Effects of Password Type and Memory Techniques on User Password Memory

Lezlie Y. España
Wisconsin Lutheran College

ABSTRACT. In an attempt to examine factors that increase the likelihood of remembering a user password, the memory technique of chunking was tested on different password types. College students, aged 18 to 22, used a given login (username and password) to play a 3-round word scramble game online. The type of password (multiword passphrase and standard password) was manipulated, as well as the strategy for remembering (chunking or no chunking). After the last round, participants’ memory for passwords was tested. Results showed that the effect of chunking on memory for passwords depended on the type of password. Chunking had a negative impact on memory for multiword passphrases but a positive impact on memory for standard passwords, $F(1, 53) = 12.74, p = .001$, partial $\eta^2 = .20$.

Implications regarding the use of memory techniques in user interfaces to improve memory for passwords and the impact of such techniques on personal and professional use are discussed.

The increasing need for numerous distinct online accounts and security of personal information on those accounts has led to a corresponding rise in the number of passwords that people need to not only generate, but also be able to remember. According to Brown, Bracken, Zoccoli, and Douglas (2004), students use on average 8.18 passwords, with 4.45 unique passwords and 1.84 uses per password. Thirty-one percent of students reported forgetting their passwords, and 22.5% experienced password mix-ups (not surprising given that 41.4% of all utilizations shared a password with two or more other utilizations; Brown et al., 2004). In light of these statistics, the overarching purpose of this study was to examine factors that increase the likelihood of remembering specific types of passwords.

Often, the creation of a new password requires adherence to many restrictions (e.g., must contain at least eight characters, at least one number, a capital letter, and a symbol). Differences in password restrictions across multiple accounts have also led to various types of passwords that people are encouraged to use such as standard passwords and passphrases. Standard passwords typically consist of a minimum number of characters containing a combination of letters, symbols, and numbers (e.g., aJ$76ui#M). Passphrases may consist of multiple compositions (e.g., a phrase like "I love to do research in psychology" could become "Iluv2do3re6rch1#p$y," or a phrase with random dictionary words like "rhyme double farther represent" could be used).

Research shows there are some discrepancies over the perceived usefulness of passphrases among users (Keith, Shao, & Steinbart, 2007). Although research shows that passphrases may be more difficult to crack, more easily remembered, and more efficient, some people perceive them as being more difficult to use than standard passwords (Keith, et al., 2007). Despite this research in favor of passphrases, the fear of an inadequate capacity of human short term and working memory may discourage the use of longer, more secure passphrases (Keith et al., 2007).

Not only does password type (standard vs. passphrase) influence memory, but so do the number of passwords a person uses, the length of these passwords, their frequency (how often they are used), and how often a new password is
created or an old one is changed (Keith et al., 2007; Payton, 2010; Vu et al., 2007). All of these factors can affect both short and long-term memory. For instance, research shows that most people can hold things temporarily in their short term memory for about 30 seconds without aids (Cowan, 2000). Interference theory also suggests that previously learned information can interfere with a person’s ability to recall new information (proactive interference) and newly learned information can interfere with a person’s ability to recall old information (retroactive interference; Roediger, Nairne, Neath, & Surprenant, 2001). This helps explain why people dislike the idea of coming up with new and unique passwords (i.e., because they fear an inability to remember their other passwords). Further evidence of this comes from Vu et al. (2007) who found that the use of multiple unique passwords often increases the number of attempts needed to recall a password, leading people to use the same password for multiple accounts.

Fortunately, there are other techniques people can use to aid their memory. The process known as chunking, which combines pieces of information in some meaningful way, thus increasing the amount of information held in working memory, can contribute to better overall memory (Dilmar, 1972; Miller, 1956). This process can occur naturally in the ways that people recode information such as in the use of mnemonic devices or in daily conversation (when people automatically regroup words or ideas and put it in their own words; Miller, 1956). However, chunking can also be used intentionally to facilitate memory (Miller, 1956). Miller (1956) suggested the “magic number seven” as a baseline for chunking information, and further research has suggested that three or four bits (or pieces) of information per chunk are best for aiding memory (Dilmar, 1972). However, recent research has indicated that there are limits to this memory technique; capacity (how many chunks) and length of individual chunks may both play a role in recall ability (Chen & Cowan, 2005; Cowan, 2000).

