Privacy Nudges and Informed Consent? Challenges for Privacy Nudge Design

Verena Zimmermann

1 Introduction to Nudging

Nudges, a term coined by Thaler and Sunstein [49], describe small decision interface tweaks supposed to support decision-making without restricting the choice set and by activating automatic cognitive processes. Much-cited examples include the image of a fly in urinals to avoid spilling or the formulation of opt-in defaults to increase the number of organ donors [49].

As several definitions of a nudge have been suggested [33] and to distinguish the nudge from related concepts such as information provision or feedback, the definition box provides an overview on common features of a nudge. For a detailed discussion and derivation of these aspects, the reader is referred to Zimmermann and Renaud [56]. First of all, a nudge is supposed to be applied for the good of the nudgee as opposed to, e.g., the good of the nudge designer or service provider [49]. Furthermore, a nudge should not restrict the choice set, i.e., no choice should be removed or prohibited. Here, it is important to distinguish between choices and options (also see [33] for a discussion of that aspect). For example, removing large plates at a buffet and only leaving small plates to reduce calorie intake instead would limit the number of options (large and small plates versus only small plates). However, the choice to eat as much as one likes would not be restricted if people were still allowed to refill their plate at the buffet without additional charge. This brings us to the next feature: Nudges should not make one choice significantly more costly than the others, be that in terms of money, time, effort, or social sanctions [25]. This feature distinguishes the nudge from the concept of financial incentivization. Next, nudges as an intervention should be implemented

V. Zimmermann (✉)
ETH Zürich, Zürich, Switzerland
e-mail: verena.zimmermann@gess.ethz.ch

N. Gerber et al. (eds.), *Human Factors in Privacy Research*,
https://doi.org/10.1007/978-3-031-28643-8_8

with care and purpose to reach an intended and predicted outcome [23, 49]. Thus, nudges should predictably influence decisions as compared to arbitrary deployed nudges producing unintended outcomes or side effects. Finally, nudges make use of automatic, cognitive processes to encourage a certain choice [12, 22, 25, 49]. Thus, with regard to dual information theories [27, 39, 45] that generally distinguish between System 1 (fast, automatic, and implicit information processing) and System 2 (slow, rational, and explicit information processing), nudges primarily target System 1 information processing. Automatic cognitive processes comprise biases, heuristics, norms, and learned associations. An example is the human tendency to comply with social norms.

Social norm nudges may thus show that one choice is socially more acceptable or that the majority of users tend to make the same choice. The chapter "The Hows and Whys of Dark Patterns: Categorizations and Privacy" provides further explanations on System 1/System 2 information processing and provides a table with more examples of heuristics and biases.

Definition: Nudges

- Are intended for the good of the nudgee.
- Retain the original choice set.
- Do not make one choice significantly more costly than the others.
- Predictably influence toward a predicted outcome.
- Target automatic cognitive processes.

see [12, 22, 25, 25, 33, 49, 56]

2 An Overview on Privacy Nudges

Digital privacy decisions are very complex for users as it is very difficult to determine what kind of data is actually collected, processed, and what future consequences and vulnerabilities may potentially arise from the decision [1]. Furthermore, privacy decisions include making nuanced trade-offs with other factors such as convenience, usability, or functionality. Besides, privacy is seldom the user's primary task [1]. Given that users are confronted with a plethora of decisions every day and that their cognitive resources to evaluate all options are limited [43], nudges appear to be a promising approach to facilitate privacy decisions for the user. Indeed, nudges have successfully been deployed beyond the physical context to support users in making a "wise" choice with regard to digital privacy decisions.

Privacy-related nudge examples include Choe et al.'s [15] use of framing nudges to encourage privacy-friendly app choices. The authors visualized the app's privacy rating and framed it either in a positive or a negative way [14]. The visualizations generally were effective in influencing the users' decisions. The framing played a role for apps with a low privacy rating, e.g., the trustworthiness for apps with a low privacy rating was lower when the privacy rating was framed positively. Apart from users, also the app developers' perspective was analyzed with regard to privacy by Balebako et al. [7]. Based on interviews and a survey with developers, the authors conclude that nudges might be a promising way to help developers overcome privacy-related hurdles such as difficulties with reading privacy policies.

Other privacy nudges analyzed by Balebako et al. [8] or Almuhimedi et al. [4] aimed to discourage unintended location disclosure. Balebako et al. [8] studied an application called Locaccino that supports users in controlling when they make their location visible to others. Almuhimedi et al. [4] provided smartphone users with an app permission manager that also included privacy nudges. For example, one privacy nudge made users aware of how many times the location has been shared with which app to encourage users to make changes to the settings. The study results showed that the implemented privacy nudges can increase the utility of the permission manager.

Masaki et al. [34] used social nudges to reduce potentially risky choices in terms of privacy, such as image disclosure, in social network services. Similar to Choe et al. [15], Masaki et al. [34] also studied framing effects in this context. The social nudges were formulated as, e.g., "90% of users would not share..." as compared to "10% of users would share...." They found that people were less likely to make potentially risky choices when presented with negative framing. However, the authors also found that the nudges can be helpful in scenarios in which people have polarized opinions but that the nudges were not effective in scenarios in which people already support privacy-concerned choices. This finding indicates challenges in designing nudges across application scenarios.

