends on cultural norms (Nissenbaum 2004). In the past, as mentioned, the industry has considered devices and accounts to be entirely personal, a false assumption (Matthews et al. 2016). Finally, there are the other social facets that device sharing features can both enable or hinder (McKay and Miller 2021).

2.1. Device and account sharing as a phenomenon

Device and account sharing as a topic with specific issues to investigate has been discussed for over a decade, known to be a prevalent practice (Brush and Inkpen 2007), with families making use of both common accounts and private profiles (Egelman, Brush, and Inkpen 2008), and it has been understood that there are many privacy issues to consider (Karlson, Brush, and Schechter 2009). There are clear privacy risks identified relating to apps and smart devices sharing data with third parties, especially related to children (Article 29 Working Party 2013; Carlsson et al. 2023), from a user privacy perspective. For instance, smart speakers have been argued to violate privacy based on device sharing (Lemmer 2019). These developments naturally coincide with the general trend of digitalization and smart device proliferation.

The social issues and human practices concerning device sharing are a research track of their own, exploring the ways and reasons sharing is done (Matthews et al. 2016), how the attitudes around sharing differ across cultures (Sambasivan et al. 2018) and showing the consequences such as stalking (Freed et al. 2018), monitoring and control (McKay and Miller 2021), and other abuse that can result. The very act of shared use requires trust between the users, especially when there's a power imbalance between them (Karnatak et al. 2023). As device sharing results in digital entanglement, it can be difficult to separate back to a non-sharing situation (Quan-Haase, Nevin, and Lukacs 2018; Sas and Whittaker 2013).

The aforementioned risks are often emphasized, but, on the other hand, users gain convenience, economics, and logistics, or simply relationship maintenance from sharing (Park et al. 2018). Despite abuse and control being a motivation for keeping privacy in reins with device sharing, there are also reasons in healthy sharing not to share everything, such as gift giving or simply setting boundaries (Park et al. 2018). People with disabilities and other vulnerable groups can gain great benefits from device sharing, especially when accessibility is otherwise not optimal (Matthews et al. 2016). Older persons can be more vulnerable to cybersecurity threats, but turning to collaboration

with communal security practices may help them to cope (Murthy et al. 2021). Patients may wish to involve their caregivers in the digital care access (Weis et al. 2020). Older persons also tend to represent each other in online banking, whether it is technologically supported or not (by password sharing) (Latulipe, Dsouza, and Cumbers 2022).

People have different motivations for device and account sharing, as discussed previously (Matthews et al. 2016). In particular, cost-splitting has been identified as a major motivation for more formal sharing arrangements (Eun Song, You, and Lee 2021). These services are considered to be *Designed for sharing*, and include explicit profiles, as opposed to sharing that happens regardless of provider intent (Obada-Obieh, Huang, and Beznosov 2020). The perception of account ownership in a multi-user setup with cloud data is not trivial, and what matters more is *control* of the profiles and accounts (Eun Song, You, and Lee 2021). On the other hand, privacy itself (as control over information) is of less importance in communal technology use, compared to other social considerations (Kraemer et al. 2023). In the digital era, the concept of personal ownership has reduced, as service providers often merely licence rights to content (Perzanowski and Schultz 2016). The rights and obligations of users and SPS providers are defined in end user licence agreements, terms of services, and privacy policies. Furthermore, privacy policies and terms of service have been found to be hard to understand, and too onerous to read, in user interviews (Abdi, Ramokapane, and Such 2019; Huang, Obada-Obieh, and Beznosov 2020). The present work attempts to further identify the actual conditions these terms outline regarding device sharing.

2.2. Device sharing in software and system design

The findings regarding social issues related to device sharing naturally have implications for the design of both hardware and software. Social cybersecurity researches how people negotiate access to shared resources, share authentication, manage self-presentation, and influence security and privacy practices of others (Wu, Edwards, and Das 2022). Research has both identified weaknesses in the current state of device sharing and proposed a number of technical solutions to address access control issues. Since the sharing culture is systemic, at least considering the global scope beyond the Western contexts (Sambasivan et al. 2010), simply locking a device is not an option in every context, and finer-grained technological features are needed for privacy (Ahmed et al. 2019).

Password management practices are one of the main causes of vulnerabilities in shared devices (Alam, Molyneaux, and Stobert 2021). The fact that shared devices are often used by multiple persons co-present, and the lack of physical separation, weakens security assumptions (Levy and Schneier 2020). There are many proposals in the literature to meet these identified challenges. The login and access issues could be remediated by more advanced access control models, such as *DiffUser* (Ni et al. 2009), *Kratos* (Sikder et al. 2020), and others (He et al. 2018; Mazurek et al. 2010). For instance, DiffUser introduces a more varied user privilege control levels to smartphones, as opposed to the two-state model of 'access' and 'no access' commonly used (Ni et al. 2009). Smartphones with sensors could even be made proactively sharing aware, sensing when there are many persons present (Chen, Hengartner, and Khan 2022). One of the design principles for sharing is 'plausible deniability', so that, for example, a device does not explicitly make users aware that there are secret accounts installed, instead of just the one shared

account (Ahmed et al. 2019). Regarding how sharing is performed, the most common way access is shared is simply keeping an account logged in on a device (Park et al. 2018), though password managers were the next most used method (Park et al. 2018), followed by less secure password sharing methods (Park et al. 2018). This culture of password sharing should be considered when designing software (Singh et al. 2007). For instance, goal-oriented access control models have been suggested as a solution to certain sharing use cases, where permission is granted, not to a user for a resource in general, but to a user for a resource only to achieve a goal (Kraemer et al. 2023). These goals could include the aforementioned sharing types, for instance. The present work shows a sample of the strategies software providers use in their policies to tackle password sharing.

In the representative person use cases, where shared technology is used, for e.g. elder monitoring, it has been shown that there is a strong need to keep some control for the vulnerable party, and this should be taken into consideration in software design (Berridge et al. 2022). There are simple design principles, such as being able to pause the technology for a private moment, trying before committing, and being reminded of data collection (Berridge et al. 2022). The present work provides some further insight into how few app and website providers explicitly consider representative persons in their policies.

Smart home systems such as intelligent assistants accessed with a speaker are becoming increasingly common, operating often in a shared space, which has specific data protection issues (Meng, Keküllüoğlu, and Vaniea 2021). These often collect data from bystanders and others who inadvertently or without choice become 'device sharers' in this manner (Bernd et al. 2022). It has been observed that device owners can also become 'victims' of device sharing misuse, when other persons, such as guests in the household, change settings, modify data, or trigger unwanted actions, etc., of their smart devices, such as television or speakers (Moh et al. 2023). It has been argued that SPS providers should create more extensive controls for device sharing use cases (Huang, Obada-Obieh, and Beznosov 2020) – with voice recognition technology, for instance. The present work is not focused on explicit privacy controls or vulnerabilities, but the conceptual model of device sharing requirements presented is a step in the way to achieving a more holistic system, which could then implement these novel access control mechanisms.

There exists, also, a business tension between the two paradigms of application and platform providers, as it is not trivial to say what is a fair share of the total revenue generated for each party (Oh, Koh, and Raghunathan 2015). This tension can manifest in different ways, one dimension of which plays out in the implementation and integration of the technical capabilities of software platforms and applications. The ecosystems of platform providers and application developers are fundamentally socio-technical systems, and influencing the system depends on the interactions of the various actors within it Lima et al. (2016). This paper investigates this issue within the specific slice of functionalities that relate to device sharing.

2.3. Device sharing and appropriateness of data flows

One way to assess the data flows in connection with device sharing is by utilizing Helen Nissenbaum's contextual integrity framework. The framework posits that privacy should

be regarded as a right to the appropriate flow of personal information. Contextual integrity is defined by context-relative informational norms, which regulate the flow of information about an information subject from one actor to another or others according to particular transmission principles. Informational norms consist of four key parameters: Contexts (conditions of application), actors (senders, recipients, and data subjects), attributes (nature of data), and transmission principles (terms and conditions under which transfers ought to happen) (Nissenbaum 2010).

Device sharing can occur in various types and contexts, including the home, school, or workplace. In device sharing, the information transferred is most often regarded as personal data. Data protection laws, such as the EU General Data Protection Regulation (GDPR),[1] regulate the processing of personal data. Thus, the GDPR can be regarded as one important source for context-relative informational norms in device sharing. The GDPR, inter alia, requires data controllers to build data protection into their services and products (Article 25 of the GDPR) and recognizes that certain groups of data subjects, such as children, should be granted special protection (see e.g. recital 75 of the preamble to the GDPR and Article 8 of the GDPR). Furthermore, provisions of consumer and contract law, as well as intermediary and e-commerce regulations, are important in the context of device sharing.

Policy and other agreement documents can be seen, from the perspective of contextual integrity, as a representation of the transmission principles by which SPSs seek to define the terms and conditions under which transfers can happen. Regarding the technological ecosystem at hand, it has been noted that platform providers play an important role as privacy regulators in the mobile device and app ecosystem, which has led to demands for more transparent privacy-related policies and practices to ensure fair competition and protect user privacy (van Hoboken and Ó Fathaigh 2021). This theoretical argument is provided empirical backing, at least within the scope of device sharing, from the analyses of the present work.

On a general level, privacy policies, including their compliance with the GDPR, have been extensively studied. The studies include, for example, analyzing textual statistics and readability (Rowan and Dehlinger 2014; Winkler and Zeadally 2016), information collection practices (Winkler and Zeadally 2016), and changes in policies due to the GDPR (Bateni et al. 2022). Transparency in privacy policies has increased since the GDPR, but improvement is needed (Kretschmer, Pennekamp, and Wehrle 2021). It has been shown e.g. that there are discrepancies in policies and analytics in practice (Heino et al. 2022), though this could be mitigated by basing privacy policies more closely to the actual functionality of a system (Hjerppe, Ruohonen, and Leppänen 2022). There is an underexplored research gap, however, in the body work of privacy policy analyses specifically on the device sharing topic – how do the policy and agreement documents address the issues. Furthermore, the policy analysis and assessment of the technical capabilities of this study sheds light on what terms and conditions the SPSs seek to establish and enforce for data flows in the context of device sharing.

One specific aspect that requires attention is the type of actors involved in device sharing. Shared use can involve vulnerable groups (Peroni and Timmer 2013) or vulnerable data subjects (Malgieri 2023) as actors. This invokes specific issues concerning, inter alia, the adequacy of legal basis for processing personal data, particularly parental consent requirements (Jasmontaite et al. 2018; Livingstone 2018), and should be

considered when applying data protection principles, such as data protection by design and by default, and a risk-based approach. Piasecki and Chen (2022) and Malgieri and Niklas (2020). In situations when a child acts both as a sender of information and a data subject, special frameworks concerning children's rights (Buitelaar 2018; Jasmontaite and De Hert 2015), as well as emphasized transparency requirements (Milkaite and Lievens 2020; Morgan 2018), must be taken into consideration in assessing contextual integrity.

Furthermore, the power imbalance between the users and SPSs, as the latter unilaterally defines the terms of policies and agreements, as well as the technical implementations, can potentially compromise users' rights as consumers and data subjects (Helberger et al. 2022; Liu 2024). Beyond compliance, in the context of using their own devices, users may have expectations and needs, such as being able to ask and receive help from a family member in the use of the application, which may contradict the terms and policies established and enforced by the SPSs. Where possible, we seek to identify these elements in the policy analysis and assess their meaning in the context of device sharing.

3. Research method and data

The study features two distinct research questions as outlined in Section 1. The first asks for a survey of device sharing policies of software product and service providers, and the second investigates their realization into practice.

The methodology used to answer RQ1 is qualitative content analysis, with a systematic mapping process. This type of qualitative analysis is a method for description and interpretation of textual data based on a systematic process of coding; the goal is to identify categories, themes, patterns, and concepts (Assarroudi et al. 2018; Elo et al. 2014). The researchers avoid preconceived categories and allow them to be identified from the data (the policy texts), by systematically reading and rereading the data set as a whole and then word for word, and refining the code set iteratively (Hsieh and Shannon 2005). These raw codes are then organized by further categorizing and abstracting the coding, using abductive reasoning, resulting in a conceptual map of the study area (Elo et al. 2014).

For the second research question RQ2, the method employed is exploratory black-box testing, a software engineering practice, with the aim to provide a light overview of how the industry approaches are realized into practice. The goal is to provide insight into the practical situation, how the device sharing reality can fit into the SPS requirements, the conceptual model needs to be formulated into verifiable test cases, which instantiate the requirements into device sharing use cases. The study approached this first by formulating testable use cases from the policy analysis conceptual model with design science requirements engineering methodology, then by systematically exploratory testing each use case for each applicable software and platform, resulting in either a validating test case or a reasoning for failure. This step from the conceptual model to the concrete is an abductive leap following the deductive analysis. Viewed as a whole, this methodology is the traditional *requirements engineering* process: domain analysis, eliciting goals, boundaries, and scenarios (van Lamsweerde 2000).