Despite this, the usefulness of chunking in aiding memory is certainly still worth consideration today as pointed out by Carstens, Malone, and McCauley-Bell (2006), who found chunking meaningful information into passwords to be beneficial. In their study, Carstens et al. (2006) explored the use of meaningful chunks of information and different password lengths. They found that using two, three, and even four chunks of information improved memory for passwords and reduced the need for participants to refer to a written password. Although there was no statistically significant difference between the chunking conditions, Carstens et al. (2006) found that using personally meaningful chunks of information in passwords improved memory compared to that of a seven-character password with no meaningful information incorporated in it. Brown et al. (2004) found that half of all password constructions in their study consisted of proper names and birthdays with two-thirds of passwords containing information about the self or personal elements, which makes it reasonable to suggest that these personally meaningful chunks do indeed aid memory. Carsten et al. (2006) also found that participants were able to remember passwords anywhere from 7 to 22 characters in length when they used chunking, showing how individuals can use chunking to create their own unique, meaningful passwords that are easy to remember.

Similarly, Bonneau and Schechter (2014) used chunking to help participants learn pass codes (consisting of just letters like “vnun” or words like “voice baker”) over a longer period of time. They used words and letters placed directly after a participant’s username and password of their own choosing, adding new chunks after each successful memorization of the previous chunk. This allowed participants to learn longer pass codes, one chunk at a time through repetition and spacing for up to two weeks. Bonneau and Schechter (2014) encouraged participants to memorize their codes by increasing the delay time before showing them the correct word or series of characters, essentially allowing participants to log in faster if they remembered the code themselves. Bonneau and Schechter (2014) were able to help 88% of participants remember their codes even three days after the initial study. Only 21% of participants reported the need to write the code down (Bonneau & Schechter, 2014), which is in direct contrast to Brown et al. (2004) who found that more than half of the students kept written records of their passwords because they could not remember them. This showed how chunking can be used in conjunction with other memory techniques to learn longer pass codes that could possibly be used either in addition to or instead of passwords. The ability to learn longer passwords would also be beneficial because length of passwords also has an effect on memory, with longer passwords being less likely to be remembered (Payton, 2010).

People need to create complex passwords to safeguard their personal information, but complex
passwords are hard to remember, leading to the present study’s purpose of examining how chunking affects recall for standard passwords and passphrases. Previous research has indicated that spacing and chunking has a positive effect on memory for pass codes when used in addition to passwords (Bonneau & Schechter, 2014). However, no one to date has examined the effects of using chunking directly within the password user interface itself (e.g., typing each “chunk” of a password into separate input boxes) and how that may affect memory for different types of passwords. It was predicted that participants using the chunking method would report better memory for both standard and passphrase passwords (as measured by the number of attempts required to remember). Because passphrases are regarded as easier to remember due to the use of words (Bonneau & Schechter, 2014; Payton, 2010), it was also predicted that this effect would be most pronounced for the standard password.

Method

Participants

Participants were recruited through an undergraduate psychology department sponsored research activity. Sixty participants completed the study, but three participants were not included in the final analyses due to incomplete data. The remaining participants included 57 (39 women, 16 men, two unreported) undergraduate students attending a small liberal arts college in the midwest. Most of the sample was White American (82.5%), with 1.8% African American, 5.3% Asian, 5.3% other, 3.5% prefer not to answer, and 1.8% who were not reported. The participants’ ages ranged from 18 to 22 (M = 18.81, SD = 2.76).

Materials and Procedure

Participants were randomly assigned to one of four conditions based on the two factors of password type and chunking: the standard password with chunking (n = 15), standard password with no chunking (n = 16), multiword passphrase with chunking (n = 13), and multiword passphrase with no chunking (n = 13). See Table 1 for demographics across conditions. Although participants did not receive formal compensation, they did receive extra credit for completing the study.

This study received Wisconsin Lutheran College Institutional Review Board approval (#41111031407). The materials used in this experiment consisted of web pages that the author created to carry out the study, in which participants logged in to play a word scramble game. After three rounds, participants were asked to recall their passwords. To discourage intentional rehearsing, participants were not informed that they would need to memorize their password. Memory for the passwords was based on how many attempts it took for the participants to remember their passwords.