Wang et al. [52, 53] also trialed privacy nudges to discourage disclosures on social networks that users might regret later. The analyzed nudges included visual reminders of the audience of the post, a time delay before posting, and feedback about how other users might perceive the post. While time delay and the visual reminder of the audience overall have been found to be a promising way to prevent unintended disclosure, especially the time delay nudge has not only been rated as beneficial but also annoying and intrusive. A potential explanation might be the higher "cost" in terms of time related to that nudge. This example also shows the challenge to design nudges that do not make one option significantly more costly than the others. For example, while a time delay of 10 s as implemented in the study by Wang et al. [52] might be rated as a burden, a time delay of five seconds might have been found more acceptable. The authors also found that the perceived benefit of the privacy nudges depended on how a person used social networks. For example, it was perceived as beneficial by individuals posting personal thoughts but less so by people who actively aimed to share information, e.g., for commercial purposes. This finding hints at different user preferences posing a challenge to design a nudge that is unanimously perceived as good by the users as intended by the nudge definition. For a description of further applications of security- and privacy-related nudges, the reader is referred to Acqusiti et al. [1].

3 Ethical Considerations

Despite the various well-intended and often successful examples of privacy nudges described above, the application of nudges is associated with several challenges. Nudging is often labeled as a soft paternalistic approach [1]. That is because nudges encourage a certain choice but do not restrict the original choice set to retain freedom of choice. In contrast, bans or laws would actively limit the choice set or require a certain choice.

However, a general criticism concerns the potential manipulation of users by nudges targeting automatic and perhaps unaware cognitive processes [23]. One concern is that nudges might lead users to make choices they might not have made without the nudge [55]. For example, a default nudge in a software wizard might be difficult to detect and go unnoticed by the users leading them to automatically installing unnecessary and unwanted software features.

A related concern is that the intended freedom of choice and human autonomy are actually endangered if users are not fully aware of their choices and the reasons for them [29, 35]. Furthermore, the role and the power of the choice architect, i.e., the person who designs and implements the decision interface including the nudge, is questioned [36]. Who is to say what the "wise" choice for the user is? In the context of security and privacy decisions, the selection of the wise choice might well change over time with technological advancements (e.g., server capacity), depend on the sensitivity of the data (e.g., banking data vs. a forum), or the target user group (e.g., lay users vs. experts).

As with many other technologies or mechanisms, the power of the choice architect or that of the nudge itself can be misused to nudge users away from what is good for them and toward what is good for the service provider or choice architect. Examples of nudges not applied for the good of the user—the so-called sludges [48] or dark patterns [37]—include attempts to sell products not needed by the user or to make the user provide personal information not necessary for a service. For the interested reader, the chapter "The Hows and Whys of Dark Patterns: Categorizations and Privacy" deals with dark patterns as a strategy to make users select a privacy choice that is beneficial for the service provider but not necessarily for users.

A prominent argument for nudging, however, is that nudges are inevitable [1, 10, 47]. Every design decision, purposefully made or arbitrary, can influence the user decision. Examples include the positioning of options, the use of colors and visualizations, or the formulation of instructions. The supporters of nudging thus argue that nudges should better be purposefully and ethically designed for the good of the user rather than influencing in unintended and perhaps negative ways. Another argument for the active use of nudges is that these can be helpful in supporting users to navigate the huge amount of complex decisions they are confronted with on a daily basis [9].

Yet, even the supporters of nudging argue for the use of transparent nudges [49] to counteract unethical deployments and to address the concerns associated with manipulation through the nudge's potentially hidden influence. Hansen and Jespersen [23] propose a taxonomy of transparent vs. non transparent and Type 1 vs. Type 2 nudges. While Type 1 nudges primarily target automatic cognitive processes, Type 2 nudges engage reflective thinking via activating automatic cognitive processes. As an example for transparent Type 2 nudges, Hansen and Jespersen [23] list green footprints leading to dustbins that aim to encourage people to use the bins rather than throw rubbish into the environment. The green footprints are easily visible for people, and their intention becomes clear when reflecting on the green color (i.e., green may be associated with something good or nature protection) and their path leading to the dustbins. In terms of ethical considerations, Hansen and Jespersen argue for the use of transparent Type 2 nudges.

Yet, the discussion calls for guidance that supports the choice architects such as service providers in designing ethically favorable and transparent nudges. Therefore, the following sections review and present guidelines for the design of ethical privacy nudges as detailed in Renaud and Zimmermann [41]. They are based on ethical guidelines for psychological research such as described by the British Psychological Society [50] or the American Psychological Association [5].

Respect for Persons Nudges should be designed in a way that they acknowledge all people regardless of individual differences such as age, gender, or religion. They should not treat certain groups of people unfairly. Ethical checklist questions addressing this principle described in [41] include whether the user is aware of the nudge or that an experiment is undertaken in case of nudge research, respectively. If the user is somehow deceived or not informed beforehand, this should be well justified. In addition, users should then be debriefed.

