Int. J. Human–Computer Studies 168 (2022) 102902

Contents lists available at ScienceDirect

International Journal of Human - Computer Studies

journal homepage: www.elsevier.com/locate/ijhcs

Reducing risk to security and privacy in the selection of trigger-action rules: Implicit vs. explicit priming for domestic smart devices

Phillip L. Morgan [a,b,*], Emily I.M. Collins [a], Tasos Spiliotopoulos [c], David J. Greeno [a,d], Dylan M. Jones [a]

[a] Centre for Artificial Intelligence, Robotics and Human-Machine Systems (IROHMS), Human Factors Excellence Research Group (HuFEx): School of Psychology, Cardiff University, 70 Park Place, Cardiff CF10 3AT, UK
[b] Visiting Professor at Luleå University of Technology, Psychology, Division of Health, Medicine and Rehabilitation, Sweden
[c] Newcastle University Business School, 5 Barrack Road, Newcastle upon Tyne NE1 4SE, UK
[d] School of Psychology, Cardiff University, 70 Park Place, Cardiff CF10 3AT, UK

ARTICLE INFO

Keywords:
Cyber security
Susceptibility
Priming
Individual differences
Trigger-action rules

ABSTRACT

Smart home device usage is increasing, as is the diversity of users and range of devices. Additionally, it is becoming increasingly common to interconnect devices (e.g., via trigger-action rules) which, while bringing benefits, can bring unforeseen security and privacy risks. Developing strategies to protect users as well as understanding what biographical or attitudinal characteristics contribute to these risks is a critical step for ensuring empowered, but safe, interconnected smart device usage. Using narrative descriptions of domestic smart devices, two experiments explored how the prevailing security/privacy contexts—priming conditions—in which 20 trigger-action rules (developed via a Delphi Study) were presented influenced the adoption of rules favoring either security or privacy. Both experiments contrasted three priming conditions: no prime, security prime, privacy prime. Experiment 1 (n = 254) used explicit priming, giving direct instruction to maximize a security *or* privacy outcome while Experiment 2 (n = 325) used implicit priming, with an apparently unrelated security or privacy problem-solving puzzle. Across both experiments, priming promoted safer rule adoption, markedly so when explicit. Explicit priming produced an asymmetry however: privacy priming improved privacy scores with security scores unchanged and security primes improved security scores while worsening privacy scores. Across experiments, two dimensions of user attitudes shaped riskier rule choice: *perceived benefits* of technology and pre-existing *trusting beliefs* in online companies. Our novel findings reveal that implicit and explicit priming shape safe use of trigger-action rules in domestic settings and that age, perceived trust and perceived benefits should be considered when designing safety messaging.

1. Introduction

The increased affordability and widening range of network-enabled smart devices means that more people than ever now have them in their homes. Statista (2021) predicted that 45.8% of UK households would have smart home technology in 2022 with this possibly increasing to 84.8% by 2026. However, alongside this growth, increasing concerns have been voiced about the security (i.e., controlling who can access, use, or alter data; Saltzer and Schroeder, 1975) and privacy (i.e., deciding when, how and to what extent information is made available to others; Westin, 1968) of smart home devices (Heartfield et al., 2018; McAlaney et al., 2018; Parks Associates, 2019; Sicari et al., 2015).

Undoubtedly, adoption of smart devices is motivated by their relative cheapness along with their perceived usefulness and ease of use (Yang et al., 2017). As their number and type increase, the potential for their joint use also increases. One way this can be achieved is via the use of *trigger-action rules*. These are rules created by the user to personalize the joint behavior of smart devices and online services (e.g., Corno et al., 2019a). For example, a user may create a rule that performs an automatic action (e.g., "Play Music") when a specific trigger (e.g., "When I return home") occurs. As the number of trigger-action rules, from an array of devices, increases then the size and complexity of domestic systems increases (see, for example, Zheng et al., 2018). Ultimately,

* Corresponding author.
E-mail address: morganphil@cardiff.ac.uk (P.L. Morgan).

https://doi.org/10.1016/j.ijhcs.2022.102902
Received 13 November 2021; Received in revised form 3 July 2022; Accepted 30 July 2022
Available online 3 August 2022

trigger-action rules allow end users to be free to fashion a system suited to their individual needs. However, while such bespoke systems increase functionality (and likely help promote user adoption), this complexity may have unforeseen consequences for security and privacy (see Manca et al., 2019) and have material consequences including increased risk to property and persons in the form of home invasion, burglary, and assault (Atlam and Wills, 2020). In our trigger-action rule example above then no music playing could indicate that the property is empty.

Aside from the possibility of ill-considered consequences of the selection and conjunction of conditional rules, bespoke systems may also lack safeguards from malevolent interference. Despite demand from users (e.g., Ogonji et al., 2020), the majority of smart and IoT devices are not created 'secure by design' when it comes to human-centered aspects of cyber security (Atlam et al., 2017), providing numerous avenues for potential attacks (Atlam et al., 2018) by malefactors with disruptive or criminal intent (Van Oorschot and Smith, 2019).

A system comprised of interconnected elements and without superordinate safeguards is only as strong as its weakest link (Atlam et al., 2018). A single smart device being hacked can easily infect other smart devices (e.g., Ronen et al., 2017) ultimately leading to a larger breach, such as an attack upon the entire home network (Check Point, 2020). The diverse nature of possible devices in terms of purpose, function, process, and design means that there is rarely a universal way in which all these devices can be protected (Dabbagh and Rayes, 2017). For instance, voice-controlled devices (e.g., *Amazon Echo, Google Home*) can be vulnerable to being accessed by those outside of the household (unless settings are chosen to prevent this), which then may grant control to devices such as smart light bulbs and thermostats, but also to the plethora of information these (and other) devices collect – e.g. giving an indication of when a house is likely occupied or not, sometimes without the householder's full understanding (Furey and Blue, 2018). Affording comprehensive protection requires the co-ordination of individual device-specific configuration, which consumers often find difficult and time-consuming (Woo and Lim, 2015; Zeng and Roesner, 2019).

Interconnectivity also means that data collected through one device can be shared or fed back through another, which in practice is an intrinsic feature of smart home devices (e.g., accessing information from a thermostat through a smartphone). However, it can cause privacy and/or security issues of which the user setting up a system may be oblivious. For example, information which is innocuous when shared in some situations (e.g., sharing details of a workout on social media), can be problematic in others (e.g., sharing details of a workout on social media whilst being absent from work due to illness; Surbatovich et al., 2017). Therefore, this facet of home security is made more acute when the data is sensitive, or alternatively, when data feels harmless enough to the user but can in fact reveal something more exploitable to malefactors – such as indications of when occupants are at home or not. Importantly, while many risks of smart home devices can be mitigated by careful configuration, up-to-date software and suitable authentication, there are still ways in which the privacy and security can be undermined through seemingly innocuous actions, for example, by the users of the systems.

2. Theoretical foundations

While rule-based applications have been addressed comprehensively through research (e.g., Barricelli et al., 2019) the focus has not typically been on the consequences to security/privacy but instead on usability and related concepts such as understandability, level of functionality, misinterpretation, errors, or rule conflicts (e.g., Brackenbury et al., 2019; Corno et al., 2019a; Desolda et al., 2017; Manca et al., 2019). Meta-level considerations of how the system meets the user's general objectives as it relates to privacy and security have received too little scrutiny given the potential risks. Very little research has focused on how effective users are at integrating trigger-action rules beyond simple cases, despite the likely impact on security and privacy. Typically, the purview of research does not extend much beyond the immediate functional purpose of the device. For instance, studies do not often consider that a social network site (e.g., *Facebook*) might be linked to a home security device (e.g., security camera) and the consequences for safety, security, and privacy this might entail (although, see Cobb et al., 2020 for some recent discussion).

With smart home device usage increasing and trigger-action rules allowing for bespoke and increasingly complex systems, it is necessary to develop and test strategies that maintain user freedom while simultaneously helping to avoid the types of unintended and unforeseen security and privacy costs outlined. We approach this problem by considering that stimuli within an individual's environment can activate, or *prime*, mental representations which consequently impact information processing and later thoughts, judgements, goals, and actions (e.g., see Bargh and Chartrand, 2000; Molden, 2014). Primes can be explicit and intentionally draw attention to them (e.g., highlighting words, using obvious phrases) or can be implicit and outside of people's awareness and both have been demonstrated to influence later behaviour. For example, making health related stimuli salient in the environment can promote healthier food choices or increases in physical activity (e.g., see Papies, 2016) and exposure to pro-environmental messaging can lead to more environmentally friendly consumer choices (Tate et al., 2014). Related to the present work, Chong et al. (2018) found that priming participants with privacy related information (e.g., reminders that personal information would be shared) helped participants make safer decisions as to which smartphone applications they downloaded. With priming successful in helping to shape behavior in many areas, we considered it a suitable candidate that could help to promote safe trigger-action rule enabling.

Given the dearth of previous work exploring trigger-action rules and their impact upon security and privacy we adopted an exploratory stance. We first developed hypothetical trigger-action rules (Delphi Study) with differential impacts on the security and privacy of a system. Then, in the two experiments that followed, the key independent variable was the context in which participants were asked to select rules they considered appropriate to activate. We contrasted one context in which security was primed, one in which privacy was primed and one in which no context was primed. Across experiments we manipulated the strength of the primed context, comparing explicit priming that provided directed and overt instructions to maximize either security or privacy (Experiment 1) and implicit priming (Experiment 2) where the context was merely the engagement in a task prior to the main experimental blocks of trials - that had either security or privacy considerations, free of direct instruction. Via the administration of questionnaires, we also collected biographical and attitudinal characteristics of the participants. As such, this gave us two primary research questions:

RQ1: Does the context under which trigger-action rules are first chosen engender less risky behavior in the selection of rules to be deployed?

RQ2: Is trigger-action rule-choice behavior linked to individuals' biographical or attitudinal characteristics?

3. Delphi study – developing trigger-action rules

When deciding upon trigger-action rules to be used in our experiments, there (to our knowledge) was no publicly available set of rules from which to draw stimulus materials. Importantly, while being representative of domestic use, it was important that any rules used were interesting, understandable, meaningful and, crucially, enshrined security and privacy considerations.

To achieve these aims we adapted the Delphi method to create a pool of trigger-action rules across three stages. The Delphi method involves the systematic collection and aggregation of informed judgment from a group of experts on specific questions and issues (see, for example, Donohoe and Needham, 2009; Linstone and Turoff, 1975). The panel for our Delphi study consisted of four participants—outside the group of

authors—each identified as an expert in security, privacy and/or human factors (one senior lecturer, one lecturer, a postdoctoral researcher partly seconded to industry as a senior scientist, and a doctoral student partly seconded to industry as a senior scientist).

The first stage was exploratory with the goal of enriching an initial set of rules devised by the research team and eliciting new suggestions from the panelists. Panelists were first shown an explanation of the study and its goal. Then, they were shown example rules from our initial corpus, with an associated 'vulnerability score'—one for security and one for privacy—and our rationale for the scores. They were then asked to generate five new rules each having security and/or privacy implications, with a vulnerability score for security and privacy along with a rationale for their assigned scores. It was emphasized to panelists that the rules be relevant, interesting, and have a meaningful balance between security and privacy.

In the second stage, panelists were shown rules selected by the research team from our original corpus and from the new rules generated in the first stage, along with their vulnerability scores and rationale. Then, we asked participants to give feedback on each of the rules; a new score if they deemed appropriate, a new rationale for a score, and any other comments.

The third stage had a similar setup to the second with the aim of reaching a final consensus on the rules and associated scoring. This adapted Delphi process was instrumental in enriching our original collection of rules and refining the scores and wording of the rules. Based on quantitative consensus measures for Delphi studies from the literature (Diamond et al., 2014; Parekh et al., 2017) and our own interpretation of the qualitative answers, we determined which of the rules had reached consensus among the participants. Of these, twenty rules were selected to be used in the experiments based on their relevance, interestingness, and balance between security and privacy implications and each had a privacy and security weighting associated with it (see below for two examples). Appendix A contains the full corpus of trigger-action rules that were identified and refined through this process, together with specific comments about the assumptions made in their selection and scoring.

