

# Serious Games for Privacy Literacy: An Overview

Tomasz Banaszewski<sup>[0009–0003–3938–2990]</sup>, Ramona Adair<sup>[0000–0002–9197–1536]</sup>,  
and Ina Schiering<sup>[0000–0002–7864–5437]</sup>

Ostfalia University of Applied Sciences  
Wolfenbüttel, Germany  
{to.banaszewski, r.adair, i.schiering}@ostfalia.de

**Abstract.** Serious games are increasingly used in privacy education, but existing approaches vary widely in topic, audience, design, and evaluation. This paper presents a structured overview of serious games and game-based learning interventions related to privacy and privacy literacy. Using a structured literature-based search, 27 cases from academic publications and grey literature were analysed. The comparison covers privacy topics, target groups and contexts of use, game formats and mechanics, as well as evaluation approaches and reported outcomes.

Recurring topics include social-network privacy and online disclosure, digital footprints, data protection and privacy rights, privacy policies and consent, app and device permissions, and deceptive patterns. Children, adolescents, and young adults are strongly represented, and most cases were coded as formal education or facilitated non-formal or research settings. Where reported, outcomes primarily concern awareness, knowledge, privacy-related competences, self-efficacy, and behavioural intention, while sustained real-world behavioural change and long-term effects are rarely examined. The paper contributes a structured comparison of existing privacy-related serious games and game-based learning interventions and identifies gaps concerning adult learning, informal contexts, underrepresented privacy domains, and more robust evaluation designs.

**Keywords:** Serious Games · Privacy Literacy · Game-based Learning · Digital Privacy

## 1 Introduction

Privacy has become a central challenge of everyday digital life. People constantly interact with platforms, apps, social media services, and connected devices that collect, process, and share personal information. In these environments, users are expected to make decisions about disclosure, consent, visibility, and protection, often without fully understanding the consequences. This makes privacy literacy an important educational and societal concern [16].

In practice, however, privacy-related attitudes and actual behaviour often diverge. Users frequently claim that privacy matters to them, yet they still disclose personal data, accept privacy policies without reflection, or neglect protective

measures. This so-called privacy paradox suggests that awareness alone is not sufficient and that people need better support for the development of informed privacy-related judgement and decision-making [12].

One promising approach is the use of serious games and game-based learning interventions. Serious games can create interactive learning environments in which complex privacy-related issues become more tangible and consequences can be explored through feedback, scenarios, and low-risk practice [28, 26, 2, 27]. Individual publications describe privacy-related serious games for different topics and settings, including school education, online safety, privacy policies, and data privacy learning [20, 32]. However, these studies differ considerably in the privacy topics, target groups, contexts of use, game formats, and evaluation approaches they address.

This makes it difficult to see which areas are covered and where gaps remain. To address this gap, this paper presents a structured overview of serious games and game-based learning interventions in the context of privacy and privacy literacy. Accordingly, this paper addresses the following questions: (1) What kinds of privacy-related serious games and game-based learning interventions have been proposed and, where applicable, evaluated so far? and (2) What patterns and research gaps exist with regard to serious games in the context of privacy literacy?

## 2 Background and Related Work

For the purposes of this overview, privacy literacy is understood as the knowledge, awareness, and competences required to understand how personal data are collected, processed, shared, and protected and to make informed privacy-related decisions [16, 27]. This distinction is important because awareness alone does not necessarily lead to privacy-protective behaviour, as discussed in relation to the privacy paradox [12]. Therefore, this overview also considers whether games address broader competences, self-efficacy, behavioural intention, or privacy-related behaviour.

In this paper, serious games are understood as analogue or digital, rule-based games with a clear primary purpose beyond entertainment and an intended transfer of the game experience to real-world learning or action [26]. This format-independent definition allows digital games, board and card games, escape rooms, and game-based simulations to be considered where they meet these defining characteristics, while distinguishing serious games from mere play and the isolated use of game elements [26]. Game-based learning refers more broadly to learning through gameplay, whereas serious games are purpose-oriented game artefacts designed for outcomes beyond entertainment [28, 26]. In privacy education, serious games can make abstract data practices, privacy risks, and decision situations more tangible through interaction, feedback, scenarios, role-play, or simulated consequences [2, 27].

Individual studies already describe privacy-related serious games for different topics and settings. These include social-network privacy, privacy policies, data

protection, privacy self-efficacy, online safety, and dark patterns [6, 32, 2, 20, 35, 15]. However, these studies differ considerably in their learning goals, target groups, contexts of use, game formats, and evaluation approaches. This makes it difficult to see which parts of privacy literacy are already covered by existing games and where gaps remain.

Existing review work covers related but narrower areas, such as professional training, security and privacy in the software development lifecycle, or cybersecurity educational games for children [25, 3, 9]. Design-oriented work also provides guidance for privacy-related serious games, for example through design suggestions for privacy decision-making [14]. However, these works remain focused on specific contexts. A broader privacy-literacy-oriented comparison across privacy topics, learner groups, application contexts, evaluation approaches, and reported outcomes still appears to be missing.

### 3 Methodology

The study is based on a structured literature-based approach for identifying and comparing serious games related to privacy and privacy literacy. Relevant publications were identified primarily through Google Scholar, IEEE Xplore, ACM Digital Library, SpringerLink, and publisher websites using combinations of keywords such as *serious games*, *privacy literacy*, *privacy education*, *digital privacy*, *privacy awareness*, *data protection*, and *game-based learning*. The search and screening process was conducted iteratively between March 2026 and July 2026. In addition to academic publications, selected grey-literature sources and publicly available descriptions of relevant games were considered where they provided useful information about the game design, target group, context of use, or evaluation.