Beneficence Nudges should be beneficial. Furthermore, users should be protected from harm or risks. Researchers or practitioners implementing nudges should thus check whether the benefit of the intended nudge has already been analyzed and if not, evaluate their benefit. Further consideration should be given to who benefits from the nudge, e.g., individuals or society at large. Users should further have the option to contact the choice architects if the nudge is not perceived as beneficial.

Justice Nudges should be just in that all people should be eligible to benefit without having to overcome undue burdens. Ethical checklist questions for this criterion thus ask whether all users can indeed benefit equally and which measurements have been undertaken in this regard. When conducting research on or using the nudge, potential concerns should be analyzed. These may, for example, be concerned with accessibility or unintended side effects of the nudge for certain groups.

Scientific Integrity The design and evaluation of the nudge should be informed by ethical and scientific standards. Based on this ethical criterion and the nudge definition's aspect to predictably influence, the design of the nudge should be based on previous research, e.g., previous empirical results or theoretic models. The designed nudge should match the implementation context such as the type of the targeted decision (e.g., a simple A/B decision vs. a complex decision).

Social Responsibility The design of nudges involves a social responsibility that should be considered, e.g., in terms of expected as well as unexpected consequences of the nudge. In terms of the ethical checklist detailed in [41], this means that researchers and practitioners should give thought to the nudge's consequences beyond the intended immediate influence on the decision. For example, also the long-term consequences should be monitored, and measures to avoid or decrease potential negative effects should be implemented. There should also be an option to deal with potential negative effects such as removing or replacing the nudge.

4 Challenges of Designing Privacy Nudges

Besides the challenges discussed above, privacy nudges require additional considerations. Identifying the "wise" choice that the user should be nudged to is challenging per se as this can vary between different groups of users, with technological advancements or new scientific insights. For example, what has been considered a good password ten years ago, might not apply any more as technologies for guessing passwords greatly advanced. The choice architect thus bears a great responsibility. The case of privacy nudges, however, is especially challenging in this regard.

For example, in terms of security decisions, such as the choice of an encrypted versus unencrypted public Wi-Fi, it is often clear which option is the more secure and thus the "wiser" choice for the user from a security perspective. Likewise, it is often easy to distinguish the more privacy-preserving option from the less privacy-preserving one. Examples are provided by the privacy nudge studies described above, such as location disclosure versus non-disclosure [4, 8] or the choice of a privacy-friendly as compared to a privacy-invasive smartphone application [15].

However, with regard to privacy, the choice is less clear when considering legal requirements. Current EU regulations such as EU-GDPR [18] suggest data minimization as a principle (EU-GDPR Article 5), i.e., the collection of data that are adequate, relevant, and necessary for the intended purpose. However, GDPR neither prohibits the collection of personal data nor prescribes the automatic selection of the more privacy-preserving option. Instead, the decision to consent to the data processing rests with the user (EU-GDPR Article 6). For the user to be able to make an informed decision, the processor needs to provide the relevant information in a transparent, concise, intelligible, and accessible way (EU-GDPR Article 12). Consenting should be as easy as withdrawing (EU-GDPR Article 7).

What does that mean for the design of privacy nudges? In line with the current legislation, already [23] Sunstein and Thaler agreed: Nudges should be applied "for good" [23]—as considered by the users themselves. Yet, from that aspect, a challenge that has also been discussed by others including Acquisti et al. [1], Albrecht [2], and Hagman et al. [21] arises: How can the "for good" aspect of the nudge be measured? One distinction of nudges is into nudges that are intended for the good of the individual user, i.e., pro-self, or for societal goals, i.e., pro-social [21]. The informed consent suggestion of EU-GDPR suggests that when it comes to privacy, the individual good is concerned. However, this might not necessarily be the most privacy-preserving option. Of course, users can choose—and might often be willing to do so—to withdraw or to select the more privacy-preserving option. However, users might also decide to consent to more excessive data processing considering convenience, functionality, social aspects, or other factors. For example, users might knowingly prefer a more privacy-invasive messenger to a privacy-friendly one if the privacy-invasive one is easier to use, provides more features, or is used by most friends and relatives. Yet, what is the criterion for measuring the success of the nudge then? The happiness of the user with the decision (or minimum regret, respectively [1])? The majority of users agreeing to the choice nudged to or the alignment of individual stated preferences with the decision as suggested by Acquisti et al. [1]? The short-term or the long-term preferences? These questions mirror the discussion in the section on ethical considerations about the power and responsibility of the choice architects to design and evaluate the nudge in line with the users' intentions.

An additional challenge with the informed consent approach lies with the term "informed." First, even though required by GDPR, can we assume that users always read and understand the provided information to make an informed decision? Previous research indicates that this is unlikely: Privacy information is often lengthy, complicated and thus seldom read [38]. Second, nudges might not be the ideal mechanism to address or change that. As defined in the introduction, nudges primarily target automated cognitive processes such as heuristics and biases rather than targeting rational information processing. Thus, as also criticized by the opponents of nudging, a "nudged" decision is not necessarily an informed one depending on the nudge design. The next section therefore discusses several approaches to designing privacy nudges in line with ethical considerations and the GDPR approach for informed consent.