RULE

Unlock the smart lock of my front door by voice (e.g., when I say 'Alexa, unlock the door', my front door unlocks).

- Security weighting: -4. Rationale: Someone might trick it by saying the phrase from outside (Symantec, 2017), and more recent work suggests that an adversary can control such systems by injecting laser-based voice commands from a great distance (Sugawara et al., 2020). It also explicitly ties the smart lock to an Amazon/Google account - thereby increasing the risk from a compromised online account.
- Privacy weighting: -1: Rationale: Ties the smart lock to an Amazon/Google account, i.e., Amazon/Google can build up data on patterns of behavior, such as when someone is at home or out.

RULE

If I'm the last person in the house and leave, send a notification to my smartwatch if any window in the house is open.

- Security weighting: +2. Rationale: Makes sure that I don't leave any windows open.
- Privacy weighting: -2. Rationale: The smart house knows where the rest of the household are (or at least that they are not at home).

The 20 trigger-action rules and associated scores for privacy and security fed through to Experiment 1 and Experiment 2.

4. Experiment 1

The main aim of Experiment 1 was to explore the effects of *explicit priming* (messaging) that directed our volunteer participants to place an emphasis on security *or* privacy in deciding upon which trigger-action rules to enable. The act of priming is one of providing a context in which subsequent behavior can be framed. In Experiment 1 it is explicit since it is directed specifically at a particular feature of the setting. The key focus was whether such messaging can impact and improve the decision-making process of individual users. By utilizing a repeated measures design it was possible to obtain a baseline level of rule-enabling behavior for each participant before establishing the precise impact of security and privacy messaging. The second aim of Experiment 1 was to explore ways in which attitudes to technology shape how participants enabled rules with the aim of identifying key traits, of which knowledge of can then be used to help improve cyber-risky behaviors.

4.1. Experiment 1 hypotheses development

While most users seem adept at setting security and/or privacy rules for single devices, especially early on (e.g., during set-up of the device), there is little research on interconnected smart IoT devices in terms of security and privacy. It is predicted, albeit with a limited evidence base (i.e., Experiment 1 is largely exploratory given its novelty), that without intervention users will not be inclined to focus on the security and/or privacy settings of devices especially in terms of how the settings for one device could impact another. Explicit priming, that places an emphasis on security when deciding upon which trigger-action rules to enable, will enhance the security integrity of enabled rules compared to the non-priming baseline condition. Priming that places an emphasis on privacy will enhance the privacy integrity relative to baseline. The inclusion of individual differences measures in Experiment 1 (e.g., technology adoption propensity, trusting beliefs) is entirely exploratory and therefore not appropriate to make specific hypotheses.

4.2. Experiment 1 method

4.2.1. Experiment 1 participants

Two hundred and fifty-four volunteer participants (all UK residents aged over 18 years, range 18-73, $M = 33.13$, $SD = 10.91$, 66.9% female, 30.5% male, 1.9% other, 0.6% undisclosed) were recruited via the *Prolific Academic Online Participant Panel* (www.prolific.co). It was advertised as a study about smart homes and smart home technologies/devices without any mention of privacy or security. Of those recruited, three potential participants failed a simple and fair attention check, two failed to provide all necessary responses and two enabled every rule in every condition and were treated as extreme outliers, giving a final sample size of 247.

Prior to the study, the procedure was piloted with 20 participants to ensure appropriate comprehension of the tasks and survey questions and to avoid any ambiguity. These participants are not included in the final sample.

We recruited only those *Prolific* participants with an excellent track record of producing trustworthy results: a minimum of 20 previous submissions on the Prolific platform with a minimum approval rate by investigators from previous studies of 98%. There were no other exclusions for participation. Participants were rewarded £3.50 for completing the study and it took ~20 minutes to complete on average, (equating to an hourly rate on Prolific of £13.93). All stages of the experiment were approved and conducted in accordance with our institution's ethics and risk assessment procedures – School of Psychology Research Ethics Committee (SREC).

4.2.2. Experiment 1 materials

As informed by the Delphi Study, a total of 20 trigger-action rules were included in this experiment and each of these rules had an assigned security and privacy score (See Appendix A).

Four individual differences scales were selected as being appropriate

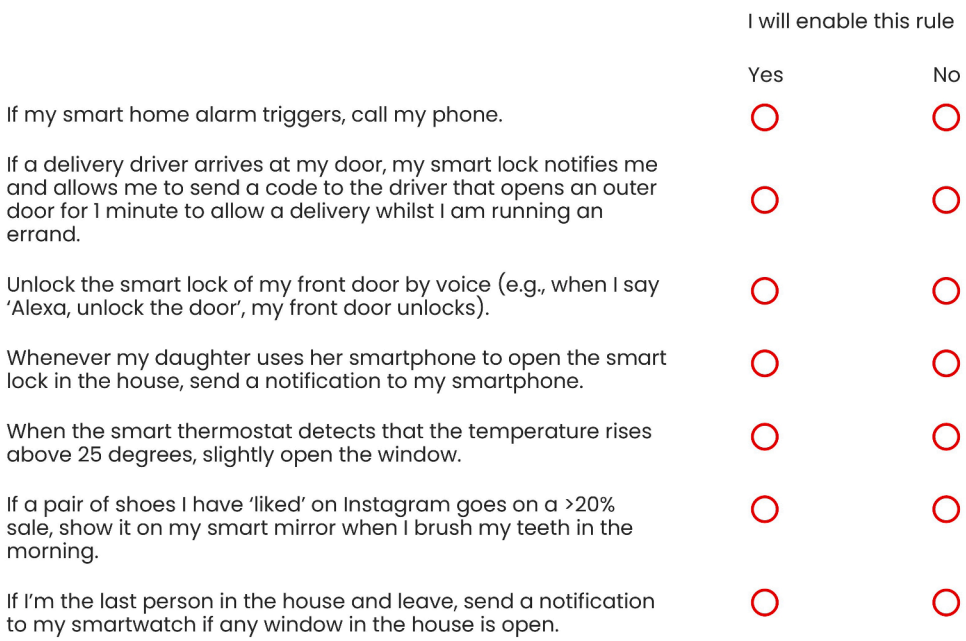

Fig. 1. Example layout of trigger-action rules in all three experimental conditions.

for the study. The first was the 14-item *Technology Adoption Propensity Index (TAP)* developed by Ratchford and Barnhart (2012). This multiple-item scale measures consumers' propensities to adopt new technologies and combines assessments of consumers' positive and negative attitudes towards technology. Within TAP are four distinct dimensions related to technology adoption: two that inhibit— (*dependence* and *vulnerability*), and two that enhance (*optimism* and *proficiency*). An individual's TAP score predicts both usage and ownership of technology. The second included scale was the 5-item *Perceived Benefits/Risks* adapted from Park et al. (2019). This scale was originally developed to examine the effects of *perceived risk, perceived benefits*, and *trust* on consumers' intention to use mobile payment systems. The third was the 10-item *Internet Users' Information Privacy Concerns* (IUIPC) developed by Malhotra et al. (2004) and drawing from social contract theory. The factor structure comprises three dimensions—*collection, control*, and *awareness*—that make it useful in the analysis of the psychometric properties of online privacy. The final included scale was the 5-item *Trusting Beliefs* (Harborth and Pape, 2020; Malhotra et al., 2004). This scale was an adaptation and extension of IUIPC that measures the impact of privacy concerns on the use of technologies.

4.2.3. Experiment 1 procedure and design

The online questionnaires and experimental tasks were designed and delivered using *Qualtrics* (www.qualtrics.com) and participants were directed to them via the *Prolific* website. Participants first read through a description of smart homes and the types of smart home device that would later be mentioned in the study. For each device there was a picture and a short paragraph with a description of the device (See Appendix B). Participants were then asked to report how familiar they are with such devices. The next screen introduced the concept of trigger-action rules and platforms such as IFTTT and asked participants to report how familiar they are with them.

Each participant then undertook the following three experimental conditions:

No Prime condition: A *neutral context* introductory paragraph was presented at the top of the screen. Participants were asked to imagine that they had all the smart devices and services introduced previously in their home and asked which trigger-action rules they would like to enable. Below the paragraph were listed each of the 20 trigger-action rules with circular radio buttons (red outline but no fill) labelled *Yes* or *No* placed adjacent to each description (see Fig. 1). When a participant clicked a button corresponding to *Yes* or *No* then the button filled red. Before the 8th and 15th rule the *Yes* and *No* labels were placed in the columns to remind participants which radio button corresponded to which response. Participants were required to pick a response for each of the rules but free to do so in any order they wished and free to alter their decisions at any point. There was no time limit and once participants were happy with their decisions, they clicked a *proceed* button at the bottom of the page.

Security Prime condition: This comprised the same 20 rules and presentation parameters as the no prime condition and once again asked participants to imagine that they had all the smart devices and services in their home. However, the introductory paragraph differed in as much as it explicitly prompted participants to consider the security implications of enabling the rules. Participants were told that it is important to maximize the security in their house (e.g., to make sure that burglaries are prevented). To ensure compliance with the task, and not risk participants simply leaving all rules switched-off (the most secure option as it prevents inter-connectedness between devices) participants were told that 1 point would be awarded for each rule used, with a cost (lost points) if there were security problems in the final configured set of rules or a gain (extra points) if the rule configuration potentially makes the house more secure. Based upon the total points scored by each participant, bonus payments, were given to the top 10% of participants.

Privacy Prime condition: This again comprised the same 20 rules and presentation parameters as the no prime condition with participants once again asked to imagine that they had all the smart services in their house. However, the introductory paragraph asked for explicit consideration of the privacy implications of enabling each rule. Participants were told that it is important to maximize the privacy in their house (e.g., "to make sure that other people don't have access to your personal details or something embarrassing about you doesn't become public"). As with the security prime condition, to ensure compliance with the task, participants were told that 1 point would be awarded for each rule used, with a cost (lost points) if there were privacy problems in the final configured set of rules or a gain (extra points) if the rule configuration potentially enhances privacy. Again, based on the total points achieved, bonus payments were given to the top 10% of participants.

The No Prime condition was always presented first with the Privacy Prime and Security Prime conditions then presented in a randomized

Table 1
Mean (and SD) Security and Privacy scores in each condition.

	Rule Weights (raw)			
	Security		Privacy	
Condition	M	SD	M	SD
No Prime	-1.03	*4.20*	-13.36	*6.93*
Security Prime	2.46	*3.97*	-15.68	*7.06*
Privacy Prime	-1.12	*5.18*	-10.45	*7.33*

order across participants. After completion of the three prime conditions participants were then required to fill out the demographic and individual differences questionnaires outlined above.

4.3. Experiment 1 results

4.3.1. Trigger-action rules (Experiment 1)

For each of the trigger-action rules enabled (*Yes* response given) the associated security and privacy weights served as the basis for giving each participant a total of six scores (i.e., the sum of the security and privacy scores, in each of the three conditions). Table 1 shows these raw scores—the sums of scores for each participant—averaged over participants and Fig. 2 shows the calculated difference scores for the security prime and privacy prime conditions relative to the no prime condition.

The change scores corresponding to the factor primes (Security Prime, Privacy Prime) and rule weightings (Security, Privacy) were subject to a repeated measures ANOVA. The pattern of results (Table 1 and Fig. 2) reveals that a focus on security led to a neglect of privacy (while increasing security) whereas a focus on privacy increased privacy scores while leaving security relatively intact. This is illustrated most forcibly in the significant interaction between primes and rule scores, $F(1, 244) = 214.2$, $MSE = 22.2$, $p < .001$, $\eta_p^2 = .47$. There were also main effects of primes, $F(1, 144) = 10$, $MSE = 16.6$, $p = .002$, $\eta_p^2 = .04$, and rule weightings, $F(1, 244) = 10.2$, $MSE = 47.8$, $p = .002$, $\eta_p^2 = .04$, subsumed within the interaction.

