Calibrating Trust Toward an Autonomous Image Classifier

Martin Ingram¹, ², Reuben Moreton², Benjamin Gancz², and Frank Pollick¹
¹ School of Psychology, University of Glasgow
² Qumodo, London

Successful adoption of autonomous systems requires appropriate trust from human users, with trust calibrated to reflect true system performance. Autonomous image classifiers are one such example and can be used in a variety of settings to independently identify the contents of image data. We investigated users’ trust when collaborating with an autonomous image classifier system (AICS) that we created using the AlexNet model (Krizhevsky et al., Advances in neural information processing systems, 2012). Participants collaborated with the classifier during an image classification task in which the classifier provided labels that either correctly or incorrectly described the contents of images. This task was complicated by the quality of the images processed by the human-classifier team: 50% of the trials featured images that were cropped and blurred, thereby partially obscuring their contents. Across 160 single-image trials, we examined trust toward the classifier, while we also looked at how participants complied with the classifier by accepting or rejecting the labels it provided. Furthermore, we investigated whether trust toward the classifier could be improved by increasing the transparency of the classifier’s interface, by displaying system confidence information (SCI) in three different ways, which were compared to a control interface without confidence information. Results showed that trust toward the classifier was primarily based on system performance, yet this also was influenced by the quality of the images and individual differences among participants. While participants typically preferred classifier interfaces that presented confidence information, it did not appear to improve participants’ trust toward the classifier.

Keywords: trust, autonomous systems, image classifier, human–machine collaboration

The success of new technologies is dependent on whether they are accepted by the end user. Our understanding of how users accept new technologies has developed over time, the initial Technology Acceptance Model (TAM) put forward by Davis et al. (1989) was heavily centred on the perceived usefulness and perceived ease of use of the system, as the primary determinants for technology acceptance. More recently, extensive work by Venkatesh et al. (2012) has sought to develop upon earlier iterations of TAM by integrating further, more diverse determinants of acceptance, such as system price, the user’s habits, and even the hedonistic pleasure gained from using the system (Venkatesh, 2015). This suggests that innovation alone is not enough for new technologies to be successful, and that there is a myriad of psychological, social, and environmental factors that inform the ultimate acceptance of technology.

While the successful adoption of new technologies is tied to users’ acceptance of them, the users also need to learn to use the technology correctly. Just because someone accepts a new technology, it does not automatically follow that they will use it appropriately. This is particularly the case with autonomous systems, which are technologies that use Artificial Intelligence (AI) to undertake tasks with a degree of independence from their user. As these autonomous systems become more advanced, their capacity for complex tasks also increases, yet with this the opportunity for errors increases too (Parasuraman et al., 2000). As such the success of autonomous systems also relies upon appropriate trust from their human user, to ensure these systems are used correctly. Ideally, operators’ trust will be calibrated to reflect the actual performance capabilities of the autonomous system, ensuring they do not distract a functional system (too little trust), or mistrust a dysfunctional system (too much trust; Muir, 1987; Parasuraman & Riley, 1997). In this study, we sought to understand how humans calibrate their trust toward an autonomous image classifier system (AICS).
Autonomous Image Classifier Systems

AICS are technologies that can independently classify the contents of image-based data, using advances in deep learning and convolutional neural network research (Chan et al., 2015; Howard, 2013). A major advantage of AICS is that they can process large quantities of data quickly and independently, thereby reducing demand on human users. For example, in the U.K., London’s Metropolitan police force is interested in using AICS to help process digital forensic evidence, to reduce their officers’ workload and limit their exposure to graphic content (Murphy, 2017). Moreover, AICS can be trained to distinguish specific, highly complicated patterns and features. An AICS was recently able to identify breast cancer with an accuracy comparable to human experts (McKinney et al., 2020). AICS can also be used in lower stakes settings, for example, the popular app “PlantNet” can provide users with classifications for images of plants and flowers that they encounter (Göéau et al., 2014). Even though these applications are impressive, the performance of AICS can reflect the expertise and potential biases of the engineers who design the systems, as well as the quality of the data set used to train their algorithms (Danks & London, 2017; Rudin, 2019). Thus, AICS are vulnerable to errors and will require appropriate trust from human operators. This is particularly important, given the potential application of AICS in a wide variety of settings, where AICS may be responsible for supporting high stakes decisions. Thus, we sought to examine how users calibrated their trust toward an AICS, and how this trust translated into compliance with the system’s decisions, when completing an image classification task. By doing so, we provide an insight into trust specifically toward AICS, which we hope will benefit the design and deployment of AICS in real-world settings, while also providing further insights for the wider trust-in-automation literature.

Understanding Trust Toward Automation

Across the literature, trust-in-automation has been studied in a wide variety of human–machine teams, and arguably has most commonly been studied with autonomous vehicles (Jing et al., 2020). When considering how technology is used in different human–machine teams, Larson and DeChurch (2020) make a distinction between technology and agents. Technology is something that is used by teams to achieve their goals, much like a tool, while agents fill a distinct role within the team which goes beyond mere augmentation, and inherently improves the team’s performance as a result (Larson & DeChurch, 2020). For agents, they also draw a distinction between robots, which are agents with embodied physical characteristics, and AI which are disembodied agents that perform tasks that traditionally require human intelligence, such as visual identification and decision-making. Trust has previously been studied with both robot-based agents (Desai et al., 2013; Selkowitz et al., 2017), and with AI-based agents, such as automated software repair systems (Ryan et al., 2019), virtual cognitive agents (de Visser et al., 2016; Hertz & Wiese, 2019), and decision support systems (Sauer et al., 2016; Yu et al., 2019; Zhang et al., 2020). Regarding AICS, these systems most closely align with the examples of AI-based agents. It should however be noted that within our experimental design, we afforded the AICS limited agency, as human users supervised each classification decision, with the authority to overrule each one. Whereas in real-world applications, AICS may be employed as agents with greater autonomy when working within teams.

