EMILY COLLINS, PHILLIP MORGAN & DYLAN JONES

IF THIS THEN...WHAT?

SECURITY AND PRIVACY IN TRIGGER-ACTION SYSTEMS

Can people be primed to think about security and privacy when setting trigger-action rules for smart home devices?

With the average UK household having more than ten Internet of Things (IoT) devices, more people are looking to find ways to connect apps and devices to create more complex systems in their homes. Trigger-action rules, such as those supported by IFTTT (short for If This Then That), are one way that this can be done.

IFTTT allows users to program a script – or 'applet' – to automate tasks, using some type of event in one app or device to trigger an output in another. For those who do not want to program their own, IFTTT estimate there are over 54 million existing applets available to download and deploy.

> Users are often not able to anticipate or fully understand the security implications of these rules, especially when multiple rules create unpredictable knock-on effects.

The ease with which multiple applets can be created and simultaneously deployed presents several security and privacy issues. Users are often not able to anticipate or fully understand the security implications of these rules, especially when multiple rules create unpredictable knock-on effects – as they are often concentrating on their goal of automating a process or creating a convenient shortcut, safety can easily be pushed into the background.

Finding ways to encourage users to consider security and privacy when choosing these rules is important in maintaining safety.

Our research at Cardiff University looked at how people make decisions when selecting IFTTT rules and whether priming them in different ways might promote greater consideration of the security and privacy implications of the rules they choose.

First, we created a series of IFTTT rules and asked independent experts to rate each on security and privacy. For example, 'When the camera on my smart doorbell detects an unknown/suspicious person (e.g. someone who lingers on my property for over 20 seconds), send a photograph of that person and a text message to my neighbours'. This created a security and privacy score for each rule.

Our research asked participants to judge which of these rules they would enable in a given context through a game-based, experimental design. Some participants were just shown the rules, whereas others were primed to think about the security and privacy of the rules that they chose.

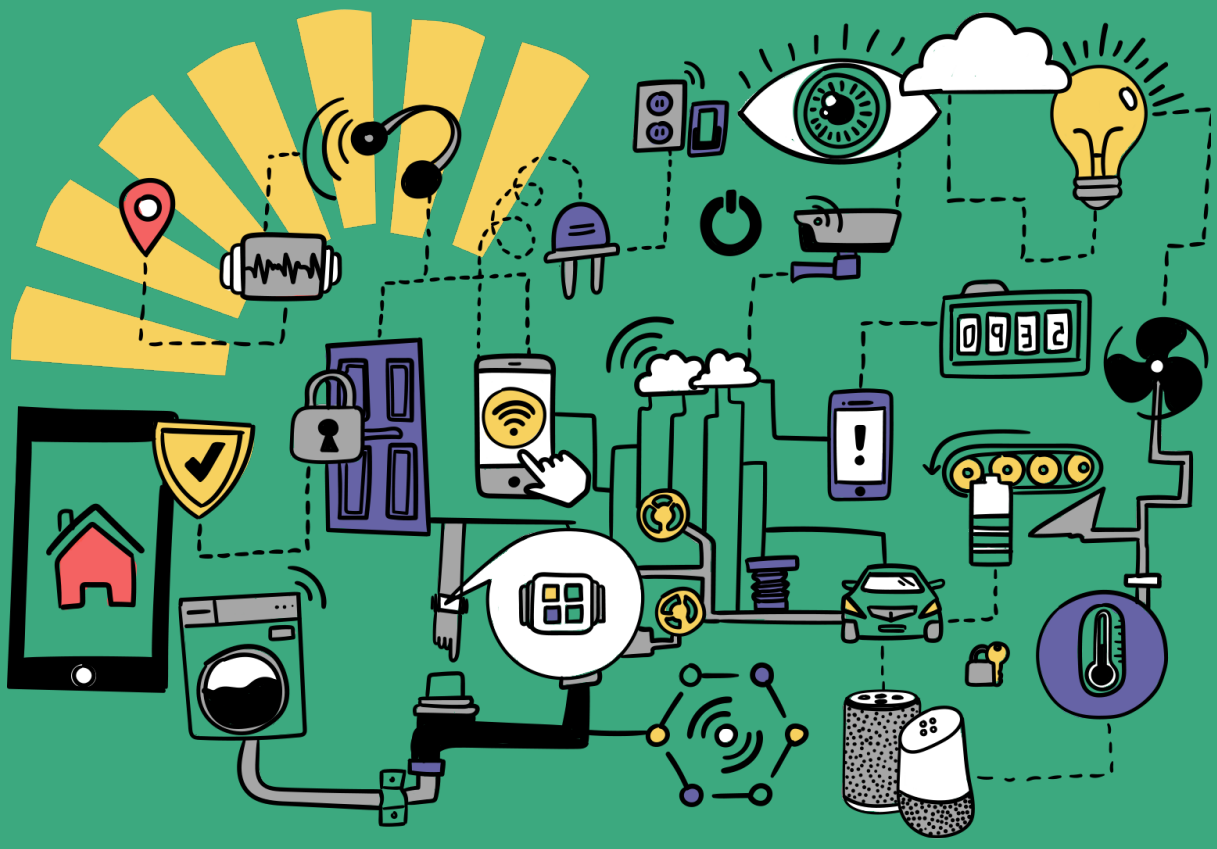
EXPLICIT PRIMING

In our first study, we used 'explicit priming', involving direct instructions to focus on either security or privacy. We found that these primes led to people choosing rules that were rated higher in security or privacy by our experts; security primes improved security scores and privacy primes improved privacy scores, although interestingly the security primes also led to lower privacy scores.

IMPLICIT PRIMING

In our second study, we used 'implicit priming' in the form of seemingly unrelated activities that involved solving a security or privacy problem. We found that these improved security scores, albeit less effectively than the explicit primes did. Overall, privacy and security priming were found to work in different ways depending on whether the priming was explicit or implicit.

Building on the work of our colleagues at the University of Bristol (What Influences Consumer Adoption and Secure Use of Smart Home Technology?), we also investigated whether



individual characteristics – namely propensity to adopt technology, perception of security risks, trusting beliefs, and privacy concerns – impacted people's choices.

FINDINGS

We found that users who showed greater awareness of the privacy practices of smart home companies tended to produce high security scores. They were less likely to take risks when enabling rules to connect devices and services.

> A preoccupation with privacy may encourage security to be neglected.

Increased concern about exercising control over personal information was associated with lower security scores, suggesting a preoccupation with privacy may encourage security to be neglected.

There were also strong suggestions that the more people trust online companies, or the more users expect to benefit from smart home technologies, the less likely they are to keep their personal information private. Enthusiasts for IFTTT and technology are more willing to put their privacy at risk, as one might expect. This shows how opinions that people hold about technology carry over to the choices they make when setting up smart home technology.

Overall, the findings of this project reinforce the importance of stressing the risks to security and privacy of IFTTT in smart home contexts. Consumers would benefit from more support in understanding how their systems are configured, as well as the potential knock-on effects of further device upgrades and additions, to facilitate the secure adoption of smart home technology.

Dr Emily I M Collins is a Lecturer in Human Factors at Cardiff University.

Professor Phillip L Morgan is a Professor in Human Factors and Cognitive Science within the School of Psychology at Cardiff University, Director of the Human Factors Excellence Research Group (HuFEx) and Director of Research within the AI, Robotics and Human Machines Systems Research Centre (IROHMS).

Professor Dylan M Jones is a Senior Professor within the School of Psychology at Cardiff University and Co-Director of HuFEx and IROHMS.