Sources were included if they described a serious game or a clearly purpose-oriented game-based learning intervention with an explicit privacy-related learning objective and provided sufficient information on the game design, target group, context of use, or evaluation. This included digital games, board and card games, escape rooms, simulations, and comparable game-based interventions in which privacy, data protection, or privacy literacy constituted a substantial part of the learning objective. Sources were excluded if they addressed general cybersecurity without a privacy-related component, described gamification without a serious game or comparable game-based learning element, or did not provide sufficient information for comparison. Works in which play primarily served as a research method [5] or formed part of a broader facilitated intervention without describing a distinct serious-game case [7] were also excluded.

The final set comprised 27 analytical cases: 21 publication-based cases and six grey-literature cases. *Space Shelter* and *Reality River* were counted as separate cases because they are distinct game artefacts, although they were used within the same classroom intervention.

Each case was coded according to source type, privacy scope and topic, target group, context of use, game format, game mechanics, learning objective, eval-

uation approach, reported outcomes, reported participant numbers, and limitations. Privacy scope was recorded descriptively as either privacy-focused or mixed with neighbouring educational topics. Each case was also assigned to one primary target group: children or tweens, adolescents or young adults, university or professional audiences, or adults and general users. These categories were based on the audience descriptions and school stages reported by the sources rather than on strict age thresholds. Each case was additionally assigned to one primary context of use: formal education, a facilitated non-formal or research setting, self-directed or everyday use, or a flexible or insufficiently specified setting. The coding was based primarily on the context in which the game was implemented or evaluated. For cases without a documented implementation or evaluation, the intended context of use described by the source was used.

Reported outcome patterns were coded separately from evaluation approach. A *Clear positive reported outcome* indicated an unambiguous improvement in the main intended outcome or outcomes without substantial contradictory findings. *Indicative positive outcome* was used for positive qualitative, perceived-learning, or incompletely documented findings. *Mixed or limited outcome* was assigned where positive findings were accompanied by null, partial, or contradictory results. *No effectiveness statement* indicated that no empirical learning or behavioural effect was reported.

Evaluation approach was coded independently according to whether and how each case was formally evaluated. The categories comprised controlled or comparative designs; pre/post, longitudinal, or multi-phase designs without a separate comparison group; post-game, qualitative, observational, or exploratory evaluations; evaluations that were reported but insufficiently documented; and cases without a formal effectiveness evaluation.

## 4 Results

### 4.1 Included Games

Table 1 presents the 27 cases included in the analysis. The table lists the 21 publication-based cases and the six grey-literature cases separately and provides a brief description of each game or game-based intervention. The privacy scope is reported descriptively as either privacy-focused or mixed with neighbouring educational topics.

Table 1: Overview of the 27 included cases

| Game / intervention                          | Brief description                                                                                                             | Privacy scope                                                 | Source |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|--------|
| <i>Publication-based cases</i>               |                                                                                                                               |                                                               |        |
| <i>A Day in the Life of the JOs</i>          | Scenario-based web game in which players make everyday digital-media decisions and receive feedback on their consequences.    | Mixed with cybersecurity, online safety, and digital literacy | [20]   |
| Bespoke privacy and online-safety board game | Question- and discussion-based board game using category and shield tokens to explore online risks.                           | Mixed with online safety, cyberbullying, and online scams     | [13]   |
| <i>Cyber Chronix</i>                         | Branching digital-comic game that introduces personal-data protection and GDPR rights through storytelling and user choices.  | Privacy-focused                                               | [10]   |
| <i>Dark Pattern</i>                          | Board game in which players install apps while limiting personal-data access and responding to dark patterns.                 | Privacy-focused                                               | [35]   |
| <i>Desperate John</i>                        | Escape-room game combining privacy puzzles with practical tasks such as changing settings and installing protective software. | Privacy-focused                                               | [27]   |
| <i>Friend Inspector</i>                      | Facebook-based game comparing users' assumptions about shared-item visibility with their actual privacy settings.             | Privacy-focused                                               | [8]    |
| <i>Guess the User?</i>                       | Deduction board game in which behavioural data are combined to identify a hidden user and illustrate profiling.               | Privacy-focused                                               | [31]   |
| <i>Immaculacy</i>                            | Interactive narrative game about surveillance, information disclosure, and the consequences of privacy decisions.             | Privacy-focused                                               | [33]   |
| Information Disclosure Game                  | Board game in which players exchange personal information for financial benefits and experience disclosure consequences.      | Privacy-focused                                               | [11]   |
| <i>LetsProtectDATA</i>                       | Digital escape-room game in which students act as data protection officers and solve workplace privacy challenges.            | Privacy-focused                                               | [2]    |
| <i>Panopticon</i>                            | Board game in which players design, critique, and revise privacy-sensitive digital services.                                  | Privacy-focused                                               | [34]   |
| <i>PrivaCity</i>                             | Chatbot adventure exploring smart-city data collection, digital footprints, data misuse, and privacy trade-offs.              | Privacy-focused                                               | [4]    |
| <i>Privacy Awareness Cards</i>               | Facilitated card activity for identifying personal data, stakeholders, privacy risks, consequences, and possible safeguards.  | Privacy-focused                                               | [19]   |
| <i>Puzzle Policy</i>                         | Escape-room game that transforms privacy-policy content into puzzles about collection, transfer, storage, and security.       | Privacy-focused                                               | [32]   |
| <i>RedCapes</i>                              | Scenario-based game for autistic children addressing personal, physical, medical, and situational privacy.                    | Privacy-focused                                               | [37]   |
| Smartwatch Games                             | Wearable maze game combining quizzes with timed tasks that require players to change privacy-relevant device settings.        | Privacy-focused                                               | [36]   |
| <i>Social4School</i>                         | Classroom social-network simulation showing how posts, likes, and shares affect one's own and others' privacy.                | Privacy-focused                                               | [6]    |