We interpreted trust toward an AICS through the lens of Hoff and Bashir (2015) model of trust toward automation, which separates trust into three broad layers. Dispositional Trust relates to stable human-centric factors, such as culture, age, and personality traits, which inform users’ general disposition toward technology. This would reflect the users’ attitudes toward the AICS, and more broadly technology in general. Situational Trust relates to fluctuating human-centric factors, such as mood and attention, as well as environmental factors, such as task difficulty, workload, and organizational setting, which can all vary over time. We believe that when using an AICS, a significant factor for operators’ trust would be the quality of images being processed, which could increase the difficulty of system classifications, particularly if the operator feels they could easily classify the images themselves. Finally, Learned Trust is split into two separate sublayers: Initial Learned Trust that reflects the user’s historical experience of similar systems, and the reputation of the current system, while Dynamic Learned Trust reflects their ongoing experiences of working with the system. When working with an AICS, Learned Trust will likely be informed by the users’ ability to interpret the system’s decision-making, particularly if the image is difficult to classify. Additionally, in industrial applications, operators may have previous experiences with other AICS, which may inform their trust toward newly introduced systems. Hoff and Bashir (2015) suggest these three layers of trust combine to ultimately inform how users rely upon the autonomous systems during collaboration, which would be crucial for appropriate use of AICS. Therefore, when investigating trust toward an AICS, we created experimental manipulations that were consistent with Hoff and Bashir (2015) model and contextualized our hypotheses and subsequent findings within their theoretical framework.

System Performance

Hoff and Bashir (2015) demonstrate the complex relationship between human, mechanical, and environmental factors that combine to inform trust toward autonomous systems. However, their model stipulates that when interacting with automation, system performance is the central modulator of trust toward automation. In this vein, Yu et al. (2019) reported close relationships between perceived system accuracy, trust, and reliance upon an automated fault detection system, and demonstrated that users will modulate their trust and reliance in response to system performance. Thus, when collaborating with an AICS, we anticipated system performance, defined as the classifier’s ability to correctly label the contents of images, will have the biggest influence on trust. (H1a) System performance, whether the classifier’s label correctly describes images, will have the strongest influence on trust toward the classifier.

Image Clarity

While system performance should be the main driver of trust toward the AICS, the classifier’s performance itself is likely to be dependent upon the quality of images being processed. Hoff and Bashir (2015) Situational Trust encompasses factors which make tasks more difficult to accomplish, and we believe image quality would be a particularly important factor within the context of AICS use. When images have lower clarity, through factors such as
occlusion and blurring, the contents of the image may be harder for human users to identify. Moreover, when an AICS processes lower clarity images, the system’s performance is also likely to be harder to evaluate, given the increased uncertainty of the contents of the images, which may itself impact upon trust toward the classifier. Thus, when working with an AICS the quality of the images processed could be considered as an environmental factor, given the operator may have limited control over image clarity. A similar issue was explored in a study by Merritt et al. (2013) involving trust toward an automated baggage scanner where trust toward the scanner was affected by the difficulty of the task. Specifically, trust was lowest in blocks where the scanner’s performance was considered as “obviously poor,” and highest when “obviously good,” given the presence of weapons was made relatively obvious to participants. However, in the more difficult, ambiguous block, where the contents of luggage were cluttered, trust was found to be lower than the “obviously good” block, yet higher than the “obviously bad” block, illustrating the effect of task difficulty. Similar findings were reported in another study that involved an automated letter detection aid, in which participants were more likely to accept the system’s advice in trials with higher difficulty (Schwark et al., 2010). This suggests that the difficulty of the task facing human–machine teams may influence how human users interpret and use automated system advice. Of course, the influence of task difficulty is likely to vary between autonomous systems, as different systems will be employed in different occupational settings, with varying consequences associated with system errors. Nonetheless, we anticipated that the relationship between system performance and trust toward the AICS would be modulated by the quality of the image being processed: (H1b) Image Clarity will significantly interact with system performance when predicting trust toward the classifier. With unclear trials, trust will be lower when the classifier is correct, and higher when the classifier is incorrect, illustrating participants’ uncertainty about the classifier’s performance.

**Individual Differences**

Trust toward an AICS could also be influenced by the operator’s cognitive understanding of the system and task, which can be prone to biases intrinsic to each individual (Israelsen & Ahmed, 2019). Some examples of these biases include: Automation Bias, where automation performance is perceived as inherently superior to human performance (Goddard et al., 2011); and Perfect Automation Schema, where individuals may believe that automation is almost always perfectly reliable (Dzindolet et al., 2002). These biases reflect differences in trust stemming from the experiences of individual human users. Hoff and Bashir (2015) characterize biases toward trusting machines as a form of Dispositional Trust, which are relatively stable over time, and reflect users’ tendencies independently of context. In order to understand how human-centric factors influenced trust toward the AICS, we considered each participant’s score in the Propensity to Trust Machines Questionnaire (PTMQ; Merritt, 2011), as a form of Dispositional Trust. PTMQ scores can be used to characterize each user’s predisposition toward trusting technology, in which higher scores represent higher self-reported tendencies to trust new technologies. The use of PTMQ was highlighted in the study by Merritt et al. (2013), which showed individuals with higher PTMQ scores had higher trust toward the automated baggage scanner when it processed luggage with cluttered contents, during the ambiguous performance block. This suggests that users with higher PTMQ scores were less likely to have their trust influenced by the difficulty of the task, even though the uncertainty of task success would make it harder to evaluate system performance more accurately. Thus, users’ existing tendencies toward trusting machines may influence trust, even when environmental factors complicate their evaluations: (H1c) Participants with higher Propensity to Trust Machines scores will trust the classifier more when processing unclear images, where performance may be more difficult to evaluate.