The interaction was explored further and one sample *t*-tests (two-tailed) revealed the interaction to be driven by privacy primes increasing privacy scores ($M = 2.9$, $SD = 8.41$), $t(244) = 5.4$, $p < 0.001$, $d = 0.35$, while leaving security scores ($M = 0.09$, $SD = 5.71$) unchanged, $t(244) = 0.26$, $p = .8$, $d = -0.02$. Security primes increased security scores ($M = 3.49$, $SD = 5.03$) markedly, $t(244) = 10.85$, $p = < .001$, $d = 0.69$, while worsening privacy scores ($M = -2.33$, $SD = 7.79$), $t(244) = 4.7$, $p < .001$, $d = -0.3$.

As a necessary consequence of our experimental procedure, the number of rules a participant could enable was free to vary. This provided an additional variable of interest when accounting for behavior. Furthermore, the more rules someone is willing to enable then the less cyber-secure their behavior could be considered. The average number of rules enabled in each condition is shown in Fig. 3.

On average, only around half the available 20 rules were enabled in each condition. Generally, the number of rules enabled was lower for the Privacy Prime than the other two conditions. An overall repeated-measures analysis of variance (ANOVA) revealed conditions to be significant, $F(2, 488) = 14.2$, $MSE = 8.08$, $p < .001$, $\eta_p^2 = .06$ with post-hoc (two-tailed, *Tukey*) tests showing that the only significant differences were between No Prime ($M = 9.78$, $SD = 3.76$) and Privacy Prime ($M = 8.79$, $SD = 4.23$), $t(488) = 3.86$, $p < .001$, $d = -0.21$, and Security Prime ($M = 10.1$, $SD = 3.25$) and Privacy Prime, $t(488) = 5.12$, $p < .001$, $d = 0.43$. The small mean difference between Security Prime and No prime was not significant: $t(488) = 1.26$, $p < .2$, $d = 0.08$.

The number of rules enabled again reveal privacy and security primes to work in different ways with a security prime leaving the number of rules enabled relatively similar (albeit with a small, but non-significant increase in mean) and a privacy prime leading to an overall reduction in the number of rules enabled. A characterization of privacy as being a more potent and generalized dimension of decision-making is suggested by the results so far.

4.3.2. Individual differences (Experiment 1)

Using the demographic and individual differences data collected during the experiment we undertook hierarchical regressions, controlling for demographic information, with the security and privacy scores as dependent variables in each of the three conditions (No Prime, Security Prime and Privacy Prime). Additionally, we undertook the same

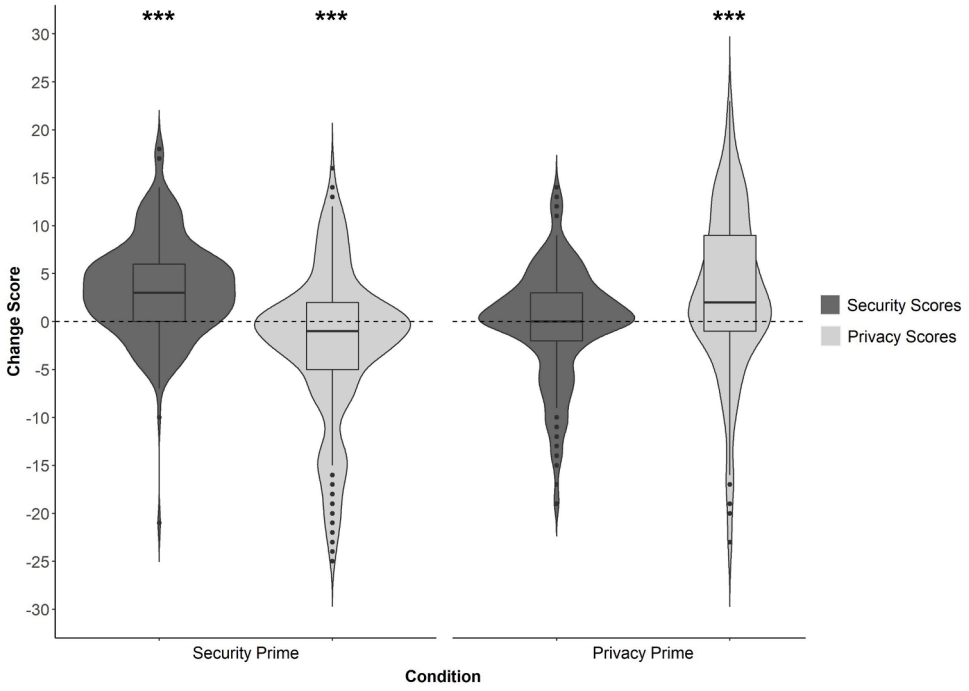

Fig. 2. Box plots with violin overlay illustrating the security and privacy change scores in each priming condition relative to no prime (dashed line).
Note. *** Significant change from No Prime at p < .001.

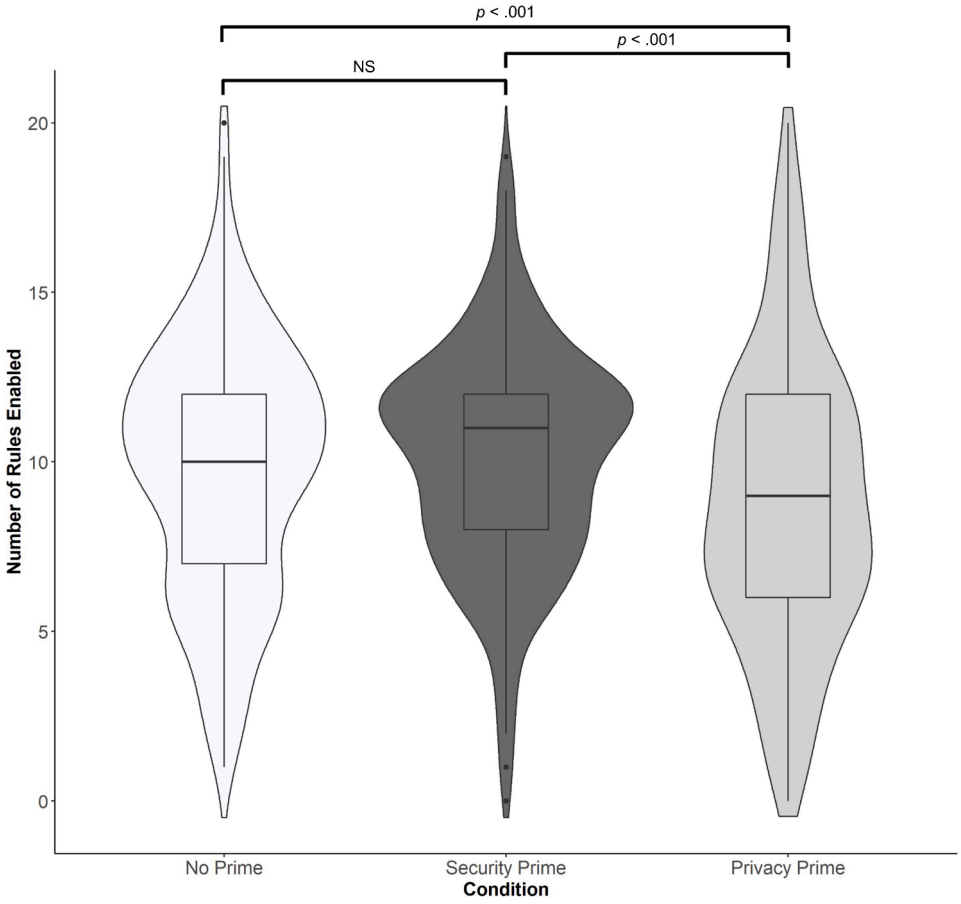

Fig. 3. Box plots with violin overlay illustrating the number of rules enabled in each of the priming conditions.

analysis on the number of rules enabled measure.

This, one must caution, was not a conservative approach, but we think necessary insofar as we were not guided by well-developed hypotheses in the individual differences' domain. In that respect the following analysis should be regarded as exploratory and its outcome only suggestive. However, at the same time, those effects emerging as predictors are likely to be the most major ones and it is anticipated that they will prove informative for use in future studies.

No Prime condition

Security scores: The regression including all predictors was significant, $F(16, 223) = 3.01$, $p < .001$, $R^2 = .18$. *IUIPC_Control (*an individual's concerns about whether they have control over personal information as manifested by the *existence of voice* e.g., such as having options to opt-in/out of data collection) was negatively related to security scores ($p = .01$). Contributing most to the model, but just failing to reach conventional levels of significance, were *TAP Vulnerability* (inhibits use of technology) which was positively correlated ($p = .06$), and *Perceived Benefits* which was negatively correlated ($p = .08$)

Privacy scores: The model including all predictors was significant, $F(16, 223) = 4.48$, $p < .001$, $R^2 = .24$. Demographic factors contributing most were *Age* ($p < .01$) and *Skill with technology* ($p = .01$). Privacy scores increased as age and skill increased. *Trusting Beliefs* ($p < .01$) and *Perceived Benefits (*$p < .001$) were both negatively correlated. Perhaps unsurprisingly, the more people trust online companies, the lower their privacy score. And again, the more benefits they expect to receive from using smart home technologies the lower their privacy score. Finally, privacy scores were positively related with *Perceived Risks* ($p < .05$) with privacy scores increasing as the perceived risks from technology increased.

Security Prime condition

Security score: The models were not significant. *Education* ($p = .06$) and *trusting beliefs* ($p < .01$) were factors contributing most to model that included all predictors though. Education was positively correlated so that security scores increased as education levels increased whereas trusting beliefs were negatively correlated with decreasing security scores as trusting beliefs increased.

Privacy score: The model including all predictors was significant, $F(16, 223) = 3.28$, $p < .001$, $R^2 = .19$. Demographic factors contributing most were *Age* ($p = .05$) and *Skill with technology* ($p < .001$). Both were positively correlated such that privacy scores improved as age and skill with technology increased. As in the No Prime condition, *Perceived Benefits (*$p < .01$), was negatively correlated. The more benefits expected from smart home technologies then the lower the privacy score.

Privacy Prime condition

Security score: The models were not significant. *IUIPC_Control* ($p = .04$) contributed most to model that included all predictors and was negatively related to security scores. The more that participants agreed with consumers having more control over their online data then the fewer rules that were enabled.

Privacy score: The model including all predictors significant, $F(16, 223) = 2.88$, $p < .001$, $R^2 = .17$. Just as in the No Prime condition, *Trusting Beliefs* ($p = .06$) and *Perceived Benefits (*$p = .03$) were both negatively correlated factors contributing to the model such that privacy scores worsen as the perceived trust and benefits increase. *Tap Optimism* ($p < .05$) was also negatively correlated with the privacy score. The more optimistic individuals were about technology then the lower their privacy scores.

Number of rules enabled measure

No Prime condition: The Model including all predictors was significant, $F(16, 223) = 5.53$, $p < .001$, $R^2 = .28$. The Demographic factor

contributing most was *Age* ($p < .01$): number of rules enabled decreased as age increased (in a similar pattern to the Privacy score data). *Trusting Beliefs* ($p < .01$) and *Perceived Benefits* ($p < .001$) were both positively correlated with the number of rules enabled. The more people trust online companies and expect to gain a benefit, then the greater number of rules enabled. *Perceived Risks* ($p = .03$) was negatively correlated with fewer rules enabled as perceived risks increased.

Security Prime condition: The Model including all predictors was significant, $F(16, 223) = 3.93$, $p < .001$, $R^2 = .22$. Demographic factors contributing most were Age ($p = .04$) and Skill with Technology ($p < 0.01$). Both were negatively correlated with the number of rules enabled: the number of rules enabled decreased as age increased and as skill decreased the number of rules enabled increased. Perceived Benefits ($p < .01$) was a positively correlated factor. The more people expect to gain from technology, then the more rules were enabled. Trusting Beliefs ($p = .06$) just failed to reach conventional significance but showed a similar pattern to the No Prime condition with increased trust in online companies resulting in more rules enabled.