Continued on next page

Table 1 – continued from previous page

| Game / intervention          | Brief description                                                                                                                                                       | Privacy scope                                                   | Source   |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|----------|
| <i>Space Shelter</i>         | Online quiz-based game in which players complete a space mission by answering questions about online safety, passwords, two-factor authentication, and data protection. | Mixed with cybersecurity and online safety                      | [38]     |
| <i>Reality River</i>         | Online quiz-based game addressing scams, phishing, hacking, account security, and the evaluation of online information.                                                 | Mixed with cybersecurity and online safety                      | [38]     |
| <i>The Watchers</i>          | Hybrid game in which children investigate data shadows, commercial data collection, trust, and online disclosure.                                                       | Privacy-focused                                                 | [29]     |
| <i>Trickery</i>              | Digital laboratory adventure that exposes players to deceptive interface patterns and requires them to resist manipulation.                                             | Mixed with deceptive-pattern education                          | [15]     |
| <i>Grey-literature cases</i> |                                                                                                                                                                         |                                                                 |          |
| <i>DATAK</i>                 | Decision-based game in which players manage personal-data dilemmas as trainee data protection officers in a fictional town.                                             | Privacy-focused                                                 | [30]     |
| <i>Dark Cookie</i>           | Cookie-banner game in which players must reject unnecessary cookies despite deceptive interface designs.                                                                | Privacy-focused                                                 | [1]      |
| <i>Data Defenders</i>        | Match-three game that reveals the hidden privacy cost of sharing information and introduces protective strategies.                                                      | Privacy-focused                                                 | [23, 22] |
| <i>myPAL Games</i>           | Child-oriented learning website whose central game asks players to identify sensitive information in simulated social-media posts.                                      | Privacy-focused                                                 | [21]     |
| <i>Privacy Pirates</i>       | Interactive learning unit for young children covering personal information, digital footprints, passwords, and data sharing.                                            | Privacy-focused                                                 | [24]     |
| <i>THE FEED</i>              | Social-media simulation in which players manage personalised feeds, collect user data, and monetise online activity.                                                    | Mixed with social-media algorithms, AI, and digital sovereignty | [18, 17] |

## 4.2 Privacy Topics and Scope

Across the 27 included cases, the analysed games and game-based interventions cover a broad range of privacy-related topics. Recurring themes include social-network privacy and online disclosure [6, 29, 8, 11], privacy policies and consent [32], privacy-protective practices and safeguards [27], device permissions and wearable privacy [36], data protection rights [10], smart-city privacy [4], privacy by design [34], dark patterns and consent-related manipulation [35, 15, 1], and commercial data collection and platform monetisation [29, 18]. Social-network and online-sharing scenarios are particularly prominent, especially in games designed for children and adolescents [6, 29, 20, 31]. Other games focus on more specific privacy problems, such as privacy policies, smartwatch permissions, cookie-banner dark patterns, or the design of privacy-sensitive data practices [32, 36, 1, 34].

The comparison also shows that privacy is sometimes embedded in a broader educational agenda. Some cases combine privacy with cybersecurity, phishing,

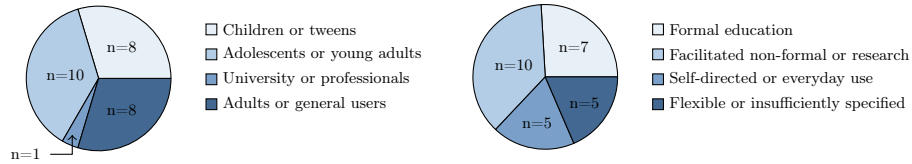
password security, online safety, or digital literacy [20, 13, 38]. Deceptive-pattern education constitutes another mixed scope because privacy-related manipulation is addressed through a broader interface-design problem [15]. Table 1 therefore reports the privacy scope descriptively as either privacy-focused or mixed with neighbouring educational topics.

Across the 27 included cases, several contemporary privacy topics remain weakly represented. Smart-home privacy does not appear as a primary topic, while workplace privacy and informal adult privacy learning occur only in a small number of cases. AI-related data practices are addressed most explicitly in *THE FEED*, where privacy is embedded in a broader focus on social-media algorithms, artificial intelligence, and digital sovereignty [18, 17].

### 4.3 Target Groups and Contexts of Use

The primary target-group distribution shows a strong representation of younger audiences. Eight cases primarily address children or tweens, ten address adolescents or tweens, ten address university or professional audiences, and eight address adults or general users. Examples range from primary-school and tween-oriented interventions [6, 20] to games for secondary-school students [2, 4] and adult users [32, 27, 36].