Considering the device sharing model that would consist of all of the features identified in the policy analysis, in order to meet this demand identified from policy, a theoretical platform could meet many (if not all) of the requirements identified in the analysis, so that the application service providers do not have to implement those themselves. The primary need considered, for the users, is being able to access these services in various shared device configurations, while maintaining control over their privacy. One relevant concern is the need to manage the issues on an application-by-application basis and input the same information multiple times. The imagined platform would implement many of the capabilities itself, while leaving it to the user to only grant permissions and, for example, consent to providing their age to a service for age gate verification.

3.1. Data collection

A consumer computing device runs on a stack of technologies, ranging from the underlying operating system to web applications executed in web browsers. In order to answer the RQs, representative sets of software products and services are required on operating systems, web browsers, web applications, and mobile applications.

Our rationale for selecting the sample software is that the products with the largest market shares deal with the most users and thus the choices their providers make have the largest impact. Aside from operating systems selection, data from the service Similarweb[2] was retrieved on 20 March 2022. The service has been argued to be a reasonable choice for selecting SPS with significance (Prantl and Prantl 2018). Given data from this service, the following SPS are covered:

- *Operating systems*: the latest versions of the most popular operating systems were selected; Android, Microsoft Windows, iOS, and macOS.
- *Web browsers*: the browsers with the largest global market share were included; Chrome, Safari, Edge, Samsung Internet, and Mozilla Firefox.
- *Mobile applications*: a sample of top-20 applications were selected from Google Play and Apple Store in Finland.
- *Web applications*: a sample of top-50 web applications were selected.

Altogether 139 software products were initially selected based on search results in May 2022. Of these, duplicates were excluded alongside software products not offered in English or Finnish. Then, the policy documents (applying to customers in Europe) of the software products were searched. During this search, those products were excluded that (a) had no documents available; (b) did not provide the documents in a form that is textually processable (e.g. in an image format); or did not have the documents available in English or Finnish. Some different software products referred to the same policy documents; in these cases, only the first instances of the documents were included. In case a product provided country-specific documents, those offered to Finnish customers were used. It should be acknowledged that the data selection strategy, though in line with the EU context of the studied regulation, biases the data set towards well-resourced, Western products. Given these processing criteria, the total number of software products covered is 75. These serve as the units of analysis: distinct software products represented by an EULA, terms of use, and a privacy policy. To illustrate the sample, we categorized

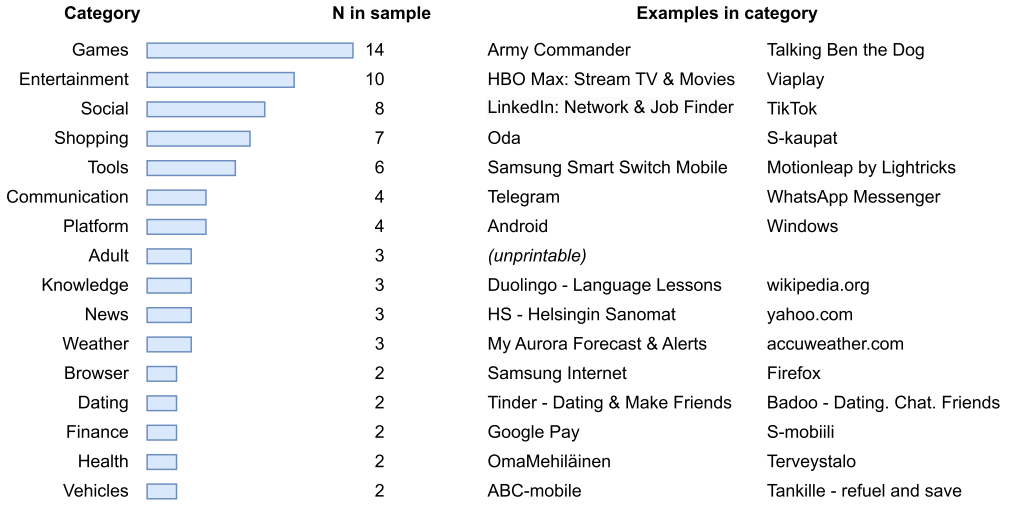

Figure 1. SPS samples per application category, based on reduced SimilarWeb categories.

them based on a reduced form of SimilarWeb categories. These are visualized in Figure 1, with some examples.

In a qualitative content analysis study, the trustworthiness of the data collection method is a critical prerequisite for the validity of the study (Elo et al. 2014). The data in the present study is unstructured, consisting of entire policy documents. The content itself should be as reliable as can be extracted from the industry: they are legal documents that *are* the requirements the SPS providers impose for the use of their products. In contrast to, for example, interview answers, these documents should not be used to make large inferences of the motivation behind them; they are as-is without explanation.

3.2. Data analysis

3.2.1. Policy analysis

The policy documents were analyzed according to the following thematic analysis process. First, the two researchers read each policy document and identified passages and terms that specifically referred to the topic at hand. The focus is partially on device sharing strategies under the GDPR, passages and terms referring to users outside of the European Union were omitted (e.g. Brazil or California in the United States). The passages and terms were collected into a separate file for later inspection, while preserving the original documents to be able to refer to the context. Second, the distilled texts that referred to device sharing were analyzed in order to codify the *strategies and assumptions* the service providers have made. Although this codifying is a qualitative process, as already noted, rigor was sought by an iterative coding procedure that required a consensus between two independently working researchers, who both coded the entire data set separately. If a new item (e.g. a strategy not identified in previously read documents) was encountered, the researchers agreed on a short definition and reprocessed each previously processed document for the item's presence. Upon a disagreement between

the two researchers in their coding, they were obliged to carry out a discussion in order to reach a conclusion. Ultimately, the result is a set of coded strategies and assumptions based on the independent evaluation of two researchers regarding the presence of each passage and term.

Qualitative content analysis is a methodology that inherently incorporates subjective elements. The validity and rigor of the analysis can be and were improved by the researchers committing to a rigorous and systematic process (Elo et al. 2014). To this end, a so-called inter-rater coding approach was used. This approach, in the domain of qualitative analysis, is generally a form of triangulation in which two or more researchers assess their qualitative categorizations against each other, discussing and negotiating a consensus in case of disagreements (Armstrong et al. 1997). The coding process necessarily has interpretation involved; the privacy policies and EULAs are written by different authors (companies) that might refer to different concepts in different contexts with the same terms, for instance. The interpretation is not an issue in the sense that the documents are meant to be understood by the reader to make clear what the conditions for software or service use are. To further justify the conformability of our interpretation, the coding researchers were from different backgrounds: software engineering and law. Despite these different points of view, through independent coding, a unified categorization was achieved. Only two researchers participated in the coding, so all potential conflicts were easily resolved; and the resulting Cohen's Kappa of 0.748 corroborates substantial agreement. The conformability of the results can be further evaluated from the replication package.

The task was to analyze what implications each passage and term in the sampled documents has for different ways of device sharing (e.g.empowering or hindering end users). The research team has expertize with the relevant data protection regulation, which can also be considered an input into the policy interpretation process. Furthermore, the goal is to analyze whether there are special provisions for sharing regarding vulnerable data subjects, or whether the strategies follow a so-called 'one-size-fits-all' principle. With the term 'vulnerable data subjects', we refer to the segments of the population requiring special protection, such as children, asylum seekers, or the elderly, and any case where there is an imbalance in the relationship between the parties (Article 29 Working Party 2017, 10). Furthermore, this article takes an interdisciplinary approach to assess the results of the policy analysis, combining software engineering with legal analysis. The doctrinal study of law approach was utilized in a supportive role in discussing the possible regulatory underpinnings of the identified strategies, particularly in Section 6 of this article.

For a synthesis of the disjoint policy results, we analyzed the different strategies with the intent to deduce common requirements as an abstract theory with a consistent conceptual model. Keeping in mind the assumption that many users would like to share devices for any kind of SPS they please, in diverse ways, regardless of provider intent, and assuming the identified strategies from the policy documents represent the way SPS providers would prefer their services to be used, we can make some mostly deductive observations. These can then be used as a framework for device sharing use cases in a theoretical SPS-environment, which would fulfill each device sharing policy and meet usability principles, that then could be tested against real-world implementations.

The analysis of the selected SPS policy documents yields a systematic map and a synthesis of the industry status. Without loss of relevant information, these were further categorized into themes.

3.2.2. Technology review

To provide some validation to RQ1 and to answer RQ2, the existence of implementations of the identified strategies was studied. It should be kept in mind that we do not propose that the entire conceptual model *ought* to be implemented as-is. Rather, we have observed these strategies as policies, and now we test for indications of the extent to which they are actually implemented.

The result of the policy analysis phase is a conceptual model of SPS provider requirements. The model is built from separate strategies of different organizations, yet it remains coherent. In this phase of the research, we then provide an indication of its external congruence with the consumer device platforms' capabilities.

The conceptual model was formulated into testable use cases with a design science step. The following design principles were used. First, the use case should implement the requirement from the conceptual model. Second, the system as a whole should follow the once-only principle of design (ask each piece of information only once from the user) (Krimmer et al. 2017). Third, the use case assumes any functionality is used in a device sharing context and should honor the users' rights to privacy and self-determination. The intention is to formulate test cases that would demonstrate if the platform in question follows the particular conceptual model aspect under question. Considering the validity of the use case definitions, it can be said that the use cases do not *follow* from the requirements, but we argue they are *derived* from them.

Following the setting, the next step in the study was testing which use cases each platform can support. We tested the use cases employing an *exploratory black-box* test method. Exploratory testing *(ET)* is a testing method where a test case is defined only by its beginning and goal states, with the execution path left for the tester to explore (Itkonen and Rautiainen 2005). Black box testing, furthermore, refers to the fact that we test the functionality of platforms and applications as they appear to their end users, without access to internal details such as the source code (Jacob and Prasanna 2016; Malkin, Wagner, and Egelman 2022). This approach has the advantage of revealing how the software functions from the perspective of the end user, but requires a larger effort in test definition and execution, and – more importantly – has the possibility of the tester missing an execution path and a functional aspect (Jacob and Prasanna 2016). ET is a widely used practice in software engineering, especially in defect finding (Di Martino et al. 2023). In ET, the test case design and execution are iterated to determine whether a system meets its requirements. This approach has the advantage of revealing interactions between components of a complex system, but lacks the formality and coverage of a fully scripted traditional test, and requires system knowledge from testers (Beer and Ramler 2008; Itkonen and Rautiainen 2005). For an ET test case to be feasible, it should not require 'proving a negative', and even positive functional testing (verifying a feature is present) assumes the system is deterministic (Dashti and Basin 2020) – which we deemed not an issue in this study, without very complex interactions under test.

Our particular test setup was as follows. We set up the tested devices to meet pre-conditions for each test: operating system ready, required accounts ready, installed applications ready (in tests where necessary), etc. Each test case was then solved by one of the authors (work split across authors 1, 4, 5, and 6), and the post-conditions were validated by the three other authors. The result was logged with values 0, 1, or 2 for *'does not meet use case'*, *'partly meets use case'*, and *'fully meets use case'*, respectively. The exploratory testing process does not follow a script, so rating principles were defined instead of hard rules: a rating of '2' fulfills the test case as expected and agreed by the researchers, and '1' fulfills it with a workaround or another technicality. We employed this three-value result instead of binary, to better indicate cases that require interpretation to fit the practicality into our conceptual model. In a strict reading, the results with '1' may be read as '0'. The inter-rater consensus method was again used to improve the quality of the interpretation.

The limitations of the study design are further elaborated in Section 5.4.

4. Results

4.1. Policy analysis

The main result of the qualitative content analysis is the 18 different strategies identified that SPS providers used to approach various issues related to device sharing. These fall within five themes identified: Access to service, Age gating, Credentials, Multiple users, and Denial. The strategies were further refined into a conceptual model of requirements.

Note that generally the identified codes are not exclusive to one another, except with definitions that imply such (e.g. *Id4-7*). The results are presented in Table 1. It should be emphasized that this is not an exhaustive list of strategies but a systematically observed set of them, as per the methodology. The codes are also not mandatory; other than that, a policy with no clauses would be coded 1 for *Id18* – for instance, a valid policy might entirely omit any age gating and would thus be coded 0 for all the codes in the theme. The conceptual model is presented as a unified package for analysis purposes. It does not follow that the sum of current industry approaches should be used as-is.

4.1.1. Access to service

Three codes were categorized under the theme *Access to service*. Over a third (37%) of the analyzed SPSs had a policy to require a *personal licence (Id1)* that is non-transferable in order to use a service. For a typical example, *Army Commander*'s EULA has this clause: *'Subject to your agreement and continuing compliance with these Terms, we grant you a non-exclusive, non-transferable, non-sublicensable, revocable limited license to access and use the Services for your own non-commercial entertainment purposes'*. These licensing clauses seek to have implications regarding software sharing, but their practical meaning in device sharing is unclear. In the strictest reading, any other shared device user (e.g. a person playing a game on a friend's mobile phone) should not be allowed to use the software or service. There are differences between the exact wordings in different agreements as well. In addition to licensing, and not exclusive to that, 24% of the observed SPS entirely and explicitly *forbid sharing (Id2)* the service with others. In contrast to the ban of sharing, some take the approach to allow sharing but explicitly

Table 1. Results of the policy document analysis.