Privacy Prime condition: The model including all predictors was significant, $F(16, 223) = 2.7$, $p < .001$, $R^2 = .16$. This showed a similar pattern to the security prime condition with *Perceived Benefits* ($p = .04$) a positively correlated factor and *Trusting Beliefs* ($p = .055$) also positively correlated but just failing to reach conventional significance

4.4. Experiment 1 discussion

Experiment 1 demonstrated that explicit priming that encourages maximization of certain outcomes produces material consequences for the rules deployed, albeit for hypothetical circumstances. Interestingly there is an asymmetry between security and privacy. Enjoining the maximization of privacy improves privacy scores while leaving security scores largely unchanged. Enjoining security produced a more symmetrical effect: it acted to improve security scores while negatively impacting privacy scores at the same time leaving the number of rules enabled relative to the No Prime condition stable. These findings suggest a degree of cognitive control with participants able to identify and select rules based directly upon the messaging received prior. Just why there is an asymmetry of this sort, is open to question. Security and privacy concerns are major concerns for users of smart home technologies (McAlaney et al., 2018; Parks Associates, 2019) and in all conditions participants were free to enable as many rules as they wished. It is positive to find that explicit security and privacy related messaging is sufficient in promoting directed, and safer, rule-enabling behavior.

The second stage of the experiment collected individual differences measures and here there were some key predictors emerging in several models. While exploratory, we take the analysis to provide useful pointers for inclusion of a sub-set of factors in future regression models. The factors that seemed to predominate in the analysis were: trusting beliefs, perceived benefits and age. If users trust technology, then there is a tendency to set security and privacy concerns aside. Trust has previously been shown to be important in predicting planned behavior within smart home services (Yang et al., 2017). However, this study is the first to demonstrate a direct association with trigger-action rule enabling behavior which is a *performed*, rather than a *planned*, action. This finding has important implications for privacy and security messaging as end user improvements may first be dependent upon sowing seeds of distrust.

Perceived benefits (Park et al., 2019) were also fairly consistent in predicting rule-enabling behavior with more rules enabled as the perceived benefits increased. Additionally, there were several instances where this came at the expense of security/privacy. Similarly, to the trusting beliefs scale, it seems that perceived benefits do not only apply to behavioral intentions but also to behavioral outcomes. Ironically, this again points to reducing rather than increasing trust and points perhaps to research investigating the power of illustrative examples as opposed to general incitement (or indeed both) as the more effective method of behavior change. Age was also a key demographic factor in several models. Older users tended to be more conservative in the number of rules enabled which suggests, in regard to trigger-action rules, that they will be exposed to fewer security/privacy risks than younger users. Although this is the first demonstration of it in the adoption of trigger-action rules it is consistent with findings across a wide range of domains (e.g., Weller et al., 2011). This finding therefore contributes to an already well-established literature and suggests an important interplay between age and perceived benefits that future regression models and behavior change interventions will need to consider.

5. Experiment 2

Experiment 2 extended upon the priming conditions explored in Experiment 1. The rule-enabling task that participants undertook was identical, but the priming task was *implicit* rather than *explicit*, that is, instead of giving specific instructions about what to achieve via the selection of the rules, participants undertook a self-contained problem-solving activity that was broadly about security, privacy or was neutral. By utilizing implicit primes, we hoped to demonstrate a broader basis of priming whereby the engagement of cognitive activity—generally about security or privacy—would reduce security and privacy risks.

We adopted a between-participants design with the three conditions—No Prime, Security Prime and Privacy Prime—all being undertaken by randomly allocated independent groups. The advantage of this design was that it eliminated the risk of contamination of effects across conditions. However, a caveat of this design choice was that it meant that individual difference data could not legitimately be used in the same way as Experiment 1. However, we were able to make principled use of the key variables identified in Experiment 1 (age, trusting beliefs and perceived benefits) to test whether they were once again predictive here.

5.1. Experiment 2 hypotheses development

Similar to Experiment 1, Experiment 2 is largely exploratory given that, to our knowledge, there has been no past research on the use of implicit priming on user settings choices regarding the security and privacy of interconnected IoT smart home devices. We can in part turn to our key findings from Experiment 1 though – that explicit security priming improved security scores but degraded privacy scores whilst explicit privacy priming improved privacy scores whilst largely leaving security scores intact. It is reasonable to expect that a non-explicit form of priming like that used in Experiment 2 will not have such marked effects as explicit priming but will be effective enough to improve overall security (in the implicit security prime condition) and privacy (in the implicit privacy prime condition). The inclusion of some individual differences measures from Experiment 1 (age, trusting beliefs and perceived benefits) is again exploratory and given the between-participants design adopted in Experiment 2 it is only appropriate to suggest that we may observe trends similar to the findings in Experiment 1.

5.2. Experiment 2 method

5.2.1. Experiment 2 participants

Conditions of recruitment, participant inclusion and payment were identical to Experiment 1 with those who had participated in Experiment 1 excluded from participating.

A total of 333 volunteer participants (all UK residents aged over 18 years, range 18-76, *M* 34.99, *SD* 12.85, 67.11% F, 32.44% M, 0.4% other) were recruited to provide a balanced independent groups design of 111 participants per cell. However, 8 participants were shown to have failed a simple and fair attention check and so were excluded from the final analysis. This left 110 participants in the no prime condition, 108 in the security condition and 107 in the privacy condition (total n = 325).

Table 2
Mean (and SD) Security and Privacy Scores in each condition.

	Rule Weights (raw)			
	Security		Privacy	
Condition	M	SD	M	SD
No Prime	-1.65	*4.27*	-13.57	*7.28*
Security Prime	-0.23	*4.19*	-13.04	*6.49*
Privacy Prime	-0.66	*4.12*	-11.5	*7.18*

Slight imbalances in cells are not considered a problem at these sample sizes (see Shaw and Mitchell-Olds, 1993). All stages of the experiment were approved and conducted in accordance with our School of Psychology Research Ethics Committee.

5.2.2. Experiment 2 materials

The same 20 trigger-action rules and associated security and privacy scores used in Experiment 1 were also used here. However, instead of explicit paragraphs prompting participants to think about security/privacy the current experiment utilized implicit priming tasks. For the No Prime condition participants were first given two tasks in which they were asked to select which smart lightbulb, from a choice of two, they would buy for a friend. Participants were presented with a list of features that were not relevant to security or privacy on which to base their decision (e.g., maximum lifespan, ease of use). For the Security Prime task participants were implicitly primed to think about the security of their home by performing two tasks asking which of two houses was more likely to be burgled based on eight characteristics (e.g., the location of the property, whether it has a garden). This task was adapted from previous literature on decision-making among expert and novice residential burglars (Garcia-Retamero and Dhami, 2009). Finally, the Privacy Prime task implicitly primed participants to think about the privacy of their data by presenting two tasks (adapted from Kelley et al., 2013) in which, based on several characteristics (e.g., access granted to contacts, access granted to photos), they had to choose which application they would be more willing to install on their smartphone. Appendix C outlines these tasks in more detail.

5.2.3. Experiment 2 procedure and design

The design and procedure were in many respects similar to Experiment 1 with all participants first receiving the same introduction to smart home technologies and trigger-action rule platforms as before. Experiment 2 utilized a between-participants design with participants then randomly assigned to complete just one of the three priming tasks detailed above (No Prime, Implicit Security Prime, or Implicit Privacy Prime). After completion of the priming task all participants were presented with the 20 trigger-action rules and free to enable as many, or as few, rules as they wished. Presentation parameters of the rules and radio buttons were identical to Experiment 1. Once completed, all participants were then required to fill out the demographic and individual differences questionnaires before the study ended with presentation of a debrief.

5.3. Experiment 2 results

5.3.1. Trigger-action rules (Experiment 2)

The scoring was identical to Experiment 1 with each trigger-action rule enabled (*Yes* response given) assigned its appropriate security and a privacy score and the sum, in each of the three conditions, calculated (See Table 2). Fig. 4 shows the calculated difference scores for the security prime and privacy prime conditions relative to the no prime condition.

Due to the nature of the between-participants design standardized change scores could not be calculated and because direct comparison of the raw security and privacy scores yields very little useful information, the exposition here treats security and privacy scores separately.

An implicit Security Prime significantly increases security scores ($M = 1.43$), but not privacy scores ($M = 1$). An implicit Privacy Prime has no significant effect on either security ($M = 0.53$) or privacy ($M = 2.07$) scores. A one-way ANOVA revealed a significant main effect of priming condition on security scores, $F(2, 322) = 3.31$, $p = 0.04$, with post-hoc tests (two-tailed, *Tukey*) showing a significant difference between No Prime and Security Prime ($p = .03$) but a non-significant difference between No Prime and Privacy Prime ($p = .19$). Analysis of privacy scores with a one-way ANOVA revealed a non-significant effect of

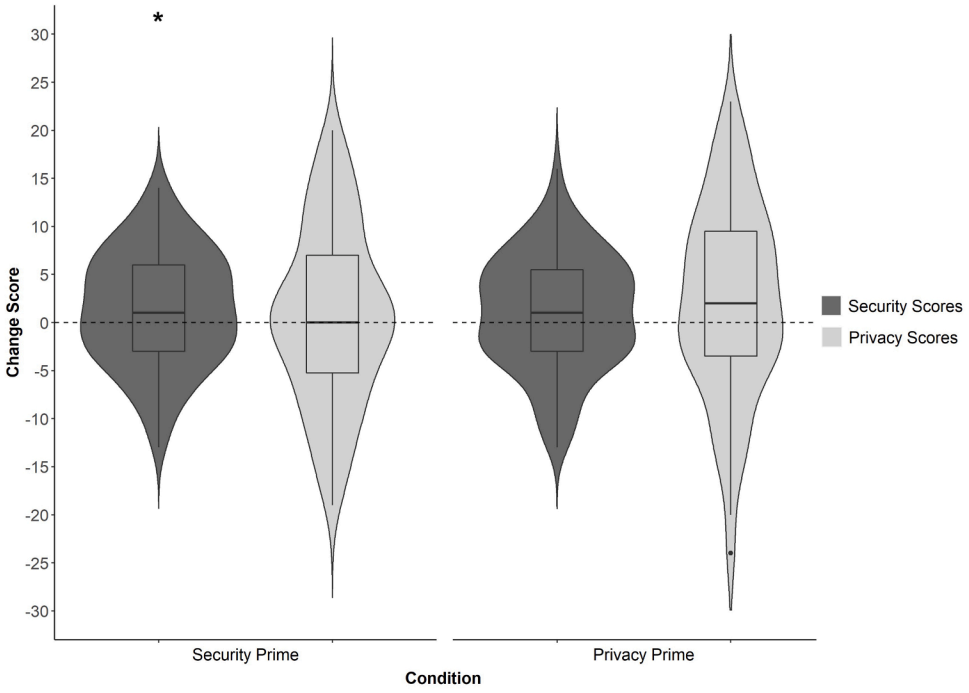

Fig. 4. Box plots with violin overlay illustrating the security and privacy change scores in each priming condition relative to no prime (dashed line).
Note. * Significant change from No Prime at $p < .05$.