**Improving Trust Through Transparency**

Trust toward autonomous systems may also be improved when system decision-making is made more transparent (Tomsett et al., 2020). For example, drivers reported greater trust toward a driving aid within an autonomous vehicle simulator when provided with explanatory feedback messages (Koo et al., 2015). The Situation awareness-based Agent Transparency (SAT) model proposes that autonomous system transparency can be improved by providing users with more detailed information about the current task (Chen et al., 2014). Within the lens of the SAT model, human users may calibrate their trust more appropriately if the system provides more detailed information about its current task (Chen et al., 2014). Using the SAT model, Selkowitz et al. (2017) report increased trust toward an autonomous robotic squad member as it provided users with more detailed situational information, such as system motivations and predicted task outcomes. However, this trend was not apparent in the condition with the most information, implying there may be a limit to how much information is beneficial to users’ trust (Selkowitz et al., 2017). Hoff and Bashir (2015) suggest that these design features which increase transparency can help users to understand the system’s purpose and process when carrying out tasks, thereby improving the user’s Learned Trust. Thus, we sought to understand if we could improve trust toward an AICS by making its decisions more transparent through displays of system confidence information (SCI).

SCI is a representation of system certainty when carrying out tasks and can benefit trust toward autonomous systems (Zhang et al., 2020). For example, SCI cues helped users to appropriately align their trust toward a navigational robot; lowering trust when confidence was low to accommodate poorer performance, and elevating trust when confidence was high (Desai et al., 2013). Similarly, Verame et al. (2016) report individuals were more likely to accept the decisions of an autonomous document reader when it displayed “very high” confidence, compared to when displaying “medium” or “low” confidence. This suggests SCI may improve system transparency, and in turn users’ trust and strategies for collaboration. However, there are a variety of ways that SCI can be represented within the interface of autonomous systems. Previous examples include confidence discretized into high/medium/low categories, represented with icons (Desai et al., 2013) or with text (Verame et al., 2016); as numerical probabilities (9/10 = high confidence; Zhang et al., 2020); or visually through the color and opacity of icons (Selkowitz et al., 2017). Within the context of the SAT model, it is possible that more detailed forms of SCI would make AICS decision-making more transparent, and therefore be most likely to improve users’ trust toward the system.
Regarding systems specifically designed to classify image-based or text-based content, Ribeiro et al. (2016) suggest SCI could be displayed through a bar graph to illustrate the probabilities of the most likely options for each decision. Arguably Ribeiro et al.’s (2016) suggestion presents SCI in a more transparent format than the previous examples above, as it provides the user with the system’s confidence for the final decision relative to the confidence for other likely classification options. However, there is conflicting evidence surrounding the utility of bar graphs when conveying information, as evidence suggests they can be difficult to comprehend (Chapfalkar & Wu, 2020), and can lead to biases in readers’ thinking (Godau et al., 2016). Contrarily, bar graphs have been considered useful when illustrating results with borderline differences, and reportedly require less time to interpret than raw data tables alone (Brewer et al., 2012). Therefore, we created three separate experimental interfaces that illustrated SCI in different formats and compared them against an interface without SCI (Control Interface). We adopted Ribeiro et al.’s (2016) recommendation of using a bar graph to illustrate SCI (Graphical Interface), we also displayed SCI using text-based percentages (0%–100%; Numerical Interface), and lastly used color cues to represent SCI discretized into high/medium/low categories (Iconography Interface). Thus, we explored the benefits of displaying SCI within the AICS interface: (H2a) Relative to the control interface, the confidence information presented within the experimental interfaces will improve overall trust toward the classifier.

We also sought to understand whether SCI would be more useful when the task difficulty increased, specifically when the classifier processes unclear images: (H2b) When processing unclear images, trust will be higher toward the experimental interfaces because they provide users with more information.

Lastly, we explored whether the addition of SCI in the experimental interfaces would increase users’ workload, measured through subjective task load, and the amount of time participants spent in each trial: (H2c) When working with the experimental interfaces, participants’ task load will be higher given interfaces with SCI present more information per trial.

### Methods

#### Participants

74 participants (37 F, 36 M, 1 Non-Binary), primarily university students (Mean Age = 26.2, Min = 19, Max = 55), were recruited through the University of Glasgow’s School of Psychology subject pool. All participants were compensated at a rate of £6 per hour for their time. 51% of participants considered themselves native English speakers. Ethical approval was obtained from the University of Glasgow, College of Science and Engineering ethics committee.

#### Design

We used a $2 \times 2 \times 4$ within-subjects design where participants saw two levels of Classifier Performance (Correct, Incorrect) combined with two levels of Image Clarity (Clear, Unclear), within each of the four Interface-specific blocks (Control, Graphical, Iconography, Numerical). In each single-image trial ($n = 160$) the classifier’s label would either correctly or incorrectly match the image displayed, which was purposely made easy or difficult to evaluate due to the clarity of the image. The ordering of blocks was randomized, as was the ordering of trials within each block ($n = 40$). The average participant took 17 s to complete each trial, and 12 min to complete each block.

### Materials

#### Image Classifier

Participants interacted with an AICS based on the AlexNet image classifier model (Krizhevsky et al., 2012), which used MATLAB’s Deep Learning and Image Processing Toolboxes (MATLAB ver. R2017a). AlexNet is a pretrained convolutional neural network, trained to classify objects within a $227 \times 227$-pixel net. To process each image, the file must first be resized to fit these dimensions, after which AlexNet is able to read the image. AlexNet can output a range of classifications and probabilities to illustrate its interpretation of images.

#### Classifier Performance

Participants viewed a series of 160 images selected from The Open Images Data set V4 (OIDV4; Kuznetsova et al., 2020). These images featured categories such as household objects, nature scenes, food items, vehicles, and animals. These were used to create four sets of 40 single-image trials, with each having 20 correct and 20 incorrect trials. The classifier’s performance was considered as correct when AlexNet provided labels that appropriately matched the image’s original label in OIDV4, otherwise performance was considered incorrect. Classifier performance was intrinsically linked to each image; performance only varied between images.

#### Image Clarity

The contents within 50% of images were made unclear to make the classifier’s performance harder to evaluate. These images were first cropped, to partially show their contents, and then overlaid with a Gaussian blur when displayed to participants (See Figure 1).