Fifteen laptop stations were set up for participants to use, with the starting page set on the Google Chrome® browser. The experiment

FIGURE 1

Login Interfaces Across Conditions

A

Round 1
Create a login to play the game. Use your school email for your username. A random password is provided for you.
Your password: g@V26qlq01
Username: _______________________
Password: _______________________

The “no chunking” interface shows the input box for the username as well as a single input box for the standard password shown.

B

Round 1
Create a login to play the game. Use your school email for your username. A random password is provided for you.
Your password: laughveinmemoanvilnap
Username: _______________________
Password: _______________________

The “no chunking” interface shows the input box for the username and password as one would normally encounter them, with the multiword passphrase shown for the participant.

C

Round 1
Create a login to play the game. Use your school email for your username. A random password is provided for you.
Your password: g@V 2& 1q01
Username: _______________________
Password: _______________________

The “chunking” interface shows the input box for the username as well as three separate input boxes for the standard password shown.

D

Round 1
Create a login to play the game. Use your school email for your username. A random password is provided for you.
Your password: laughveinmemoanvilnap
Username: _______________________
Password: _______________________

The “chunking” interface shows input boxes for the username and password, with five separate input boxes for multiword passphrase shown for the participant.
TABLE 1  
Participant Demographics by Manipulation Type

| Manipulation Type | Standard, No Chunking | Standard, Chunking | Passphrase, No Chunking | Passphrase, Chunking |
|-------------------|-----------------------|-------------------|------------------------|----------------------|
|                   | Count                 | Count             | Count                  | Count                |
| Sex               |                       |                   |                        |                      |
| Male              | 4                     | 7                 | 3                      | 2                    |
| Female            | 12                    | 8                 | 9                      | 10                   |
| Unreported        | 0                     | 0                 | 1                      | 1                    |
| Race              |                       |                   |                        |                      |
| White             | 14                    | 10                | 11                     | 12                   |
| African American  | 1                     | 0                 | 0                      | 0                    |
| Asian             | 0                     | 3                 | 0                      | 0                    |
| Other             | 1                     | 2                 | 1                      | 1                    |
| Unreported        | 0                     | 0                 | 1                      | 0                    |

Note. M = male, F = female, R = race category, No = no, Chunking = chunking.

TABLE 2  
Descriptive Statistics by Manipulation Type

| Password Type | Number of Recall Attempts | Mean (M) | Standard Deviation (SD) | Count (n) |
|---------------|---------------------------|----------|-------------------------|-----------|
| Standard      | No Chunking               | 3.81     | 1.83                    | 16        |
|               | Chunking                  | 3.00     | 2.00                    | 15        |
|               | Total                     | 3.41     | 1.92                    | 31        |
| Passphrase    | No Chunking               | 2.23     | 1.74                    | 13        |
|               | Chunking                  | 4.69     | 1.11                    | 13        |
|               | Total                     | 3.46     | 1.43                    | 26        |
|               | No Chunking               | 3.10     | 1.93                    | 29        |
|               | Chunking                  | 3.79     | 1.83                    | 28        |
|               | Total                     | 3.45     | 1.88                    | 57        |

Note. Ms and SDs correspond to number of recall attempts according to each condition: standard password with chunking, standard password with no chunking, multiword passphrase with chunking, and multiword passphrase with no chunking.

FIGURE 2  
Mean Number of Recall Attempts Across Conditions

Note. Lower Ms indicate better memory for passwords. Error bars: 95% CI.

TABLE 2  
Descriptive Statistics by Manipulation Type

| Password Type | Number of Recall Attempts | Mean (M) | Standard Deviation (SD) | Count (n) |
|---------------|---------------------------|----------|-------------------------|-----------|
| Standard      | No Chunking               | 3.81     | 1.83                    | 16        |
|               | Chunking                  | 3.00     | 2.00                    | 15        |
|               | Total                     | 3.41     | 1.92                    | 31        |
| Passphrase    | No Chunking               | 2.23     | 1.74                    | 13        |
|               | Chunking                  | 4.69     | 1.11                    | 13        |
|               | Total                     | 3.46     | 1.43                    | 26        |
|               | No Chunking               | 3.10     | 1.93                    | 29        |
|               | Chunking                  | 3.79     | 1.83                    | 28        |
|               | Total                     | 3.45     | 1.88                    | 57        |

Note. Ms and SDs correspond to number of recall attempts according to each condition: standard password with chunking, standard password with no chunking, multiword passphrase with chunking, and multiword passphrase with no chunking.