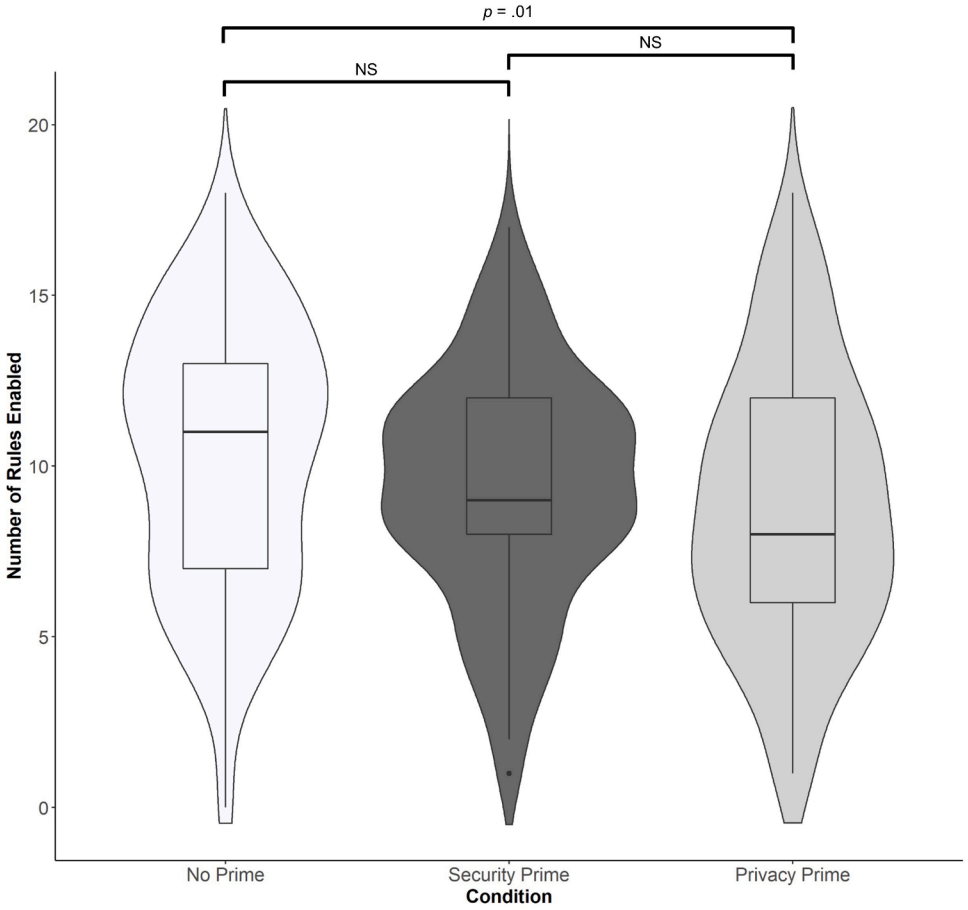

Fig. 5. Box plots with violin overlay illustrating the number of rules enabled in each of the priming conditions.

Table C1
Task used within the No Prime condition.

	Product 1	Product 2
Connectivity	Wi-Fi	Bluetooth, Wi-Fi
Integration	Amazon Alexa, Google Assistant, IFTTT	Amazon Alexa
Maximum est. lifespan	23 years	18 years
Dimmable	Yes	Yes
Ease of use	****	****
Set-up	****	*****
Colour quality	****	*****
Price	£24.99	£29.99

Table C2
Task used within the Security Prime condition.

	Property 1	Property 2
Garden in the property	Tall hedges/bushes	Short hedges/bushes
Signs of care	Not well-kept property	Not well-kept property
Type of property	Flat	House
Light in the property	On	On
Letter box	Empty	Stuffed with post
Location of the property	Corner of the street	Middle of the street
Access to the property	Doors/windows on ground floor	Doors/windows on second floor
Security in the property	No burglar alarm system	Burglar alarm system

Table C3
Task used within the Privacy Prime condition.

	Calorie Tracker 1	Calorie Tracker 2
Privacy Facts: This app collects your		
Personal information	Yes	Yes
Contacts	No	Yes
Location	No	Yes
Diet/nutrition	No	Yes
Health/medical	No	No
Photos	No	No
Usage analytics	Yes	Yes
Price	Free	£4.99

priming condition, $F(2,322) = 2.57$, $p = .08$.

Number of rules enabled: A prime tended to diminish the number of rules enabled and this was most marked with the Privacy Prime condition (see Fig. 5). A one-way ANOVA revealed a significant main effect of priming condition, $F(2, 322) = 4.1$, $p = .02$, and post-hoc comparisons (two-tailed with Tukey's HSD) revealed the only significant difference to be between No Prime and Privacy Prime conditions ($p = .01$) with remaining comparisons non-significant ($ps > 0.05$).

5.3.2. Individual differences (Experiment 2)

A caveat of using a between-participants design is that it loses power to detect smaller effects. However, we did identify three key variables in Experiment 1 – age, trusting beliefs and perceived benefits – which meant we could use the individual differences data collected in Experiment 2 to establish whether those variables are consistent predictors

and whether they generalize across experiments. Similar to Experiment 1, we undertook regressions using the security and privacy scores as dependent variables in each of the three conditions (No Prime, Security Prime and Privacy Prime) but, unlike Experiment 1, only including the three key variables identified. Secondly, we undertook the same analysis on the number of rules enabled measure.

No Prime condition

Security scores: The model was not significant, $F(3, 105) = 1.35$, $p = .26$, $R^2 = .04$.

Privacy scores: The model including the three predictors was significant, $F(3, 105) = 15.1$, $p < .001$, $R^2 = .3$, with both perceived benefits ($p < .001$) and trusting beliefs ($p < .001$) providing significant contributions to the model. As in Experiment 1, these were both negatively correlated so that privacy scores worsened as perceived benefits and trusting beliefs increased.

Security Prime condition

Security score: The model including the three predictors was significant, $F(3, 100) = 4.42$, $p = .006$, $R^2 = .12$, but only perceived benefits ($p < .001$) provided a significant contribution to the model. Again, this was a negative relationship: security scores diminished as perceived benefits increased.

Privacy score: The model including the three predictors was significant, $F(3, 100) = 17.0$, $p < .001$, $R^2 = .34$, with perceived benefits ($p < .001$) and trusting beliefs ($p = .055$) contributing most to the model. These were once again negative relationships with privacy scores worsening as perceived benefits and trusting beliefs increase.

Privacy Prime condition

Security score: The model including the three predictors was significant, $F(3, 102) = 4.17$, $p = .008$, $R^2 = .11$, but only trusting beliefs ($p < .05$) providing a significant contribution to the model. This was once again a negative relationship with security scores worsening as trusting beliefs increase.

Privacy score: The model including the three predictors was significant, $F(3, 102) = 9.73$, $p < .001$, $R^2 = .22$, with perceived benefits ($p < .001$) providing a significant contribution to the model and trusting beliefs ($p = .054$) and age ($p = .054$) both providing a substantial (albeit just reaching conventional significance thresholds) contribution to the model. Once again, the relationship was negative with increases in perceived benefits and trusting beliefs associated with worsening privacy scores. Age had the opposite effect with improvements in privacy scores as age increased.

Number of rules enabled measure

No Prime Condition: The model including the three predictors was significant, $F(3, 105) = 15.4$, $p < .001$, $R^2 = .31$, with both perceived benefits ($p < .001$) and trusting beliefs ($p < .001$) providing significant contributions to the model. The relationship here was positive with the number of rules enabled increasing as trusting beliefs and perceived benefits increase.

Security Prime Condition: The three predictors model was significant, $F(3, 100) = 15.4$, $p < .001$, $R^2 = .32$, with perceived benefits ($p < .001$) providing the most significant contribution to the model. Again, this relationship was positive with the number of rules enabled increasing as the perceived benefits increase.

Privacy Prime Condition: Here again the three predictors model was significant, $F(3, 102) = 10.3$, $p < .001$, $R^2 = .23$, with both perceived benefits ($p < .001$) and trusting beliefs ($p = .02$) providing significant contributions to the model. The relationships here were again positive with the number of rules enabled increasing as trusting beliefs and perceived benefits increase.

5.4. Experiment 2 discussion

Experiment 2 tested whether implicit priming is sufficient to promote positive changes in trigger-action rule-enabling behavior. While the overall effects were of a smaller magnitude than those obtained via explicit priming in Experiment 1, the implicit primes still produced statistically reliable consequences. More precisely, implicit security priming specifically led to a change in rule-enabling behavior so that security risks were mitigated to some extent compared to those receiving a neutral prime. In contrast to the outcome of Experiment 1, this improvement in security scores was not achieved at the expense of privacy. Additionally, there was a general effect of priming upon the overall number of rules enabled indicating that any kind of task (whether including an implicit security, or privacy message) can help promote more cautious decision making that would ultimately lead to more secure systems. It should be noted that the tasks used were very subtle in the nature of their messaging and yet still elicited significant changes in behavior. As indicated by Experiment 1, as the messaging shifts to being more explicit even further mitigation of risk would be the most likely outcome.

Furthering the predictive value of the key variables identified in Experiment 1 – age, perceived benefits and trusting beliefs – these produced significant regression models of behavior in all but one instance (security scores in the no prime condition). Additionally, perceived benefits and trusting beliefs emerged as significant contributors in a number of the models. In all instances they were indicative of more risky security and privacy related decision making with increases in the overall number of rules enabled and worsening security and privacy scores. Because, along with Experiment 1, these variables consistently emerged as significant predictors it suggests that they are key variables for predicting rule-enabling behavior. As such, they are also ones in which future research should be highly considerate of. However, in contrast to Experiment 1, age was a significant predictor variable in only one regression model. It may be that age is less relevant than indicated by Experiment 1 although there is a wealth of research (e.g., Weller et al., 2011) indicating the importance of age. Most likely is that the failure to find consistent significant effects of age in the present experiment is that it is reflective of the between-subjects design choice. Not only does a reduction in participant numbers lead to reduced power but also reduces the possible variability of ages, of which to use when establishing whether a relationship exists, within the participant pool.

6. General discussion

The present series of experiments assessed the impact that explicit (Experiment 1) and implicit (Experiment 2) security and privacy related messaging has upon trigger-action rule enabling behavior. Additionally, they sought to identify key individual differences that underlie the decision-making process. Overall, both explicit and implicit messaging had positive impacts upon rule-enabling behavior with some general reductions identified in the total number of rules enabled. Additionally, security messaging, whether delivered implicitly or explicitly led to improvements in security scores. In Experiment 1 this improvement in security scores came at the expense of privacy scores suggesting that an explicit focus on security leads to a neglect of privacy. However, this same pattern was not evident in Experiment 2. Implicit privacy messaging, although leading to directional improvements in security and privacy scores failed to reach significance. However, explicit privacy messaging led to robust improvements in privacy scores while leaving security scores at similar levels to no prime. Security and privacy have been shown to concern users (McAlaney et al., 2018; Parks Associates, 2019) and the current experiments demonstrate that highlighting security and privacy implications, explicitly or implicitly, can lead to measurable positive changes in behavior.

It is perhaps unsurprising, intuitively, that explicit instructions result in a change of behavior. However, that there is a significant effect of implicit priming is perhaps a little unexpected on some counts, suggesting as it does a relatively passive process, one of general sensitization to a prevailing cognitive activity and its generalization beyond its immediate context. Implicit messaging in other domains (e.g., food preference decisions; Whalen et al., 2018) is considered a strong driver of decision making though so it is also not entirely unreasonable to

suspect that similar processes could possibly influence security and privacy related decisions. We would encourage further testing on the efficacy of implicit messaging before it is advocated as a potential solution for risky cyber behavior but from the present experiment it seems a useful avenue to pursue.

Privacy and security seemingly operated in different ways across the experiments. In Experiment 1, explicit security messaging promoted an improvement in security at the expense of privacy while privacy messaging led to privacy improvements while keeping security relatively intact compared to no prime. The pattern in Experiment 2 was slightly different with implicit security messaging increasing security scores while privacy scores also remained positive and not significantly different from no prime. However, the bundling of many conditions and many scenarios within our experimental design is unrepresentative of everyday life. This limitation may have had particular consequences here because of the way in which the many different conditions potentially acted as a basis of comparison for each other, comparisons that would not ordinarily be available to the consumer. So, using a repeated measures design as we did in Experiment 1 runs the risk that when the participant comes to selecting a type of trigger-action rule, the selection will be a product in part of other judgments that have been made in other stages of the experiment. The asymmetry we observed may have been a quirk of cross-condition comparisons, ones absent from Experiment 2, rather than revealing a genuine tendency to neglect privacy in favor of security. However, we can be confident that, in general, priming—implicit and explicit—does have the desired behavior change effects, even if we possibly need to be a bit circumspect about the trade-off observed in Experiment 1.