### Figure 1

#### Preparation of Images

(A) Image Preparation:

(B) Image Classified As:

Note. Each trial featured a single image. Classifier performance was based on AlexNet’s classification for the image (B), while Image Clarity was based on the quality of the image (A). Clear trials featured images with unobscured contents, while unclear trials featured cropped images that were overlaid with a Gaussian blur when presented to participants.
Across all 160 trials, participants saw 40 trials of each combination of Classifier Performance and Image Clarity: Correct-Clear, Correct-Unclear, Incorrect-Clear, Incorrect-Unclear, which were evenly distributed and mixed across four sets of images. These sets were organized to ensure they contained the same quantity of categories (animals, vehicles, objects, etc.), while the average classifier confidence was made similar in each set of images (Min = .5, Max = 53.6). Each set of images was randomly matched to an interface for each participant. Data associated with one image was corrupted during data collection, and therefore unusable (74 trials removed from initial 11,840 observations).

**Image Classification Task**

Participants used a mouse and keyboard to interact with the classifier’s Graphical User Interface (GUI), built within the MATLAB app designer, (MATLAB ver. R2017a) (See Figure 2). The classifier’s label for each image appeared in a box underneath the image, while participants could overwrite the classifier with their own label for each image. If participants did not understand the classifier’s label, they could specify this with a small button beside the label. Additionally, if participants believed the classifier’s label was wrong, yet were unable to provide a better correction themselves, they wrote “No” or “Don’t Know” in their own user label box.

Participants rated the classifier’s performance on a visual analog scale within the GUI, using three different interactive sliders corresponding with: (a) How familiar they were with the contents in each image, (b) How accurately they believed the classifier’s label described the image, (c) Their trust toward the classifier. They were instructed that ratings of label accuracy should reflect the classifier’s performance in each individual single image trial, while ratings of trust should represent their continuous interaction with the classifier throughout the experiment. All sliders went from 0%–100%, represented with visual anchor points of “Not at all” and “Entirely.” Data was collected from each slider after each trial and would reset to the midpoint (50%) between trials. Each slider would change color (blue) to cue participants toward the rating they needed to provide next, guiding the participant throughout each trial. Compliance with the classifier was defined as trials where the participant did not overwrite the classifier’s label. Participants moved between trials by using the “Next Image” button, which only became active after all three sliders had been used.

**Interface Design**

All four interfaces contained the same basic features but varied in the SCI they displayed (See Figure 2). The Control interface provided no SCI. The Iconography interface provided the simplest form of SCI, discretized as low, medium, or high confidence, represented by the classifier’s label changing color to be red, yellow, or green, respectively. The Numerical condition was more precise, presenting SCI as a text-based numerical percentage, ranging from 0%–100% representing low–high confidence. The Graphical condition was the most complex representation of SCI, illustrated as a horizontal bar graph visualizing the distribution of the classifier’s five most probable labels for each image.

**Questionnaires**

**NASA-TLX.** After each task block, participants reported their subjective task load when working with each GUI, on a low–high scale (0%–100%; Hart & Staveland, 1988).

**Propensity to Trust Machines Questionnaire.** A series of six questions where participants rated on a 7-point Likert scale how likely they are to trust machines (Merritt et al., 2013). Half of the participants completed the PTMQ before the experiment started, and the rest after completing the experiment.

**Debriefing Questionnaire.** Participants answered seven short questions detailing their thoughts about the classifier (Appendix), which they completed following the last block of the experiment. They could also expand on each answer by writing a short paragraph, to explain these thoughts in further detail.

**Procedure**

All participants read an information sheet explaining the nature of the experiment, before giving written consent. Before the experiment began, they were taught to use the basic elements within the GUI. All participants were briefly informed how AlexNet could provide labels for each image. They were told that in certain blocks AlexNet would also display different forms of SCI, to help support its labeling decisions. They were given further specific instructions about each type of SCI prior to the relevant blocks. In each trial, the participant first rated how familiar they were with the image. The classifier then provided the label for each image, to ensure participants’ familiarity was not informed by the classifier’s label. Participants then rated the accuracy of the classifier’s label, and their trust toward the classifier. Lastly, participants decided to keep or replace the classifier’s label for the image, before moving to the next trial. Following completion of the experiment and questionnaires, all participants were given a debriefing form, which explained the study in further detail.

**Analysis**

**ANOVA**

Our data were not normally distributed, therefore we had to depart from canonical tests and instead opted for a nonparametric...
alternative: The Aligned Ranks Transform ANOVA (ART-ANOVA; Wobbrock et al., 2011). This test allowed for examination of multiple factors and their interactions within our repeated measures design. Our primary dependent variable of interest was: (a) participants’ trust toward the classifier (Trust). In addition to this, we wanted to explore how trust reflected participants’ behavior, and examined (b) how participants decided to accept/reject the classifier’s labels for images (Compliance). To assess whether our stimuli selection was balanced (c) we also looked at participants’ familiarity with the images presented (Familiarity). Lastly, we considered (d) the average time taken for trials in each combination of conditions, as an objective measure of task load (Trial Time). Consequently, four ART-ANOVA models were conducted, all containing the same three main factors and their interactions: Classifier Performance, Image Clarity, and Interface, using the “ARTool” package in R version 4.0.2 (Kay & Wobbrock, 2020; R Core Team, 2020). Additionally, a Kruskal–Wallis test was also conducted to examine the effect of interface on subjective task-load scores (NASA-TLX). Effect sizes were calculated for each main effect using partial eta squared. Pairwise comparisons for significant main effects were carried out using contrasts from the “emmeans” package, with Bonferroni corrections applied to account for multiple comparisons (Lenth, 2020).

Additional Analyses

Nonparametric Kendall’s tau correlations were used to examine the relationships between participants’ PTMQ scores and their average trust toward the classifier, as well as their average compliance with the classifier, which we compared across each combination of Classifier Performance and Image Clarity.

Visualizations

Static and interactive visualizations were created using the “ggplot2” and “plotly” R packages (Sievert, 2020; Wickham, 2016).

Data Availability

An anonymized version of this data set is available through the U.K. Data Service ReShare repository here: https://dx.doi.org/10.5255/UKDA-SN-854151. The U.K. Data Service is funded by the Economic and Social Research Council (ESRC) who provided funding for this project.