Theme	Id	Code	Description	*n*
Access to SPS				
	1	Personal licence	Require a personal, non-transferable licence in order to use SPS.	28
	2	Forbid sharing	Explicitly forbid sharing of SPS with others.	18
	3	Owner is liable	Allow sharing of SPS, but explicitly pass liability to owner.	12
Age gating				
	4	Require legal maturity	Require anyone using SPS to be of legal age (or 18). [Not referring only to purchases or registering].	8
	5	Forbid use under 16	Forbid children under 16 years old from providing personal data to SPS.	6
	6	Forbid use under 13	Forbid children under 13 years old from providing personal data to SPS.	14
	7	Forbid use under local law age	Forbid children under users 'local age limit' from providing personal data to SPS.	8
	8	Not knowingly collect	Plead that the SPS does 'not knowingly collect data of children'.	10
	9	Parental consent mechanism	Mention an explicit mechanism for verifying parental consent.	7
	10	Parents' assistance	Allow a minor to use the SPS only with parents' assistance, or under other parental control mechanisms.	14
Credentials				
	11	Forbid login information sharing	Explicitly forbid sharing of login information (e.g. a password) to others.	39
	12	Confidentiality of credentials	Ask user to maintain confidentiality of login information.	10
	13	Unauthorized access responsibility	Require user to prevent unauthorized access to their account.	30
Multiple users				
	14	One account with profiles	Offer mechanism to create multiple profiles or users under a single service account. [Including kids' profiles etc.]	9
	15	Multiple linked accounts	Offer mechanisms to link distinct accounts together. [Into 'families' etc.], including one account having control over the others	11
	16	Representative person	Explicitly allow a person to act as an agent for another [natural] person.	7
	17	Shared device personal data	Explicitly consider how multiple persons using a single device affects other users [e.g. data visibility to others].	9
Denial				
	18	Ignore the topic	Entirely ignore the topic of device sharing in policy [for SPS that do process personal data].	4

state that the *owner remains liable (Id3)*. Clauses that entirely forbid or limit sharing can be simpler for the user to interpret than clauses concerning licensing. For instance, *'Tinder – Dating & Make friends'* has the clear wording of 'you agree that you will not: […] use another member's account, share an account with another member, or maintain more than one account'. These identified approaches are most likely aimed at managing sharing behavior types such as borrowing, mutual use, and, in some cases, potentially also broadcasting.

4.1.2. Age gating

The policies were found to contain multiple strategies related to the theme of *Age gating*. Different SPS had different age requirements for usage. Some (11%) *require legal maturity (Id4)* to use the SPS (not only to make purchases or to register). Others took the approach of forbidding children, 8% under 16 years old *(Id5)*, 19% under 13 years old *(Id6)*, from sending personal data to the service. Some SPS providers took a 'dynamic' approach and forbade children under the children's local age limit from sending personal data

(Id7). These had wording such as *'If you're based in the EEA, you may only use Pinterest if you are over the age at which you can provide consent to data processing under the laws of your country'*. In addition to the explicit age gates, 13% of SPSs state in their policy that they 'do not knowingly collect data of children' *(Id8)*. Regarding parental consent, only 9% had a policy term about an explicit parental consent verification mechanism *(Id9)*, although this result does not imply that such an implementation does not exist. Furthermore, 18% of the sample had a policy that minors should only use the service under the supervision of a parent or with other parental control mechanisms. The exact verification process was rarely explained in the policies. The identified strategies under age gating theme can relate to and aim to limit almost any sharing behavior type mentioned in Section 2, such as borrowing, mutual use, broadcasting, helping, and even accidental sharing. For example, a child borrows a parent's device to watch a YouTube video while the adult is logged in with an adult profile, versus the situation where a child uses YouTube Kids application with a profile controlled by the parent.

4.1.3. Credentials

The theme *Credentials* features strategies that the sample SPSs had taken to consider secrecy. The majority of policies (52%) explicitly forbid sharing login information (e.g. username and password) with others *(Id11)*, which clearly has implications for device sharing. Others (13% of the sample) had a less explicit policy that asks users to maintain the confidentiality of their login information *(Id12)*. It is not evident whether confidentiality includes sharing the information with chosen parties. A large percentage of the policy documents pass the responsibility of preventing unauthorized access to the user *(Id13)*, e.g. considering any action under the account to be performed by the owner. Here appears, it seems, a crux: the explicit clause (Id11) is clear to the agreeing parties. However, it is difficult (if not impossible) to fully codify all device sharing behaviors in this way. Thus, the implicit clause (Id12) seems to consider diverse needs better, despite its lack of clarity. Explicitly forbidding the user from sharing their login information with other users can, from the perspective of the SPS provider, help prevent unwanted behavior such as the person borrowing a friend's Netflix credentials instead of subscribing themselves.

4.1.4. Multiple users

The policy documents were found to feature different approaches to multiple persons sharing an SPS. These were categorized under the theme *Multiple users*. Two distinct strategies for multiple persons using the same service were identified. Firstly, support for *one account with multiple profiles (Id14)* was identified in 12% of the sample. Secondly, support for *multiple distinct accounts with mechanisms to link them together (Id15)* was identified in 15% of the sample. One case supported both of these approaches. These approaches seem to recognize mutual use as a sharing behavior type, possibly also as an alternative to borrowing or broadcasting, and seek to mold the users' behavior into a form that would be preferred by the SPS provider. Support for a person acting as an agent for another person, as their 'representative' *(Id16)*, was found in 9% of the sample. Explicit consideration for the data protection issues within the context of shared device use (e.g. how one user's data could become visible to others) was identified in 12% of the sample policies *(Id17)*. The identified strategy concerning representative persons *(Id16)*

is clearly related to acknowledging sharing behavior, such as helping (for example, a parent books a doctor's appointment for their child).

4.1.5. Denial

Finally, four out of the sample SPSs (5%) completely ignored the issues surrounding device sharing in their policy documents, despite processing personal data *(Id18)*. This approach was categorized as *Denial*.

4.1.6. Cross-section comparisons

To gain further insight into the makeup of the result, we cross-tabulated the identified policies by the respective categories of the samples. These are visualized in Figures 2–7. The number of categories is large, so the number of expected samples in each is small. Therefore, statistical analysis such as the chi-square test is not useful for the data as a whole (Howell 2011), and one should avoid making large leaps in logic based on the distributions. Some outliers do appear evident; for instance, games seem to be over-represented in forbidding password sharing (Id2) as well as in requiring users to fulfil the local consent age limits (Id7) and seeking exemption from children-specific data protection provisions by citing that they do not knowingly collect personal data of children (Id8). We interpret the especially strong rejection of password sharing in games as a sign that companies are guarding *fairness* in online play. For instance, in the EULA of *Pokemon GO*, the prohibition of account sharing is found under the section *Cheating*. This highlights the competing interests issue: that service providers have more reasons, beyond simply wanting more paying accounts, to limit how users use and share their services. This might also suggest why games also have less presence in the Multiple users theme, as indicated in Figure 6.

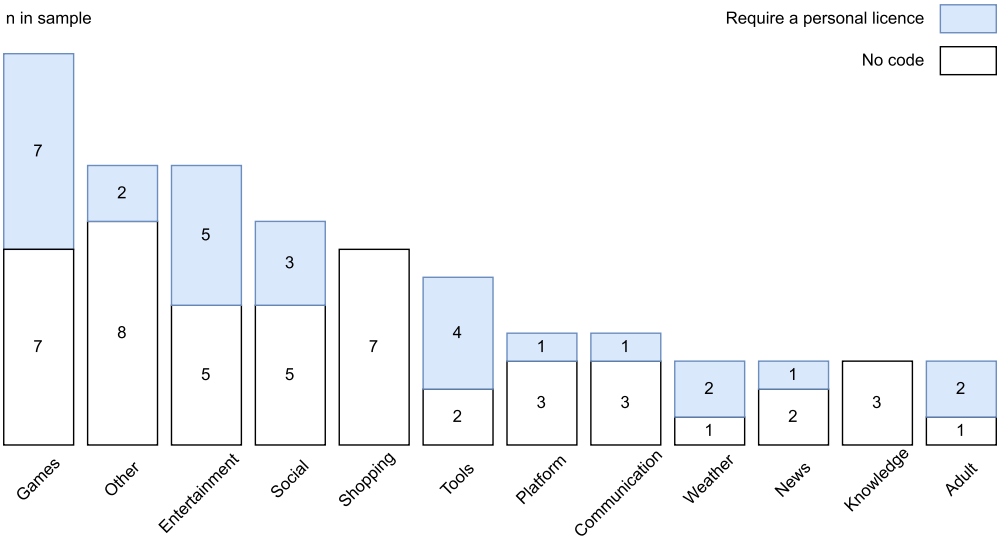

Figure 2. Occurrence of identified codes within the theme *Access to SPS* of codes Id1: Require a personal licence.

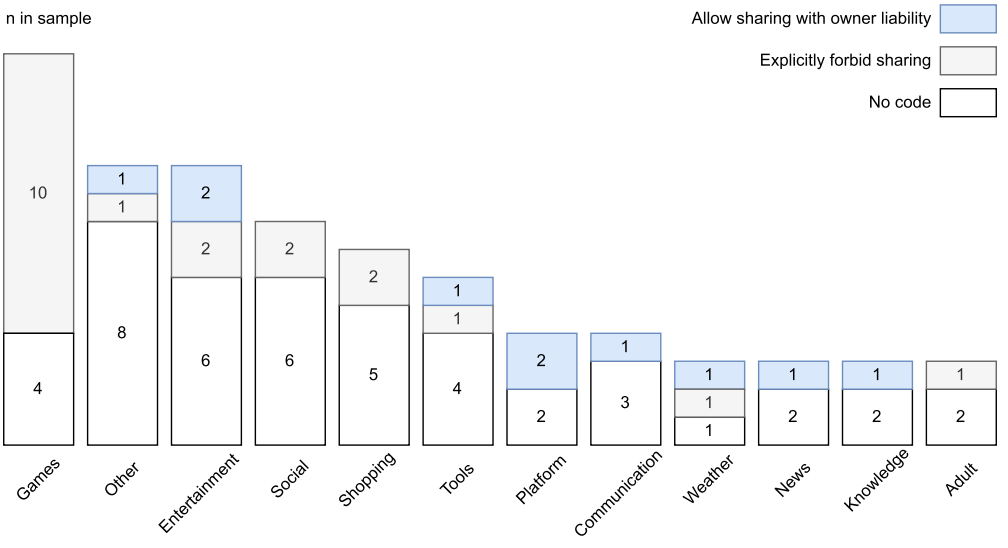

Figure 3. Occurrence of identified codes within the theme *Access to SPS* of codes Id2: Explicitly forbid sharing and Id3: Allow sharing with owner liability.

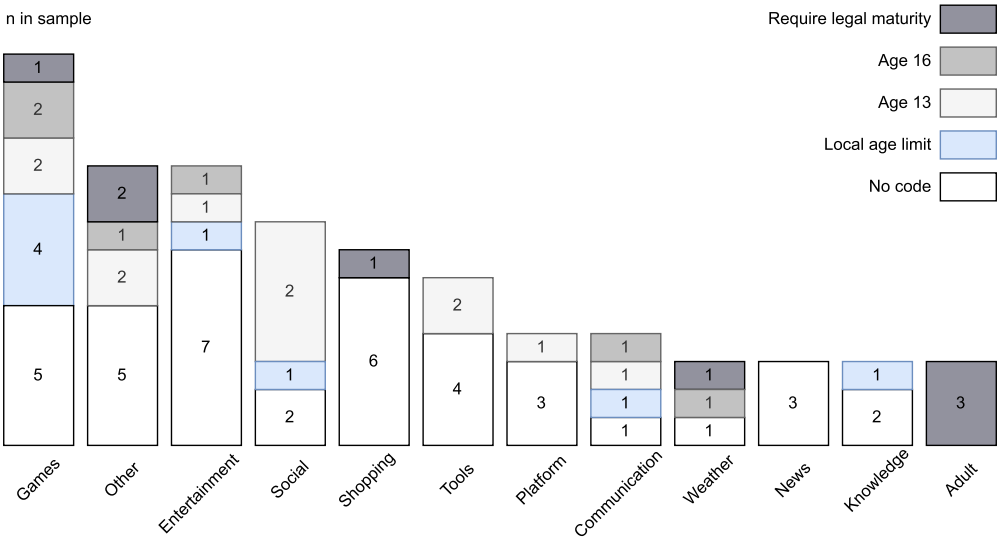

Figure 4. Occurrence of identified codes within the theme *Age gating*.

Explicit support for accounts with multiple profiles (Id14), or accounts linked together (Id15) appears often in the platforms and entertainment categories. This result is consistent with our intuitive expectations. On the other hand, social media and games tend to link accounts together into a network of friends, etc., but this was not evident in our results. Perhaps these types of relationships do not warrant an explicit mention in the agreement between the user and the SPS, in contrast to the tighter integration in other services?