Context of use was analysed separately from target group. Seven cases were coded as formal education, ten as facilitated non-formal or research settings, five as self-directed or everyday use, and five as flexible or insufficiently specified settings. Formal educational settings include classroom and university-based interventions [6, 2, 34], whereas workshops and facilitated studies form part of the non-formal or research category [19, 27, 37]. Thus, 17 of the 27 cases were coded as formal education or facilitated non-formal or research settings, whereas self-directed or everyday use was less common. This distinction is important because many privacy decisions occur outside organised learning settings, for example when users install apps, configure devices, encounter cookie banners, or interact with online platforms [35, 36, 1, 18].



**Fig. 1.** Distribution of primary target groups and contexts of use across the 27 included cases.

### 4.4 Game Formats and Mechanics

The analysed set includes a wide variety of game formats. Digital formats include online simulations, mobile applications, chatbot games, smartwatch games,

decision-based games, match-three games, interactive learning units, cookie-banner games, and social-media simulations [6, 4, 36, 30, 23, 22, 21, 24, 1, 18, 17, 33]. Escape-room formats are also represented [32, 27, 2]. Non-digital and hybrid formats include board games, card-based activities, and hybrid investigation games [29, 13, 35, 31, 34, 19]. This diversity shows that privacy learning is not tied to a single game format.

Several recurring mechanics can be identified. Many games use role-play, perspective-taking, decision-making, scoring, quizzes, feedback, narrative scenarios, or simulated consequences [10, 29, 33, 6, 20, 35, 4]. Some games make hidden privacy consequences visible through scores or feedback [6, 20, 35], while others use social simulations, escape-room puzzles, or scenario discussions [6, 32, 27, 29, 19]. Particularly interesting are games that reverse the usual perspective: instead of playing only as privacy-protecting users, players may act as designers, platform operators, data collectors, or other system actors [34, 18, 17]. Such mechanics can make otherwise invisible privacy infrastructures more tangible.

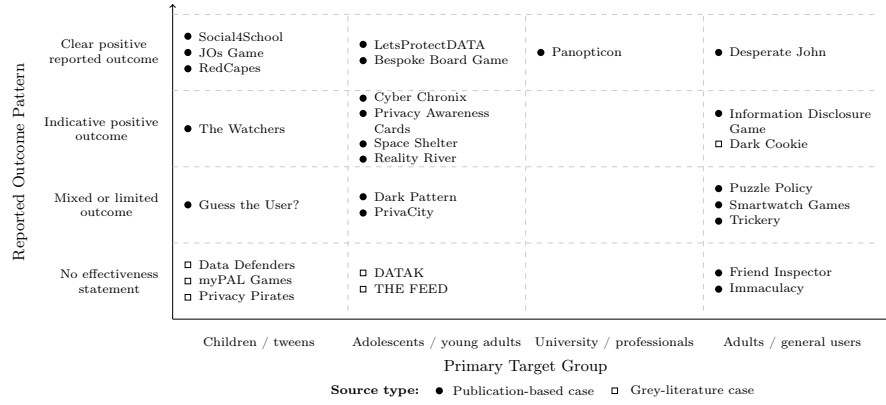
However, in the coded sample, many games still focus on awareness and reflection rather than sustained practice of privacy competences. Only a small number of games require players to perform concrete privacy-relevant tasks that are close to real-world behaviour, such as configuring device settings, engaging with privacy-policy information, or designing privacy-sensitive data practices [36, 32, 27, 34].

#### 4.5 Reported Outcomes and Evaluation Approaches

Across the included cases, the reported outcomes cover privacy awareness, knowledge, competences, self-efficacy, behavioural intention, simulated decisions, and privacy-related behaviour. Four descriptive outcome patterns were distinguished. Seven cases reported clear positive outcomes, seven provided indicative positive findings, six produced mixed or limited results, and seven provided no empirical effectiveness statement. Their distribution across the primary target groups is shown in Fig. 2. Markers are positioned within each category cell only to avoid overlap; their positions within a cell do not encode an additional metric.

Clear positive findings occurred across different outcome types and game formats. These included safer simulated decisions in *Social4School*, improvements in knowledge and behavioural intention in *A Day in the Life of the JOs*, increased self-efficacy in *LetsProtectDATA*, gains in privacy competences in *Desperate John*, and improved privacy-design performance in *Panopticon* [6, 20, 2, 27, 34]. Positive changes were also reported for children’s disclosure judgements in *RedCapes*, while the bespoke privacy and online-safety board game yielded positive focus-group findings and perceived learning [37, 13].

Seven cases provided positive indications without a direct or sufficiently detailed measurement of change. These comprised *Cyber Chronix*, *The Watchers*, *Space Shelter*, *Reality River*, the *Privacy Awareness Cards*, the *Information Disclosure Game*, and *Dark Cookie*. Their positive indications were based on perceived learning, qualitative findings, participant discussions, or preliminary and incompletely documented empirical results [10, 29, 38, 19, 11, 1]. The findings for



**Fig. 2.** Reported outcome patterns across primary target groups.

*Space Shelter* and *Reality River* derive from the same classroom intervention and therefore do not represent two independent evaluations [38]. Mixed findings were reported for *Puzzle Policy*, which improved recall but not privacy attitudes; the smartwatch games, which affected some device settings but not application permissions; and *PrivaCity*, where awareness gains were clearer than intended behavioural changes [32, 36, 4]. *Dark Pattern*, *Guess the User?*, and *Trickery* likewise showed only partial understanding, continuing misconceptions, or positive results for only some of the assessed concepts [35, 31, 15].