5 Discussion of Approaches

Apart from privacy-preserving nudges, this chapter also discusses options for and challenges associated with designing privacy nudges that align with the suggestion for informed consent.

5.1 Design of Privacy-Preserving Nudges

So far, many privacy nudges described in the literature have been designed as preventative nudges that aim to encourage the more privacy-preserving choice, such as preventing unintended disclosure in social networks. And there seems to be a good reason for that. First, granting access to personal information or disclosing personal data cannot always be reversed. For example, when disclosing privacy-invasive information in posts within social networks, it can be stored or shared by others even before the user has the option to delete the information. Likewise, when the user agrees to sharing personal data with service providers who might again share the information with third parties, it might be difficult to impossible to revoke that later. Also, research showed that users sometimes regret their choice to disclose later [54].

Second, service providers that have an interest in the user's personal information for financial or marketing reasons might deploy strategies to encourage users to choose the more privacy-invasive option, the so-called sludges [48] or dark patterns [20, 37]. They have, for example, been studied in detail in the context of cookie banners that nudge users to accept all even if they are not necessary for the functionality of the service [19, 20, 30, 37, 44]. Thus, to protect the users from unintentionally disclosing information or to counteract existing dark patterns, it might make sense to nudge users toward the privacy-preserving option. Along with the mentality to rather be safe than sorry, it might be "wiser" for the users to first select the privacy-preserving option that can often easily be changed later rather than the privacy-invasive option that is not always easily reversible. Furthermore, privacy-preserving nudges can be helpful in identifying the privacy-preserving option in the first place in cases in which this is not easily visible for the user. For example, highlighting the privacy-preserving option can provide support for users searching for that option within the often lengthy and complicated privacy information.

However, as outlined in the section above, the privacy-preserving option might not always be the option perceived as most favorable by the user. As shown in the study by Wang et al. [52], the privacy-preserving nudges were not unanimously perceived as beneficial by all users, but less so by users who actively aimed to share information for financial reasons. Thus, when considering additional factors such as commercial interests, convenience, or functionality, users might willingly tend toward the more privacy-invasive option.

Therefore, when considering the GDPR requirement for informed consent, several implications for the design of privacy-preserving nudges arise:

- Privacy-preserving nudges should be transparent and easily visible for the user so that they are not nudged toward the privacy-preserving option unawares. The design of a nudge toward the privacy-preserving option bears the same ethical considerations as the design of a nudge toward other options. Here, the reader is referred to Hansen's and Jespersen's proposal of transparent Type 2 nudges [23] as described in the Ethical Considerations section. For example, labeling the privacy-preserving option as such or rating the privacy invasiveness of different options might be easily visible and understandable approaches allowing for an informed decision. In contrast, a default selection of the privacy-preserving option with the other options not easily visible or hidden behind a button might lead users to accept the default selection without being aware what they agreed to.

- The selection of the more privacy-invasive option should be as easy as the selection of the more privacy-preserving option. Following the above example, hiding the privacy-invasive options behind buttons, or forwarding users to separate pages, would pose an additional effort for the user.
- Ideally, measures should be in place to detect a potential mismatch between the implemented nudge and the users' wishes. For example, testing the nudge in a study before its actual implementation in practice might reveal deviations between the researcher's and the users' intentions. In real-life settings, users might have the option to express thoughts or concerns concerning the nudge design via provided contact details or survey instruments. If a mismatch or unintended side effects are detected, the nudge design can be adapted accordingly.

5.2 Design of Nudges that Target Reflective Thinking

Another option to address the requirement for informed privacy decisions might be to design nudges that do not directly target either the more or the less privacy-preserving option, but the interaction or engagement with the decision as such. The question is: Can we design nudges that encourage users to read privacy policies? Or can we design nudges that make users reflect on their choice? As described in the definition section, the nudges per se do not primarily target reflection and rational information processing. Thus, measures that directly prompt reflection on the decision might exceed the definition of the nudge. Examples might be an intervention that asks users to reflect on their choice before they can proceed and to rate all options in terms of their perceived privacy invasiveness on a scale ranging from 1 to 10, or to ask users to write down a reason for their choice. This does not mean that these interventions are not feasible, but only that they might not be classified as a nudge. For a discussion on ideas for combining nudges with other approaches, see Sect. 5.4.

However, nudges might still be used as a tool to encourage users to choose options that include reflective elements. Furthermore, certain types of nudges, i.e., transparent Type 2 nudges [23], might have the potential to activate reflective information processes via automatic cognitive processes. Even though further research on these questions is definitely needed, examples from related research areas provide ideas on what nudges that target reflective thinking could look like. For example, Caraban et al. [13] conducted a literature research on nudging in the HCI domain and categorized the nudges according to their mechanism such as facilitation, confrontation, or reinforcement.

The following list details ideas on nudges that may foster engagement with privacy information, reflection on the decision, or throttle quick unthinking choices.