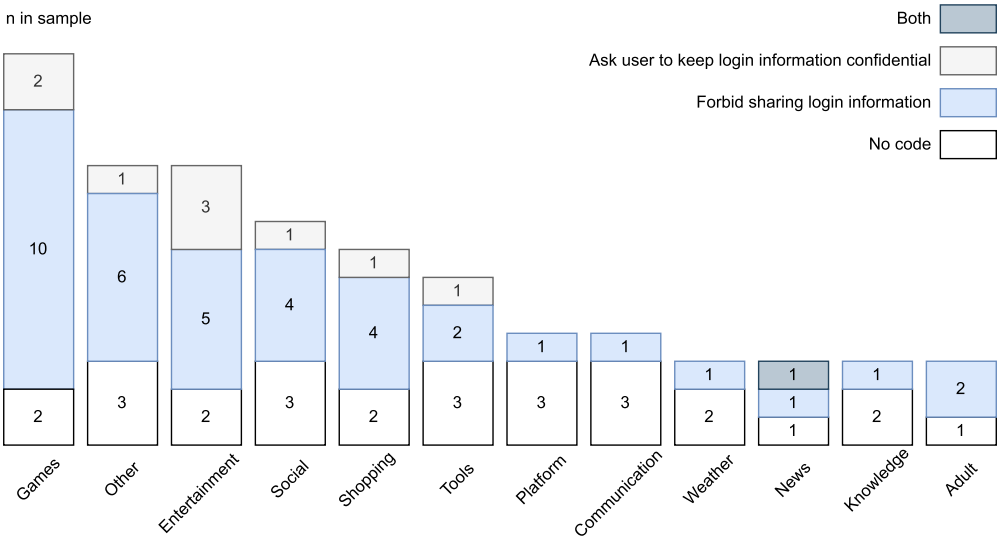

Figure 5. Occurrence of identified codes within the theme *Credentials* of codes Id11: Forbid login information sharing and Id12: Confidentiality of credentials.

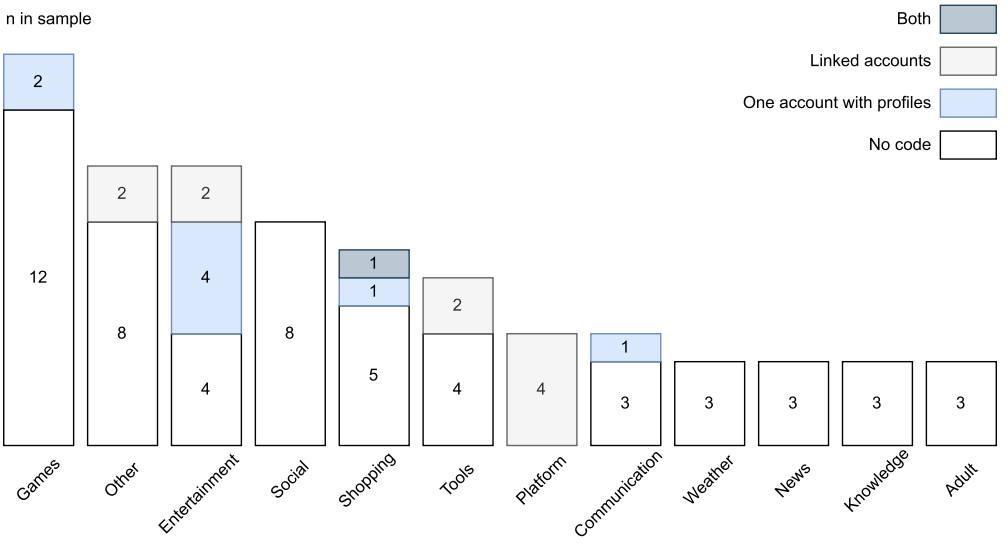

Figure 6. Occurrence of identified codes within the theme *Multiple users* of codes Id14: One account with profiles and Id15: Multiple linked accounts.

In addition, social media services seem to often follow the strategy of forbidding children under 13 years from providing personal data to the SPS (ID6). In general, age gating related strategies seem to be common, in addition to previously mentioned games and social, also in application categories of communication and adult.

Furthermore, explicit mentions of users having representative persons were scarce in the sample, with seven occurrences, though, for instance, both of the healthcare apps in the sample had those. Of course, not having explicit mentions in policy

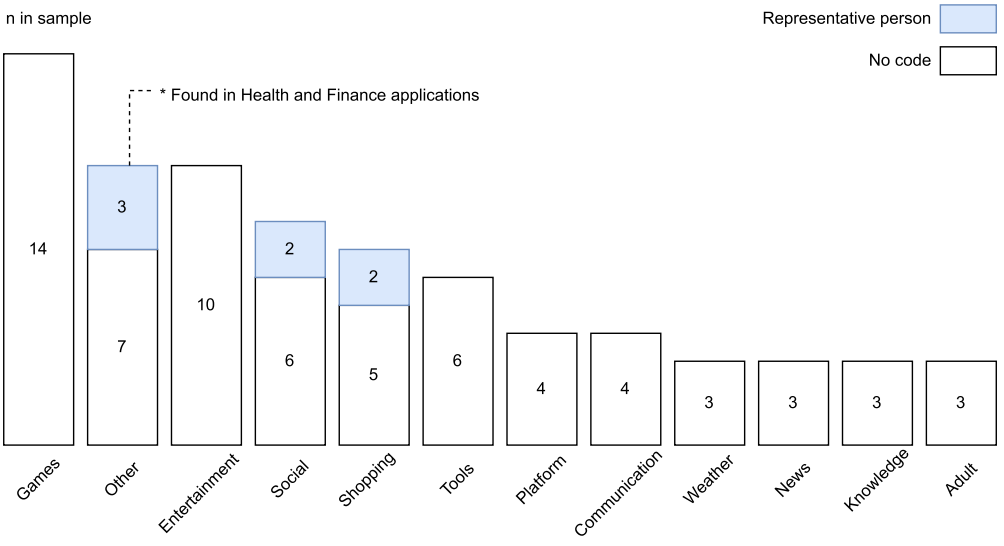

Figure 7. Occurrence of identified codes within the theme *Multiple users* of code Id16: Representative person.

does not mean the SPSs do not support representatives. Perhaps further support for the important sharing type for vulnerable persons is a development direction for the future.

Regarding the terminology in the findings, the point of view is the requirement analysis for an SPS provider. Consider an *SPS* to be a software product or service used by persons (users) sharing a *device*. In order to receive service, the provider might require an *account* for the users. The account represents the customer-ship of the users, purchases, and so on. One person is the *owner* of the account, regardless how it is used. The account is typically created when the user accepts the terms of using the SPS. Thus, the user should also have the legal capacity to enter into a binding contract. Minors under the required age limit can, for example, be allowed to have a shared account with their legal guardian or an account that is controlled by the guardian. EU data protection law defines the age limit for parental consent and special safeguards for processing personal data of minors, which are connected to the age of legal capacity, but separate from the contractual relationship (DE/HE, EDPBI:DEHE: OSS:D:2021:296 2021; Irish Supervisory Authority 2022b, 2022c).

In addition to an account, each person has a distinct *identity*, representing their personal information, whether it is modeled in the SPS or not. The SPS is installed or accessed from a device that connects to an account and is protected with *credentials* (e.g. passwords). The account houses all data related to users within the SPS. In order to personalize data for multiple users in an account, some services provide the possibility to create *profiles* for different users. It should be noted that the information discussed here is for establishing the business relationship between the users and the SPS provider, and it does not necessarily represent anything within the service (e.g. a user alias in a game).

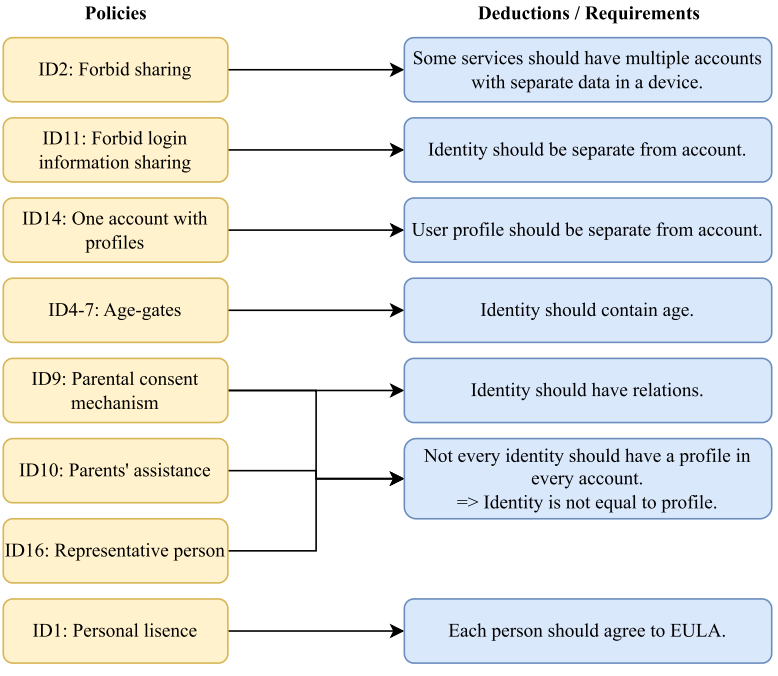

Figure 8. Summary of the requirements for a conceptual model analyzed from the policy strategies.

4.1.7. Conceptual model of requirements

The strategies in the policies were further refined into a conceptual model of requirements. These are presented in Figure 8. Firstly, from the requirement to be able to entirely forbid sharing (Id2) and considering many users would prefer to use an SPS on the same device, it follows that *some services should be able to have multiple accounts with separate data in a device*. The requirement to forbid login information sharing, combined with account sharing, implies that *identity should be modeled separately from the account*. It was identified that multiple services prefer to have personalized profiles for many users within one account (Id14), i.e. that *profiles should not equal to accounts*. The strategies related to various age-gates (Id4-7) indicate that identity should model user age. In the same vein, the requirements for verifiable parental consent and assistance, and representative persons imply the need for identities to have relations to each other. The same requirements imply that not every identity should have a profile in every account, i.e. identity is not equal to profile in the model. For instance, a child (identity) using a shared device should not have access (profiles) in a SPS that is for adults only.

Finally, the requirement for personal licences (granted on the condition of agreeing to the terms of the SPS) implies that EULA should be presented to each person using the service, not exclusively to the account.

The deductions made in the analysis, though non-exhaustive, appear to be non-contradictory to each other. It seems feasible, then, that a software platform could implement these principles as features.

Table 2. Use cases to test indications for content analysis implementations.

Basis	Conceptual model requirement	Id	Use case
Id11	Identity should be separate from account.	Uc1	As two or more users are sharing a device, each is able to login to the device with personal credentials.
		Uc1.1	Login (to different identities) should be possible immediately from 'lock-screen'.
		Uc1.2	In a device with biometric login, device should login to correct identity with zero user friction.
		Uc1.3	Device owner can specify which identities may login to device.
		Uc2	As a user, I can create an account to an SPS by using a single identity, i.e. that used on the device.
Id2	Some services should have multiple accounts with separate data in a device.	Uc3	As two or more users sharing a device, each is able to use a service that forbids sharing without interfering with other accounts.
		Uc3.1	Installing an application that forbids sharing does not install it for other identities on the device.
		Uc3.2	Service data is separate across accounts in the same device.
Id14	User profile should be separate from the account.	Uc4	In a device with two platform users (identities), it is possible to add a platform user as a profile to a service account without typing separate information (once-only principle).
		Uc4.1	Installing an application with profiles installs it for the other identities of those profiles on device.
		Uc4.2	Service data is able to persist across profiles.
		Uc4.3	Account owner specifies which identities may have profiles.
Id4-7	Identity should contain age [at least in bands of 13 to 16 to 18]	Uc5	As a user, I need to be able to indicate my age to service providers.
		Uc5.1	As a child, I should not be offered services I am not allowed to use in the platform 'app stores'.
		Uc5.2	As a user, I should not have to input my age for each service separately (asked consent for release only).
Id8,10,16	Identity should have relations.	Uc6	As a parent, I should be able to define my children's identities to be my children.
		Uc6.1	As a user, I should not have to input parent-child -relations for each service separately (asked consent for release only).
Id9,10,16	Not every identity should have a profile in every account.	Uc7	As a parent/representative person, I should be asked for verifiable consent for my children/dependant to use personal data processing applications.
		Uc7.1	As a parent, I should be able to manage my consents in a unified way.
Id1	Each user should agree to EULA.	Uc8	As a user of a shared device, I should be able to consider service related agreements and consents personally.
		Uc8.1	As a mobile app user, I should be able to read and agree to terms of use even if another person installed an application.
		Uc8.2	As a web browser user, I should be asked for cookie consent regardless of previous users' choices.