Consisted of three rounds of a word scramble game that required participants to log in with their usernames and the passwords shown to them on the screen. The system randomly assigned each participant to a particular password type (standard: “g@V2&lq0!” or passphrase: “laughveinmomaanvilnap”) so that participants saw the password at the top of the screen with an input box directly below it. Instructions at the top of the screen read: “Create a login to play the game. Use your school e-mail for your username. A random password is provided for you.” Participants in the no chunking condition saw one box for the entire password (either a standard password or multiword passphrase; see Figures 1A and 1B, respectively). Participants in the chunking condition saw either three separate boxes placed side by side for standard password input (one box for each chunk of the password; see Figure 1C) or five separate boxes placed side by side for multiword passphrase input (one box for each chunk [i.e., word] of the passphrase; see Figure 1D). Spaces at appropriate breaking points between characters in the passwords shown on the screen indicated to participants that passwords should be chunked.

After successfully entering the correct password, participants played the word scramble game for 30 s before moving on to the next round. The game contained 10 scrambled words each round, which the participants were asked to unscramble (e.g., ylogychpso = psychology). Passwords were shown on the screen for each round, along with the same prompts described above.

At the end of three rounds, participants were given five attempts to recall their password (Vu et al., 2007) without any cues. The system tracked the number of attempts that participants took to try to remember their passwords, whether they remembered or not, and the last password they attempted to use to log in. After completing the final login, participants completed the demographics questionnaire online, at which point the next participants were able to start the study. The entire process took participants 5 to 10 min to complete.

Results

To explore the impact of chunking and password type on memory, the author conducted a 2 x 2 between-groups Analysis of Variance (ANOVA) with chunking (chunking, no chunking) and password type (standard password, multiword passphrase) as between-participant independent variables and number of attempts required to recall the password as the dependent variable. There was a statistically
significant interaction between chunking and password type, $F(1, 53) = 12.74, p = .001$, partial $\eta^2 = .20$ (see Figure 2). Simple main effects analysis revealed that participants who received a standard password needed significantly fewer attempts to correctly remember the password when using the chunking strategy compared to no strategy, $F(1, 53) = 6.04, p = .02$, partial $\eta^2 = .10$, 95% CI [1.99, 4.01] [2.90, 4.73], respectively. However, those participants who received a multiword passphrase did better without the chunking strategy than those who did use chunking as a strategy, $F(1, 53) = 6.71, p = .01$, partial $\eta^2 = .11$, 95% CI [1.29, 3.18] [4.09, 5.30], respectively (see Table 2 for means across conditions). The main effect for chunking, $F(1, 53) = 3.23, p = .08$, 95% CI [2.96, 3.93], partial $\eta^2 = .06$, was not statistically significant. The main effect for password type, $F(1, 53) = .92, p = .36$, 95% CI [2.94, 3.94], was also not statistically significant, and the partial $\eta^2 = .00$.

**Discussion**

With this study, the author sought to investigate the effects of password type and use of memory techniques on memory for passwords. The results of this study suggested that the effectiveness of chunking on the ability to remember passwords depends on the type of password being used. Specifically, participants who were asked to remember a standard password did better when using chunking, but participants who were asked to remember a multiword passphrase did better without the use of chunking.

These results are especially interesting due to the lack of research taking into account both different password types and the memory technique of chunking within the password interface. Keith et al. (2007) found that password type alone does not affect the ability to remember passwords. Bonneau and Schechter (2014) found that the use of spacing and chunking improved memory for pass codes consisting of words only. Carstens et al. (2006) suggested a model for creating passwords incorporating participants’ personal and meaningful information while using chunking. So although research has considered password type and memory technique, more research is needed to confirm the results found here, which indicated that the interaction between the two is important to consider, and may vary depending on password type and composition.

Although the finding that using chunking was helpful in remembering passwords is in line with previous research (Carstens et al., 2006), the finding that chunking actually hindered one’s ability to remember a passphrase is somewhat surprising and unexpected. One possible explanation is that chunking did in fact make it more difficult to remember passphrases. However, an alternative explanation is that the interface and presentation of the passwords required a greater amount of processing to use them. In the case of multiword passphrases in particular, the chunking condition showed the passphrase with spaces between each word, making it easier for participants to see and process each word. For those participants in the no chunking condition, however, the passphrase was shown as one continuous string of words with no spaces. The amount of mental processing used to read and use this version of the passphrase may account for the lowered number of recall attempts needed. Essentially, if participants worked harder to use the passphrase without chunking than those who used chunking, they might have had an easier time remembering it later. Future research could work to explore this interaction further and better understand the nature of passwords, memory, and the interfaces used in greater detail.