Engaging with privacy information:

- In general, the same nudge mechanisms deployed to encourage, e.g., the privacy-preserving choice might be applicable to encourage users to read a short text, to look at a graphical description of the privacy policy, or to click on a button labeled "more information." These may include visual highlighting (e.g., bold text or green color), positioning (e.g., upmost or central position), social comparisons (e.g., an indication that reading the information is socially desirable), or the default selection of the choice (e.g., button "more information" is pre-selected). However, it remains unclear whether nudging users to, e.g., click on a button labeled "more information" actually leads to users engaging with the text behind the button or rather to frustration that the privacy decision is delayed. Thus, nudges in this regard should be designed carefully with a focus on the effort for the user and evaluated in future work.

Reflecting on the decision:

- As outlined above, designing nudges that target reflection on the decision is a challenging task as the original definition of the nudge includes targeting automatic cognitive processes instead of reflective cognitive processes.
- In the context of information disclosure, some studies successfully tested nudges that made users aware of and potentially reflect on the consequences of their choices. For example, Wang et al. [52, 53] confronted users with visual reminders of the audience of their social media post to prevent them from disclosures they might regret later. Harbach et al. [24] made users aware of the potential consequences of the app permissions granted. For example, if an app had been granted access to the user's photos, the user was shown a random photo stored on their phone along with the message that the specific app had access to this photo.
- A common password nudge is a so-called password meter [17, 51, 56]. It often takes the form of a bar that dynamically provides visual and textual feedback on the strength of the currently selected password. It is supposed to nudge users to increase password strength and close potential gaps between user's security perception and technical security requirements. This type of nudge can be classified as a transparent Type 2 nudge as it is not only easily visible for the user but also triggers reflective processes. For example, users might ask themselves why their password score is low and try to enhance their score so that the bar fills and changes its color from red to green. Thereby, users might reflect on the changes they made to their password. Similar feedback meters have already been applied to other authentication mechanisms such as pattern unlock [46] and might also be helpful for supporting informed privacy decisions. For example, users might receive feedback on the "privacy score" of their selected option that might trigger them to rethink their choice and to try different options to see how the score changes. A similar approach has already been tested in the context of privacy risks related to app permissions by Kang et al. [28].

Throttling mindless choices:

- In the contexts of phishing [6] and information disclosure in social networks, nudges [52, 53] have been trialed that aim to prevent quick, unthinking choices, e.g., by implementing a timer. After users have made a selection, a timer delays the realization of the choice for some seconds providing users with the option to cancel the process or change their selection. While Wang et al. [52, 53] generally evaluated the delay nudge as a promising approach, it was not unanimously liked by all users, but also rated as annoying. Further research might be necessary to find a good balance for the timer, i.e., the time should be long enough to rethink and change the selection while not being perceived as significant burden. Also, options to skip the timer as implemented by Wang et al. might be a suitable compromise.

5.3 Ask the Users

Several researchers have argued that nudges are not “one-size-fits-all” solutions [11, 13, 26], but that their effectiveness depends on the characteristics of the individual user, their aims, and the context the nudge is deployed in. As such, it cannot be assumed that all users in all contexts favor the same privacy decision or might benefit similarly from the same choice. As an example, the study by Wang et al. [52] revealed that users who had a financial interest in disclosing information rated the privacy-preserving nudges differently than people who had no financial interests. Therefore—and in line with the requirement for informed consent—some researchers suggest personalization of nudges. The following list provides some examples:

- Acquisti et al. [1] suggest designing nudges for disclosures that users are likely to regret later (e.g., when made under the influence of alcohol) or that align behavior with stated preferences. As an example, they describe that many users are concerned about disclosing their political or religious affiliation with potential employers. These specific cases might thus be contexts in which privacy-preserving nudges are warranted as compared to deploying privacy-preserving nudges across all types of data disclosure.
- Another option for personalizing nudges is provided by personalized privacy assistants (PPAs) that first ask users for their preferences and needs before supporting them in implementing these preferences across decisions or services. Examples are provided by Liu et al. [32] who implemented and tested a PPA for mobile app permissions that also included daily privacy nudges. Das et al. [16] summarize current research on PPAs for the Internet of Things with a focus on the infrastructure that is needed to detect nearby sensors and devices and to inform users about their data-handling practices (see also the chapter “Increasing Users’ Privacy Awareness in the Internet of Things: Design Space and Sample Scenarios” for a discussion of this topic). Salem et al. [42] designed a nudge-based recommender system for social media use. It balances recommendations for privacy protection with individual preferences and sharing needs. The system objectively evaluates risks and compares these with the users’ personal willingness to share personal information, i.e., their subjective privacy

threshold. The users' behavior following the system's recommendations is then again used to update the subjective threshold.

5.4 Choose a Combination of Approaches

Finally, nudges are not the only or the exclusive way forward. Even though they have been shown to be effective measures across many physical and digital decision contexts, including security and privacy decisions, other measures might be equally or even more suitable for certain cases. This includes interactive approaches that support users in reaching their aims, such as the use of gamification or persuasive technologies. Furthermore, when focusing on the "informed" in informed consent, measures that primarily target rational information processing, such as information provision, feedback mechanisms, or reflection might be beneficial. Here, it is important to mention that sometimes the border between nudges and other forms of interventions is not crystal clear. Certain types of nudges such as password meters also provide users with feedback. Others, such as privacy ratings of app permissions, also transport privacy information. Likewise, nudges are often included in larger gamified environments as motivational elements as illustrated in the examples below. However, when we understand nudges and related interventions as a toolbox to support users in making privacy-related decisions, this is not a problem but can be an advantage. The combined power of approaches may lead to positive outcomes that cannot be achieved by the exclusive use of one strategy. Depending on the deployment context and the aim of the researcher, it is just important to be aware of the limits of certain strategies and of potential side effects triggered by the combination of approaches. There might be combinations of strategies that contradict each other or that reduce the impact of the other strategy. Thus, careful consideration is necessary not only when designing a nudge but also when combining nudges with other approaches.