4.2. Technology testing

According to the study design, we formulated testable use cases that represent aspects of the strategies identified in the policy analysis. The set of use cases elicited is presented in Table 2. The use cases are split into main use cases, which specify a high-level concept, and detailed use cases to test specific user experience details. The resulting set features eight main use cases and fourteen detailed use cases, which gives an indication of how a specific requirement could be supported by a platform while following good privacy

design and minimizing users' inputting duplicate information to the system. The use cases should be interpreted as arbitrary, yet quantified, metrics that indicate whether a platform implements a particular strategy from the conceptual model.

These use cases identified (especially as a set) should not be interpreted as the globally optimal feature set, as a note on the validity of the results. Rather, they represent a collection of different, separate needs identified from SPS policies. User needs are very diverse, for instance, in terms of ways of sharing or the way they wish to represent themselves in a particular service.

The results concerning platform capabilities are summarized in Table 3. The results should be considered as indicative and do not merit too large conclusions about the operating systems' strategies. We can, however, advance some observations based on them.

First, there are clearly differences between the operating systems for the capabilities, even differences between two systems of the same company. Second, while no system

Table 3. Results of use case testing of operating system capabilities.

Id	Use case	Android	Windows	iOS	macOS
Uc1	As two or more users are sharing a device, each is able to login to the device with personal credentials.	●	●	○	●
Uc1.1	Login (to different identities) should be possible immediately from 'lock-screen'.	●	◒	○	●
Uc1.2	In a device with biometric login, device should login to correct identity with zero user friction.	◒	–	○	●
Uc1.3	Device owner can specify which identities may login to device.	●	●	○	●
Uc2	As a user, I can create an account to an SPS by using a single identity, i.e. that used on the device.	●	●	●	●
Uc3	As two or more users sharing a device, each is able to use a service that forbids sharing without interfering with other accounts.	●	●	○	●
Uc3.1	Installing an application that forbids sharing does not install it for other identities on the device.	●	●	○	◒
Uc3.2	Service data is separate across accounts in the same device.	●	●	○	●
Uc4	In a device with two platform users (identities), it is possible to add a platform user as a profile to a service account without typing separate information (once-only principle).	○	●	○	○
Uc4.1	Installing an application with profiles installs it for the other identities of those profiles on device.	○	○	○	●
Uc4.2	Service data is able to persist across profiles.	●	○	○	●
Uc4.3	Account owner specifies which identities may have profiles.	○	●	○	○
Uc5	As a user, I need to be able to indicate my age to service providers.	◒	●	●	●
Uc5.1	As a child, I should not be offered services I am not allowed to use in the platform 'app stores'.	◒	◒	○	○
Uc5.2	As a user, I should not have to input my age for each service separately (asked consent for release only).	◒	◒	◒	◒
Uc6	As a parent, I should be able to define my children's identities to be my children.	●	●	●	●
Uc6.1	As a user, I should not have to input parent-child -relations for each service separately (asked consent for release only).	◒	◒	◒	◒
Uc7	As a parent/representative person, I should be asked for verifiable consent for my children/dependant to use personal data processing applications.	●	○	●	●
Uc7.1	As a parent, I should be able to manage my consents in a unified way.	◒	◒	●	●
Uc8.1	As a mobile app user, I should be able to read and agree to terms of use even if another person installed an application.	●	●	○	●
		Chrome	Safari	Edge	Firefox
Uc8.2	As a web browser user, I should be asked for cookie consent regardless of previous users' choices.	●	●	●	●

Notes: A filled circle represents the platform fully supporting the use case, a half-filled circle partial support, and empty circle no support. The dash is a non-tested use case.

fully met all the use case criteria, *some* system did meet each at least partially. The areas with most 'weakness' across the whole sample were those considering children: age limits and parental consent *(Uc5.1, Uc5.2, Uc6.1)*. The platforms do provide some capability for these use cases, but their limitations lead to custom implementations by application providers.

As for the use cases that concern web browsers and applications, the results were as follows. Web browsers were found to meet the criteria proposed in most of the cases, in that they integrate platform login seamlessly *(Uc2)* and do support multiple users having separate local data *(Uc8.2)*.

Mobile applications, which – according to their policy documents – would be subject to each use case, were tested for the presence of custom implementations. The results of these tests are summarized in Table 4. Many of these use cases had a low sample size with applications that presented the need in policy, but the results can give some direction on where to investigate further. A large part of the sample had a full custom implementation for asking the age of the user *(Uc4.3)*. None of the applications tested had an actual verifiable mechanism for parental consent *(Uc7)*. This could indicate the boundary within the platform provider strategies – most of the platforms provide an integrated consent mechanism in the app stores, but do not provide the age of the user to the applications themselves, thus prompting custom implementations.

5. Discussion

5.1. On shared devices data protection issues

Some of the strategies we identified, such as age limitations for consent and the requirement of legal maturity, seek to limit the range of users and appear to have a clear link to the protection of children, as recognized under data protection and contract law, as well as intermediary liability regimes. The study found that SPS providers seem to respond to these regulatory requirements with different strategies, varying from fixed age limits to clauses requiring users to know the local age limits and to disclaimers that they do not knowingly collect children's data. Some of the identified strategies may contradict the transparency and fairness standards under EU law and children's rights. Overall, our results demonstrate room for improvement in addressing children as (co-)users of SPSs, both from a policy and technical perspective. Beyond children and other vulnerable data subjects, any shared use of devices and SPSs must strike a balance between implementing adequate privacy and data-protection safeguards and enabling efficient data sharing.

Table 4. Results of use case testing applications with custom implementations for profiles, age gating, and parental consent.

Use case	Applications tested	Full feature	Partial	None
4.3	8	3	2	3
5	33	19	10	4
6	4	0	1	3
7	4	0	1	3

Article 8 of the GDPR sets the age limit for parental consent required to offer information society services to a minor. The age limit set forth by the GDPR, and the similar age limitation requirements originating from other data protection laws, result in the emergence of strategies *(Id5)*, *(Id6)*, and *(Id7)*, concerning the age limits for providing personal data. For example, Article 8(1) of the GDPR sets forth an age limit of 16 years for processing personal data of a child when offering information society services such as social media services or communication services to a child. However, EU Member States are allowed to provide by law for a lower age as long as the said lower age is not below 13 years. The age limit of 13 years for parental consent is also used in the context of online privacy regulations in the US (Children's Online Privacy Protection Act 1998, 15 U.S.C. 6501–6505). The age limit of 13 was identified as the most common age limit among the studied SPSs. The results in Section 5.1 indicated that the age gating theme strategies were common in, inter alia, categories of social and communication, which would seem to be in harmony with the said legislative frameworks.

Considering the applications analyzed were offered in the EU, finding this much variance within the age limits is interesting. Nevertheless, the results appear to be in line with the previous research (Livingstone 2018), which has addressed the lack of harmonization of age limits across Europe. Varying age limits of different countries have also led to questionable solutions, as strategy *(Id7)* demonstrates. Clauses that require the user to know the age limit of the region without it being explicitly told to them are unlikely to be considered transparent or fair for the user, corroborating the wider challenge of appropriately informing children online (Milkaite and Lievens 2020; Morgan 2018). Overall, our results indicate a fixed approach to age limits rather than efficiently taking into consideration children's evolving capacities as required under the UN Convention on the Rights of Child. Buitelaar (2018); Vänskä et al. (2023).

We also identified a strategy *(Id8)* that explicitly states that 'we do not knowingly collect data of children'. This, as a strategy, seeks an exemption from the special obligations concerning, e.g. parental consent. This defensive strategy is understandable in light of previous work, such as Livingstone (2018); data protection for children has special cases and thus is more burdensome to comply. Its prevalence is surprising, though, and its effectiveness can be questioned as reports and research show that children can be users of SPSs regardless of age limits (Meyran et al. 2024; Nagata et al. 2025; Ofcom 2024). Whether the services market to children, even with this provision in place, is another issue.

The said age gating strategies typically were addressed in the privacy policy documents of the studied SPSs. Strategies *(Id9)* and *(Id10)*, concerning parental control methods, are also likely related to data protection and digital service law provisions, such as Article 8 of the GDPR and Article 35(1)(j) of the Digital Services Act (DSA).[3] Article 8 of the GDPR requires service providers to 'make reasonable efforts to verify [–] that consent is given or authorized by the holder of parental responsibility over the child, taking into consideration available technology'. Article 35(1)(j) of the DSA requires providers of very large online platforms and of very large online search engines to put in place 'reasonable, proportionate and effective mitigation measures' tailored to the specific identified risks, such as measures to protect the rights of the child, including age verification and parental control tools. These strategies require an involvement from the guardian of the minor in the use of SPSs, potentially leading to some level of

shared use. However, for these strategies mentioned in the policies to be efficient, they need to be paired with technical measures that ensure identification and control over minors' use of SPSs (European Commission 2025).

Our results showed that many applications requested the user's age (Uc4.3), but none of them had a verifiable mechanism for parental consent (Uc7). This could, in some cases, indicate a shortcoming with complying with Article 8 of the GDPR, but also with the principle of data protection by design, which requires efficiently implementing data protection principles, such as accountability, to products and services (Article 5(2) and 25 of the GDPR). Furthermore, depending on the domain and risk level, if parental controls have not been properly implemented, inter alia, DSA's provisions concerning protection of minors may have been compromised. As we collected the studied materials of this research prior to the effectiveness of the DSA, further research concerning the effects of the DSA's provisions on SPS policies and technical solutions is needed.

Our findings indicate that the defined use cases (Uc5.1, Uc5.2, Uc6.1) around children's age limits and parental consent had the most weaknesses when testing operating systems for capabilities, and this led to custom implementations by application providers. There seem to be some obstacles with the features for sharing information between the different SPSs, if striving for effortless data flow.

Sharing and using information indicating the age of the user can, for example, help to protect underage users from harmful content and, thus, can be regarded as a positive thing from the perspective of protecting users' privacy and safety. On the other hand, enabling third-party data transfers may compromise users' privacy and data protection. Thus, conducting proper data protection impact assessments under Article 35 of the GDPR is particularly important where the data flows involve children or other vulnerable data subjects (Article 29 Working Party 2017, 10). Furthermore, a special emphasis must be given to assuring that the possible consent collecting mechanisms and information notices effectively ensure the user's awareness of, inter alia, the shared data types, recipients of the data, and the purposes of sharing and enable users' data protection rights to be executed in all occasions and with regard to all parties involved in processing. Taking into consideration that the use of consents as a basis for processing personal data and the individual's capacity to decide for themselves in complex digital environments has been widely questioned, e.g. Koops (2014), Blume (2012), and Buitelaar (2012), this is not necessarily a simple task.

In addition to limiting strategies, some services addressed the sharing of devices extensively in their policy documents due to their business model, such as broadcasting services. In these services, it is typical that the service is used within the family, potentially also by child users. Thus, one family member can create an account under which other members can have their own designed profile and preferences *(Id14)*. These services typically also explicitly consider how multiple persons using a single device affect other users *(Id17)* and address this in their policy documents. SPS providers also have clear commercial interests to be able to profile different users accurately, i.e. to distinguish which data relates to each person to which aim providing separate profiles contributes. On the other hand, some SPSs required all users to create their own account, but provided methods for parents to control minors' usage of the SPSs *(Id15)*. This was typical for service providers like Google, which allow users to sign in to different services with the same account. Having a separate account for all users in cases where the account has single sign-on functionality furthers data security of users, but also allows efficient profiling of the users.

These findings give us a more concrete picture of the industry situation around multiple user solutions, and thus give further weight to research discussing sharing practices such as Murthy et al. (2021) or Berridge et al. (2022).

The current paradigm for device sharing appears to settle on using individual user accounts for each sharee. This must be a reasonable conclusion for some of the sharing use cases (elaborated in Section 2), such as mutual use, but it is not perfect. Is the SPS provider supposed to offer the GDPR controls, such as access to user data, to anyone who claims they used a shared device? Whose data is it, anyway? These are not trivial to define and it remains to be seen how, for instance, what kinds of solutions the privacy engineering community can provide. The shared device domain is not fully explored – though the industry ought to begin by just fulfilling the rights of a single user. Shared use has not typically been recognized as a factor that should be taken into consideration in developing industry best practices and guidelines in a broader sense, even if efficient implementation of GDPR's parental consent rules and special protection of children is recognized as important.

The device sharing 'issue' is not simple to solve, because the user needs are very diverse and even contradictory. As discussed (e.g. Levy and Schneier 2020), there is a real risk of facilitating abuse or other privacy threats in intimate relationships when designing device sharing features. Data leaks should be considered a threat even in a shared environment. For instance, in the example use cases presented in this work, we do not intend any data to share automatically, without direct user consent. Despite the risks, these features have real, positive uses that help vulnerable individuals, such as the elderly, cope with a digitizing world. It seems clear that software producers ought to consider different device sharing cases in their data protection impact assessments, even if those are not their primary intended audiences. Based on the policy analysis in the present work, the vast majority of SPS policies have some clauses that do affect device sharing, but this method cannot reveal whether they were considered as a whole in design, or just as incidental, separate items.