Results

Classifier Performance and Image Clarity

Trust

Overall, trust was highest in trials where the classifier was correct, and lowest in trials where the classifier was incorrect (Figure 3, and Table 1). However, this relationship was complicated by the clarity of the image. Participants’ trust tended to be closest to the grand mean (M = 45.77) when processing unclear images, and furthest when processing clear images. For example, if the classifier’s label was correct yet the image was unclear (Correct-Unclear: M = 51.25, SD = 16.02), trust tended to be lower toward the classifier, compared to when the images were clear (Correct-Clear: M = 72.07, SD = 16.02).

Figure 3

Trust Scores for Each Image Used in the Experiment, Arranged by Accuracy

Note. Stimuli arranged by participants’ average accuracy rating of classifier’s label for the image. Dashed line represents grand median trust.
$SD = 22.77$). Inversely, when the classifier was incorrect trust was higher for unclear images (Incorrect-Unclear: $M = 36.12, SD = 15.50$), and lower for clear images (Incorrect-Clear: $M = 23.62, SD = 16.75$). ART-ANOVA for Trust revealed a significant interaction between Classifier Performance and Image Clarity $F(1, 73) = 205.27, p < .001, \eta^2 = 0.74$, and significant main effects for both Classifier Performance $F(1, 73) = 226.49, p < .001, \eta^2 = 0.76$, and Image Clarity $F(1, 73) = 24.8, p < .001, \eta^2 = 0.25$. This supports H1a: The classifier’s performance was the main driver of trust toward the classifier. This also supports H1b: Image Clarity significantly interacted with system performance when influencing trust toward the classifier.

### Compliance

A similar pattern emerged when examining how participants accepted and rejected the classifier’s labels (Figure 4, Table 1). ART-ANOVA for Compliance revealed a significant interaction between Classifier Performance and Image Clarity $F(1, 73) = 544.24, p < .001, \eta^2 = 0.88$, and a main effect for Classifier Performance $F(1, 73) = 1275.09, p < .001, \eta^2 = 0.95$. However, there was no significant main effect for Image Clarity $F(1, 73) = 1.21, p = .27, \eta^2 = 0.02$.

### Familiarity

In general, participants were more familiar with the images in the Correct-Clear and Incorrect-Clear combinations, and less familiar with the images in the Correct-Unclear and Incorrect-Unclear combinations, as we expected (Table 1). While there was no difference in familiarity between the Correct-Clear ($M = 92.89, SD = 8.58$) and Incorrect-Clear ($M = 92.31, SD = 9.15$) stimuli, there was however a difference between the stimuli in the Correct-Unclear ($M = 41.30, SD = 14.39$) and the Incorrect-Unclear combinations ($M = 29.89, SD = 12.82$). Therefore, we cannot rule out the possibility that some of the differences in Trust and Compliance were related to differences in Image Familiarity in the unclear images. ART-ANOVA for Image Familiarity revealed a significant

### Table 1

<table>
<thead>
<tr>
<th>Performance Type</th>
<th>Trust (%)</th>
<th>Label accuracy (%)</th>
<th>Classifier compliance (%)</th>
<th>Familiarity of images (%)</th>
<th>Time per trials (Seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correct &amp; clear</td>
<td>72.07</td>
<td>92.19</td>
<td>86.89</td>
<td>92.89</td>
<td>13.10</td>
</tr>
<tr>
<td>Correct &amp; unclear</td>
<td>51.25</td>
<td>59.30</td>
<td>60.20</td>
<td>41.30</td>
<td>17.66</td>
</tr>
<tr>
<td>Incorrect &amp; unclear</td>
<td>36.12</td>
<td>34.46</td>
<td>31.29</td>
<td>29.89</td>
<td>20.26</td>
</tr>
<tr>
<td>Incorrect &amp; clear</td>
<td>23.62</td>
<td>10.32</td>
<td>6.62</td>
<td>92.31</td>
<td>19.98</td>
</tr>
</tbody>
</table>

Note. Stimuli arranged by participants’ average accuracy rating of classifier’s label for the image.
interaction between Classifier Performance and Image Clarity $F(1, 73) = 175.22, p < .001, \eta^2 = 0.71$, and main effects for both Classifier Performance $F(1, 73) = 226.94, p < .001, \eta^2 = 0.76$, and Image Clarity $F(1, 73) = 798.24, p < .001, \eta^2 = 0.92$.

Propensity to Trust Machines

Trust

Participants’ total scores in the PTMQ were distributed as follows: $M = 28.25, SD = 7.03, \text{Range} = 11.25–39.30$. PTMQ scores predicted higher trust toward the classifier in three of the four different combinations of Classifier Performance and Image Clarity (Figure 5). While these relationships are relatively weak, they suggest that individual differences may inform trust toward an AICS, particularly when processing unclear images, where system performance may be harder to evaluate. Specifically, participants with higher PTMQ scores were more likely to trust the classifier during Incorrect-Clear trials: $r_t = 0.09, p < .05$, Incorrect-Unclear trials: $r_t = 0.12, p < .01$, and during Correct-Unclear trials $r_t = 0.14, p < .001$, yet interestingly this relationship was not present during Correct-Clear trials $r_t = 0.06, p = .101$. Nonetheless, this supports H1c: Participants with higher PTMQ scores tended to trust the classifier more when processing unclear images, where performance may be more difficult to evaluate.

Compliance

PTMQ scores predicted higher compliance with the classifier in only two of the four different combinations of Classifier Performance and Image Clarity (Figure 6). Specifically, participants with higher PTMQ scores were more likely to accept the classifier’s label only when the classifier was correct, during Correct-Clear trials: $r_s = 0.15, p < .001$, and Correct-Unclear trials: $r_s = 0.1, p < .05$. PTMQ scores did not predict greater compliance during Incorrect-Unclear trials: $r_s = 0.01, p = .83$, and Incorrect-Clear trials: $r_s = -0.02, p = .62$.