For example, nudges are known to make use of automatic and perhaps unaware cognitive processes. This raises the question of whether the power of nudges is reduced when combining them with information that targets rational and aware information processing. Research in this regard has shown that the combination of nudges and information provision, also labeled as hybrid nudge [56], can have beneficial rather than adverse effects as outlined in the examples below. Also Sunstein agrees that nudges can be educative and that nudges and education do not contradict but can complement each other [47]. By targeting both System 1 and System 2 information processing, the combination of approaches may be a suitable option for nudging toward informed consent to privacy decisions.

The following list illustrates some examples of combining nudges with other mechanisms but is of course not exhaustive. Other combinations have already been trialed or are well possible and should be further investigated:

- Kroese, Marchiory and de Ridder [31] combined nudges and information provision outside the privacy and security context: To encourage healthy food choices, they repositioned food in a store. They found that healthy food choices increased, regardless of whether the intervention was not disclosed to customers or transparently combined with an information sign that explained the intervention. Thus, even though customers were aware of the nudge, this did not diminish its effectiveness. Furthermore, many customers agreed with the intervention as it aligned with their own intention for healthy food choices. This implies that bringing nudges to the users' awareness and combining it with information may also have the advantage of facilitating the detection of mismatched nudges.
- Zimmermann and Renaud [56] tested the impact of no intervention, a nudge, information provision, and a combination of a nudge and information, i.e., a hybrid nudge, in the context of four different security- and privacy-related decisions. This included password selection, the choice to encrypt one's smartphone, the choice of a public WiFi, and the selection of a cloud service provider. Across all decisions and nudges deployed, the study revealed that the hybrid nudge was always at least as or even more effective in encouraging secure choices as compared to single nudging or information provision.
- In a study by Petrykina, Schwartz-Chassidim and Toch [40], nudges were included into a gamification environment called security bot that rewards secure online behavior. Their results revealed a reduction of downloaded malware without reducing productivity.
- Alemany et al. [3] included personalized privacy nudges into an online social network called PESEDIA that also had the purpose to educate users about privacy and to enhance awareness for privacy risks.

6 Summary

Overall, the key points with regard to designing privacy nudges can be summarized as follows:

- Privacy nudges aim to support users in making complex privacy decisions by purposefully altering the decision interface to encourage the "wise" choice. They are intended for the good of the user and work by targeting automatic cognitive processes. Nudges do not limit the choice set nor do they make one option significantly more costly.
- Numerous examples from the literature show that privacy nudges can successfully influence users' privacy decisions, e.g., by increasing awareness for data sharing practices or visualizing privacy ratings.
- The design of privacy nudges requires ethical considerations given that nudges target automatic cognitive processes and thus might not always be visible or comprehensible for the user. Ethical guidelines therefore call for transparent

nudges designs that are noticeable for the user so that they can resist their influence in case it does not align with their intentions.

- Another challenge is the selection of the "wise" or "good" choice, respectively. Given rapid technological advancements and legal guidance suggesting informed consent rather than the automatic selection of the most privacy-preserving option, it is difficult to determine which option is actually intended for the good of the user.
- This chapter discusses four approaches to address this challenge:
  - *Design of privacy-preserving nudges:* Often privacy nudges are designed to encourage the privacy-preserving option as the one protecting users from potentially unintended data disclosure. These nudges should be designed transparently so that users can easily identify the most privacy-preserving option but can also easily select another option.
  - *Design of nudges that target reflective thinking:* Certain types of nudges can activate reflective System 2 information processing via targeting automatic System 1 information processing. These nudges might be used to nudge users toward engaging with the privacy decision rather than toward a final decision.
  - *Ask the users:* User intentions can vary depending on individual preferences and needs. One option would thus be to first ask the users for their privacy preferences before implementing nudges that align with the users' aims.
  - *Choose a combination of approaches:* Nudges can be successfully combined with other approaches such as information provision or feedback. These combinations have the potential to encourage a certain choice while informing users on the reasons for or implications of that choice.