An important feature of this study to consider is the composition of the passwords used for each condition. Two passwords were used: one for the standard composition (g@V2&dqo!) and one for the multiword passphrase composition (laughveinmemomenvilnap). For the chunking conditions, the standard password was split into three chunks consisting of three, two, and four characters each, and the passphrase was split into five chunks according to each of the five meaningful words. To make the standard password manageable, the author kept the length at nine characters (most restrictions require at least eight characters), but made the passphrase longer in an attempt to ensure a similar level of difficulty. This difference in length could be a limitation to the study, but the author felt it necessary to keep the difficulty levels of each password composition relatively the same. Perhaps further research could explore how the number of chunks, number of characters in each chunk, and word or character composition for passwords affects memory. For example, variations of the passphrase structure could be studied further to see whether the use of chunking helps memory for a passphrase that introduces other characters in place of words or for shortened words that do not chunk as naturally at the onset.

The effort each individual put into solving the
Effects of Password Type and Memory

Word scramble could have affected the amount of interference caused by the distracter. Participants were not scored on the word scramble, nor were their answers tracked. Presumably, the random assignment to conditions should account for any individual differences in effort. However, the interference caused by the game could be an unforeseen limitation to the study because there is no way to determine the effort used to solve each word. Furthermore, the length of the game was only 30 s for each round. This short delay of (at the very least) 1 min 30 s from first seeing the password to needing to recall the password does not accurately depict a natural setting. In many cases, a user would create a password and then possibly not see or need to use it until logging in again (which could be a few hours, days, or weeks, depending on the situation). Given that using chunking with standard passwords did improve memory for the short term, perhaps continuing to use chunking with passwords over time would also see positive results.

Due to the prevalence of password use in current technology, continued research in this area has potential, especially with the variety of behaviors exhibited by people to manage their passwords and the different circumstances that influence such decisions. Researchers found that computer scientists, administrative staff, and students view passwords differently in regard to costs and benefits (Duggan, Johnson, & Grawemeyer, 2012). Memory constraints, the subjective utility of the password in a particular environment, and the person’s own knowledge of security all play a role in how people approach the creation and management of passwords (Duggan et al., 2012; Huang, Rau, Salvendy, Gao, & Zhou, 2011). Other issues include the need for multiple passwords, whether or not people actually comply with password restrictions (Campbell, Ma, & Kleeman, 2011; Huang et al., 2011), and elements of social engineering and desirability (e.g., choosing to share passwords with others; Stamp, 2006).

Unsurprisingly, people try different techniques to help themselves remember passwords. The generation effect (Mulligan, 2004), in which information is better remembered when created or generated on one’s own, could assist in memory for passwords. The processes of rehearsal, elaboration, repetition, and spacing also lead to automaticity and facilitate storage in long-term memory, which may explain why frequently used passwords are easier to remember (Roediger et al., 2001). Although the technique of learning an item through spacing repetition over a period of time (distributed practice) tends to be slower (depending on the amount of time used and the frequency of repetition), the advantages of long-term retention and enhancements in learning is well-known in the realms of both psychology and information security (Bonneau & Schechter, 2014; Karpicke & Roediger, 2007). All of these techniques could be explored further and used in password creation and in educating people on better ways to remember their passwords. Other memory techniques could also be explored such as allowing for more elaborate encoding of passwords or using pictures or instructions for how to encode a particular password (e.g., providing prompts for a ridiculous story or using pictures to create a mind palace for the password). Further research could also look toward the use of randomly generated passwords, user-generated passwords, other password/passphrase types, as well as different password lengths.