6.1. Implications

We argue that the novel method and findings provide a suitable base from which to build a body of evidence in what has been, until now, an under researched area. The outcome of our study also provides an evidence base on which to begin suggesting practical steps for everyday use. Having a message that prompts users to focus on privacy or security leads to a significant reduction in rule enabling behavior and seemingly more cognitive control over the decision-making process. Such messaging could very easily be incorporated into trigger-action rule platforms at appropriate stages. For example, if a user is creating a trigger-action rule involving a smart lock then a message prompting the user to consider security risks may help mitigate some instances of risky rule-enabling behavior. Likewise, before a rule can be enabled, a reminder to consider privacy concerns (e.g., like Chong et al. 2018) may mitigate some users granting inappropriate access to social media sites or other personal details. Understandably, such rules being enabled, and access being granted to various sources, help generate revenue for various outlets (e.g., via advertising). However, at least some trade-off between encouraging the enabling of rules combined with explicit prompts to carefully consider the security and privacy implications will, in all likelihood, lead to further trust and uptake in the use of such platforms rather than risk users continuing to be averse to smart technology because of security and privacy concerns online (e.g., McAlaney et al., 2018; Parks Associates, 2019).

The insight gained from the present experiments into traits driving rule-enabling decision-making means that tailored messaging could be incorporated within trigger-action rule platforms. For example, depending on the demographic age group of the user some additional security/privacy messaging may mitigate some riskier decisions among younger users. Additionally, questions asked when installing the app (e.g., selected from perceived benefits, Park et al., 2019 or trusting beliefs scales, Harborth and Pape, 2020; Malhotra et al., 2004) could lead to effective individually tailored messaging being presented to the user. The association of rule choice with age is consistent with results in other contexts and with attitude change with age more generally (e.g., Weller et al., 2011). It should be noted that, for smart home technologies, privacy concerns may reduce as time spent with the technology increases (see e.g., Ghorayeb et al., 2021). A consequence is that we should not be complacent in thinking older adults will always be more cautious. Even cautious older users may eventually begin to adopt more rules after familiarization with trigger-action platforms. It may be the case that messaging needs to be introduced as the time spent with technology increases and, to complement our findings, future research may wish to further explore the relationship between age, messaging and rule choice but over extended periods of time.

6.2. Limitations

In studies like ours, there are very real issues about realism. They run the possibility that volunteers are invited to engage in a variety of hypothetical and schematic scenarios—without material consequences for the individual—and in which they could feasibly either understate or perhaps even overstate the likely real-world reaction. Additionally, with instructions and incentives necessary to ensure engagement with tasks there is a danger too of participants using online studies as a game. Quite aside from issues of realism, there are also issues of representativeness, ones that can be manifest in many different forms. The outcomes of rule choices are not consequential in our study and, of course, the imperatives of safety and security are more real and consequential in the 'real' world. This suggests that we cannot be completely sure that what we have shown will also be observed in naturalistic settings. That being said, trigger-action rule platforms, such as IFTTT, are based online. Upon downloading and installing the app, *suggested rules* (e.g., 'Get an email with the latest IFTTT updates') are immediately presented to the user with activation achievable via a single click. In that sense, the degree of difference between the current study—in which rules could be activated via a single click— and the platforms to which we investigated, are perhaps not so far removed. Future research would benefit from using interfaces more closely resembling the platforms of interest though to ensure a higher degree of overlap between the experimental and 'real life' setting.

Somewhat relatedly, participants may have interpreted the messaging as part of the general 'demand characteristic' (Orne, 1962) of the experiment. That is, they will have guessed the purpose of the experiments and complied with its explicit or implicit requirements. This possibly could be exacerbated by the Prolific experiment platform whereby participants receive approval ratings based on how well they perform in studies. A motivation to perform tasks in such a way that they enhance the experimenter's outcome (and in-turn receive positive feedback) is thought to promote demand characteristics (e.g., Nichols and Maner, 2008). Future studies, with a further degree of realism as suggested previously may help to mitigate this issue further.

6.3. Future work

Certainly, in carrying the work forward the task should reflect the increasing complexity available to users when creating trigger-action rules (see Manca et al., 2019). Our task used rules that were single, isolated instances of IFTTT logic, therefore lacking the complexity and multifariousness of real-world settings. Combinations of rules, even two or three rules, will pose an appreciable challenge to the user (Huang and Cakmak, 2015) which will take on several forms. One is that the user will have to anticipate the implications for the safety of each rule, as we have done here. However, as the number of rules increases so does the cognitive load on decision making and short-term memory which is likely to be even more detrimental for security/privacy decision making (e.g., Morgan et al., 2018; Williams et al., 2017). The implication of complex rules will have to be considered in combination, posing yet further challenges which are likely to exceed mental capacity, and instead require the support of tools to chart the various combinations and associated consequences (Brackenbury et al., 2019; Ur et al., 2016) or be reliant on third-party tailored suggestions (e.g., Manandhar et al.,

2020). There will also be emergent consequences that cannot be predicted from considering each rule in isolation and, as the level of complexity increases so do the demands on knowledge and understanding of the pragmatic consequences (Palekar et al., 2019). The precise effect all this will have on security and privacy for the individual user is currently unknown and clearly an important avenue of future research. It may be that users are aware of their own capacities and understanding and thus only adopt simple trigger-action rules. However, it is also entirely possible this is not the case and that without formal systems of support (e.g., software mapping IFTTT networks which should undergo further development; Corno et al., 2019b) users may inadvertently increase their privacy and security risk as a result of incorporating ever more complicated sets of rules.

Participants in our experiments were given pre-written rules which they could choose to enable. Trigger-action platforms usually include suggested rules and so this approach maintains some realism. However, on most trigger-action platforms users are also free to design their own rules, which is a departure from the present work. While messaging may help mitigate the enabling of suggested rules, whether this will extend to bespoke rules is beyond the scope of the present work. Future work should explore this, by giving participants more freedom to select which devices they would choose to include in the rules or by having them designing their own rules entirely and scoring those choices on security/privacy.

Finally, self-reported gender distribution among our participants was predominantly female. It was not our aim to research gender differences and the distribution of self-reported gender we obtained, unless specific controls are in place, is reflective of much psychology research. However, it should be acknowledged that research has suggested that the uptake and interest of smart home technology among women is lower than that of men (e.g., Strengers et al., 2019) with men tending to use them more in areas such as research and retail purchases (e.g., Canziani and MacSween, 2021). Future research may wish to explore whether there are gender influences upon rule-enabling behavior.

7. Conclusion

Overall, the current paper has highlighted the potential for unintended and unforeseen security and privacy risks that using trigger-action rule platforms (e.g., IFTTT) impose upon the user. Prompting users with explicit or implicit priming messaging goes some way to mitigate these risks by encouraging the engagement of fewer trigger-action rules. Explicit priming has a positive effect on security (albeit at a cost to privacy) and privacy (with no cost to security) with implicit priming only having a positive effect on security and not privacy. Additionally, traits such as age, perceived benefits and trusting beliefs were shown to drive riskier trigger-action rule enabling behavior. As such, when designing privacy and security safety messaging for users of interconnected smart home devices, not only should developers ensure to bring these themes to the user's attention but also consider these pre-existing traits when doing so.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This research was undertaken at the School of Psychology, Cardiff University, as part of a 2019-2020 CREST-funded project: 'Understanding the role of individual differences in the adoption, use and exploitation of smart home technology' (Principal Investigator: Emma Williams, University of Bristol; with Duncan Hodges, University of Cranfield, Emma Slade, University of Bristol). We thank three anonymous reviewers for their useful and insightful comments on an earlier draft of the paper / manuscript.

We dedicate this article to our great colleagues and dear friends, Professor William 'Bill' J Macken (16th May 1965 – 17th Feb 2020) and Professor Dylan M Jones OBE (30th Mar 1948 – 8th Apr 2022) who were Co-Investigators on the CREST project.

Appendix A

Trigger-action rules, along with their security and privacy weightings

The first stage of the Delphi study had an exploratory character, and it involved the identification of meaningful rules that could practically be included in the study. Between rules suggested by the Delphi participants and those provided by the authors (who acted as the Delphi administrators) 30 rules were created. Out of these 30 rules 20 were ultimately selected for inclusion in the study, based on a balance between expected privacy and security scores and the diverse use of devices.

This appendix presents a corpus of 30 trigger-action rules that were identified for this study. Each rule comes with two scores from -5 to +5. These scores describe the judged severity of potential security and privacy implications for using this rule (i.e., a negative security score represents a potential security breach, while a positive score suggests that this rule strengthens the security of the smart home). Of these 30 rules, 20 were selected for study.

Notes on scoring: Our study has an explicit focus on the trigger-action rules, rather than other aspects of security and privacy. Our rules and scores have been selected to reflect this. In particular, it is important to acknowledge that connected devices can be compromised from more than one entry point. For example, research has shown that a single smart device that gets hacked can infect other smart devices (Ronen et al., 2017) and can lead to a larger breach in the house, such as an attack to the home network (Check Point, 2020). This is particularly important for our scenarios, as this means that if someone hacks one device/service, it is possible for them to trigger certain actions to others. So, the more rules one uses, the more vulnerable they are. In addition, there is the risk of the trigger-action service itself being compromised, which is an important extra consideration (Fernandes et al., 2018).

Apart from a few exceptions (e.g., when completely irrelevant services are included, such as social media or other online services), we have not taken these factors into account for our scoring, due to the complexity of the assumptions we would have to make about the hypothetical user's cybersecurity practices. Finally, we have not taken into account the security and privacy of single devices and services, such as the security vulnerabilities of smart locks (Ho et al., 2016) or the privacy implications of AI voice assistants (Vox, 2020), as our focus is on the added problems or solutions created by linking these devices and services. However, future studies that may be willing to also consider factors like the above, may adjust scores accordingly.

Here are the trigger-action rules that were adopted in the study along with their security and privacy scores, together with the rationale for each. To reiterate, the rules were presented to the participants without the scores and rationale. A list of rules not adopted follows them.

Trigger-Action Rules and their weightings

If my smart alarm triggers, call my phone.

- *security*: +2. I have instant notification when something is potentially wrong (+3). A determined intruder could repeatedly set off the alarm without breaking in to reduce the owner's perception that the alarm being triggered is linked to a security incident (-1).
- privacy: 0.

If a delivery driver arrives at my door, my smart lock notifies me and allows me to send a code to the driver that opens an outer door for 1 minute to allow a delivery whilst I am running an errand.

- *security*: -3. The delivery driver has been given access to the property, albeit minimal and for a very limited time.
- privacy: -0.

Unlock the smart lock of my front door by voice (e.g., when I say 'Alexa, unlock the door', my front door unlocks).

- *security*: -4. Someone might trick it by saying the phrase from outside (Symantec, 2017), and more recent work suggests that an adversary can control such systems by injecting laser-based voice commands from a great distance (Sugawara et al., 2020). Also explicitly ties the smart lock to an Amazon/Google account - thereby increasing the risk from a compromised online account.
- *privacy*: -1: Ties the smart lock to an Amazon/Google account, i.e., Amazon/Google can build up data on patterns of behaviour, such as when someone is at home or out.

Whenever my daughter uses her smartphone to open the smart lock in the house, send a notification to my smartphone.

- *security*: 0. We assume that the daughter uses this instead of a physical key (so both a physical key and the smartphone can be stolen to gain unauthorised access to the house).
- *privacy*: -2. I know the location of my daughter.

When the smart thermostat detects that the temperature rises above 25 degrees, slightly open the window.

- *security*: -3. An adversary may attempt to raise the temperature from outside, e.g. by blocking an outside air conditioning fan].
- privacy: -0.

If a pair of shoes I have 'liked' on Instagram goes on a >20% sale, show it on my smart mirror when I brush my teeth in the morning.

- security: 0.
- *privacy*: -3. My Instagram 'likes' are shared with the smart mirror company.

If I'm the last person in the house and leave, send a notification to my smartwatch if any window in the house is open.

- *security*: +2. Makes sure that I don't leave any windows open.
- *privacy*: -2. The smart house knows where the rest of the household are (or at least that they are not at home).

Five minutes before I need to leave for my next appointment (based on my calendar information), my smart mirror turns on and shows me the route I should take to drive there (or walk there, based on my previous behaviour).

- security: 0.
- *privacy*: -3; My smart mirror connects to my calendar and knows my current and future location.

If my smart mattress detects that I'm sleeping and someone rings the doorbell, do not ring the bell (so as not to wake me up).

- *security*: -2. Ringing the bell is a common way for burglars to scope a house.
- *privacy*: -2. The smart doorbell has knowledge of my sleeping habits.