The GDPR sets forth obligations on the SPS providers concerning, for example, data security, risk-based approach, and the implementation of data protection by design and by default principles into their products and services (see e.g. Articles 25 and 32 of the GDPR). Thus, the foreseeable shared use of SPSs could be taken into consideration in the technical features and policies of their products and services as part of implementing these principles, furthering users' right to privacy and data protection. This is particularly important when co-users belong to a vulnerable group or are otherwise in a vulnerable position in the co-user relationship.

5.2. On platform and application providers

The gap between the strategies software providers employ in their policies and the capabilities of the platforms evidences a lack of alignment in the overall offerings. It remains to be seen whether that stems from the competing business interests, differing data protection goals, or something else altogether. Based on the technology review phase, however, at least some platforms did implement each tested use case in some capacity. This could indicate that the potential exists to align the user needs with technology wants. Nonetheless, unsurprisingly, none of the surveyed platforms fully met the tested use cases. Further

extrapolating from the results of our findings, we can identify pain points around specific device sharing use cases and offer some suggestions that could result in a win-win-win scenario for the platform providers, platform consumers, and end users alike. The discussion is within the context of the platform economy, where the incentives of the actors do not always align – thus, influence should come from mutual advantages or common regulation, or governance structures (Gorwa 2019).

The first point to discuss is the attitude and approach to device sharing in general. There are contrasts in how the different consumer platforms accept sharing. For instance, the Apple iOS does not support multiple users, but the desktop macOS does. The same comment applies to the software producers as well; a significant share outright forbids shared use in their EULAs, but this information is not exactly prominent in the interface. End users could benefit from these being more explicitly presented as options of the products, and the entire use case being more integrated, where allowed.

Let us review some of the specific results: A significant share of the policies forbid sharing passwords with any other person. The platforms surveyed do offer a single sign-on feature to use the platform account as an identity in an application, which is user-friendly, this does not extend to other users of the device. For instance, despite creating a 'family' in a Google profile, the model is not usable for the application; i.e. the user must maintain, for example, a separate family of profiles in the Disney Plus application. All of the surveyed platforms had a family feature in their platform accounts, but defining parental controls for children is not the entire picture of device sharing: consider, for example, elders who need assistance from their children, or other representative user groups.

Many of the shared device controls rely on operating system and app store features. Does this mean native mobile applications are in a better position compared to web applications? Further integrating the controls through the entire stack from platform to browser to web application is not an unreasonable task, either. Is there an alternative that does not rely on proprietary platform features within an open web ecosystem? This corroborates previous work, which argues that platform providers themselves are becoming de facto privacy regulators, and that this could be mitigated by clear disclosures from the platforms (van Hoboken and Ó Fathaigh 2021).

Apart from clearly data protection compliance-related strategies, sharing was addressed in connection with the licensing terms that required 'a personal, non-transferable license' *(Id1)* for using the SPS. The provisions of the EULAs and terms of service that seek to limit the transferability or sharing of the product or service typically have financial aims, from the legal perspective. Under copyright laws, end user licences aim to limit users' rights to protect the commercial interests of the copyright holders. This strategy can potentially have implications for the sharing behavior of users if they understand the limitation and take it seriously. It seems safe to claim that the current commonly found licence clause does not set the expectation clearly in layperson's terms, which is problematic from the perspective of fairness and transparency. Furthermore, prohibiting device sharing can have an unreasonable impact on such vulnerable groups, who, in practice, need support in using services or products. Overall, limiting how users share SPSs by forcing them to accept non-negotiable terms, which are neither transparent nor fair, and enforcing these terms through technical features, is one reflection of the power asymmetries present in modern digital environments, particularly between consumers and service providers, and between data subjects and controllers. These kinds of limitations may also

contradict users' (rightful) expectations relating to everyday use cases of SPSs, such as short-term borrowing or helping others.

Strategies *(Id11)*, *(Id12)*, and *(Id13)*, which concern a ban on sharing login information, request to maintain confidentiality of user credentials, and requirement for the user to prevent unauthorized access to their account, seem to relate to data security aspect of the services, and, thus, also to data protection law compliance. Nevertheless, at the same time they are likely to also contribute to the risk and liability management interests of the SPS providers. In case of unauthorized access causing harm to the user, the SPS providers could invoke the term requiring cautiousness from the user, and, thus, potentially limit their liability. Cautious use of credentials is also likely to reduce the costs associated with service requests related to unauthorized use. As argued in previous literature, simple access control schemes are unlikely to be effective in complex user sharing cases (Ahmed et al. 2019). Considering the advanced schemes available in the literature (e.g. Chen, Hengartner, and Khan 2022), this finding does show that many SPS providers rely merely on policies in password sharing, and thus raises a question: is the non-adoption by IT-managers a lack of willingness or knowledge? The responsibilities between platform providers and service providers on the platforms are not delineated well, as previous work has argued (Lambrecht, Verdoodt, and Bellon 2018) – our results corroborate this from the sharing feature perspective.

In the platform economy, providers have their commercial and liability-avoiding interests. Many of the identified strategies are likely connected to this – the strategies related to data security and strategies *(Id2)* and *(Id3)*. Particularly in strategy *(Id3)* the issue of liability was addressed in the sense that the liability of sharing was defined to remain with the owner of the account. In general, sharing of the product or service may cause some effects on the SPS provider, so they have an interest in trying to control the practice. Reflecting on Oh, Koh, and Raghunathan (2015), the right question might be: whose control, platform, or application? This question ties the present results to the discussion on *platform governance*. An increasingly large share of the digital economy is controlled by international platforms, and they operate in an ecosystem of various actors, including different governments, which both govern and are governed (Gorwa 2019). Unless the platforms create conditions for good governance, including respecting the rights and freedoms of the users across the entire platform, they risk being subjected to interventions from different directions. This should be an incentive for platform providers to facilitate application providers in implementing device sharing features, rather than blocking them.

5.3. Future directions

The parental control and age gating mechanisms displayed a pattern of keeping tight reins on the data in the surveyed platforms. One observation made was that custom consent verification mechanisms were uncommon. This can be recognized as a positive observation: application providers can rely on the platforms for this feature. On the other hand, applications frequently asked the age of the user in a separate form. This happens, presumably, because the platforms do not provide the information for applications even when they have it. Supposedly, the application providers do need this data (for instance, to comply with age-dependent data protection rules), and thus they must ask the user to enter the same information twice. It appears to be a low-hanging

fruit for platform providers to extend to. The mentioned specific features outline a pattern of ambiguity. The industry would do well for the users to clarify the responsibilities between platform and application providers in these use cases.

Beyond the evident commercial value of separating data of different users to the service providers, these strategies can also be addressed from the perspective of how they further or diminish users' right to privacy and data protection in the context of shared devices, particularly taking into consideration data protection by design and default principle under Article 25 of the GDPR. Thus, requiring individual accounts from all users may provide a more privacy-friendly option (at least between users) for shared devices users, requiring that all users follow this separation. On the other hand, for example, allowing the creation of a secret, limited-access, profile under a shared account could be a valuable option in cases where shared device users may not be able to decide freely and are aggressively monitored by the co-user (McKay and Miller 2021). The balance of empowerment and control should be addressed from the perspective of what kind of capabilities SPSs include in the context of shared use of devices, when considering the children's right to privacy. Ensuring children's right to privacy and data protection requires that the protective measures are implemented efficiently. These results emphasize the requirement of data-protection-by-design and might prompt both the industry and the regulators to elucidate what the principle entails in detailed use cases.

Many of the device sharing use cases feature a vulnerable person as a party. The results of the study indicate that children are given special consideration in SPS features, which is reasonable in terms of prevalence. The industry should not forget other vulnerable groups either, the elderly, for instance. It is not always the parent who needs the parental controls. Only seven of the sample policies displayed support for a generic representative person. Take another second to consider vulnerable users before writing *'A User may never allow anyone else to use a User's Account (except for Guardians in the case of a Minor User)'* (Roblox) in your terms of use. This clause would disqualify a Guardian of an elderly user, despite possibly not being the intention, since the situation is otherwise similar. According to previous work (Levy and Schneier 2020), vulnerable users face intimate threats, and immature sharing features might worsen the problem. Explicitly forbidding sharing strategies were present in 24% of the sample *(Id2)*. In the future, progressive digitization of products and services is likely to further increase the need for solutions supporting privacy-friendly representatives and shared use. It is possible that platform features that would make sharing more structured could entice the software providers to soften these stances.

There are also some points that we can raise about the agreements between users and SPS providers and the provided policies (EULAs, terms of use, and privacy policies). Firstly, the results of this study support the intuition that EULAs and other user agreements are very varied and complex. There are many different approaches companies take regarding just device sharing. It might be unreasonable for a user to remember in practice how each service agreement supports what; which of all applications are you allowed to even share at all, let alone details. These clauses are buried in agreements and policies, not visible in practice, and this might be something the platforms could provide visibility to (similar to app permissions, for instance). Secondly, consideration should be taken when crafting these agreement and policy texts. Evaluating the clauses from a device sharing perspective reveals, perhaps, how an explicit term might be clear, but too rigid for diverse use cases of the users. An implicit term (e.g. 'the user must keep their account secure'

rather than 'the user must not share their password') on the other hand, allows for leeway in the usage, even beyond what the provider imagines.

The frictions identified in this research are not necessarily critical errors in usability or data protection; rather, we present ways to further align industry actors while also considering user needs for sharing and privacy. Device sharing is a developing area for the ecosystem as a whole. Should the industry not reach a satisfactory state for the rights of the consumers, the regulators might intervene. In light of our results, these suggestions could be considered in public policy:

(1) Forbid terms of service that rule out sharing a service in its entirety, as these may exclude vulnerable users and contradict with users' rights as consumers and data subjects.
(2) Facilitate adoption for representative person use cases and explicit parental consent mechanisms, for instance, with features in identity solutions or as requirements for gatekeeping platforms.
(3) Elucidate the extent and implementation of the data protection by design principle with regard to device sharing use cases, for example, by providing new or updating existing guidelines.

5.4. Limitations

Firstly, let us acknowledge that this study is an exploratory review of an emerging topic of interest. It is subject to various limitations, which ought to be considered when making inferences based on the results. The essence of this study was to create an initial conceptual model from verifiable software policy into practice. This should not be read as a global optimum; rather, it is a one-pass analysis – the next natural step would be to revisit policy after critical examination of the results, and then again matching to practice, in iterative improvement. The study consists of several dependent phases, with a mix of empirical and constructive research – and thus the different results have different reliability. Several steps rely on abductive reasoning and design, which can introduce bias and a loss of generality. Overall, the qualitative methodology with thematic analysis and design science carries the risk of lower external validity, and the result is not trivial to verify. We have mitigated these issues, as per the methodology, by synthesizing the work of independent authors and publishing a replication package.

The data collection strategy limits the results to the EU industry. For a clearer and more representative picture of the industry, further research might use a larger and more global sample. The framing and regulatory context of this paper is EU law, and a global legal comparison is not within the scope – though it would be useful. The policy content analysis and use case formulation rely on qualitative judgement, both of which should be read with a critical perspective. Furthermore, we do not claim that the conceptual model of device sharing strategies identified in the policy analysis is optimal, only that it is present in the current documents and appears internally non-contradictory. The technology review phase carries the risk of mistakes inherent in the exploratory testing methodology, and is limited to a small sample of available operating system and hardware configurations. The use cases tested do not map exactly to the conceptual model, but we argue they serve as indicators. Among the more confident results, there are those with less confidence in them, marked as 'partly meets use case', which could be

disambiguated with future work and a further developed conceptual model. This part of the study should be considered supplementary to the more reliable policy analysis, and the results should be more of an indication of the situational industry picture.

6. Conclusion

This paper examined the state of device sharing capabilities from policies to implementation, in the context of EU data protection regulation, and vulnerability and power imbalances. The topic was approached via two research questions: creating a systematic map of device sharing strategies from software terms of use and privacy policies (RQ1), and surveying platform capabilities and application implementations to support device sharing use cases (RQ2). The results provide a preliminary overview and systematization of the landscape and highlight areas with a lack of alignment between industry actors.

For RQ1, we identified 18 repeatedly used approaches in policies to manage different aspects of device sharing. For RQ2, we explored the differences between the operating systems, and the interface between platforms and applications. The identified strategies range from entirely forbidding sharing in terms of use, to explicit support with various mechanisms; there are no standards, but repeating themes were identified. To gain exploratory insight into the user experience in practice in RQ2, the policy level analysis was used as an input to design for testable use cases, which were then performed with consumer devices. The result is an overview of the support for device sharing in practice. Each of the tested use cases was found to be supported in some platform, but few were supported in each type. A common issue identified industry-wide was in age gating features, which result in friction in many device sharing scenarios.

We discussed the implications of the results from three perspectives. Firstly, on shared devices data protection issues, the policy analysis identified many strategies with clear links to compliance. Children and consent, for instance, which had various approaches but also limitations and conflicts. Secondly, the ecosystem of platforms and applications was identified as misaligned to some extent from the end-user perspective: it can be argued that the providers both strive against each other for control, but also intentionally limit sharing features for users as a business decision. With features deprioritized, vulnerable users' rights are at risk.