Of course, there are security issues to keep in mind as people also adapt different strategies to changing situations (i.e., bank accounts vs. lower-risk accounts) that allow them to reconcile costs and benefits associated with the use of passwords (Tam, Glassman, & Vandenuwaver, 2010). If changes in the interface compromise the security of the password itself, then it may not be as useful. The potential benefits may outweigh the costs if people are not as inclined to write down the password once they know it well enough and if they can remember longer passwords. By making the password process automatic (through having them memorized), security could potentially increase because people would not need to write passwords down and leave them in the reach of others. If something as simple as implementing a different interface to encourage chunking can help people remember their passwords, then there is potential to help web users and administrators in all walks of life.

References

Bonneau, J., & Schechter, S. (2014). Towards reliable storage of 56-bit secrets in human memory. Proceedings of the 23rd USENIX Security Symposium. Retrieved from http://research.microsoft.com/apps/pubs/default.aspx?id=216723
Brown, A. S., Bracken, E., Zoccoli, S., & Douglas, K. (2004). Generating and remembering passwords. Applied Cognitive Psychology, 18, 641–651. doi:10.1002/acp.1014
Campbell, J., Ma, W., & Kleeman, D. (2011). Impact of restrictive composition policy on user password choices. Behaviour and Information Technology, 30, 379–386. doi:10.1080/0144929X.2010.492876
Carstens, D. S., Malone, L. C., & McCauley-Bell, P. (2006). Applying chunking theory in organizational password guidelines. Journal of Information, Information Technology, and Organizations, 1, 97–113. doi:10.1.1.97.2792
España | Effects of Password Type and Memory

Chen, Z., & Cowan, N. (2005). Chunk limits and length limits in immediate recall: A reconciliation. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, 31, 1235–1249. doi:10.1037/0278-7393.31.6.1235

Cowan, N. (2000). The magical number 4 in short-term memory: A reconsideration of mental storage capacity. *Behavioral and Brain Sciences*, 24, 87–185. doi:10.1017/S0140525X01003922

Dilmar, D. K. (1972). Most efficient chunk sizes. *Cognitive Psychology*, 3, 355–359. doi:10.1016/0010-0285(72)90012-6

Duggan, G. B., Johnson, H., & Grawemeyer, B. (2012). Rational security: Modelling everyday password use. *International Journal of Human-Computer Studies*, 70, 415–431. doi:10.1016/j.ijhcs.2012.02.008

Huang, D., Rau, P. P., Salvendy, G., Gao, F., & Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human-Computer Studies*, 69, 870–883. doi:10.1016/j.ijhcs.2011.07.007

Karpicke, J. D., & Roediger, H. L. (2007). Expanding retrieval practice promotes short-term retention, but equally spaced retrieval enhances long-term retention. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, 33, 704–719. doi:10.1037/0278-7393.33.4.704

Keith, M., Shao, B., & Steinbart, P. J. (2007). The usability of passphrases for authentication: An empirical field study. *International Journal of Human-Computer Studies*, 65, 17–28. doi:10.1016/j.ijhcs.2006.08.005

Miller, G. A. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information. *Psychological Review*, 63, 81–97. doi:10.1037/h0043158

Mulligan, N. W. (2004). Generation and memory for contextual detail.

Payton, L. (2010). Memory for passwords: The effects of varying number, type, and composition. *Psi Chi Journal of Undergraduate Research*, 15, 209–213. Retrieved from http://www.psichi.org/?154JNWinter2010

Roediger, H. L., Nairne, J. S., Neath, I., & Surprenant, A. M. (Eds.). (2001). *The nature of remembering: Essays in honor of Robert G. Crowder*. Washington, DC: American Psychological Association.

Stamp, M. (2006). *Information security: Principles and practice*. Hoboken, NJ: John Wiley & Sons, Inc.

Tam, L., Glassman, M., & Vandenbergouwer, M. (2010). The psychology of password management: A tradeoff between security and convenience. *Behaviour and Information Technology*, 29, 233–244. doi:10.1080/01449290903121386

Vu, K. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B., Cook, J., & Schultz, E. E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies*, 65, 744–757. doi:10.1016/j.ijhcs.2007.03.007

Authors Note. Lezlie Y. España, Departments of Psychology and Computer Science, Wisconsin Lutheran College.

Lezlie Y. España is now at the Department of Neurosurgery, Medical College of Wisconsin.

Special thanks to Wendy Close, Department of Psychology, Wisconsin Lutheran College, for her assistance, patience, and guidance in editing and preparing this manuscript.

Correspondence concerning this article should be addressed to Lezlie España. E-mail: lespana@mcw.edu