Interface Differences

Trust

Across the classifier’s different interfaces, trust was highest toward the Numerical interface ($M = 47.45, SD = 25.27$), and lowest toward the Control interface ($M = 44.74, SD = 26.05$; Figure 7, Table 2). Despite this, trust toward the classifier was not significantly increased when participants worked with the experimental interfaces. While they did not improve trust, most participants reported an explicit preference for working with the interfaces that displayed SCI, suggesting they still found them beneficial on some level (Table 2). ART-ANOVA for Trust revealed no significant main effect of Interface $F(3, 219) = 1.66, p = .18$, $\eta^2 = 0.02$. Thus, H2a was not supported: SCI did not improve overall trust toward the classifier. Moreover, there was no interaction between Interface and Classifier Performance, nor was there between Interface and Image Clarity. Thus, when the classifier’s performance was difficult to evaluate, SCI did not improve participants’ trust toward the classifier. This means that H2b was also not supported: confidence information did not improve trust when processing unclear images.

Figure 5

Correlations Between Participants’ PTMQ Scores and Average Trust Toward the Classifier

Note. Correlations calculated for each type of performance in each block.
Compliance

Participants were most likely to accept the classifier’s label when working with the Graphical interface ($M = 47.34, SD = 35.84$), and least likely when working with the Iconography interface ($M = 45.27, SD = 36.17$; Figure 7, Table 2). Despite there being no difference in trust between experimental interfaces, there were small significant differences in compliance with the classifier, suggesting some participants may have been more likely to accept the label provided by the classifier when it provided them with confidence information. ART-ANOVA for Compliance revealed a small main effect of Interface $F(3, 219) = 3.26, p < .05, \eta^2 = 0.04$. However, pairwise comparisons suggest the differences between interfaces were nonsignificant: with the most notable being between the Graphical and Iconography interfaces ($p = .098$) and between the Graphical and Numerical Interfaces ($p = .134$). There were no interactions involving the interface factor.

Task Load

NASA-TLX

A Kruskal–Wallis test on participant’s subjective task load scores revealed no differences between the experimental and control interfaces $H(3) = 0.401, p = .94$. (See Table 2). This suggests that the extra information presented by the classifier’s experimental interfaces did not increase participants’ subjective workload.

Trial Time

On average, participants spent the most time (seconds) per trial when working with the Graphical interface ($M = 19.24, SD = 7.21$), and the least time with the Control interface ($M = 16.43, SD = 6.83$). This suggests that participants did not necessarily ignore the extra information presented within the experimental interfaces, particularly when working with the Graphical interface. There were also significant differences in Trial Time relating to Classifier Performance and Image Clarity, however, these were less interesting. This was because participants were expected to take longer in trials when the classifier was incorrect, given they had to overwrite the classifier’s label, and in trials with unclear images, given the classifier's performance is harder to interpret. ART-ANOVA on Trial Time revealed a main effect of Interface $F(3, 219) = 11.47, p < .001, \eta^2 = 0.14$, which suggests that participants took longer to complete trials when presented with the classifier’s SCI. Pairwise comparisons illustrated most of the significant differences were attributable to the Graphical interface, in comparison to the Control ($p < .001$), Iconography ($p < .001$), and Numerical interfaces ($p < .05$). There were also significant main effects for Classifier Performance $F(1, 73) = 206.14, p < .001, \eta^2 = 0.74$, and Image Clarity $F(1, 73) = 41.77, p < .001, \eta^2 = 0.36$, as well as an interaction between Classifier Performance and Image Clarity $F(1, 73) = 91.95, p < .001, \eta^2 = 0.55$. 

Figure 6

Correlations Between Participants’ PTMQ and Average Compliance With the Classifier

Note. Correlations calculated for each type of performance in each block.
Thus, H2c was not completely supported outright, as SCI presented in the experimental interfaces did not increase subjective participants’ task load scores. However, there were significant differences attributable to experimental interfaces when considering the average time spent per trial as an objective measure of task load, with the Graphical interface generally being the most time-consuming.

**Discussion**

This study sought to understand how individuals calibrated their trust toward an AICS when completing an image classification task. Trust toward the classifier was primarily based on the accuracy of the system’s description of images. Trust tended to be highest when the classifier’s label was correct, and lowest when incorrect. However, the clarity of the image being processed also influenced trust, such that if the contents of the image were clear then participants were more extreme with their trust, yet with unclear images their trust regressed toward the mean. Moreover, there was also evidence of individual differences among participants. The participants with a positive bias toward machines, as indicated by higher scores on the PTMQ, tended to trust the classifier slightly more when processing unclear images. Thus, this study provides an insight into how human users place trust in a system designed to make classifications on image-based data, and expands upon this by also exploring how environmental and interpersonal factors contribute to users’ trust.

Table 2

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trust the classifier (%)</th>
<th>Label accuracy (%)</th>
<th>Classifier compliance (%)</th>
<th>Familiarity of images (%)</th>
<th>Time per trials (Seconds)</th>
<th>Task load (NASA-TLX)</th>
<th>Aesthetic rating (1–7)</th>
<th>Favorite interface (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control</td>
<td>44.74 26.05 49.28 32.19</td>
<td>46.21 36.52</td>
<td>64.35 30.73</td>
<td>16.43 8.83</td>
<td>224.20 77.83</td>
<td>4.51 1.43</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Graphical</td>
<td>45.27 25.44 49.98 31.56</td>
<td>47.34 35.84</td>
<td>63.76 31.40</td>
<td>19.24 7.21</td>
<td>230.68 78.47</td>
<td>4.54 1.39</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>Iconography</td>
<td>45.60 25.25 47.75 32.53</td>
<td>45.27 36.17</td>
<td>63.81 31.44</td>
<td>17.14 8.02</td>
<td>231.43 85.08</td>
<td>4.62 1.40</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>Numerical</td>
<td>47.45 25.27 49.27 32.77</td>
<td>46.18 37.16</td>
<td>64.49 30.59</td>
<td>18.18 8.23</td>
<td>225.57 80.12</td>
<td>4.53 1.48</td>
<td>26</td>
<td></td>
</tr>
</tbody>
</table>
toward the system. Additionally, we further built upon this by investigating whether trust toward the classifier could be improved by increasing system transparency through different displays of SCI, yet found little support with the formats we used. The implications of these findings are discussed below.