Every time my smart alarm changes mode (i.e., becomes armed or disarmed), track this in a Google Spreadsheet so that I keep a record.

- *security*: -2. Someone may hack or otherwise access my Google account and get access to whether my alarm is armed or not, or derive a pattern.
- privacy: -0.

When my smart lock becomes locked, arm my smart alarm.

- *security*: +2. I will not forget to arm my smart alarm.
- privacy: 0.

When my smart lock becomes unlocked, disarm my smart alarm.

- *security*: -3. The alarm is not armed if I forget to lock my door, or if I don't lock the door when I am inside; if the smart lock is hacked/tricked then the smart alarm is also disarmed.
- privacy: 0.

When a Google Calendar event matches a phrase I choose (e.g., whenever the event 'Dog Walker' starts), disarm my smart alarm system.

- *security*: -2. Someone can hack my calendar account; some people have automatic addition to the calendar of events from social media or have events automatically added to their calendar from emails.
- privacy: -0.

When I arrive home, cameras on my smart lock use facial recognition in combination with smart watch fitness data to detect my mood and play different types of music accordingly.

- *security*: 0.
- *privacy*: -3. The music service and the smart lock service can collect and track my mood data.

When someone rings the smart doorbell and the facial recognition algorithm on the camera of my doorbell recognizes that it's my sister, unlock the door and disarm the alarm.

- *security*: 0. We assume that the facial recognition algorithm is very accurate and cannot be fooled (i.e. iPhone grade, such that it cannot be fooled by a photograph) and we ignore issues similar to the ones reported with smart lock authorization management. In that sense it is still safer than giving a physical key to a family member (+1). However, it still connects the smart lock to the alarm (-1).
- *privacy*: -2. The picture of my sister is given to the smart alarm company.

When the camera on my smart doorbell detects an unknown/suspicious person (e.g., someone that lingers in my property for over 20 seconds), send a photograph of that person and a text message to my neighbours.

- *security*: +2. The neighbours can be on the lookout.
- *privacy*: -3. The person whose picture is being taken and shared has not consented to that. If done on a scale can lead to a more collective breach of privacy and mass surveillance (Paul, 2019).

When my connected car moves into a 30m radius from my home, open the garage door and disarm the alarm.

- *security*: -2. Someone who steals the car can also enter the house; someone may wait outside and sneak in when the car approaches.
- *privacy*: -0. The smart garage door and the smart alarm company have some location data of my car, but that is minimal and inconsequential (only when the car enters a geofenced location).

Whenever I click a physical button near the front door when I'm

leaving the house: i) turn off all my smart lights, ii) turn down the temperature to 20 degrees on my smart thermostat, iii) turn off all electricity on my smart plugs, iv) arm my smart alarm, v) close the window blinds.

- *security*: 0. Provides a comprehensive security setup, i.e., I will not forget to set up the alarm (+1). It is a pattern of life indicator (-1).
- privacy: -0.

If the supermarket I usually go to has an offer on products that I usually buy, show a notification on the screen of my smart fridge.

- security: 0.
- *privacy*: -3. My buying habits are shared between the supermarket chain and the smart fridge company.

If any local supermarket has an offer on products similar to the ones I usually buy, show a notification on the screen of my smart fridge.

- security: 0.
- *privacy*: -4. My buying habits and my potential purchases are shared between many supermarket chains and the smart fridge company.

Rules not included in experiments

As part of the Delphi Study the following rules were suggested/developed but not adopted:

If it is after midnight and my smart alarm becomes armed, create a 'scene' (dim the living room lights to 20% and the kitchen lights to 40% so that it seems that someone is inside).

- *security*: +1. It gives an occupancy cue to a casual observer or opportunistic burglar (+2). Criminals who are engaging in reconnaissance activities are likely to realise this pattern, which also gives a false sense of security (-1).
- privacy: 0.

When I arrive home (based on my phone's location sensing), disable the smart alarm of the house.

- *security*: -2. Someone may steal my smartphone and gain access. Someone may spoof the location data of my phone and gain access.
- privacy: -0.

When my smart lock gets unlocked, change a little light in my living room to green; When my smart lock gets locked, change a little light in my living room to red (so that I know the status of my front door at all times).

- *security*: -3. Essentially a visual indicator from outside whenever the door is locked/unlocked.
- privacy: -0.

When a drone arrives at my window carrying the food I ordered online, open the window so that the drone can get in.

- *security*: -3. Someone can follow the drone from outside and take advantage of the open window. Someone can mount a camera on the drone and record/see what is happening inside my house.
- *privacy*: -2. Someone can mount a camera on the drone and record/see what is happening inside my house.

If the facial recognition algorithm on the camera of my smart doorbell recognizes someone that I've been exchanging messages with on Tinder, then initiate a romantic 'scene' (turn the lights to an appropriate colour, initiate a romantic playlist on Spotify, turn up the thermostat to 28 degrees).

- security: 0.
- *privacy*: -3. My smart alarm bell system/company has information about my social network activities.

If it is sunny and I am out of the house, activate the robotic lawn mower.

- *security*: -1. An attacker with knowledge of the rule will identify if I am away.
- privacy: -0.

If I am close to a specific supermarket (based on my smart phone location), my smart fridge checks the contents of my fridge and sends me a shopping list.

- *security*: -1. My smart fridge is aware of how far away from the house I am.
- *privacy*: -1. My smart fridge stores consumer data and can manipulate purchasing behaviours.

If I open my treat cupboard more than 5 times within a 12 hour period, then donate £1 to the Childhood Obesity Foundation.

- *security*: 0. Someone who is aware of this rule (e.g., a friend/visitor) can open the cupboard. But the impact would be minimal.
- privacy: 0.

When my blood glucose level drops below a certain value, buzz my smartphone.

- security: 0.
- privacy: 0.

When the soil in my plants dries out, send a notification to my phone to water them.

- security: 0.
- privacy: 0.

Appendix B

The introduction to smart home devices and associated descriptions presented at stage 1 of the experiment are shown below. In addition to the text, participants also saw an accompanying image of the smart device being described.

Smart homes use smart devices that are constantly connected to the internet. These devices can send messages and information to other devices, users and service providers; and they can receive messages and instructions from other devices, users and providers. You can control smart devices through a control panel in your home, an app on your smartphone or tablet (via the cloud), or any Internet-connected computer. Some examples of current and future smart home devices include:

Smart locks replace traditional door locks. Typically, they come with a mobile or web/desktop app that you can use to lock and unlock the door with an icon tap on your smartphone, add permanent and temporary users and set access schedules for specific days and times. Besides front doors, the same concept can be used to open, close and manage smart garage doors and smart windows.

Smart doorbells are equipped with a camera that can record audio and video when someone (e.g., a visitor or a trespasser) is in view. They can send notifications or call the owner's smartphone when someone presses the doorbell button and can enable the owner to speak to whoever is at the door via their smartphone or other internet-connected device.

Smart alarms (or smart home security systems) are sophisticated, internet-connected burglar alarms. They include the functionality of smart locks and smart doorbells, but they also come with contact sensors, motion detectors and sirens. They can be armed, disarmed,

managed and monitored by an internet connected device such as a smart phone, a tablet or a computer.

Smart lights systems consist of internet-connected lightbulbs. This means that one can power the lightbulbs on and off, and adjust the brightness and colour for any lightbulb or groups of lightbulbs from any internet connected device.

In-home *voice assistants* are smart speakers that use Artificial Intelligence to interact, converse and take voice commands from the inhabitants of a smart home. Examples include Apple's HomePod, Amazon's Echo and Google Home.

Smart thermostats connect the home heating system to the internet and let you change the temperature, switch the heating on or off, and create and manage heating schedules from any internet connected device.

Smart mirrors are internet-connected mirrors that can also display information, such as time, weather, calendar, news etc.

Smart fridges are connected to the internet and have an interactive display. So, the fridge can use internet resources (e.g., look up recipes), send or receive messages from a smartphone, or be managed by the interactive display or a smartphone app (e.g., control the temperature or track the contents via an internal camera).

Smart window blinds can be opened and closed via an internet connected device.

Smart plugs are plugged into power outlets and can transform home appliances into smart devices. These devices can then be controlled and managed with an app via any internet-connected device. So, one can turn on and off the plugged-in devices, but also monitor their energy consumption.

Connected cars are vehicles with internet access. This allows devices, both inside (e.g., sensors and on-board computers) and outside the car (e.g., other cars, houses, and infrastructure), to interact with each other.

Appendix C

The below outlines the implicit tasks used in Experiment 2:

No Prime Condition: This was the control condition inasmuch as it was neutral with regard to security or privacy. This condition used as a decision-making activity involving two tasks that required participants to select between two smart light-bulbs based on their features (Table C1). By way of example, one of these tasks was as follows:

'A friend of yours has decided to buy smart light bulbs for their new home. After an internet search you come across the following table. Based on the characteristics of the two smart light bulbs below, which product would you recommend to your friend?'

Security Prime Condition: Participants were implicitly primed to think about the security of their home by performing two exercises that asked them to select which of two houses was more likely to be burgled based on eight characteristics of each house (Table C2). This exercise was adapted from previous literature on decision-making among expert and novice residential burglars (Garcia-Retamero and Dhami, 2009) and one of the two problem-solving tasks follows:

'Based on the description of the two residential properties below, which one do you think would be more likely to be burgled?'

Privacy Prime Condition: Participants were implicitly primed to think about the privacy of their data by requiring them to perform two exercises that asked them to select between which application they would be willing to install on their smartphone (Table C3). The first exercise asked them to select between two calorie trackers and the second between word games.

One of the exercises was as follows:

'You have decided to track your calories, because you are concerned that you have started putting on some weight lately. After an internet search you come across the following table describing two popular calorie tracker applications for your smartphone. Which one would you install?

References

Atlam, H.F., Alenezi, A., Walters, R.J., Wills, G.B., Daniel, J., 2017. Developing an adaptive Risk-based access control model for the Internet of Things. In: 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, pp. 655–661.

Atlam, H.F., Walters, R.J., Wills, G.B., 2018. Fog computing and the internet of things: a review. In: Big Data Cognit. Comput., 2, p. 10. https://doi.org/10.3390/bdcc2020010.

Atlam, H.F., Wills, G.B., 2020. IoT security, privacy, safety and ethics. In: Farsi, M., Daneshkhah, A., Hosseinian-Far, A., Jahankhani, H. (Eds.), Digital Twin Technologies and Smart Cities. Internet of Things (Technology, Communications and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-18732-3_8.

Bargh, J.A., Chartrand, T.L., 2000. The mind in the middle: a practical guide to priming and automaticity research. In: Reis, H.T. (Ed.), Handbook of Research Methods in Social and Personality Psychology. Cambridge University Press, New York, NY, pp. 253–285.

Barricelli, B.R., Cassano, F., Fogli, D., Piccinno, A., 2019. End-user development, end-user programming and end-user software engineering: A systematic mapping study. J. Syst. Softw. 149, 101–137. https://doi.org/10.1016/j.jss.2018.11.041.

Brackenbury, W., Deora, A., Ritchey, J., Vallee, J., He, W., et al., 2019. How users interpret bugs in trigger-action programming. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, pp. 1–12. https://doi.org/10.1145/3290605.3300782.

Canziani, B., MacSween, S., 2021. Consumer acceptance of voice-activated smart home devices for product information seeking and online ordering. Comput. Hum. Behav. 119, 106714 https://doi.org/10.1016/j.chb.2021.106714.

Check Point (2020). The dark side of smart lighting: Check Point research shows how business and home networks can be hacked from a lightbulb. Check Point Blog. Retrieved March 9, 2020 from https://blog.checkpoint.com/2020/02/05/the-dark-side-of-smart-lighting-check-point-research-shows-how-business-and-home-networks-can-be-hacked-from-a-lightbulb/.

Chong, I., Ge, H., Li, N., Proctor, R.W., 2018. Influence of privacy priming and security framing on mobile app selection. Comput. Secur. 78, 143–154. https://doi.org/10.1016/j.cose.2018.06.005.