Seven cases provided no empirical effectiveness statement. These comprised the publication-based cases *Friend Inspector* and *Immaculacy*, together with the grey-literature cases *DATAK*, *Data Defenders*, *myPAL Games*, *Privacy Pirates*, and *THE FEED* [8, 33, 30, 23, 22, 21, 24, 18, 17]. These cases are not interpreted as showing no effect; rather, no corresponding effect was empirically assessed. Five of the six grey-literature cases fell into this category; *Dark Cookie* was the only grey-literature case with a reported player evaluation [1].

Direct measurement of real-world privacy behaviour and longer-term effects was uncommon. The smartwatch study logged privacy-relevant device settings over time, while *A Day in the Life of the JOs* included a one-week follow-up [36, 20]. Most other studies measured immediate knowledge, awareness, self-efficacy, intention, simulated decisions, or performance within an educational task. Positive and mixed findings occurred across different formats, mechanics, and target groups. However, because the studies differ substantially in their interventions, participants, outcome measures, and designs, the results do not demonstrate that one format, mechanic, or target group is associated with consistently stronger effects. The included cases differed substantially in their evaluation approaches. Table 2 groups all 27 cases according to the primary evaluation approach reported, including cases without a formal effectiveness evaluation. The categories describe how, or whether, the cases were formally evaluated and do not constitute a ranking of methodological quality.

**Table 2.** Primary evaluation approaches across the 27 included cases

| Primary evaluation approach                                                       | Number of cases |
|-----------------------------------------------------------------------------------|-----------------|
| Controlled or comparative design                                                  | 5               |
| Pre/post, longitudinal, or multi-phase design without a separate comparison group | 7               |
| Post-game, qualitative, observational, or exploratory evaluation                  | 6               |
| Evaluation reported but insufficiently documented                                 | 1               |
| No formal effectiveness evaluation                                                | 8               |
| <b>Total</b>                                                                      | <b>27</b>       |

Controlled or comparative designs included a separate control, comparison, or alternative-intervention condition. The second group comprised pre/post assessments, longitudinal observation, and multi-phase evaluations without a separate comparison group. The third group relied primarily on post-game questionnaires, qualitative observations, interviews, discussions, or participatory evaluation. The *Privacy Awareness Cards* were assigned to the indicative positive outcome category because the source reports qualitative workshop observations, although it does not provide a formal effectiveness evaluation [19]. Reported evaluation samples ranged from small exploratory samples to more than 450 participants. Participant numbers were not aggregated into a separate case-level distribution because several sources reported multiple evaluation phases, incomplete sample information, or shared intervention samples. In particular, *Space Shelter* and *Reality River* were evaluated with the same group of 41 students [38]. Several studies were additionally limited by short follow-up periods, reliance on self-report, or the absence of direct behavioural measures [2, 27, 32, 36, 20].

## 5 Discussion

The results show that privacy-related serious games and game-based learning interventions form a heterogeneous field. The analysed cases cover different privacy topics, game formats, target groups, and evaluation approaches, but this coverage is uneven. Awareness and reflection are prominent learning objectives across the analysed cases. Frequently addressed privacy topics include disclosure, social-network privacy, data protection, privacy policies, and deceptive patterns. By contrast, smart-home privacy, workplace privacy, AI-related data practices, and informal adult learning remain weakly represented in the coded sample.

As shown in Fig. 1, children, adolescents, and young adults are strongly represented, while formal or facilitated settings account for most included cases. This indicates that organised settings play a prominent role in how privacy-related serious games are described, implemented, or examined. Such settings can support explanation, reflection, and discussion. At the same time, many privacy decisions occur outside organised learning environments. Users configure devices, install apps, respond to cookie banners, and interact with online platforms in

everyday situations. The current sample therefore leaves open questions about adult learners, informal learning contexts, workplace situations, and self-directed privacy learning.

The evaluation approaches reveal another limitation of the field. As summarised in Table 2, the included cases differ substantially in whether and how they were evaluated. Among the evaluated cases, many rely on exploratory approaches, self-report measures, or descriptive accounts, whereas only some include comparison groups, longitudinal observation, or direct behavioural measures. This does not mean that these games are not useful. Many cases provide useful design concepts, while evaluated cases often report promising engagement or productive discussion [10, 4, 37, 15, 19]. Design-oriented cases without a formal effectiveness evaluation also contribute practical ideas for privacy education [8, 33]. However, the reported outcomes support only cautious claims about learning effects. This is particularly relevant in light of the privacy paradox, because measures of awareness or intention alone cannot show whether game-based learning helps reduce the gap between privacy attitudes and actual privacy behaviour [12]. Stronger claims about durable privacy competences, behavioural transfer, or long-term changes in privacy behaviour require more robust evaluation designs, delayed measurements, and behavioural or task-based outcome measures. Future evaluations should also examine whether engagement and learning differ across learner groups and stakeholders, and whether repeated exposure supports continued reflection or instead leads to habituation.

Transferability remains an open question. Most of the included games were developed for a specific target group and context, but the available studies rarely examine whether the same game could also be used with other audiences. Games designed for children may address privacy problems that are also relevant to adults, while their language, narratives, level of difficulty, or need for facilitation may still be closely tailored to younger learners [6, 20, 29, 37]. Future research should therefore distinguish between games that are specific to one target group and games whose central design can be adapted to other audiences and contexts.