References

1. Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR), 50*(3), 1–41.
2. Albrecht, L. (2017). How behavioral economics is being used against you. MarketWatch https://www.marketwatch.com/story/nobel-prize-winning-economist-richard-thalers-nudge-theory-has-a-dark-side-too-2017-10-17
3. Alemany, J., del Val, E., & García-Fornes, A. (2020). Assisting users on the privacy decision-making process in an OSN for educational purposes. In *International Conference on Practical Applications of Agents and Multi-Agent Systems* (pp. 379–383). Springer.
4. Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Cranor, L. F., & Agarwal, Y. (2015). Your location has been shared 5,398 times! A field study on mobile app privacy nudging. In *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI)* (pp. 787–796). ACM.
5. American Psychological Association. (2016). Ethical principles of psychologists and code of conduct. http://www.apa.org/ethics/code/

6. Antonucci, A. E., Levy, Y., Dringus, L. P., & Snyder, M. (2022). Experimental study to assess the impact of timers on user susceptibility to phishing attacks. *Journal of Cybersecurity Education, Research and Practice, 2021*(2), 6.
7. Balebako, R., & Cranor, L. (2014). Improving app privacy: Nudging app developers to protect user privacy. *IEEE Security & Privacy, 12*(4), 55–58.
8. Balebako, R., Leon, P. G., Almuhimedi, H., Kelley, P. G., Mugan, J., Acquisti, A., Cranor, L. F., & Sadeh, N. (2011). Nudging users towards privacy on mobile devices. In *Proceedings of the CHI Workshop on Persuasion, Nudge, Influence and Coercion* (pp. 1–4). ACM.
9. Blumenthal-Barby, J. S., & Naik, A. D. (2015). In defense of nudge–autonomy compatibility. *The American Journal of Bioethics, 15*(10), 45–47.
10. Brooks, T. (2013). Should we nudge informed consent? *The American Journal of Bioethics, 13*(6), 22–23.
11. Brown, P. (2012). A nudge in the right direction? Towards a sociological engagement with libertarian paternalism. *Social Policy and Society, 11*(3), 305–317.
12. Calo, R. (2014). Code, nudge or notice? *Iowa Law Review, 99*, 773.
13. Caraban, A., Karapanos, E., Gonçalves, D., & Campos, P. (2019). 23 ways to nudge: A review of technology-mediated nudging in human-computer interaction. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19 (pp. 1–15). Association for Computing Machinery.
14. Castano, E., Yzerbyt, V., Paladino, M.-P., & Sacchi, S. (2002). I belong, therefore, I exist: Ingroup identification, ingroup entitativity, and ingroup bias. *Personality and Social Psychology Bulletin, 28*(2), 135–143.
15. Choe, E. K., Jung, J., Lee, B., & Fisher, K. (2013). Nudging people away from privacy-invasive mobile apps through visual framing. In *Proceedings of the IFIP Conference on Human-Computer Interaction* (pp. 74–91). Springer.
16. Das, A., Degeling, M., Smullen, D., & Sadeh, N. (2018). Personalized privacy assistants for the Internet of Things: Providing users with notice and choice. *IEEE Pervasive Computing, 17*(3), 35–46.
17. Dupuis, M., & Khan, F. (2018). Effects of peer feedback on password strength. In *Proceedings of the APWG Symposium on Electronic Crime Research (eCrime)* (pp. 1–9). IEEE.
18. EU GDPR Compliant (2018). Cookies consent under the GDPR. February 14 https://eugdprcompliant.com/cookies-consent-gdpr/
19. Graßl, P., Schraffenberger, H., Zuiderveen Borgesius, F., & Buijzen, M. (2021). Dark and bright patterns in cookie consent requests. *Journal of Digital Social Research, 3*(1), 1–38.
20. Gray, C. M., Santos, C., Bielova, N., Toth, M., & Clifford, D. (2021). Dark patterns and the legal requirements of consent banners: An interaction criticism perspective. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21. Association for Computing Machinery.
21. Hagman, W., Andersson, D., Västfjäll, D., & Tinghög, G. (2015). Public views on policies involving nudges. *Review of Philosophy and Psychology, 6*(3), 439–453.
22. Hansen, P. G. (2016). The definition of nudge and libertarian paternalism: Does the hand fit the glove? *European Journal of Risk Regulation, 7*, 155–174.
23. Hansen, P. G., & Jespersen, A. M. (2013). Nudge and the manipulation of choice: A framework for the responsible use of the nudge approach to behaviour change in public policy. *European Journal of Risk Regulation, 4*(1), 3–28.
24. Harbach, M., Hettig, M., Weber, S., & Smith, M. (2014). Using personal examples to improve risk communication for security & privacy decisions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14 (pp. 2647–2656). Association for Computing Machinery.
25. Hausman, D. M., & Welch, B. (2010). Debate: To nudge or not to nudge. *Journal of Political Philosophy, 18*(1), 123–136.
26. Johnson, E. J., Shu, S. B., Dellaert, B. G., Fox, C., Goldstein, D. G., Häubl, G., Larrick, R. P., Payne, J. W., Peters, E., Schkade, D., Wansink, B., & Weber, E. U. (2012). Beyond nudges: Tools of a choice architecture. *Marketing Letters, 23*(2), 487–504.

27. Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.
28. Kang, J., Kim, H., Cheong, Y. G., & Huh, J. H. (2015). Visualizing privacy risks of mobile applications through a privacy meter. In *International Conference on Information Security Practice and Experience* (pp. 548–558). Springer.
29. Kelly, D., & Morar, N. (2016). Nudging and the ecological and social roots of human agency. *The American Journal of Bioethics, 16*(11), 15–17.
30. Krisam, C., Dietmann, H., Volkamer, M., & Kulyk, O. (2021). Dark patterns in the wild: Review of cookie disclaimer designs on top 500 German websites. In *European Symposium on Usable Security 2021* (pp. 1–8). Association for Computing Machinery.
31. Kroese, F. M., Marchiori, D. R., & de Ridder, D. T. (2015). Nudging healthy food choices: A field experiment at the train station. *Journal of Public Health, 38*(2), e133–e137.
32. Liu, B., Andersen, M. S., Schaub, F., Almuhimedi, H., Zhang, S. A., Sadeh, N., Agarwal, Y., & Acquisti, A. (2016). Follow my recommendations: A personalized privacy assistant for mobile app permissions. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)* (pp. 27–41).
33. Marchiori, D. R., Adriaanse, M. A., & De Ridder, D. T. (2017). Unresolved questions in nudging research: Putting the psychology back in nudging. *Social and Personality Psychology Compass, 11*(1), e12297.
34. Masaki, H., Shibata, K., Hoshino, S., Ishihama, T., Saito, N., & Yatani, K. (2020). Exploring nudge designs to help adolescent SNS users avoid privacy and safety threats. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20 (pp. 1–11). Association for Computing Machinery.
35. Mitchell, G. (2004). Libertarian paternalism is an oxymoron. *Northwestern University Law Review, 99*, 1245–1277.
36. Murray, P. R. (2017). Who will nudge the nudgers. *Regulation, 40*, 55.
37. Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20 (pp. 1–13). Association for Computing Machinery.
38. Obar, J. A., & Oeldorf-Hirsch, A. (2016). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. In *Proceedings of the Research Conference on Communication, Information and Internet Policy (TPRC 44).*
39. Osman, M. (2004). An evaluation of dual-process theories of reasoning. *Psychonomic Bulletin & Review, 11*(6), 988–1010.
40. Petrykina, Y., Schwartz-Chassidim, H., & Toch, E. (2021). Nudging users towards online safety using gamified environments. *Computers & Security, 108*, 102270.
41. Renaud, K., & Zimmermann, V. (2018). Ethical guidelines for nudging in information security & privacy. *International Journal of Human-Computer Studies, 120*, 22–35.
42. Salem, R. B., Aïmeur, E., & Hage, H. (2020). A nudge-based recommender system towards responsible online socializing. In *OHARS@ RecSys* (pp. 23–39).
43. Simon, H. A. (1957). *Models of man; social and rational.* Wiley
44. Soe, T. H., Nordberg, O. E., Guribye, F., & Slavkovik, M. (2020). Circumvention by design—dark patterns in cookie consent for online news outlets. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society* (pp. 1–12). Association for Computing Machinery.
45. Stanovich, K. E., & West, R. F. (2000). Individual differences in reasoning: Implications for the rationality debate? *Behavioral and Brain Sciences, 23*(5), 645–665.
46. Sun, C., Wang, Y., & Zheng, J. (2014). Dissecting pattern unlock: The effect of pattern strength meter on pattern selection. *Journal of Information Security and Applications, 19*(4–5), 308–320.
47. Sunstein, C. R. (2015). Nudges do not undermine human agency. *Journal of Consumer Policy, 38*(3), 207–210.
48. Thaler, R. H. (2018). Nudge, not sludge. *Science, 361*(6401), 431–431.

49. Thaler, R. H., Sunstein, C. R., & Leonard, T. C. (2008). Nudge: Improving decisions about health, wealth, and happiness. *Constitutional Political Economy, 19*(4), 356–360.
50. The British Psychological Society (2014). Code of human research ethics. https://cms.bps.org.uk/sites/default/files/2022-06/BPS%20Code%20of%20Human%20Research%20Ethics%20%281%29.pdf
51. Ur, B., Alfieri, F., Aung, M., Bauer, L., Christin, N., Colnago, J., Cranor, L. F., Dixon, H., Emami Naeini, P., Habib, H., Johnson, N., & Melicher, W. (2017). Design and evaluation of a data-driven password meter. In *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI)* (pp. 3775–3786). ACM.
52. Wang, Y., Leon, P. G., Acquisti, A., Cranor, L. F., Forget, A., & Sadeh, N. (2014). A field trial of privacy nudges for Facebook. In *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI)* (pp. 2367–2376). ACM.
53. Wang, Y., Leon, P. G., Scott, K., Chen, X., Acquisti, A., & Cranor, L. F. (2013). Privacy nudges for social media: An exploratory Facebook study. In *Proceedings of the 22nd International Conference on World Wide Web*, WWW '13 Companion (pp. 763–770). Association for Computing Machinery.
54. Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P. G., & Cranor, L. F. (2011). "I regretted the minute I pressed share": A qualitative study of regrets on Facebook. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, SOUPS '11. Association for Computing Machinery.
55. Wilkinson, T. M. (2013). Nudging and manipulation. *Political Studies, 61*(2), 341–355.
56. Zimmermann, V., & Renaud, K. (2021). The nudge puzzle: Matching nudge interventions to cybersecurity decisions. *ACM Transactions on Computer-Human Interaction (TOCHI), 28*(1), 1–45.