Cobb, C., Surbatovich, M., Kawakami, A., Sharif, M., Bauer, L., Das, A., Jia, L., 2020. How risky are real users'{IFTTT} applets?. In: Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020), pp. 505–529.

Corno, F., De Russis, L., Monge Roffarello, A., 2019a. Empowering end users in debugging trigger-action rules. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, pp. 1–13. https://doi.org/10.1145/3290605.3300618.

Corno, F., De Russis, L., Monge Roffarello, A., 2019b. My IoT puzzle: debugging IF-THEN rules through the jigsaw metaphor. In: Malizia, A., Valtolina, S., Morch, A., Serrano, A., Stratton, A. (Eds.), End-User Development. IS-EUD 2019. Lecture Notes in Computer Science. Springer, Cham, pp. 18–33. https://doi.org/10.1007/978-3-030-24781-2_2.

Dabbagh, M., Rayes, A., 2017. Internet of Things security and privacy. Internet of Things from Hype to Reality. Springer, Cham, pp. 211–238. https://doi.org/10.1007/978-3-319-44860-2_8.

Desolda, G., Ardito, C., Matera, M., 2017. Empowering end users to customize their smart environments: model, composition paradigms, and domain-specific tools. ACM *Trans. Comput.-Hum. Interaction* 24 (2), 1–52. https://doi.org/10.1145/3057859.

Diamond, I.R., Grant, R.C., Feldman, B.M., Pencharz, P.B., Ling, S.C., Moore, A.M., Wales, P.W., 2014. Defining consensus: a systematic review recommends methodologic criteria for reporting of Delphi studies. J. Clin. Epidemiol. 67 (4), 401–409. https://doi.org/10.1016/j.jclinepi.2013.12.002.

Donohoe, H.M., Needham, R.D., 2009. Moving best practice forward: Delphi characteristics, advantages, potential problems, and solutions. Int. J. Tour. Res. 11 (5), 415–437. https://doi.org/10.1002/jtr.709.

Fernandes, E., Rahmati, A., Jung, J., Prakash, A., 2018. Decentralized action integrity for trigger-action iot platforms. In: Proceedings 2018 Network and Distributed System Security Symposium. https://doi.org/10.14722/ndss.2018.23119.

Furey, E., Blue, J., 2018. She knows too much–voice command devices and privacy. In: 2018 29th Irish Signals and Systems Conference (ISSC). IEEE, pp. 1–6.

Garcia-Retamero, R., Dhami, M.K., 2009. Take-the-best in expert-novice decision strategies for residential burglary. Psychon. Bull. Rev. 16 (1), 163–169. https://doi.org/10.3758/PBR.16.1.163.

Ghorayeb, A., Comber, R., Gooberman-Hill, R., 2021. Older adults' perspectives of smart home technology: are we developing the technology that older people want? Int. J. Hum. Comput. Stud. 147, 102571 https://doi.org/10.1016/j.ijhcs.2020.102571.

Harborth, D., Pape, S., 2020. How Privacy concerns, trust and risk beliefs, and privacy literacy influence users' intentions to use privacy-enhancing technologies. ACM SIGMIS Database 51 (1), 51–69. https://doi.org/10.1145/3380799.3380805.

Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine, J.R., Filippoupolitis, A., Roesch, E., 2018. A taxonomy of cyber-physical threats and impact in the smart home. Comput. Secur. 78, 398–428.

Huang, J., Cakmak, M., 2015. Supporting mental model accuracy in trigger-action programming. In: Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing, pp. 215–225. https://doi.org/10.1145/2750858.2805830.

Ho, G., Leung, D., Mishra, P., Hosseini, A., Song, D., Wagner, D., 2016. Smart locks: lessons for securing commodity Internet of Things Devices. In: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, pp. 461–472. https://doi.org/10.1145/2897845.2897886.

Kelley, P.G., Cranor, L.F., Sadeh, N., 2013. Privacy as part of the app decision-making process. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 3393–3402.
Linstone, H.A., Turoff, M., 1975. The Delphi Method: Techniques and applications. Addison-Wesley Educational Publishers Inc, London.
Malhotra, N.K., Kim, S.S., Agarwal, J., 2004. Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. Inf. Syst. Res. 15 (4), 336–355. https://doi.org/10.1287/isre.1040.0032.
Manandhar, S., Moran, K., Kafle, K., Tang, R., Poshyvanyk, D., Nadkarni, A., 2020. Towards a natural perspective of smart homes for practical security and safety analyses. In: 2020 IEEE Symposium on Security and Privacy (sp). IEEE, pp. 482–499. https://doi.org/10.1109/SP40000.2020.00062.
Manca, M., Paternò, F., Santoro, C., Corcella, L., 2019. Supporting end-user debugging of trigger-action rules for IoT applications. Int. J. Hum. Comput. Stud. 123, 56–69.
McAlaney, J., Frumkin, L.A., Benson, V. (Eds.), 2018. Psychological and Behavioral Examinations in Cyber Security. IGI Global, 10.4018/978-1-5225-4053-3.
Molden, D.C., 2014. Understanding priming effects in social psychology: what is "social priming" and how does it occur? Soc. Cogn. 32, 1–11. Supplement.
Morgan, P.L., Williams, E.J., Zook, N.A., Christopher, G., 2018. Exploring older adult susceptibility to fraudulent computer pop-up interruptions. In: International Conference on Applied Human Factors and Ergonomics, pp. 56–68.
Nichols, A.L., Maner, J.K., 2008. The good-subject effect: Investigating participant demand characteristics. J. Gen. Psychol. 135 (2), 151–166. https://doi.org/10.3200/GENP.135.2.151-166.
Ogonji, M.M., Okeyo, G., Wafula, J.M., 2020. A survey on privacy and security of internet of things. Computer Science Review 38, 100312. https://doi.org/10.1016/j.cosrev.2020.100312.
Orne, M.T., 1962. On the social psychology of the psychological experiment: with particular reference to demand characteristics and their implications. Am. Psychol. 17 (11), 776–783. https://doi.org/10.1037/h0043424.
Palekar, M., Fernandes, E., Roesner, F., 2019. Analysis of the susceptibility of smart home programming interfaces to end user error. In: Proceedings of the 2019 IEEE Symposium on Security and Privacy Workshops, pp. 138–143. https://doi.org/10.1109/SPW.2019.00034.
Papies, E.K., 2016. Health goal priming as a situated intervention tool: how to benefit from nonconscious motivational routes to health behaviour. Health Psychol. Rev. 10 (4), 408–424. https://doi.org/10.1080/17437199.2016.1183506.
Parekh, G., DeLatte, D., Herman, G.L., Oliva, L., Phatak, D., Scheponik, T., Sherman, A. T., 2017. Identifying core concepts of cybersecurity: results of two Delphi processes. IEEE Trans. Educ. 61 (1), 11–20. https://doi.org/10.1109/TE.2017.2715174.
Park, J., Amendah, E., Lee, Y., Hyun, H., 2019. M-payment service: Interplay of perceived risk, benefit, and trust in service adoption. Hum. Factors Ergon. Manuf. Serv. Ind. 29 (1), 31–43. https://doi.org/10.1002/hfm.20750.
Parks Associates (2019). *79% of consumers are concerned about data security or privacy issues*. https://www.parksassociates.com/blog/article/pr-07092019.
Paul, K., 2019. Amazon's doorbell camera Ring is working with police – and controlling what they say. The Guardian. Retrieved March 2, 2020 from https://www.theguardian.com/technology/2019/aug/29/ring-amazon-police-partnership-social-media-neighbor.
Ratchford, M., Barnhart, M., 2012. Development and validation of the technology adoption propensity (TAP) index. J. Bus. Res. 65 (8), 1209–1215. https://doi.org/10.1016/j.jbusres.2011.07.001.
Ronen, E., Shamir, A., Weingarten, A.O., O'Flynn, C, 2017. IoT goes nuclear: creating a ZigBee chain reaction. In: 2017 IEEE Symposium on Security and Privacy (SP), pp. 195–212.
Saltzer, J.H., Schroeder, M.D., 1975. The protection of information in computer systems. Proc. IEEE 63 (9), 1278–1308.
Shaw, R.G., Mitchell-Olds, T., 1993. ANOVA for unbalanced data: an overview. Ecology 74 (6), 1638–1645.
Statista (2021). *Smart home United Kingdom.* https://www.statista.com/outlook/dmo/smart-home/united-kingdom.
Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A., 2015. Security, privacy and trust in Internet of Things: the road ahead. Comput. Netw. 76, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008.
Strengers, Y., Kennedy, J., Arcari, P., Nicholls, L., Gregg, M., 2019. Protection, productivity and pleasure in the smart home: emerging expectations and gendered insights from Australian early adopters. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, pp. 1–13. https://doi.org/10.1145/3290605.3300875.
Sugawara, T., Cyr, B., Rampazzi, S., Genkin, D., Fu, K., 2020. Light Commands:{Laser-Based} Audio Injection Attacks on {Voice-Controllable} Systems. In 29th USENIX Security Symposium (USENIX Security 20) 2631–2648.
Surbatovich, M., Aljuraidan, J., Bauer, L., Das, A., Jia, L., 2017. Some recipes can do more than spoil your appetite: analyzing the security and privacy risks of IFTTT recipes. In: Proceedings of the 26th International Conference on World Wide Web, pp. 1501–1510. https://doi.org/10.1145/3038912.3052709.
Symantec. (2017). *ISTR special report: a guide to the security of voice-activated smart speakers*. Retrieved March 2, 2020 from https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-security-voice-activated-smart-speakers-en.pdf.
Tate, K., Stewart, A.J., Daly, M., 2014. Influencing green behaviour through environmental goal priming: the mediating role of automatic evaluation. J. Environ. Psychol. 38, 225–232. https://doi.org/10.1016/j.jenvp.2014.02.004.
Ur, B., Ho, M.P.Y., Brawner, S., Lee, J., Mennickenz, S.P., et al., 2016. Trigger-action programming in the wild: an analysis of 200,000 IFTTT recipes. In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, pp. 3227–3231. https://doi.org/10.1145/2858036.2858556.
Van Oorschot, P.C., Smith, S.W., 2019. The Internet of Things: security challenges. IEEE *Secur. Privacy* 17 (5), 7–9. https://doi.org/10.1109/MSEC.2019.2925918.
Vox. (2020). *Alexa records you more often than you think*. Retrieved March 2, 2020 from https://www.vox.com/recode/2020/2/21/21032140/alexa-amazon-google-home-siri-apple-microsoft-cortana-recording.
Weller, J.A., Levin, I.P., Denburg, N.L., 2011. Trajectory of risky decision making for potential gains and losses from ages 5 to 85. J. Behav. Decis. Making 24 (4), 331–344.
Westin, A.F., 1968. Privacy and freedom. Washington Lee Law Rev. 25 (1), 166.
Whalen, R., Harrold, J., Child, S., Halford, J., Boyland, E., 2018. The health halo trend in UK television food advertising viewed by children: the rise of implicit and explicit health messaging in the promotion of unhealthy foods. Int. J. Environ. Res. Public Health 15 (3), 560. https://doi.org/10.3390/ijerph15030560.
Williams, E.J., Morgan, P.L., Joinson, A.N., 2017. Press accept to update now: Individual differences in susceptibility to malevolent interruptions. Decis. Supp. Syst. 96, 119–129. https://doi.org/10.1016/j.dss.2017.02.014.
Woo, J.B., Lim, Y.K., 2015. User experience in do-it-yourself-style smart homes. In: Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing, pp. 779–790. https://doi.org/10.1145/2750858.2806063.
Yang, H., Lee, H., Zo, H., 2017. User acceptance of smart home services: an extension of the theory of planned behavior. Ind. Manag. Data Syst. 117 (1), 68–89. https://doi.org/10.1108/IMDS-01-2016-0017.
Zeng, E., Roesner, F., 2019. Understanding and improving security and privacy in multi-user smart homes: a design exploration and in-home user study. In: 28th {USENIX} Security Symposium, pp. 159–176.
Zheng, S., Apthorpe, N., Chetty, M., Feamster, N., 2018. User perceptions of smart home IoT privacy. Proc. ACM Hum.-Comput. Interact. 2 (CSCW), 1–20.