A similar distinction is needed for privacy topics and game mechanics. Mechanics such as role-play, perspective-taking, feedback, and simulated consequences may be adaptable across different privacy topics, whereas other elements are closely connected to a specific problem, such as privacy policies, smartwatch settings, or social-network disclosure [32, 36, 6, 34]. Comparative studies could examine which mechanics and learning activities can be transferred and which require substantial adaptation.

Taken together, these findings point to a need for broader thematic and contextual coverage and for evaluations that more directly assess durable competences and behaviourally relevant outcomes.

## 6 Limitations and Future Work

This overview has several limitations. First, the study is based on a structured but iterative literature-based search rather than a fully systematic review. Rele-

vant publications were searched across several academic databases and publisher platforms, and the search was extended through grey-literature sources. However, privacy-related serious games are not always labelled consistently. Some works use terms such as privacy awareness, data protection, online safety, cybersecurity, digital literacy, or game-based learning instead of privacy literacy or serious games [20, 13, 38, 15, 18]. Additional relevant cases may therefore exist that were not identified during the search.

The inclusion criteria also required privacy to constitute a substantial part of the learning objective. This helped to delimit the analysis, but it may have under-represented games in which privacy is only one element of broader cybersecurity, online-safety, or digital-literacy education. Future research could examine these boundary areas more systematically and distinguish between games in which privacy is the primary learning objective and those in which it forms part of a broader intervention.

Second, the sources vary substantially in scope and detail. The grey-literature cases listed in Table 1 were retained because they document practical resources that would be missed by restricting the overview to peer-reviewed work, but not every comparison dimension was available for every case. The outcome categories therefore summarise only the direction and consistency of reported findings; they are not standardised or directly comparable effect sizes, and cases within a category may differ in evaluation design, measurement instruments, and empirical support. Participant numbers are likewise not directly comparable because some sources report multiple phases, shared samples, or incomplete data. Although *Space Shelter* and *Reality River* were treated as separate game cases, their intervention-level outcomes came from the same classroom study and should not be interpreted as independent evaluations [38]. Assigning one primary target group and one primary context also simplifies cases that address multiple audiences or settings. Where no implementation or evaluation was documented, context coding relied on intended rather than observed use.

Third, transferability remains largely untested. The discussion of potentially transferable target groups, contexts, topics, and mechanics is based mainly on the reported designs of the games rather than on empirical studies in new settings. Concrete claims about transferability would require games to be adapted and evaluated with different audiences, privacy topics, or contexts of use. Future work could, for example, examine whether games developed for children can also support adult privacy learning and whether mechanics such as role-play, perspective-taking, feedback, and simulated consequences can be applied across different privacy topics.

Further research should also address privacy areas that remain weakly represented, including smart-home privacy, workplace privacy, AI-related data practices, and informal adult learning. Evaluations would benefit from larger and more diverse samples, direct behavioural or task-based measures, delayed follow-up assessments, and comparisons across learner groups and stakeholders.

## 7 Conclusion

This paper presented a structured overview of 27 analytical cases concerning privacy-related serious games and game-based learning interventions, drawing on academic publications and grey literature. The identified cases demonstrate that privacy education is addressed through a diverse range of digital, analogue, and hybrid formats, including simulations, escape rooms, board and card games, chatbot and wearable games, interactive learning units, and hybrid activities. Common mechanics include decision-making, role-play, perspective-taking, quizzes, puzzles, feedback, and simulated consequences. The games cover topics ranging from social-network disclosure, digital footprints, privacy policies, data protection rights, and device permissions to deceptive patterns, privacy by design, and commercial data practices. Awareness and reflection are prominent objectives, but some cases extend beyond these goals by addressing knowledge, privacy-related competences, self-efficacy, privacy-design skills, behavioural intention, or privacy-related behaviour.

The available evidence presents a promising but fragmented picture. Evaluation approaches range from controlled and comparative designs to pre/post, longitudinal, qualitative, observational, and exploratory studies, while eight cases had no formal effectiveness evaluation. Clear or indicative positive findings were reported for several learning outcomes, but mixed and limited results were also common. Because the interventions, participants, measurements, and evaluation designs differ substantially, the findings do not show that a particular game format, mechanic, or target group consistently produces stronger outcomes. Moreover, most evaluations concern immediate awareness, knowledge, competences, or intentions, whereas sustained real-world behavioural change and longer-term effects remain rarely examined.

Several broader patterns emerge from the overview. Younger audiences are strongly represented, with 18 cases primarily addressing children, tweens, adolescents, or young adults. Formal education and facilitated non-formal or research settings account for 17 of the 27 cases. Adult learning, self-directed or everyday use, workplace privacy, smart-home privacy, and AI-related data practices remain comparatively underrepresented, and transferability across audiences, settings, and privacy topics is rarely evaluated empirically.

Overall, the analysed cases show that serious games can make privacy issues more tangible, interactive, and open to reflection. They provide diverse approaches to privacy education and several encouraging learning outcomes, but the field does not yet offer robust evidence that these effects consistently transfer to durable privacy-protective behaviour. Future work should therefore combine broader thematic and contextual coverage with more comparable outcome reporting, behavioural and task-based measures, delayed follow-ups, and greater attention to differences between learner groups and stakeholders. It should also examine whether repeated exposure supports continued learning and reflection or leads to habituation.