Future work on the topic could (e.g.) extend the analysis beyond the policies offered to EU citizens as, as noted, the device sharing practice is especially prevalent in the Global South. Further insight is available in comparative legal analysis across other jurisdictions, within this theme. The exploratory testing could well be further developed with other perspectives and integration.

Notes

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EU (General Data Protection Regulation). Official Journal of the European Union, L 119, 4 May 2016.
2. https://similarweb.com
3. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). Official Journal of the European Union, L 277, 27.10.2022.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This paper was partially funded by the Strategic Research Council at the Academy of Finland (grant number 327391).

ORCID

Kalle Hjerppe http://orcid.org/0000-0002-3737-4669

Data availability statement

A replication package for the study including the data is available online at https://github.com/kallehjerppe/replication-package-shared-devices.

References

Abdi, Noura, Kopo M. Ramokapane, and Jose M. Such. 2019. "More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants." In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security, SOUPS'19*, 451–466, USA: USENIX Association.

Ahmed, Syed Ishtiaque, Md. Romael Haque, Irtaza Haider, Jay Chen, and Nicola Dell. 2019. "'Everyone Has Some Personal Stuff': Designing to Support Digital Privacy with Shared Mobile Phone Use in Bangladesh." In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, CHI '19*, 1–13. New York, NY, USA: Association for Computing Machinery.

Alam, Aniqa, Heather Molyneaux, and Elizabeth Stobert. 2021. "Authentication Management of Home IoT Devices." In *International Conference on Human-Computer Interaction*, 3–21. Cham: Springer, Springer International Publishing.

Armstrong, David, Ann Gosling, John Weinman, and Theresa Marteau. 1997. "The Place of Inter-rater Reliability in Qualitative Research: An Empirical Study." *Sociology* 31 (3): 597–606. https://doi.org/10.1177/0038038597031003015.

Article 29 Working Party. 2013. "Opinion 02/2013 on Apps on Smart Devices." Adopted on 27 February 2013.

Article 29 Working Party. 2017. "Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is 'Likely to Result in a High Risk' for the Purposes of Regulation 2016/679." Adopted on 4 April 2017.

Assarroudi, Abdolghader, Fatemeh Heshmati Nabavi, Mohammad Reza Armat, Abbas Ebadi, and Mojtaba Vaismoradi. 2018. "Directed Qualitative Content Analysis: The Description and Elaboration of Its Underpinning Methods and Data Analysis Process." *Journal of Research in Nursing* 23 (1): 42–55. https://doi.org/10.1177/1744987117741667.

Bateni, Nastaran, Jasmin Kaur, Rozita Dara, and Fei Song. 2022. "Content Analysis of Privacy Policies before and after GDPR." In *2022 19th Annual International Conference on Privacy, Security & Trust (PST)*, 1–9. Los Alamitos, CA, USA: IEEE Computer Society, IEEE Computer Society.

Beer, Armin, and Rudolf Ramler. 2008. "The Role of Experience in Software Testing Practice." In *2008 34th Euromicro Conference Software Engineering and Advanced Applications*, 258–265. Los Alamitos, CA, USA: IEEE, IEEE Computer Society.

Bernd, Julia, Ruba Abu-Salma, Junghyun Choy, and Alisa Frik. 2022. "Balancing Power Dynamics in Smart Homes: Nannies' Perspectives on How Cameras Reflect and Affect Relationships." In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, 687–706. Boston, MA, USA: USENIX Association.

Berridge, Clara, Yuanjin Zhou, Amanda Lazar, Anupreet Porwal, Nora Mattek, Sarah Gothard, and Jeffrey Kaye. 2022. "Control Matters in Elder Care Technology: Evidence and Direction for Designing It in." In *Proceedings of the 2022 ACM Designing Interactive Systems Conference, DIS '22*, 1831–1848. New York, NY, USA: Association for Computing Machinery.

Blume, Peter. 2012. "The Inherent Contradictions in Data Protection Law." *International Data Privacy Law* 2 (1): 26–34. https://doi.org/10.1093/idpl/ipr020.

Brush, A. J. Bernheim, and Kori M Inkpen. 2007. "Yours, Mine and Ours? Sharing and Use of Technology in Domestic Environments." In *UbiComp 2007: Ubiquitous Computing: 9th International Conference, UbiComp 2007, Innsbruck, Austria, September 16-19, 2007. Proceedings 9*, 109–126. Berlin, Heidelberg: Springer, Springer Berlin Heidelberg.

Buitelaar, J. C. 2012. "Privacy: Back to the Roots." *German Law Journal* 13 (3): 171–202. https://doi.org/10.1017/S2071832200020460.

Buitelaar, J. C. 2018. "Child's Best Interest and Informational Self-Determination: What the GDPR Can Learn from Children's Rights." *International Data Privacy Law* 8 (4): 293–308. https://doi.org/10.1093/idpl/ipy006.

Carlsson, Robin, Sampsa Rauti, Samuli Laato, Timi Heino, and Ville Leppänen. 2023. "Privacy in Popular Children's Mobile Applications: A Network Traffic Analysis." In *2023 46th MIPRO ICT and Electronics Convention (MIPRO)*, 1213–1218. New York, USA: IEEE.

Chen, Jiayi, Urs Hengartner, and Hassan Khan. 2022. "Sharing without Scaring: Enabling Smartphones to Become Aware of Temporary Sharing." In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, 671–685. USA: USENIX Association.

Corbett, Susan. 2019. "Computer Game Licences: The EULA and Its Discontents." *Computer Law & Security Review* 35 (4): 453–461. https://doi.org/10.1016/j.clsr.2019.03.007.

Dashti, Mohammad Torabi, and David Basin. 2020. "A Theory of Black-Box Tests." arXiv preprint arXiv:2006.10387.

DE/BB, EDPBI:DEBB:OSS:D:2019:53. 2019. "Final Decision of 2 October 2019." Accessed 01 June 2023. https://edpb.europa.eu/sites/default/files/article-60-final-decisions/publishable_de_brandenburg_2019-10_right_of_access_decisionpublic.pdf.

DE/HE, EDPBI:DEHE: OSS:D:2021:296. 2021. "Final Decision of 19 November 2021." Accessed 01 June 2023. https://edpb.europa.eu/system/files/2022-02/de_-_he_2021-11_right_to_rectification_decisionpublic.pdf.

Di Martino, Sergio, Anna Rita Fasolino, Luigi Libero Lucio Starace, and Porfirio Tramontana. 2023. "GUI Testing of Android Applications: Investigating the Impact of the Number of Testers on Different Exploratory Testing Strategies." *Journal of Software: Evolution and Process* 36 (7): e2640.

Egelman, Serge, A. J. Bernheim Brush, and Kori M. Inkpen. 2008. "Family Accounts: A New Paradigm for User Accounts within the Home Environment." In *Proceedings of the 2008 ACM Conference on Computer Supported Cooperative Work*, 669–678. New York, NY, USA: Association for Computing Machinery.

Elo, Satu, Maria Kääriäinen, Outi Kanste, Tarja Pölkki, Kati Utriainen, and Helvi Kyngäs. 2014. "Qualitative Content Analysis: A Focus on Trustworthiness." *SAGE Open* 4 (1): 1–10. https://doi.org/10.1177/2158244014522633.

Eun Song, Ji, Jaeyoun You, and Joongseek Lee. 2021. "'I Might Be Using His… but It Is Also Mine!': Ownership and Control in Accounts Designed for Sharing." In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, CHI '21*, New York, NY, USA: Association for Computing Machinery.

European Commission. 2025. "Communication to the Commission: Approval of the Content on a Draft Communication from the Commission – Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online, Pursuant to Article 28(4) of Regulation (EU) 2022/2065, 14.7.2025.".

Freed, Diana, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. ""A Stalker's Paradise" How Intimate Partner Abusers Exploit Technology." In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–13. New York, NY, USA: Association for Computing Machinery.

Gorwa, Robert. 2019. "What Is Platform Governance?" *Information, Communication & Society* 22 (6): 854–871. https://doi.org/10.1080/1369118X.2019.1573914.

He, Weijia, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. 2018. "Rethinking Access Control and Authentication for the Home Internet of Things (IoT)." In *USENIX Security Symposium*, 255–272. USA: USENIX Association.

Hein, Andreas, Maximilian Schreieck, Tobias Riasanow, David Soto Setzke, Manuel Wiesche, Markus Böhm, and Helmut Krcmar. 2020. "Digital Platform Ecosystems." *Electronic Markets* 30:87–98. https://doi.org/10.1007/s12525-019-00377-4.

Heino, Timi, Robin Carlsson, Sampsa Rauti, and Ville Leppänen. 2022. "Assessing Discrepancies between Network Traffic and Privacy Policies of Public Sector Web Services." In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 1–6. New York, NY, USA: Association for Computing Machinery.

Helberger, N., M. Sax, J. Strycharz, and H.-W. Micklitz. 2022. "Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability." *Journal of Consumer Policy*45:275–200. https://doi.org/10.1007/s10603-021-09500-5.

Hjerppe, Kalle, Jukka Ruohonen, and Ville Leppänen. 2022. "Extracting LPL Privacy Policy Purposes from Annotated Web Service Source Code." *Software and Systems Modeling* 22 (1): 1–19.

Howell, David C. 2011. "Chi-Square Test: Analysis of Contingency Tables." In *International Encyclopedia of Statistical Science*, 250–252. Berlin, Heidelberg: Springer Berlin Heidelberg.

Hsieh, Hsiu-Fang, and Sarah E. Shannon. 2005. "Three Approaches to Qualitative Content Analysis." *Qualitative Health Research* 15 (9): 1277–1288. https://doi.org/10.1177/1049732305276687.

Huang, Yue, Borke Obada-Obieh, and Konstantin (Kosta) Beznosov. 2020. "Amazon Vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks." In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, CHI '20*, 1–13. New York, NY, USA: Association for Computing Machinery.

Irish Supervisory Authority. 2022a. "Final Decision of 2 September 2022 (Meta)." Accessed 01 June 2023. https://edpb.europa.eu/system/files/2022-09/in-20-7-4_final_decision_-_redacted.pdf.

Irish Supervisory Authority. 2022b. "Final Decision of 31 December 2022 (Facebook)." Accessed 01 June 2023. https://www.dataprotection.ie/sites/default/files/uploads/2023-04/Meta%20FINAL%20DECISION%20%28ADOPTED%29%2031-12-22%20-%20IN-18-5-5%20%28Redacted%29%.pdf.

Irish Supervisory Authority. 2022c. "Final Decision of 31 December 2022 (Instagram)." Accessed 01 June 2023. https://www.dataprotection.ie/sites/default/files/uploads/2023-04/Meta%20FINAL%20Decision%20%28ADOPTED%29%20-%20IN-18-5-7%20-%2031-12-22%20%28Redacted%29.pdf.

Italian Supervisory Authority. 2021. "Decision of 22 January 2021 (Tiktok)." Accessed 01 June 2023. https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9524194.

Itkonen, Juha, and Kristian Rautiainen. 2005. "Exploratory Testing: A Multiple Case Study." In *2005 International Symposium on Empirical Software Engineering, 2005*, 10–pp. Los Alamitos, CA, USA: IEEE, IEEE Computer Society.

Jacob, Pramod Mathew, and M. Prasanna. 2016. "A Comparative Analysis on Black Box Testing Strategies." 2016 International Conference on Information Science (ICIS), Cherthala, India.

Jasmontaite, Lina, and Paul De Hert. 2015. "The EU, Children under 13 Years, and Parental Consent: A Human Rights Analysis of a New, Age-Based Bright-Line for the Protection of Children on the Internet." *International Data Privacy Law* 5 (1): 20–33. https://doi.org/10.1093/idpl/ipu029.

Jasmontaite, Lina, Irene Kamara, Gabriela Zanfir-Fortuna, and Stefano Leucci. 2018. "Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR." *European Data Protection Law Review* 4 (2): 168–189. https://doi.org/10.21552/edpl/2018/2/7.

Karlson, Amy K, A. J. Bernheim Brush, and Stuart Schechter. 2009. "Can I Borrow Your Phone? Understanding Concerns When Sharing Mobile Phones." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1647–1650. New York, NY, USA: Association for Computing Machinery.

Karnatak, Nimisha, Brooke Loughrin, Tiffany Amy Kuo, Odeline Mateu-Silvernail, Indrani Medhi Thies, William Thies, and Mohit Jain. 2023. "'Is It Even Giving the Correct Reading or Not?': How Trust and Relationships Mediate Blood Pressure Management in India." *ACM Transactions on Computer-Human Interaction* 30 (6): 335–361. https://doi.org/10.1145/3609327.

Knowles, Bran, and Stacey Conchie. 2023. "Un-paradoxing Privacy: Considering Hopeful Trust." *ACM Transactions on Computer-Human Interaction* 30 (6): 235–258. https://doi.org/10.1145/3609329.

Koops, Bert-Jaap. 2014. "The Trouble with the European Data Protection Law." *International Data Privacy Law* 4 (4): 250–252. https://doi.org/10.1093/idpl/ipu023.