### Trust Toward an AICS

In line with previous research, system performance was the primary driver of trust toward the AICS (Hoff & Bashir, 2015; Yu et al., 2019). This is unsurprising, given autonomous systems are typically designed to handle a specific set of tasks, and therefore task errors represent a violation of their fundamental purpose. However, evaluations of AICS performance seemed to extend beyond simple correct versus incorrect judgments, as trust toward the classifier varied within correct and incorrect trials. This possibly reflects the nuance in the image classification task, where the classifier must go into more detail than the simpler yes/no type judgments provided by other autonomous systems (Merritt et al., 2013; Yu et al., 2019). At the same time, we should also consider that the classification of images is a relatively familiar task that the human user can often complete by themselves. By contrast in Selkowitz et al.’s (2017) study, the robotic squad member provided users with various forms of navigational and situational data and is therefore arguably a more complicated task for the user to undertake. Undoubtedly, the greatest benefits of AICS will arise in applied settings when users are tasked with processing large quantities of data, instead of individual images. Nonetheless, our results provide an interesting insight into how individuals perceive the decisions of AICS systems. For example, when the classifier incorrectly labeled one image of a rowboat as a speedboat participants’ average compliance was low, yet trust remained relatively high, despite the error (Figure 4). This illustrates how participants were able to accommodate errors when there is categorical overlap between classifications, and may itself be worth further, more rigorous investigation in future studies.

Evaluations of classifier performance were also informed by how difficult the image was to classify: If the contents of the image were clear, trust was generally higher when correct, and lower when incorrect, compared to when processing images with unclear contents. This appears in line with previous research where trust toward an autonomous baggage scanner was also influenced by the difficulty of the task (Merritt et al., 2013). By building on this, our study illustrates how task difficulty, considered as a component of Situational Trust within Hoff and Bashir (2015) model, can also influence trust toward AICS. Moreover, participants’ compliance with the classifier was also informed by the difficulty of the task. Compliance was typically highest in trials where the classifier was clearly correct, and lowest in trials where it was clearly incorrect. However, this compliance was less uniform in trials with unclear images, suggesting participants were more likely to replace the classifier’s labels in difficult trials. Similar to this, changes in task difficulty have been shown to influence how medical practitioners use Clinical Decision Support Systems (CDSS). Goddard et al. (2014) report that practitioners were more likely to switch decisions when working with a CDSS in scenarios requiring difficult prescriptions. While this uncertainty may appear detrimental to the operator, Lye et al. (2018) report that using CDSS helped lower users’ cognitive load when dealing with more difficult prescriptions. Therefore, when working with autonomous systems to overcome difficult tasks, the advice of the system may still be beneficial even if the system’s decision is ultimately replaced or overruled by the operator. While it is worth noting that the increase in difficulty in the previous studies differs from the methods used in the current study, our findings provide further illustration of how changes in the difficulty of the task may influence how operators use autonomous systems.

Additionally, there were individual differences between participants’ trust toward the classifier, which may be attributable to their PTMQ scores. Specifically, individuals with higher PTMQ scores tended to have slightly higher trust toward the classifier, particularly during trials with unclear images. Interestingly, higher PTMQ scores also correlated with higher compliance with the classifier, but only in trials where the classifier was correct. This may suggest that while the individuals with higher PTMQ scores tended to trust the classifier more, they remained critical of its performance and their positive bias did not correspond with higher acceptance of incorrect labels. Within Hoff and Bashir (2015) model, these individual differences are indicative of Dispositional Trust specific to each operator. The importance of individual differences is also illustrated within models of technology acceptance, which recognize the influence of moderating factors such as the age, gender, and experiences of the operator (Venkatesh et al., 2012). Here, we used convenience sampling in our participant recruitment, and therefore primarily focussed on PTMQ scores as a measure of individual differences. Nonetheless, this echoes previous findings where individuals with higher PTMQ scores and greater Automation Bias tended to place more trust in autonomous technologies (Goddard et al., 2014; Merritt et al., 2013). Therefore, our findings support previous literature suggesting that individual differences can influence trust and attitudes toward autonomous technology. In particular, we demonstrate that biases toward technology could make individuals more likely to trust an AICS when working with it, yet crucially these biases do not automatically translate into making the individual more likely to accept erroneous decisions from the system.

### Improving Trust

Both the SAT model (Chen et al., 2014) and Hoff and Bashir (2015) model suggest that users are more likely to trust autonomous systems with more transparent interfaces. However, we found little support for SCI improving trust toward the AICS, despite previous evidence suggesting confidence information can benefit trust toward autonomous systems (Desai et al., 2013; Zhang et al., 2020). For example, there was no apparent benefit to trust during the more difficult trials with unclear images, despite SCI providing greater information about the classifier’s decision. It is possible that the formats we used to convey SCI were not optimal, and that participants were unable to effectively extract the information. This possibility is consistent with previous evidence suggesting that individuals may have difficulty understanding information presented in formats such as bar graphs (Chaphalkar & Wu, 2020; Godau et al., 2016). Likewise, as discussed above, the image classification task itself may have been relatively easy for participants to complete by themselves, meaning that the classifier’s decisions, and by extension SCI, may have been of limited use to participants. Additionally, any potential benefits from SCI may have been lost due to the low overall reliability of the classifier.
within our experiment, which stemmed from our experimental design. Hoff and Bashir (2015) consider system reliability as a subcomponent of system performance, and while design features such as SCI can improve system transparency, any benefits to trust may be lost due to system reliability being more influential than transparency. This could be supported by participants’ responses during debriefing, where they rated the classifier as more a tool than a teammate, and often found it unpredictable (Table 3). Future studies may benefit from employing high and low reliability conditions, in order to explore this further.