## References

1. Akinyemi, O.P.: “Dark Cookie”: A Serious Game to Train Users to Spot and Interact with Dark Patterns in Cookie Banners. Master’s thesis, University of Luxembourg (2022)
2. Bahr, T., Kostron, P., Zinn, B.: A serious game to promote self-efficacy regarding data privacy among secondary school students. *Journal of Computers in Education* (Dec 2025). <https://doi.org/10.1007/s40692-025-00377-8>
3. Bellemans, J., Van Landuyt, D., Sion, L., Desmet, L.: Gamified or Glorified? A systematic review of serious games for security & privacy in the SDLC. *Information and Software Technology* **188**, 107850 (Dec 2025). <https://doi.org/10.1016/j.infsof.2025.107850>
4. Berger, E., Sæthre, T.H., Divitini, M.: PrivaCity: A Chatbot Game to Raise Privacy Awareness Among Teenagers. In: Pozdniakov, S.N., Dagienė, V. (eds.) *Informatics in Schools. New Ideas in School Informatics*, vol. 11913, pp. 293–304. Springer International Publishing, Cham (2019). [https://doi.org/10.1007/978-3-030-33759-9\\_23](https://doi.org/10.1007/978-3-030-33759-9_23)
5. Berkholz, J., Rahman, A., Stevens, G.: Playing with Privacy: Exploring the Social Construction of Privacy Norms Through a Card Game. *Proceedings of the ACM on Human-Computer Interaction* **9**(1), 1–23 (Jan 2025). <https://doi.org/10.1145/3701202>
6. Bioglio, L., Capecchi, S., Peiretti, F., Sayed, D., Torasso, A., Pensa, R.G.: A Social Network Simulation Game to Raise Awareness of Privacy Among School Children. *IEEE Transactions on Learning Technologies* **12**(4), 456–469 (Oct 2019). <https://doi.org/10.1109/TLT.2018.2881193>
7. Cardoso, F., Andreoletti, D., Ferrari, A., Botturi, L., Fioroni, T., Beretta, C., Picco Schwendener, A., Marazza, S., Giordano, S.: Playing for Privacy Awareness: Learning from a “Wow-Moment” with iBuddy. *European Conference on Games Based Learning* **16**(1), 128–138 (Sep 2022). <https://doi.org/10.34190/ecgb.16.1.490>
8. Cetto, A., Netter, M., Pernul, G., Richthammer, C., Riesner, M., Roth, C., Sängler, J.: Friend Inspector: A Serious Game to Enhance Privacy Awareness in Social Networks (Feb 2014). <https://doi.org/10.48550/arXiv.1402.5878>
9. Damenu, T.K., Gökbay, İ.Z., Covaci, A., Li, S.: Cyber Security Educational Games for Children: A Systematic Literature Review (Aug 2025). <https://doi.org/10.48550/arXiv.2508.17414>
10. Di Gioia, R., Chaudron, S., Gemo, M., Sanchez, I.: Cyber Chronix, Participatory Research Approach to Develop and Evaluate a Storytelling Game on Personal Data Protection Rights and Privacy Risks. In: Liapis, A., Yannakakis, G.N., Gentile, M., Ninaus, M. (eds.) *Games and Learning Alliance*, vol. 11899, pp. 221–230. Springer International Publishing, Cham (2019). [https://doi.org/10.1007/978-3-030-34350-7\\_22](https://doi.org/10.1007/978-3-030-34350-7_22)
11. Fatima, R., Yasin, A., Liu, L., Wang, J., Afzal, W., Yasin, A.: Sharing information online rationally: An observation of user privacy concerns and awareness using serious game. *Journal of Information Security and Applications* **48**, 102351 (Oct 2019). <https://doi.org/10.1016/j.jisa.2019.06.007>
12. Gerber, N., Gerber, P., Volkamer, M.: Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security* **77**, 226–261 (Aug 2018). <https://doi.org/10.1016/j.cose.2018.04.002>