Kraemer, Martin J., George Chalhoub, Helena Webb, and Ivan Flechais. 2023. "'It Becomes More of an Abstract Idea, This Privacy'–Informing the Design for Communal Privacy Experiences in Smart Homes." *International Journal of Human-Computer Studies* 180:103138. https://doi.org/10.1016/j.ijhcs.2023.103138.

Kretschmer, Michael, Jan Pennekamp, and Klaus Wehrle. 2021. "Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web." *ACM Transactions on the Web (TWEB)* 15 (4): 1–42. https://doi.org/10.1145/3466722.

Krimmer, Robert, Tarmo Kalvet, Maarja Toots, Aleksandrs Cepilovs, and Efthimios Tambouris. 2017. "Exploring and Demonstrating the Once-Only Principle: A European Perspective." In *Proceedings of the 18th Annual International Conference on Digital Government Research, Dg.o '17*, 546–551. New York, NY, USA: Association for Computing Machinery.

Lambrecht, Ingrid, Valerie Verdoodt, and Jasper Bellon. 2018. "Platforms and Commercial Communications Aimed at Children: A Playground under Legislative Reform?" *International Review of Law, Computers & Technology* 32 (1): 58–79. https://doi.org/10.1080/13600869.2018.1443378.

Latulipe, Celine, Ronnie Dsouza, and Murray Cumbers. 2022. "Unofficial Proxies: How Close Others Help Older Adults with Banking." In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, CHI '22*, New York, NY, USA: Association for Computing Machinery.

Lemmer, Sophie-Charlotte. 2019. "Alexa, Are You Friends with My Kid? Smart Speakers and Children's Privacy under the GDPR." *Smart Speakers and Children's Privacy under the GDPR (September 2, 2019). King's College London Law School Graduate Student Research Paper* 20189-6: 1–56.

Levy, Karen, and Bruce Schneier. 2020. "Privacy Threats in Intimate Relationships." *Journal of Cybersecurity* 6 (1): 1–13. https://doi.org/10.1093/cybsec/tyaa006.

Lima, Thaiana, Rodrigo Pereira dos Santos, Jonice Oliveira, and Cláudia Werner. 2016. "The Importance of Socio-Technical Resources for Software Ecosystems Management." *Journal of Innovation in Digital Ecosystems* 3 (2): 98–113. https://doi.org/10.1016/j.jides.2016.10.006.

Liu, Michelle. 2024. "Digital Vulnerability: Rethinking Power Imbalances in the Digital Age." *European Review of Private Law* 32 (5): 827–848. https://doi.org/10.54648/ERPL2024043.

Livingstone, Sonia. 2018. "Children: A Special Case for Privacy?" *Intermedia* 46 (2): 18–23.

Malgieri, Gianclaudio. 2023. *Vulnerability and Data Protection Law*. Oxford, UK: Oxford University Press.

Malgieri, Gianclaudio, and Jędrzej Niklas. 2020. "Vulnerable Data Subjects." *Computer Law & Security Review* 37 (105415): 1–16.

Malkin, Nathan, David Wagner, and Serge Egelman. 2022. "Can Humans Detect Malicious Always-Listening Assistants? A Framework for Crowdsourcing Test Drives." *Proceedings of the ACM on Human Computer Interaction* 6 (CSCW2): 1–28, Article No.: 500. https://doi.org/10.1145/3555613.

Matthews, Tara, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. 2016. "'She'll Just Grab Any Device That's Closer' A Study of Everyday Device & Account Sharing in Households." In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 5921–5932. New York, NY, USA: Association for Computing Machinery.

Mazurek, Michelle L, J. P. Arsenault, Joanna Bresee, Nitin Gupta, Iulia Ion, Christina Johns, Daniel Lee, et al. 2010. "Access Control for Home Data Sharing: Attitudes, Needs and Practices." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 645–654. New York, NY, USA: Association for Computing Machinery.

McKay, Dana, and Charlynn Miller. 2021. "Standing in the Way of Control: A Call to Action to Prevent Abuse through Better Design of Smart Technologies." In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–14. New York, NY, USA: Association for Computing Machinery.

Meng, Nicole, Dilara Keküllüoğlu, and Kami Vaniea. 2021. "Owning and Sharing: Privacy Perceptions of Smart Speaker Users." *Proceedings of the ACM on Human Computer Interaction* 5 (CSCW1): 1–29, Article No.: 45. https://doi.org/10.1145/3449119.

Meyran, Boniel-Nissim, Marino Claudia, Galeotti Tommaso, Blinka Lukas, Ozoliīa Kristīne, Craig Wendy, Lahti Henri, et al. 2024. "A Focus on Adolescent Social Media Use and Gaming in

Europe, Central Asia and Canada." *Health Behavior in School-Aged Children International Report from the 2021/2022 Survey*.

Milkaite, Ingrida, and Eva Lievens. 2020. "Child-Friendly Transparency of Data Processing in the EU: from Legal Requirements to Platform Policies." *Journal of Children and Media* 14 (1): 5–21. https://doi.org/10.1080/17482798.2019.1701055.

Moh, P., P. Datta, N. Warford, A. Bates, N. Malkin, and M. L. Mazurek. 2023, May. "Characterizing Everyday Misuse of Smart Home Devices." In *2023 IEEE Symposium on Security and Privacy (SP)*2835–2849. Los Alamitos, CA, USA: IEEE Computer Society.

Morgan, A. 2018. "The Transparency Challenge: Making Children Aware of Their Data Protection Rights and the Risks Online." *Communications Law* 23 (1): 44–47.

Murthy, Savanthi, Karthik S. Bhat, Sauvik Das, and Neha Kumar. 2021. "Individually Vulnerable, Collectively Safe: The Security and Privacy Practices of Households with Older Adults." *Proceedings of the ACM on Human Computer Interaction* 5 (CSCW1): 1–24, Article No.: 138. https://doi.org/10.1145/3449212.

Nagata, Jason M., Zain Memon, Jonanne Talebloo, Karen Li, Patrick Low, Iris Y. Shao, Kyle T. Ganson, et al. 2025. "Prevalence and Patterns of Social Media Use in Early Adolescents." *Academic Pediatrics* 25 (4): 102784. https://doi.org/10.1016/j.acap.2025.102784.

Naveed, Sheza, Hamza Naveed, Mobin Javed, and Maryam Mustafa. 2022. "'Ask This from the Person Who Has Private Stuff': Privacy Perceptions, Behaviours and Beliefs beyond W.E.I.R.D." In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, CHI '22*, New York, NY, USA: Association for Computing Machinery.

Ni, Xudong, Zhimin Yang, Xiaole Bai, Adam C. Champion, and Dong Xuan. 2009. "DiffUser: Differentiated User Access Control on Smartphones." In *2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems*, 1012–1017. Los Alamitos, CA, USA: IEEE, IEEE.

Nissenbaum, Helen. 2004. "Privacy as Contextual Integrity." *Washington Law Review* 79: 119–158.

Nissenbaum, Helen. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

Obada-Obieh, Borke, Yue Huang, and Konstantin Beznosov. 2020. "The Burden of Ending Online Account Sharing." In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13. New York, NY, USA: Association for Computing Machinery.

Ofcom. 2024. "Children and Parents: Media Use and Attitudes Report".

Oh, Jungsuk, Byungwan Koh, and Srinivasan Raghunathan. 2015. "Value Appropriation between the Platform Provider and App Developers in Mobile Platform Mediated Networks." *Journal of Information Technology* 30 (3): 245–259. https://doi.org/10.1057/jit.2015.21.

Park, Cheul Young, Cori Faklaris, Siyan Zhao, Alex Sciuto, Laura Dabbish, and Jason Hong. 2018. "Share and Share Alike? an Exploration of Secure Behaviors in Romantic Relationships." In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, 83–102. Baltimore, MD, USA: USENIX Association.

Peroni, Lourdes, and Alexandra Timmer. 2013. "Vulnerable Groups: The Promise of an Emerging Concept in European Human Rights Convention Law." *International Journal of Constitutional Law* 11 (4): 1056–1085. https://doi.org/10.1093/icon/mot042.

Perzanowski, Aaron, and Jason Schultz. 2016. *The End of Ownership: Personal Property in the Digital Economy*. Massachusetts, USA: The MIT Press.

Piasecki, Stanislaw, and Jiahong Chen. 2022. "Complying with the GDPR When Vulnerable People Use Smart Devices." *International Data Privacy Law* 12 (2): 113–131. https://doi.org/10.1093/idpl/ipac001.

Prantl, David, and Martin Prantl. 2018. "Website Traffic Measurement and Rankings: Competitive Intelligence Tools Examination." *International Journal of Web Information Systems* 14 (4): 423–437. https://doi.org/10.1108/IJWIS-01-2018-0001.

Quan-Haase, Anabel, Andrew D. Nevin, and Veronika Lukacs. 2018. "Romantic Dissolution and Facebook Life: A Typology of Coping Strategies for Breakups." In *Networks, Hacking, and Media–CITA MS@ 30: Now and Then and Tomorrow*, Vol. 17, 73–98. UK: Emerald Publishing Limited.

Rowan, Mark, and Josh Dehlinger. 2014. "A Privacy Policy Comparison of Health and Fitness Related Mobile Applications." *Procedia Computer Science* 37: 348–355. https://doi.org/10.1016/j.procs.2014.08.051.

Sailaja, Neelima, and Abigail Fowler. 2022. "An Exploration of Account Sharing Practices on Media Platforms." In *ACM International Conference on Interactive Media Experiences*, 141–150. New York, NY, USA: Association for Computing Machinery.

Sambasivan, Nithya, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth F. Churchill. 2018. "'Privacy Is Not for Me, It's for Those Rich Women': Performative Privacy Practices on Mobile Phones by Women in South Asia." In *SOUPS@ USENIX Security Symposium*, 127–142. USA: USENIX Association.

Sambasivan, Nithya, Ed Cutrell, Kentaro Toyama, and Bonnie Nardi. 2010. "Intermediated Technology Use in Developing Communities." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '10*, 2583–2592. New York, NY, USA: Association for Computing Machinery.

Sandeen, Sharon. 2003. "The Sense and Nonsense of Web Site Terms of Use Agreements." *Hamline Law Review* 26 (3): 500–553.

Sas, Corina, and Steve Whittaker. 2013. "Design for Forgetting: Disposing of Digital Possessions after a Breakup." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '13*, 1823–1832. New York, NY, USA: Association for Computing Machinery.

Sikder, Amit Kumar, Leonardo Babun, Z Berkay Celik, Abbas Acar, Hidayet Aksu, Patrick McDaniel, Engin Kirda, and A Selcuk Uluagac. 2020. "Kratos: Multi-user Multi-Device-Aware Access Control System for the Smart Home." In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 1–12. New York, NY, USA: Association for Computing Machinery.

Singh, Supriya, Anuja Cabraal, Catherine Demosthenous, Gunela Astbrink, and Michele Furlong. 2007. "Password Sharing: Implications for Security Design Based on Social Practice." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '07*, 895–904. New York, NY, USA: Association for Computing Machinery.

van Hoboken, Joris, and R Ó Fathaigh. 2021. "Smartphone Platforms as Privacy Regulators." *Computer Law & Security Review* 41:105557. https://doi.org/10.1016/j.clsr.2021.105557.

van Lamsweerde, Axel. 2000. "Requirements Engineering in the Year 00: a Research Perspective." In *Proceedings of the 22nd International Conference on Software Engineering, ICSE '00*, 5–19. New York, NY, USA: Association for Computing Machinery.

Vänskä, Annamari, Sini Mickelsson, Daria Morozova, Heidi Härkönen, Olga Gurova, and Elina Pirjatanniemi. 2023. "Arctic Childhood in Data-Driven Culture: Wearable Technology and Children's Right to Privacy in Finland." *Critical Studies in Fashion & Beauty* 14 (2): 261–283. https://doi.org/10.1386/csfb_00067_1.

Weis, Aline, Sabrina Pohlmann, Regina Poss-Doering, Beate Strauss, Charlotte Ullrich, Helene Hofmann, Dominik Ose, Eva C Winkler, Joachim Szecsenyi, and Michel Wensing. 2020. "Caregivers' Role in Using a Personal Electronic Health Record: A Qualitative Study of Cancer Patients and Caregivers in Germany." *BMC Medical Informatics and Decision Making* 20 (1): 1–12. https://doi.org/10.1186/s12911-020-01172-4.

Winkler, Stephanie, and Sherali Zeadally. 2016. "Privacy Policy Analysis of Popular Web Platforms." *IEEE Technology and Society Magazine* 35 (2): 75–85. https://doi.org/10.1109/MTS.2016.2554419.

Wu, Yuxi, W. Keith Edwards, and Sauvik Das. 2022. "SoK: Social Cybersecurity." In *2022 IEEE Symposium on Security and Privacy (SP)*, 1863–1879. San Francisco, CA, USA: IEEE.

Zhang, Wei, and Chris Challis. 2022. "Towards Addressing Unauthorized Sharing of Subscriptions." *Applied Intelligence* 52 (15): 1–13.