Despite this low reliability, participants still found the classifier helpful (Table 3). Moreover, they overwhelmingly preferred working with the classifier’s SCI interfaces (Table 2) and did not appear to feel encumbered by the extra information, which still suggests SCI is potentially beneficial. Furthermore, participants spent the most time per trial with the experimental interfaces, particularly the Graphical interface (Table 2). While this does not automatically mean that SCI improved participants’ comprehension of the classifier’s decisions, it does suggest some processing of this confidence information. While we were primarily interested in trust toward an AICS, it would be beneficial to examine whether SCI can improve users’ understanding of these systems. Alongside developing appropriate trust toward autonomous systems, there is also a growing interest in promoting the explainability of autonomous systems, particularly given the “black box” nature of contemporary machine learning approaches (Abdul et al., 2018). In future studies, it would be useful to examine whether displays of SCI can improve the explainability of AICS decisions. This may be particularly well-suited to cases when a classifier assigns the same classification to two distinctly different objects that share similar image features, such as texture and shape.

**Beyond Confidence Information**

Ultimately, trust toward the AICS could be limited by the way that AICS systems use deep learning techniques when learning to classify images, which can make their decision-making inherently difficult to explain (Gilpin et al., 2019). As a result, these systems may lack the explainability of other autonomous systems, which may make them fundamentally difficult to trust completely (Rudin, 2019). A recent article by Chen et al. (2019) suggested that the decisions of AICS can be made easier to interpret by highlighting important features within sections of an image, through visual cues such as bounding boxes, in order to support the classification for the full image. By doing so, Chen et al. (2019) argue that AICS can mimic the reasoning process of humans when classifying images, where the system can illustrate to the user that the classification is based upon shared features with a prototypical image of the classification, essentially: “this image looks like that image.” Thus, the “black box” nature of AICS systems might mean that providing SCI alone could be inappropriate for improving trust, and instead users’ trust could ultimately benefit from efforts that make AICS decisions more easily interpreted. Our lack of empirical support for SCI improving trust toward the AICS may be disappointing for potential designers, however, these findings still raise important considerations. Designing interfaces for autonomous systems is a complex process, and based on our evidence, simply providing a single indicator of system decision-making such as SCI, may not be the best way to improve users’ trust, at least in the case of AICS. While displays of SCI have shown promise in previous studies, (Verame et al., 2016; Zhang et al., 2020), it may not be a “magic bullet” for improving trust toward all automation. Nonetheless, while SCI did not explicitly improve participants’ trust toward the AICS, most participants still preferred interfaces that displayed SCI, which suggest it might be beneficial to some degree. Thus, this study motivates further research into developing novel methods for conveying the decision-making of systems like AICS.

**Limitations**

This study involved interaction with an AICS in a relatively low stakes task, where participants worked with the classifier to label neutral stimuli. Applied uses of AICS may also include higher stakes tasks, such as identifying patients with diseases (McKinney et al., 2020). In such cases, trust toward an AICS may be even more susceptible to system errors, given the more serious consequences of false alarms and missed cases. By contrast, in our experiment, there were no consequences associated with system errors. Regardless, participants still modulated their trust in response to system successes and errors, while they tended to comply with the classifier only when it was correct, suggesting they took the task seriously.

---

**Table 3**

*Descriptive Statistics for Responses to Questions 1–6 From Debriefing Questionnaire*

<table>
<thead>
<tr>
<th>Question</th>
<th>M</th>
<th>SD</th>
</tr>
</thead>
<tbody>
<tr>
<td>How helpful did you think the classifier was?</td>
<td>4.63</td>
<td>0.87</td>
</tr>
<tr>
<td>&lt;Not at all/A great help&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>How predictable was the classifier’s behavior?</td>
<td>4.64</td>
<td>1.38</td>
</tr>
<tr>
<td>&lt;Predictable/Unpredictable&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>How specific did you think the classifier’s labels were?</td>
<td>3.44</td>
<td>1.12</td>
</tr>
<tr>
<td>&lt;Too specific/Too general&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If you had to describe it to someone, how would you characterize the classifier?</td>
<td>5.48</td>
<td>1.50</td>
</tr>
<tr>
<td>&lt;Teammate/Tool&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If you had to classify another set of images, would you want to work with the classifier again?</td>
<td>2.97</td>
<td>1.37</td>
</tr>
<tr>
<td>&lt;With classifier/Alone&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If you had to classify another set of images, which type of collaborator would you prefer?</td>
<td>4.54</td>
<td>1.51</td>
</tr>
<tr>
<td>&lt;Computer/Human&gt;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
despite these low stakes. Future studies may wish to build upon these findings by introducing greater consequences for task errors.

**Conclusion**

During a human–computer image classification task, trust toward an AICS was primarily based on the classifier’s ability to label images. Additionally, image clarity significantly interacted with AICS performance, and further informed participants’ ratings of trust and compliance, illustrating the role of task difficulty in their evaluations. Furthermore, some of the variance in trust toward the AICS appeared to have been attributable to individual differences among participants, as those with higher propensity to trust machine scores tended to have slightly higher trust toward the classifier. Lastly, while most participants preferred interfaces that displayed SCI, it did not appear to improve their trust toward the classifier, despite previous studies suggesting confidence information can improve trust.

**References**


(Appendix follows)
Appendix

Debriefing Questionnaire

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>How helpful did you think the classifier was?</td>
</tr>
<tr>
<td>2.</td>
<td>&lt;Not at all/A Great Help&gt;</td>
</tr>
<tr>
<td>3.</td>
<td>How predictable was the classifier’s behavior?</td>
</tr>
<tr>
<td>4.</td>
<td>&lt;Predictable/Unpredictable&gt;</td>
</tr>
<tr>
<td>5.</td>
<td>How specific did you think the classifier’s labels were?</td>
</tr>
<tr>
<td>6.</td>
<td>&lt;Too Specific/Too General&gt;</td>
</tr>
<tr>
<td>7.</td>
<td>If you had to describe it to someone, how you would characterize the classifier?</td>
</tr>
<tr>
<td>8.</td>
<td>&lt;Teammate/Tool&gt;</td>
</tr>
<tr>
<td>9.</td>
<td>If you had to classify another set of images, would you want to work with the classifier again?</td>
</tr>
</tbody>
</table>

Received January 20, 2020
Revision received December 21, 2020
Accepted January 24, 2021