13. Henriksen-Bulmer, J., Rosenorn-Lanng, E., Corbin-Clarke, S., Ware, S., Melacca, D., Fenge, L.A.: Using game-based learning to teach young people about privacy and online safety. *Interactive Learning Environments* **32**(10), 6430–6450 (Nov 2024). <https://doi.org/10.1080/10494820.2023.2265424>
14. Jost, P., Divitini, M.: Designing Analytic Serious Games: An Expert Affordance View on Privacy Decision-Making. In: Fletcher, B., Ma, M., Göbel, S., Baalsrud Hauge, J., Marsh, T. (eds.) *Serious Games*, vol. 12945, pp. 3–19. Springer International Publishing, Cham (2021). [https://doi.org/10.1007/978-3-030-88272-3\\_1](https://doi.org/10.1007/978-3-030-88272-3_1)
15. Kronhardt, K., Rolfes, K., Gerken, J.: Trickery: Exploring a Serious Game Approach to Raise Awareness of Deceptive Patterns. In: *Proceedings of the International Conference on Mobile and Ubiquitous Multimedia*. pp. 133–147. ACM, Stockholm Sweden (Dec 2024). <https://doi.org/10.1145/3701571.3701588>
16. Kumar, P.C., Subramaniam, M., Vitak, J., Clegg, T.L., Chetty, M.: Strengthening Children’s Privacy Literacy through Contextual Integrity. *Media and Communication* **8**(4), 175–184 (Nov 2020). <https://doi.org/10.17645/mac.v8i4.3236>
17. Landesanstalt für Kommunikation Baden-Württemberg: MEIN FEED: Social-media-journal (2025)
18. Landesanstalt für Kommunikation Baden-Württemberg: THE FEED: Begleitheft für lehrkräfte (2025)
19. Lorenz, T., Pleger, M., Böhm, T., Schiering, I.: Privacy Awareness Cards -A Serious Game for Privacy Awareness. In: Friedewald, M., Karaboga, M. (eds.) *Freedom in digital infrastructures. Poster-Proceedings. Research Papers of the Platform Privacy*. pp. 13 – 16. No. 4, Fraunhofer ISI (2024). <https://doi.org/10.24406/publica-3685>
20. Maqsood, S., Chiasson, S.: Design, Development, and Evaluation of a Cybersecurity, Privacy, and Digital Literacy Game for Tweens. *ACM Transactions on Privacy and Security* **24**(4), 1–37 (Nov 2021). <https://doi.org/10.1145/3469821>
21. McComiskey, T.: If You Give a Website a Cookie: Educating Children About Online Privacy (Jun 2025). <https://doi.org/10.15760/honors.1729>
22. MediaSmarts: Data defenders: Guide for parents. Parent guide (2018), <https://mediasmarts.ca>
23. MediaSmarts: Data defenders: Teacher’s guide. Teacher’s guide (2018), <https://mediasmarts.ca>
24. MediaSmarts: Privacy pirates: An interactive unit on online privacy (ages 7–9). background information for parents and teachers. Guide for parents and teachers (2021), <https://mediasmarts.ca>
25. Moumouh, C., García-Berná, J.A., Chkouri, M.Y., Fernández-Alemán, J.L.: Serious Games to Improve Privacy and Security Knowledge for Professionals: A Systematic Literature Review. *International Journal of Serious Games* **12**(1), 3–24 (Feb 2025). <https://doi.org/10.17083/ijsg.v12i1.825>
26. Olejniczak, K., Newcomer, K.E., Meijer, S.A.: Advancing Evaluation Practice With Serious Games. *American Journal of Evaluation* **41**(3), 339–366 (Sep 2020). <https://doi.org/10.1177/1098214020905897>
27. Papaioannou, T., Kokotos, S.E., Tsohou, A.: Educational Escape Rooms for Raising Information Privacy Competences: An Empirical Validation (Nov 2024). <https://doi.org/10.21203/rs.3.rs-5277322/v1>
28. Plass, J.L., Homer, B.D., Kinzer, C.K.: Foundations of Game-Based Learning. *Educational Psychologist* **50**(4), 258–283 (Oct 2015). <https://doi.org/10.1080/00461520.2015.1122533>

29. Raynes-Goldie, K., Allen, M.: Gaming privacy: A canadian case study of a co-created privacy literacy game for children. *Surveillance & Society* **12**(3), 414–426 (2014). <https://doi.org/10.24908/ss.v12i3.4958>
30. RTS Découverte: Datak: The game that helps you get to grips with your personal data. Teaching aid (2017), <https://www.rts.ch/datak>
31. Sasaki Otani, M.E.: “Guess the User?”: A Board Game Approach to Children’s Digital Privacy Rights and Data Awareness. In: *Proceedings of the 24th Interaction Design and Children*. pp. 748–751. ACM, Reykjavik Iceland (Jun 2025). <https://doi.org/10.1145/3713043.3731475>
32. Stellmacher, C., Ternieten, J., Soroko, D., Schöning, J.: Escaping the Privacy Paradox: Evaluating the Learning Effects of Privacy Policies With Serious Games. *Proceedings of the ACM on Human-Computer Interaction* **6**(CHI PLAY), 1–20 (Oct 2022). <https://doi.org/10.1145/3549495>
33. Suknot, A., Chavez, T., Rackley, N., Kelley, P.G.: Immaculacy: A game of privacy. In: *Proceedings of the First ACM SIGCHI Annual Symposium on Computer-human Interaction in Play*. pp. 383–386. ACM, Toronto Ontario Canada (Oct 2014). <https://doi.org/10.1145/2658537.2662971>
34. Tian, Y., Chu, S.Y., Liu, Y., Jin, H.: Panopticon: The Design and Evaluation of a Game that Teaches Data Science Students Designing Privacy. *Proceedings on Privacy Enhancing Technologies* **2025**(3), 398–414 (2025). <https://doi.org/10.56553/popets-2025-0105>
35. Tjostheim, I., Ayres-Pereira, V., Wales, C., Manna, A., Egenfeldt-Nielsen, S.: Dark Pattern: A Serious Game for Learning About the Dangers of Sharing Data. *European Conference on Games Based Learning* **16**(1), 774–783 (Sep 2022). <https://doi.org/10.34190/ecgbl.16.1.872>
36. Williams, M., Nurse, J.R., Creese, S.: Smartwatch games: Encouraging privacy-protective behaviour in a longitudinal study. *Computers in Human Behavior* **99**, 38–54 (Oct 2019). <https://doi.org/10.1016/j.chb.2019.04.026>
37. Yuan, X., Ye, H., Tang, Z., Zhu, X., Yao, Y., Tong, X.: RedCapes: The Design and Evaluation of a Game Towards Improving Autistic Children’s Privacy Awareness. In: *Proceedings of the Eleventh International Symposium of Chinese CHI*. pp. 110–126. ACM, Denpasar, Bali Indonesia (Nov 2023). <https://doi.org/10.1145/3629606.3629618>
38. Zempila, G., Xinogalos, S.: Investigating the role of serious games on raising students’ awareness on safety and data protection on the Internet. *Discover Education* **4**(1), 268 (Aug 2025). <https://doi.org/10.1007/s44217-025-00722-0>